Cisco Packet Data Serving Node (PDSN) Release 3.0 for Cisco IOS Release 12.4(11)T

Feature History

Release	Modification
12.3(14)YX1	Release 3.0 of the Cisco Packet Data Serving Node (PDSN) software. The following new feature is introduced: • **Support for Mobile Equipment Indentifier (MEID)**
12.3(14)YX	Release 3.0 of the Cisco Packet Data Serving Node (PDSN) software. The following new features are introduced: • **Packet Data Service Access, page 14** – **Simple IPv6 Access** • **Session Redundancy Infrastructure, page 21** • **Radius Server Load Balancing, page 60** • **Closed-RP/Open-RP Integration, page 47** • **Subscriber Authorization Based on Domain, page 62** • **PDSN MIB Enhancement, page 79** – **PPP Counters in Release 3.0** – **RP Counters in Release 3.0** • **Conditional Debugging Enhancements, page 100** – **Trace Functionality in Release 3.0**
12.3(11)YF3	Added support for **Mobile IP Dynamic Home Address Deletes Older Sessions With Different IMSI**. The following new command was added: • **ip mobile cdma imsi dynamic**

12.3(11)YF2	Added support for **Identification of Data Packets For SDB Indication**, **SDB Indicator Marking for PPP Control Packets**, and **Support for G17 Attribute in Acct-Stop and Interim Records**. The following new commands were added or modified: • **cdma pdsn a11 dormant sdb-indication match-qos-group** • **cdma pdsn compliance** • **cdma pdsn attribute send g17**
12.3(11)YF1	A restriction for Registration Revocation was removed. New commands were added, including: • **cdma pdsn compliance** • **debug cdma pdsn prepaid** • **debug cdma pdsn radius disconnect nai** • **show cdma pdsn statistics prepaid** Existing commands were modified, including: • **clear cdma pdsn session** • **clear cdma pdsn statistics** adds RADIUS statistics • **cdma pdsn mobile-advertisement-burst** • **ip mobile foreign-service**
12.3(11)YF	Release 2.1 of the Cisco Packet Data Serving Node (PDSN) software. Four new features were added, including the Closed-RP Interface.
12.3(8)XW	Release 2.0 of the Cisco Packet Data Serving Node (PDSN) software.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
12.2(8)ZB8	One new CLI command was added.
12.2(8)ZB7	Six CLI commands were added or modified.
12.2(8)ZB6	Two CLI commands were added or modified.
12.2(8)ZB5	Four new CLI commands were added.
12.2(8)ZB1	This feature was introduced on the Cisco 7600 Internet Router.
12.2(8)ZB	This feature was introduced on the Cisco Catalyst 6500 Switch.
12.2(8)BY	This feature was introduced on the Cisco 7200 Series Router.

This document describes the Cisco Packet Data Serving Node (PDSN) software for use on the Cisco 7200 Series router, and the Cisco Multi-processor WAN Application Module (MWAM) that resides in the Cisco Catalyst 6500 Switch, and the Cisco 7600 Internet Router. It includes information on the features and functions of the product, supported platforms, related documents, and configuration tasks.

This document includes the following sections:

Feature Overview

A PDSN provides access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations using a Code Division Multiple Access 2000 (CDMA2000) Radio Access Network (RAN). The Cisco PDSN is a Cisco IOS software feature that runs on Cisco 7200 routers, and on MWAM cards on the 6500 routers, and the Cisco 7600 Internet Router, where it acts as an access gateway for Simple IP and Mobile IP stations. It provides foreign agent (FA) support and packet transport for virtual private networking (VPN). It also acts as an Authentication, Authorization, and Accounting (AAA) client.

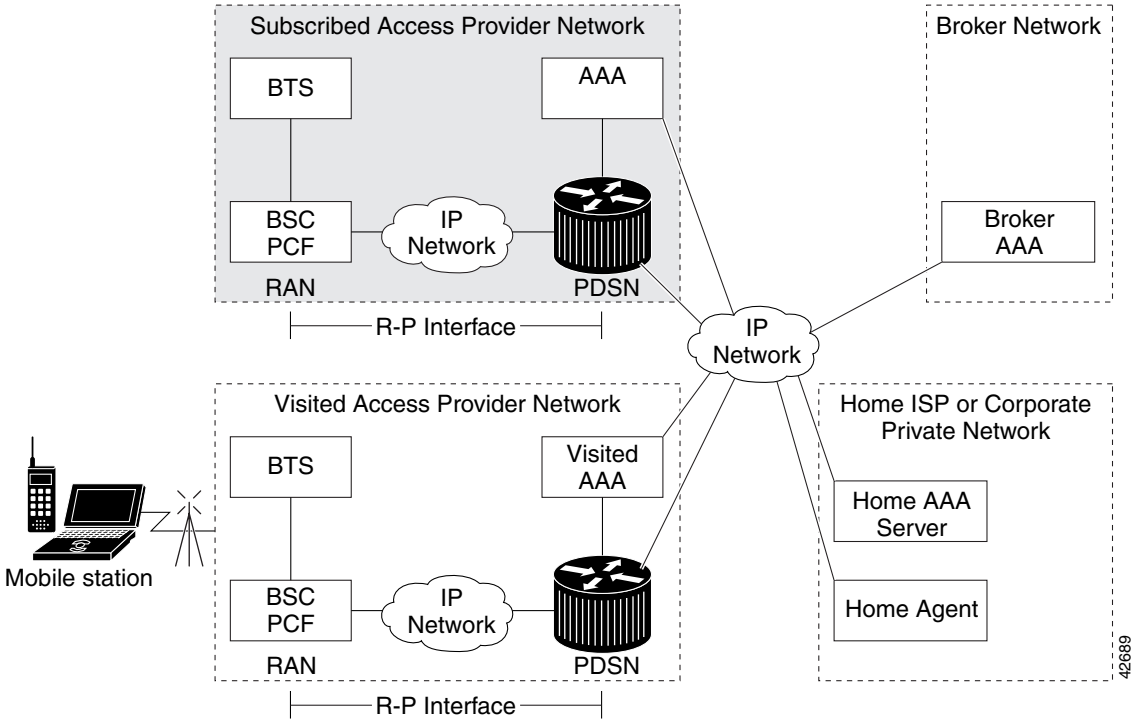
The Cisco PDSN supports all relevant 3GPP2 standards, including those that define the overall structure of a CDMA2000 network, and the interfaces between radio components and the PDSN.

System Overview

CDMA is one of the standards for Mobile Station communication. A typical CDMA2000 network includes terminal equipment, mobile termination, base transceiver stations (BTSs), base station controllers (BSCs / PCFs), PDSNs, and other CDMA network and data network entities. The PDSN is the interface between a BSC / PCF and a network router.

Figure 1 illustrates the relationship of the components of a typical CDMA2000 network, including a PDSN. In this illustration, a roaming mobile station user is receiving data services from a visited access provider network, rather than from the mobile station user's subscribed access provider network.

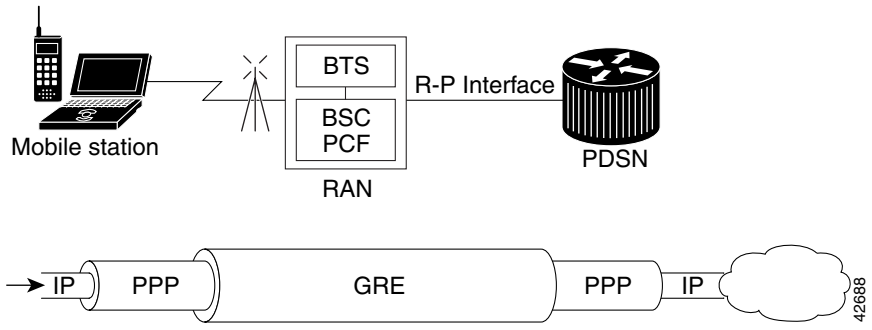
Figure 1 The CDMA Network



As the illustration shows, the mobile station, which must support either Simple IP or Mobile IP, connects to a radio tower and BTS. The BTS connects to a BSC, which contains a component called the Packet Control Function (PCF). The PCF communicates with the Cisco PDSN through an A10/A11 interface. The A10 interface is for user data and the A11 interface is for control messages. This interface is also known as the RAN-to-PDSN (R-P) interface. For the Cisco PDSN Release 2.0 and above, you must use a Fast Ethernet (FE) interface as the R-P interface on the 7200 platform, and a Giga Ethernet (GE) interface on the MWAM platform.

Figure 2 illustrates the communication between the RAN and the Cisco PDSN.

Figure 2 RAN-to-PDSN Connection: the R-P Interface



The IP networking between the PDSN and external data networks is through the PDSN-to-intranet/Internet (P_i) interface. For the Cisco PDSN Release 2.0 and above, you can use either an FE or GE interface as the P_i interface.

For “back office” connectivity, such as connections to a AAA server, or to a RADIUS server, the interface is media independent. Any of the interfaces supported on the Cisco 7206 can be used to connect to these types of services; however, Cisco recommends that you use either an FE or GE interface.

How PDSN Works

When a mobile station makes a data service call, it establishes a Point-to-Point Protocol (PPP) link with the Cisco PDSN. The Cisco PDSN authenticates the mobile station by communicating with the AAA server. The AAA server verifies that the user is a valid subscriber, determines available services, and tracks usage for billing.

The method used to assign an IP address and the nature of the connection depends on service type and network configuration. Simple IP operation and Mobile IP operation are referred to as *service types*. The service type available to a user is determined by the mobile station, and by the type of service that the service provider offers. In the context of PDSN, a mobile station is the end user in both Simple IP and Mobile IP operation.

Once the mobile station is authenticated, it requests an IP address. Simple IP stations communicate the request using the Internet Protocol Control Protocol (IPCP). Mobile IP stations communicate the request using Mobile IP registrations.

The following sections describe the IP addressing and communication levels for each respective topic:

- Cisco PDSN Simple IP
- Cisco PDSN Mobile IP
- PMTU Discovery by Mobile IP Client

Cisco PDSN Simple IP

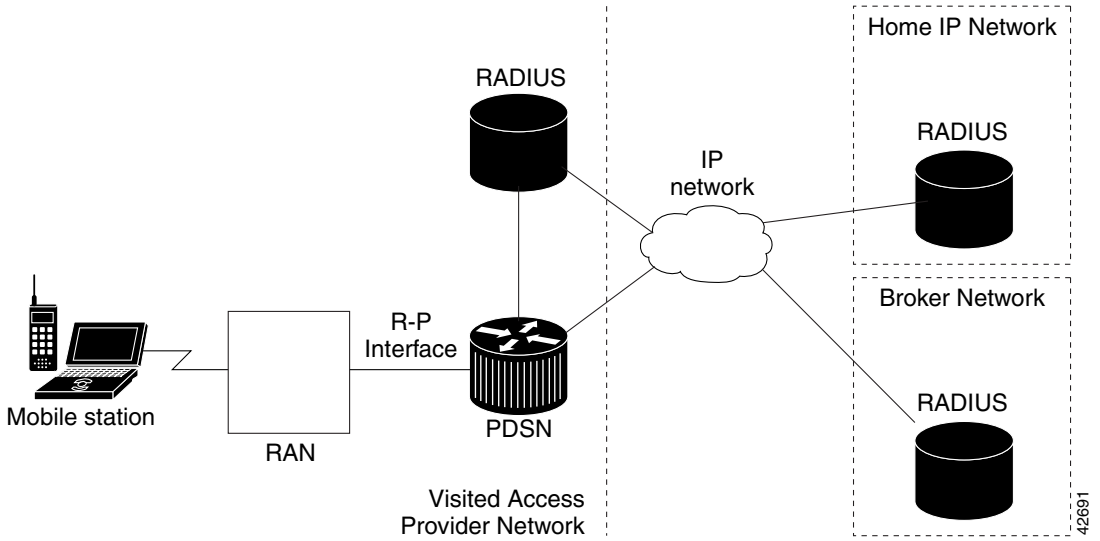
With Simple IP, a service provider’s Cisco PDSN assigns a dynamic or static IP address to the mobile station during the PPP link setup. The mobile station retains this IP address as long as it is served by a radio network that has connectivity to the address-assigning PDSN.

Therefore, as long as the mobile station remains within an area of RANs that is served by the same PDSN, the MS can move or roam inside the coverage area and maintain the same PPP links. If the mobile station moves outside the coverage area of the given PDSN, the mobile station is assigned a new IP address, and any application-level connections are terminated.

Note A static IP address can be requested by the mobile station, and will be assigned if the address is within the pool of addresses and is available. Also an IP address can be statically specified in the AAA profile of the user using the “Framed-IP-Address” attribute.

Figure 3 illustrates the placement of the Cisco PDSN in a Simple IP scenario.

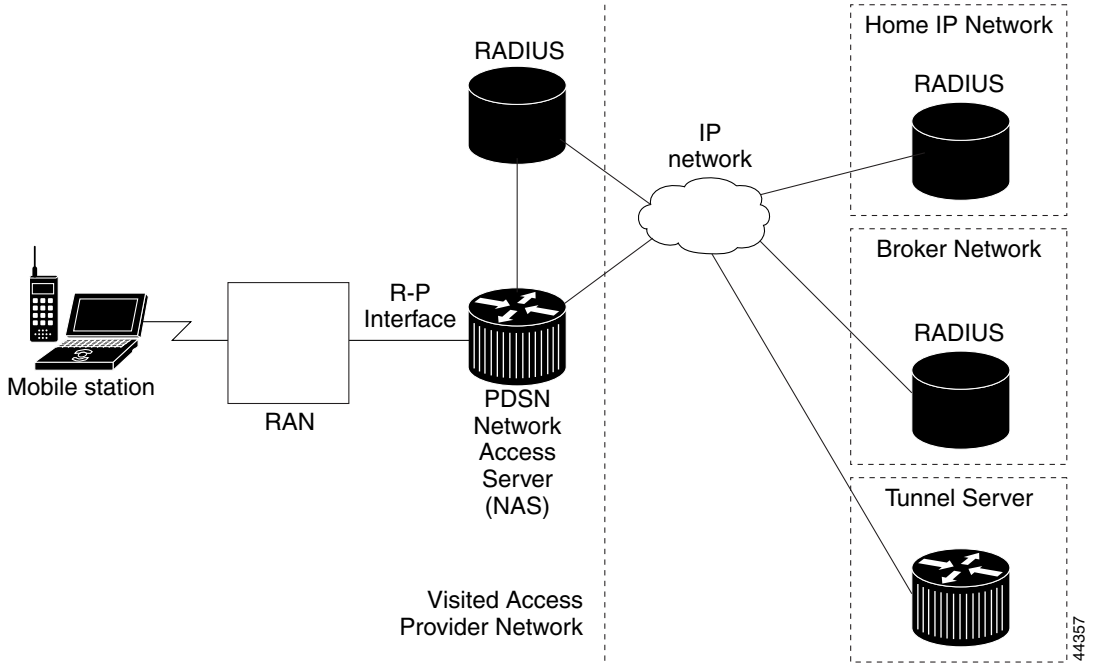
Figure 3 CDMA Network - Simple IP Scenario



Cisco PDSN Simple IP with VPDN Scenario

A Virtual Private Data Network (VPDN) allows a private network dial-in service to span to remote access servers called Network Access Servers (NAS). Figure 4 illustrates a VPDN connection in the PDSN environment with Simple IP. In this scenario, the PDSN is acting as the NAS.

Figure 4 CDMA Network —Simple IP with VPDN Scenario



A VPDN connection is established in the following order:

1. A PPP peer (mobile station) connects with the local NAS (the Cisco PDSN).
2. The NAS begins authentication when the client dials in. The NAS determines that the PPP link should be forwarded to a tunnel server for the client. The location of the tunnel server is provided as part of the authentication by the Remote Authentication Dial-in User Service (RADIUS) server.
3. The tunnel server performs its own authentication of the user and starts the PPP negotiation. It performs authentication for both the tunnel setup and the client.

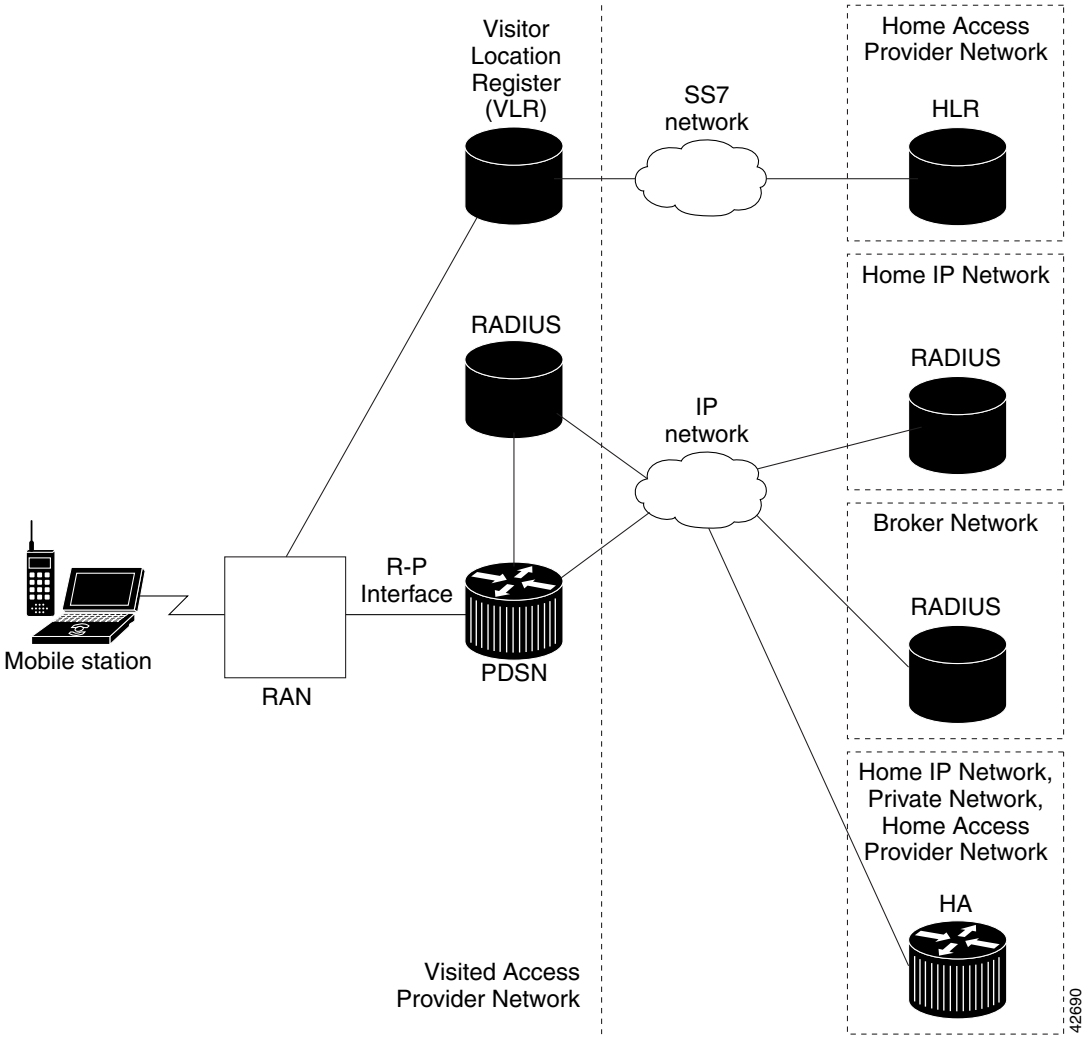
   The PPP client is forwarded through a Layer 2 Tunneling Protocol (L2TP) tunnel over User Datagram Protocol (UDP).
4. The PPP setup is completed and all frames exchanged between the client and tunnel server are sent through the NAS. The protocols running within PPP are transparent to the NAS.

Cisco PDSN Mobile IP

With Mobile IP, the mobile station can roam beyond the coverage area of a given PDSN and still maintain the same IP address and application-level connections.

Figure 5 shows the placement of the Cisco PDSN in a Mobile IP scenario.

Figure 5 CDMA Network —Mobile IP Scenario



The communication process occurs in the following order:

1. The mobile station registers with its Home Agent (HA) through an FA; in this case, the Cisco PDSN.
2. The HA accepts the registration, assigns an IP address to the mobile station, and creates a tunnel to the FA. This results in a PPP link between the mobile station and the FA (or PDSN), and an IP-in-IP or Generic Routing Encapsulation (GRE) tunnel between the FA and the HA.

   As part of the registration process, the HA creates a binding table entry to associate the mobile station's home address with its Care-of address.

   Note While away from home, the mobile station is associated with a care-of address. This address identifies the mobile station's current, topological point of attachment to the Internet, and is used to route packets to the mobile station. In IS-835-B networks, the foreign agent's address is always used as the Care-of address.

3. The HA advertises that the network is reachable to the mobile station, and tunnels datagrams to the mobile station at its current location.

4. The mobile station sends packets with its home address as the source IP address.
5. Packets destined for the mobile station go through the HA; the HA tunnels them through the PDSN to the mobile station using the care-of address.
6. When the PPP link is handed off to a new PDSN, the link is re-negotiated and the Mobile IP registration is renewed.
7. The HA updates its binding table with the new care-of address.

Note For more information about Mobile IP, refer to the Cisco IOS Release 12.2 documentation modules *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command Reference.* RFC2002 describes the specification in detail. TIA/EIA/IS-835-B also defines how Mobile IP is implemented for PDSN.

Mobile IP Dynamic Home Address Deletes Older Sessions With Different IMSI

The PDSN cannot recognize 1xRTT to EVDO as a handoff due to a change of IMSI. The result is that the "cdma-reason-ind" in the account stop message will not reflect the same.

By default, the PDSN keeps the first call session if the Mobile does a static home address. In this release, the PDSN supports deleting the first call session for dynamic home address cases (for example, 1x-RTT to EVDO handoff where the IMSI changes during the handoff).

The old call scenario is established as follows:

1. Mobile Node with IMSI = imsi1, NAI = nai1 establishes session.
2. When PDSN receives an RRQ from the same mobile node with the same NAI but with different IMSI (with IMSI = imsi2, NAI = nai1), currently a new session does not come up on the PDSN, and old session remains.
3. During the mobile handoff between 1XRTT and EVDO call, handoff will not succeed due to the above behavior of PDSN.

A new CLI is introduced in this release that allows you to delete the old session. When you issue the **ip mobile cdma imsi dynamic** command, the PDSN releases the old session and allows the new session to come up.

PMTU Discovery by Mobile IP Client

FTP upload and ping from the end node may fail when PMTU Discovery (done by setting the DF bit) is done by a MobileIP client (an end node) for packet sizes of about 1480. Due to failure of PMTUD algorithm, the IP sender will never learn the smaller path MTU, but will continue unsuccessfully to retransmit the too-large packet, until the retransmissions time out.

Please refer to http://www.cisco.com/warp/public/105/38.shtml#2000XP for disabling PMTUD for Windows 2000/XP platforms.

Cisco PDSN Proxy Mobile IP

Currently, there is a lack of commercially-available Mobile IP client software. Conversely, PPP, which is widely used to connect to an Internet Service Provider (ISP), is ubiquitous in IP devices. As an alternative to Mobile IP, you can use Cisco's proxy Mobile IP feature. This capability of the Cisco PDSN, which is integrated with PPP, enables a Mobile IP FA to provide mobility to authenticated PPP users.

Note In Proxy Mobile IP, the MS can have only one IP flow per PPP Session.

The communication process occurs in the following order:

1. The Cisco PDSN (acting as an FA) collects and sends mobile station authentication information to the AAA server.
2. If the mobile station is successfully authenticated to use Cisco PDSN Proxy Mobile IP service, the AAA server returns the registration data and an HA address.
3. The FA uses this information, and other data, to generate a Registration Request (RRQ) on behalf of the mobile station, and sends it to the HA.
4. If the registration is successful, the HA sends a registration reply (RRP) that contains an IP address to the FA.
5. The FA assigns the IP address (received in the RRP) to the mobile station, using IPCP.
6. A tunnel is established between the HA and the FA/PDSN. The tunnel carries traffic to and from the mobile station.

PDSN on MWAM

The MWAM supports the feature set of PDSN Release 3.0, and functionality remains the same as on the Cisco 7200 platforms. The significant difference between the Cisco PDSN on the Cisco 7200 router and on the MWAM is that a Cisco Catalyst 6500 or Cisco 7600 chassis will support a maximum of 6 application modules. Each application module supports 5 IOS images, each with access to 512 Megabytes of RAM. Up to five of these images can function as a PDSN.

Additionally, instances of the cluster controller functionality will be configured as required. One active and one standby controller are required for a cluster of 48 PDSN instances or less. Each PDSN image supports 20,000 sessions. For every 10 PDSNs configured in the chassis, one active and one standby controller is required. Internal to the chassis, the PDSN images are configured on the same VLAN in order to support the Controller-Member architecture (although the architecture itself does not require this). Load balancing external to the chassis is determined by the physical proximity of the chassis and the network architecture. It is possible that you require both a VLAN approach, and a more traditional routed approach.

Features

New Features in This Release

This section describes the following key features of the Cisco PDSN Release 3.0:

Features From Previous Releases

This section lists features that were introduced prior to Cisco PDSN Release 3.0

Note The Cisco PDSN software offers several feature options which are available on four different images. Some features are image-specific, and are not available on all images. The PDSN 2.1 Feature Matrixin Table 1 lists the available images for PDSN 2.0, and identifies the features available on each image.

Table 1 PDSN 2.1 Feature Matrix

Feature Name	c7200-c6is-mz	c7200-c6ik9s-mz	c6svc5fmwam-c6is-mz
Session Redundancy			X
Simple IPv6	X	X	**X(P)**
Closed/Open RP Integration			X
Resource Revocation Per User	X	X	X
Trace Functionality	X	X	X
Radius server load balancing			X
Selection of RADIUS Server Based On Realm	X	X	X
PPPoGRE RP Interface	X(P)	X(P)	X(P)
A11 Session Update	X	X	X
SDB Indicator Marking	X	X	X
Packet of Disconnect	X	X	X
Resource Revocation	X	X	X
IS-835-B Compliant Static IPSec		X*	X*
On-Demand Address Pools	X	X	X
Always On Feature	X	X	X
NPE-G1 Platform Support	X	X	
PDSN MIB Enhancements	X	X	X
Conditional Debugging	X	X	X
10000 Sessions	X	X	
20000 Sessions	X(P)	X(P)	X
Prepaid Billing (IS-835-C)	X(P)	X(P)	X(P)
PDSN Controller / Member Clustering	X	X	X
PDSN Peer-to-Peer Clustering	X	X	

Table 1 PDSN 2.1 Feature Matrix (Continued)

Feature Name	c7200-c6is-mz	c7200-c6ik9s-mz	c6svc5fmwam-c6is-mz
1xEV-DO Support	X	X	X
ESN in Billing	X	X	X
3DES Encryption		X*	X*
PPP Optimization	X	X	X

P indicates that this feature is only available with a Premium license.

* Requires appropriate hardware support.

Note If you require higher performance values for PDSN selection, use the c6is-mz images; these images contain the PDSN controller-member cluster feature for PDSN selection.

PDSN Performance Metrics

Performance metrics for the Cisco PDSN software on 7200 Platform include the following:

- 20000 user sessions per on 7206VXR with NPE-400 with 512MB DRAM and on 7206VXR NPE-G1 with 1G DRAM.
- Maximum of 200,000 user sessions per PDSN cluster configured according to the controller/member architecture (10 members) without the clustering enhancement.
- Throughput on the R-P interface for non-fragmented packets of size 64, 512 and 1024 bytes.
- Throughput on the R-P interface for fragmented packets of size 64, 512 and 1024 bytes with 20 byte fragmentation.
- Maximum call setup rate for Simple IP and Mobile IP sessions for a stand alone PDSN.
- Maximum call set up rate for a cluster with 8 members configured in a controller/member cluster for Simple IP and Mobile IP Sessions.
- Maximum of 3000 L2TP tunnel endpoints with a maximum of 20000 sessions distributed across those tunnels.
- Maximum of 3000 Mobile IP tunnels.
- Maximum of 5000 IPSec tunnels with VAM2 hardware support on 7200 platforms.

The following performance metrics apply to the Cisco 6500 and 7600 series platforms. The quoted figures are per image, and each MWAM supports 5 PDSN images.

- 20000 user sessions.
- Maximum call setup rate for Simple IP and Mobile IP sessions for a standalone PDSN.
- Maximum of 200,000 user sessions per PDSN cluster configured according to the controller/member architecture, without R2.0 clustering enhancement. Supported cluster configuration is 10 members and 2 controllers of which one is an active controller and the other a standby.
- Cluster member architecture with 48 members and clustering enhancement.
- Throughput on the R-P interface for non-fragmented packets of size 64, 512 and 1024 bytes.
- Throughput on the R-P interface for fragmented packets of size 64,512 and 1024 bytes with 20 byte fragmentation.
- Call set up rate for a stand-alone PDSN for Simple IP and Mobile IP Sessions.
- Maximum call set up rate for a cluster with 8 members configured in a controller/member cluster for Simple IP and Mobile IP Sessions.
- Maximum of 3000 L2TP tunnel endpoints with a maximum of 20000 sessions distributed across those tunnels per image.
- Maximum of 3000 Mobile IP tunnels per image.
- Maximum of 8000 IPSec tunnels with VPNSM hardware support (This figure is for the chassis; IPSec resources are not linked with PDSN images on MWAM, they are a separate resource).
- Maximum call set up rate for a cluster with *n* members configured in a controller-member cluster for Simple IP and Mobile IP Sessions with clustering enhancements

Packet Data Service Access

The PDSN supports two types of service accesses. The type of service access for a mobile session is determined by the capabilities of the mobile station:

- Simple IP based service access
- Mobile IP based service access

Simple IP Based Service Access

The PDSN facilitates a mobile user to access the internet and corporate intranet by using Simple IP based service access. Simple IP mode of access, however, limits user mobility to the coverage area of the serving PDSN. Inter-PDSN handoff causes re-negotiation of PPP between the mobile station and the new PDSN. The old IP address assigned at the previous PDSN can usually not be assigned to the mobile user from the new PDSN, and results in reset and restart of user applications.

Some of the salient features for Simple IP based service access include:

- Support for static IP Addresses
- Public IP addresses
- Private IP addresses, e.g. for VPDN service
- Support for dynamic IP Addresses

- Public IP addresses
- Private IP addresses, e.g for VPDN service
- Support for PPP PAP/CHAP authentication
- Support for MSID based service access
- Support for packet data accounting per TIA/EIA/IS-835-B
- Support for packet filtering
- Ingress address filtering
- Input access lists
- Output access lists

User NAI is available during the PPP CHAP/PAP authenticating phase. Domain name information in the NAI determines the domain responsible for user authentication. Based on the type of packet routing model, Simple IP based service access can be categorized as follows.

- Simple IP Routed Access
- Simple IP VPDN Access
- Proxy-Mobile IP services

Simple IP Routed Access

After receiving username and password during PPP LCP negotiations, the PDSN forwards authentication information to the local AAA server via an access request message. This, in turn, may be proxied to the AAA server in the user's home domain, via broker AAA servers, if necessary. On successful authentication, the user is authorized services based on its service profile. User Class/CDMA_IPTECH information, along with other authorization parameters are returned to the PDSN using an access accept message from the home AAA. On successful negotiation of an IP address, Simple IP based services are made available to the mobile user.

Simple IP routed access method is applicable for users that are not configured for VPDN or proxy-Mobile IP services. With PPP terminated at the PDSN, uplink user traffic is routed towards the IP network from the PDSN. The address assigned to the mobile user would be from within the PDSN routable domain. Private addresses may also be used if a NAT is configured. User mobility is limited to the PDSN coverage area. Inter-PCF handoffs do not disrupt service. Inter-PDSN handoffs, however, result in PPP renegotiation at the new PDSN, another IP address being assigned at the new PDSN, and reset and restart of user applications.

Simple IP VPDN Access

After receiving username and password during PPP LCP negotiations, the PDSN forwards authentication information to the local AAA server via an access request message. This, in turn, may be proxied to the AAA server in the user's home domain, via broker AAA servers, if necessary. On successful authentication, the user is authorized services based on user's service profile. If the user is configured for VPDN based access services, User Class information, along with other authorization parameters including tunneling options and tunneling parameters, are returned to the PDSN via an access accept message from the home AAA. The following types of VPDN services are supported at the PDSN:

L2TP - Layer 2 Tunneling Protocol

For L2TP type layer2 tunneling, the PDSN establishes an L2TP tunnel with the tunneling endpoints specified by the tunneling parameters. The L2TP tunnel would be established between the LAC at the PDSN and LNS at the NAS in user's home domain. The PPP connection would be between the mobile station and the LNS in the home network. Despite the PPP connection termination at the LNS, the PDSN monitors the PPP session for inactivity. Status of the PPP connection is also linked with the state of the underlying A10 connection. PPP connection is deleted when the underlying A10 connection is deleted. IPSec encryption methods can also be enabled over the L2TP tunnels for enhanced security.

On successful negotiation of an IP address between the mobile and the LNS, IP-based services are made available to the mobile.

The LNS may be configured to authenticate the mobile user based on the challenge and challenge response information from the PDSN. Additionally, the LNS may also be configured to challenge the user again after the layer2 tunnel has been established. The following authentication options are supported for L2TP:

- L2TP With Proxy-Authentication

  The LAC (PDSN) challenges the mobile user and forwards authentication related information to the LNS as part of tunnel setup parameters. The LNS may be configured to authenticate the user either locally or via the home AAA, based on the authentication related information from the LAC (PDSN). On successful authentication, the mobile and the LNS proceed with the IPCP phase and negotiate an IP address for the user session. Call establishment procedures for this scenario are illustrated in Figure 16.

- L2TP With Dual Authentication

  The LAC (PDSN) challenges the mobile and forwards authentication related information to the LNS as part of tunnel setup parameters. The LNS may be configured to authenticate the user either locally or via the home AAA, based on the authentication related information from the LAC (PDSN). On successful authentication, the LNS challenges the mobile again. After successful authentication, the LNS and the mobile proceed with IPCP phase and negotiate the IP address for the user session.

Proxy-Mobile IP Access

After receiving username and password during PPP LCP negotiations, the PDSN forwards authentication information to the local AAA server via an access request message. This, in turn, may be proxied to the AAA server in the user's home domain, using broker AAA servers, if necessary. On successful authentication, the user is authorized services based on its service profile. User Class information, along with other authorization parameters are returned to the PDSN via an access reply from the home AAA.

If the user is configured for proxy-Mobile IP based access, authorization parameters from the home AAA include the Home Agent (HA) address, and the security parameter (SPI) to be used for computing the MN-HA Authentication extension for the mobile station. The Home Agent is allocated from the list of

Home Agents configured at the home AAA server. Round robin or hashing algorithms based on user NAI can be used for allocating a Home Agent at the AAA. Other authorization attributes returned from the AAA include MN-AAA authenticating extension as defined in RFC 3012. Based on this information, the PDSN performs proxy-Mobile IP procedures on behalf of the mobile user by sending a Mobile IP Registration Request message to the allocated HA. On successful authentication of the mobile with the AAA, and registration at the Home Agent, the Home Agent assigns a home address for this mobile user This address is returned to the mobile during IPCP IP address negotiation phase.

On successful negotiation of an IP address, proxy-Mobile IP based services are made available to the mobile user. To the mobile, these services are no different from Simple IP services with tunneling being done via the Home Agent. This feature, however, extends the coverage area of the call beyond coverage area of the serving PDSN. If, as a result of a handoff event, another PDSN is allocated to the call, the target PDSN performs Mobile IP registration with the Home Agent thereby ensuring that the same home address is allocated to the mobile.

Mobile IP Based Service Access

The PDSN allows a mobile station with Mobile IP client function, to access the internet and corporate intranet using Mobile IP based service access. With this mode of service access, user mobility is extended beyond the coverage area of currently serving PDSN. Resulting from a handoff, if another PDSN is allocated to the call, the target PDSN performs Mobile IP registration with the Home Agent thereby ensuring that the same home address is allocated to the mobile.

Some of the salient features for Mobile IP services access include:

- Support for static IP Addresses
- Public IP addresses
- Private IP addresses
- Support for dynamic IP Addresses
- Public IP addresses
- Private IP addresses
- Multiple Mobile IP user flows over a single PPP connection
- Multiple flows for different NAIs using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge procedures in RFC 3012
- Mobile IP Agent Advertisement Challenge Extension
- MN-FA Challenge Extension
- MN-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
- MN-HA Authentication Extension
- MN-FA Authentication Extension
- FA-HA Authentication Extension
- Mobile IP Extensions specified in RFC 3220
- Authentication requiring the use of SPI.
- Mobile NAI Extension, RFC 2794
- Reverse Tunneling, RFC 2344

- Multiple tunneling Modes between FA and HA
- IP-in-IP Encapsulation, RFC 2003
- Generic Route Encapsulation, RFC 2784
- Support for PPP PAP/CHAP authentication
- Support for MSID based service access
- Binding Update message for managing zombie PPP connections
- Flow based packet data accounting per TIA/EIA/IS-835-B
- Support for Packet Filtering
- Ingress address filtering
- Input access lists
- Output access lists

A Mobile IP capable mobile client may be configured to skip PAP/CHAP based authentication during the PPP LCP phase. Once the PPP is established, the PDSN sends a burst of Mobile IP Agent Advertisement messages that include the Mobile IP Agent Advertisement Challenge extension specified in RFC 3012. The number and timing of the burst is configurable. The mobile user responds with a Mobile IP Registration Request message that includes the mobile user's NAI and MN-FA Challenge extension in response to the challenge in the Agent Advertisement message. If the mobile user does not respond to the initial burst, advertisements can be solicited.

The Foreign Agent function at the PDSN can be configured to authenticate the mobile user by forwarding an access request message to the local AAA server. The local AAA server would proxy the message to the home AAA server, via broker AAA server(s), if necessary. On successful authentication, the home AAA may assign a Home Agent to the call and return its address in the access reply message. Other authorization parameters in the access-reply message include the SPI and IPSec shared key to be used between the FA and the HA. The PDSN/FA and Home Agent establish a secure IPSec tunnel, if required, and the PDSN/FA forwards the Registration Request message to the Home Agent. The Registration Request message includes the NAI and MN-FA-Challenge Extension also. It may also include MN-AAA Authentication extension.

The Home Agent can be configured to authenticate the mobile again with the home AAA. On successful authentication and registration, the Home Agent responds with a Registration Reply message to the PDSN/FA, which is forwarded to the mobile station. The Registration Reply message contains the home address also (static or dynamically assigned) for the user session.

Potential home addresses are available to the PDSN from the following:

- Mobile IP Registration Request received from the Mobile Node
- FA-CHAP response received from the HAAA
- Mobile IP Registration Reply received from the Home Agent

The mobile may be configured to perform PPP PAP/CHAP authentication in addition to performing Foreign Agent Challenge based authentication specified in RFC 3012. In this case the PDSN would support one Simple IP flow, in addition to one or more Mobile IP flows.

For Mobile IP services, the Home Agent would typically be located within an ISP network or within a corporate domain. However, many of the ISPs and/or corporate entities may not be ready to provision Home Agents by the time service providers begin rollout of third-generation packet data services. Access service providers could mitigate this situation by provisioning Home Agents within their own domain, and then forward packets to ISPs or corporate domains via VPDN services.

Binding Update Procedures

When a mobile first registers for packet data services, a PPP session and associated Mobile IP flow(s) are established at the PDSN. In the event of an inter-PDSN handoff, another PPP session is established at the target PDSN, and the mobile registers with the Home Agent via the new PDSN/FA. The Visitor list binding and the PPP session at the previous PDSN are, however, not released until the PPP inactivity timer expires.

Idle/unused PPP sessions at a PDSN consume valuable resources. The Cisco PDSN and Home Agent support Mobile IP Resource Revocation as defined in IS83C and Cisco Proprietary Binding Update and Binding Acknowledge messages for releasing such idle PPP sessions as soon as possible. Mobile IP Resource Revocation is described in Section 16 in greater detail

If Cisco Proprietary binding update feature is used, in the event of an inter-PDSN handoff and Mobile IP registration, the Home Agent updates mobility binding information for the mobile with the Care-of-Address (COA) of the new PDSN/FA. If simultaneous bindings are not enabled, the Home Agent sends a notification in the form of a Binding Update message to the previous PDSN/FA. The previous PDSN/FA acknowledges with Binding Acknowledge, if required, and deletes visitor list entry for the Mobile IP session. The previous PDSN/FA initiates the release of the PPP session when there are no active flows for that mobile station.

The sending of the binding update message is configurable at the Home Agent.

Note When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required as this is used for maintaining more than one flow to the same IP address.

Simple IPv6 Access

The PDSN simple IP service has been enhanced to allow both simple IPv4 and simple IPv6 access. These protocols can be used one at a time, or at the same time. The ipcp and the ipv6cp are equivalent for each protocol.

An IPv6 access uses the same PPP LCP authentication and authorization procedures, as well as the AAA access. When an RP connection is established, the MS sends a PPP Link Control Protocol (LCP) Configuration-Request for a new PPP session to the PDSN. The PPP authentication (CHAP/PAP/none) is one of the parameters negotiated during the LCP phase. After the LCP parameters are negotiated between the MS and the PDSN, an LCP Configure-Acknowledge message is exchanged. Once LCP is up, the PPP authentication is started.

The authentication phase uses CHAP, PAP, or none, depending on the configuration and LCP negotiation. After authentication, the NCPs, ipcp and/or ipv6cp, can be started. A simultaneous IPv4 and IPv6 access from an MS shares the common LCP authentication and authorization as well as the AAA correlation-id parameter.

The ipv6cp protocol negotiates a valid non-zero 64-bit IPv6 interface indentifier for the MS and the PDSN. The PDSN has only one interface-identifier associated with the PPP connection, so it will be unique. Once ipv6cp has been successfully negotiated, the PDSN and MS both generate unique link-local addresses for the IPv6 interface. The link-local addresses are generated by pre-pending the link-local prefix, FE80:/64, to the 64-bit interface-identifier negotiated during the ipv6cp phase (for example, FE80::205:9AFF:FEFA:D806). This gives a 128-bit link-local address.

The PDSN immediately sends an initial unsolicited Router Advertisement (RA) message on the PPP link to the MS. The link-local address of the PDSN is used as the source address and the destination address will be FF02::1, the "all nodes on the local link" IPv6 address. The PDSN includes a globally unique /64 prefix in the RA message sent to the MS. The prefix may be obtained from a local prefix pool or from AAA. The MS will construct a global IPv6 unicast address by prepending the prefix received in the RA to the lower 64-bit interface identifier. You should carefully configure the PDSNs so that the /64 prefix is globally unique for each MS.

After a successful ipv6cp negotiation phase and configuration of the link-local address, the MS transmits a Router Solicitation (RS) message if an RA message has not been received from the PDSN within some specified period of time. The RA is necessary for the MS to construct its 128-bit global unicast address.

In contrast to IPv4, an IPv6 MS will have multiple IPv6 addresses, including:

- Link-local address
- Global unicast address
- Various multicast addresses used for IPv6 Neighbor Discovery and IPv6 ICMP messages

An IPv6 address is 128-bits for both source and destination addresses. The /64 designation means that 64-bits are used for the prefix (upper 64-bits). This is similar to an IPv4 netmask. A /128 address would mean that the entire address is used. Refer to RFC-3513 for additional IPv6 addressing details and information.

Configuring Simple IPV6

The following commands are used to configure simple IPV6 on the Cisco PDSN, and are listed in the Command Reference:

- The **cdma pdsn ipv6** command enables the PDSN IPv6 functionality.
- The **cdma pdsn ipv6 ra-count** *number* command configures the number of IPv6 Route Advertisements (RA).
- The **cdma pdsn ipv6 ra-count** *number* **ra-interval** *number* command controls the number and interval of RAs sent to the MN when an IPv6CP session comes up.
- The **cdma pdsn accounting send ipv6-flows** command control the number of flows and UDR records used for simultaneous IPv4, IPv6 sessions.
- The **show cdma pdsn flow mn-ipv6-address** command shows CDMA PDSN user information by MN IPv6 address.
- The **show cdma pdsn flow service simple-ipv6** command displays flow-based information for simple IPV6 sessions.
- The **debug cdma pdsn ipv6** command displays IPV6 error or event messages.

The following configuration commands are required for IPv6:

Global Configuration Commands

- **ipv6 unicast-routing** – IPv6 is off by default
- **ipv6 cef** – enables cef switching
- ipv6 local pool PDSN-Ipv6-Pool 2001:420:10::/48 64 – enables a pool of IPv6 prefix addresses that can be sent to the MS as a Routing Advertisement (RA)

Virtual-template interface commands:

- **ipv6 enable** - enables IPv6 on this interface
- **no ipv6 nd suppress-ra** - do not suppress the Neighbor Discovery Routing Advertisement messages (suppressed on non-ethernet interfaces)
- **ipv6 nd ra-interval** 1000 - send a ND Routing Advertisement every 1000 seconds
- **ipv6 nd ra-lifetime** 5000 - lifetime for the ND Routing Advertisement is 5000 seconds
- peer default ipv6 pool PDSN-Ipv6-Pool - use this pool for RA prefixes

Other commands

- **show ipv6**

Please refer to the *Cisco IOS IPV6 Command Reference* at the following URL for more detailed information regarding these configuration commands:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a00801d661a.html

Session Redundancy Infrastructure

Note Session redundancy is only available on the MWAM platform.

PDSN session redundancy is focused on preserving user flows on fail-over. Support for the continuity of billing records, internal counters, and MIB variables is secondary. The following conditions need to exist for fail-over to be successful on the PDSN:

- Users perceive no service interruption.
- Users do not experience excessive or incorrect billing.
- Users are able to re-initiate data service after fail-over.

Functional Overview

The PDSN Session Redundancy feature provides user session failover capability to minimize the impact of a PDSN failure on the mobile user experience. The PDSN uses a 1:1 redundancy model, with a standby present for every active PDSN. The active PDSN sends state information to the standby PDSN for synchronization on an as-needed basis. When a PDSN failure occurs, the standby PDSN has the necessary state information to provide service to all existing sessions. It then takes over as the active PDSN and services user sessions, thus providing session redundancy. When the previously active PDSN comes back online, it assumes the role of standby for the now active PDSN, and receives state information for all existing sessions from the newly active PDSN.

Under normal operating conditions, the active and standby PDSN pairs are two separate PDSN images that have identical configurations. They share one or more HSRP interfaces, which are used by all external entities to communicate with them. The active PDSN synchronizes session data to the standby PDSN based on events described below.

Session Events

When a new user session needs to be established, the PCF first sets up an A10 connection to the active PDSN, via the HSRP address known to the PCF. The MN then sets up a PPP connection with the active PDSN, via the A10 tunnel. Once the call is in a stable state, i.e., the PPP session is successful, the active PDSN then syncs relevant state information to the standby PDSN. The standby then duplicates the actions of the active PDSN with regards to the A10 connection and the PPP session, and awaits further updates from the active. When any of the other events as listed below occurs, the active PDSN sends state information to the standby.

In order to minimize the loss of accounting data in the event of a failover, a periodic accounting update, with configurable frequency shall run on the active PDSN. Every periodic update for a session shall trigger a sync sent to the standby PDSN, which shall update its accounting data. Only counters and attributes that undergo a change on the active PDSN are synced to the standby periodically. Information since the last accounting synchronization point will be lost. Also, in order to ensure that the latest information is correctly conveyed to the billing system, the standby unit will never send out any accounting records to the AAA server. The records are always sent from the Active Unit.

Session events that lead to a sync are:

- Call Setup
- Call teardown
- Flow setup
- Flow teardown
- Dormant-Active transition
- Handoff
- A11 Re-registrations
- Periodic accounting sync
- PPP renegotiation

IP Address Management and ODAP

IP addresses allocated to the user by the active PDSN are communicated to the standby PDSN, which will honor them. This is true no matter what allocation mechanism is used.

Both the DHCP ODAP subnet allocation server and the ODAP manager supports the PDSN session redundancy functionality. The DHCP ODAP subnet allocation server runs on the PDSN MWAM Cluster Controller. It synchronizes the allocated subnet pool information to the backup DHCP ODAP subnet allocation server located on the Backup MWAM Cluster Controller.

Similarly, the ODAP manager on the PDSN synchronizes the IP subnet pool and allocation information to a backup PDSN image.

If either the DHCP ODAP subnet allocation server or the ODAP manager fails, the backup takes over. This allows existing PDSN sessions to remain, and for new session requests to be properly processed.

Active PDSN Failure

In the event that the standby PDSN detects that the active PDSN has failed (using HSRP), it then takes over as the active PDSN. Since all external entities, including PCFs, AAA servers, and Home Agents are configured to communicate with the PDSN pair only using the HSRP addresses, once the standby PDSN takes over those addresses, they are unable to detect a failure. All stable calls also have their state synced to the standby; therefore the standby is able to start forwarding user traffic once it takes over as active. On the standby all timers (such as A11 lifetime, PPP timers, and Mobile IP lifetime) are started at the time it takes over as active. Accounting data is also synchronized to the extent that the periodic accounting sync timer has been configured on the PDSNs.

Standby PDSN Start-up

When a PDSN comes up when there is an existing active, it takes over the standby role. When the active PDSN learns that a standby PDSN is available, it goes through a process of transferring state data for all existing user sessions to the standby, called a Bulk Sync. Once this process is complete, the standby PDSN is then ready to take over as active in the event of a failure.

Handling Active-Active Scenario

If there is a link failure or a failure in an intermediate node, HSRP packets sent will not reach the peer and the standby node would assume that the active has reloaded and transitioned to active state. This leads to a situation of Active-Active PDSN nodes. The requirement is that, in case one of the PDSNs continues to receive traffic while the other is isolated from the network, it is ensured that the node which received traffic should remain active once the link is restored.

To achieve this, an application tracking object is introduced and HSRP priority is altered based on whether PDSN is processing traffic after the HSRP peer is lost. For details on configuration refer to section 20.4.9. The PDSN will lower its HSPR priority once it detects that the peer PDSN is lost. Afterward, when PDSN processes traffic (either control or data packets), it would raise its priority back to the configured value. This helps to choose the active node after the link is restored between the PDSNs. So the node which received traffic in Active-Active situation remains to be Active after link restoration.

Other Considerations

A Redundancy Framework (RF) MIB is available in order to monitor the active and standby status of the two PDSNs. Other MIB variables and internal counters are not synchronized between the Active and Standby. They start from the values following IOS-Load or Reload on the backup image. The backup image is treated as a new box.

The PDSN redundant pair is treated as a single member by the cluster controller, and is transparent to the PDSN clustering mechanism. The cluster controller is oblivious to a failover from an active PDSN to its redundant standby.

Similarly, a PDSN redundant pair appears as a single PDSN to all external entities, such as the PCF, the HA, and the AAA server.

IPSec security associations for FA-HA connectivity are maintained across fail-over.

Note Currently, VPDN, Closed RP, IPv6 and Prepaid services are not supported by the Session Redundancy implementation.

Note Configuration synchronization between the active and standby units is not supported for R3.0. The operator needs to enter configuration commands on both the Active and Standby units.

In Process Sync Events

The following subsections explain the expected behavior of the PDSN under session redundancy for various sync events in process.

Call Setup

The state of “sessions-in-progress” is not preserved during fail-over. Mechanisms such as R-P connection retry from the PCF will ensure that sessions will be established as required.

It is possible that a fail-over can occur when the PCF has established an R-P session for a user flow, but user flow establishment is not completed. In this case, fail-over will result in the R-P session not being present on the standby. The PCF will timeout the R-P session on the next R-P session lifetime refresh. If the user attempts to establish a new session during this time, a new session will be created.

Call Teardown

There are four scenarios for session termination. These include the following:

- Mobile Terminal initiates session teardown
- PPP Idle Timeout expires on PDSN
- PDSN initiates a Registration Update
- PCF initiates a Registration request with lifetime 0

For each of these cases, session teardown is a multi-step process. For example, a fail-over can occur when a Registration Update message has been sent from the PDSN and the acknowledgement has not been received. In this case, the standby PDSN will already have been told to delete the session. The active PDSN will not wait for an update acknowledgement from the PCF.

If a fail-over occurs after sending the Registration Update to the PCF but before the standby has been told to delete the session, or the request to delete the session is lost, the session will remain established on the standby.

Another case is that the PPP context has been deleted as a result of mobile-initiated termination, and then fail-over occurs prior to the R-P session being terminated.

Similarly, expiry of the PPP Idle timer on the PDSN could also result in deletion of PPP context followed by fail-over prior to R-P session termination.

In these cases, either the Mobile IP Registration Lifetime or the PPP Idle Timeout will expire, and the session is terminated.

Flow Setup

Flows that are in the process of being established are not preserved. You will see this as failure to establish the flow, and you will have to re-establish the flow.

Flow Teardown

This section applies when a session has two or more flows. Currently only a MoIP call supports this case. For an SIP call, only one flow is allowed.

Although a MoIP flow is preserved after switchover, it is possible that registration lifetime expiration will lead to deletion of the flow. If the same user registers again before the lifetime expires, it will be considered as a re-registration since this is an existing visitor. However, the re-registration may or may not succeed, depending on the following conditions:

1. If the user got a Registration Reply (RRP) for its previous de-registration from the active node before the switchover and if the Foreign Agent Challenge (FAC) included in that RRP is not synced to the now active node (very likely, otherwise, the flow would have been deleted from this node), this re-registration will be rejected with an invalid challenge error. The user has to initiate a solicitation to the new active node, receive a new challenge and then resend a Registration Request (RRQ). This time, the RRQ is treated as a valid re-registration and the lifetime is refreshed. It also gets the same IP address as the previous one even though the user considers this as a new registration (it is a re-registration from the FA's and HA's view).
2. If the user did not get a RRP for its previous de-registration from the active node before the switchover, de-registration is resent to the now-active node. This de-registration is likely to be rejected due to invalid FAC, which depends on whether the latest FAC is synced to the standby before the switchover. Then the user can either send a solicitation to get a new FAC and then sends de-registration again or simply give up. In the latter case, 1 above applies.

Dormant-Active Transition

The transition is synchronized between active and standby, and would fall into following scenarios:

1. If the PCF receives a RRP in response to the RRQ, and if the transition state is synced to the standby before the switchover, the now-active node will have the right session state and the transition is successful.
2. If the PCF receives a RRP in response to the RRQ but the transition state is not synced to the standby before the switchover, the now-active node will have the wrong session state (e.g. session is marked as dormant while it should be active).

   However, packets will be switched and counted. The PDSN-related **show** commands may not show all the right information about the session. The subsequent transition from active to dormant will not cause difficulties as the session remains dormant on the PDSN.
3. If the PCF did not receive an RRP in response to the RRQ before the switchover and if it tries again with the now-active node, this is handled as today.
4. If the PCF did not receive a RRP in response to the RRQ before the switchover, and if it exceeds the maximum number of retries with the now-active node, this is handled as 2 above.

Handoff

Inter-PCF Handoff (Dormant or Active) - Same PDSN

The most significant problem with hand-off is to re-establish the data path between the target PCF and the now-active PDSN for the preserved session, irrespective of whether this is an active or dormant handoff. Again, there is a window between handoff actually being completed and the state being synchronized within which a fail-over can occur.

There are the following scenarios:

1. If the target PCF received an RRP from the active PDSN, and the handoff state is synchronized to the standby before switchover, the data path between the target PCF and the now-active PDSN is established for the handed-off session and the user would not perceive any service disruption. The old PCF may or may not receive the Registration Update from the previously active node, depending on the exact point of switchover. If it receives the Registration Update and sends out a RRQ (lifetime=0), the call should be treated correctly at the old PCF. In case that the old PCF does not receive the Registration Update, and that the session is handled back to it again, it's not clear how PCF will handle this case (this is similar to that the PCF has an existing call for a user and then receives a new call request from the same user). If the PCF ignores the new request, the correct data path is not present and therefore a user is not able to transfer traffic.
2. If the target PCF received the RRP from the active PDSN, but the handoff state is NOT synchronized to the standby before switchover, the data path between the target PCF and the now-active PDSN will not be established (the session still points to the old PCF). As a result, the end user will notice service disruption. The user cannot gracefully de-register as PPP packets for call termination (TERMREQ) cannot reach the now-active PDSN, and the RRQ (lifetime=0) from the target PCF arrives on the now-active PDSN but the session does not recognize this as a valid remote tunnel endpoint. As a result, de-registration is ignored. The session will eventually be deleted on expiry of the PPP idle timer or registration lifetime. If the user re-registers again, this will be treated as hand-off since the session's current remote tunnel endpoint (the old PCF) is different from the target PCF. This time, the data path is established and the user will receive service.
3. If the target PCF did not receive an RRP from the active PDSN before switchover, and if the PCF tries again with the now-active PDSN, the hand-off is processed the same as of today.

Inter-PCF Handoff (Dormant or Active) - Different PDSN

This kind of handoff is indicated to the PDSN by receipt of an A11 Registration Request containing the PANID and CANID. It also includes the Mobility Event Indicator and Accounting Data (R-P Session Setup Air-link Record). From the perspective of High Availability, this looks like a new session establishment on the newly active PDSN and a 'regular' session termination on the old PDSN.

A11 Re-registrations

A11 Re-registration RRQ is received by the active unit. The registration life timer does not start on the standby, but it keeps track of the life timer value so that it can restart the life timer once it becomes active. If the lifetime in the re-registration RRQ is different from the previous RRQ, the new lifetime is synced to the standby. For example, if a previous RRQ carries a lifetime of 300 seconds and now a new RRQ has the value changed to 500 seconds, the new value is synced to the standby. Other significant parameters included in the re-registration RRQ are also synced to the standby.

Now, in the above example, if the failover occurs before syncing the new lifetime to the standby, the standby will start the lifetime for 300 seconds.

PPP Re-negotiation

Upon PPP renegotiation, the PDSN deletes all the flows on the RP session and sends accounting STOP for each flow. Once PPP is up again, the PDSN creates new flow(s) for the session. Therefore, when PPP renegotiation happens on the active, the active unit will send a PPP renegotiation notification to the standby which will then delete all the flows from the RP session on the standby. Once PPP is up again and a new flow is created on the active, the active unit sends each flow's data to the standby. If the failover occurs during PPP re-negotiation, the re-negotiation will fail, and the session may be torn down on the newly active unit.

Other Considerations

Timers

The following timers are normally running when a session is established

- R-P Session Lifetime
- PPP Idle Timeout
- Mobile IP Registration Lifetime
- PPP Absolute Session Timeout

The following timers may be running, depending on configuration

- Periodic accounting (not to be confused with the sync timer mentioned above).

These timers are restarted on the standby when fail-over occurs, and the elapsed time is not synchronized to the standby. The effect will be to extend the timers beyond their original values by a time equal to the time that has already expired. This ensures that the user will not perceive a session failure on fail-over.

Restrictions

The following restrictions exist for the PDSN Session Redundancy Feature:

- Limitation for Resource Revocation with SR Setup.

  Setting the revocation timestamp to “msec” (**ip mobile foreign-service revocation timeout** 5 **retransmit** 4 **timestamp** *msec*) for PMIP flows with Session Redundancy is not permitted.

  The “msec” option puts the uptime in the timestamp field, and the uptime of the standby router is expected to be lower after switchover when the standby PDSN takes over as active (and when the PMIP flow was closed). Therefore, revocation on HA will be ignored because the identifier value in the revocation message is less than what is expected by HA.

- The **ip radius source interface** command does not support virtual address (HSRP), and hence the IP address configured under Loopback interface to be used as source interface (NAS IP address) for reaching AAA in SR setup

Internals

The following sections identify information that is synced to the standby unit:

AHDLC

The control character mapping per used AHDLC channel is preserved. As the default is normally used, only those that are different are synchronized. The AHDLC channel number is not synchronized; an available channel will be selected independently on the standby.

GRE - RP Interface

The GRE Key is synchronized. The flags are synchronized as the sequence flag can be set on a per user basis.

RP Signaling

The contents of the A11 messaging will be treated as described below.

- Flags - Fixed - No synchronization required.
- Lifetime - Synchronized.
- Home Address - No synchronization required.
- Home Agent - No synchronization - This is the HSRP address of the R-P interface. This is used for proposing a PDSN IP address when clustering is configured. This will be the HSRP address of the proposed PDSN. It is only used prior to session establishment.
- Care-of-Address - Synchronized - This is the PCF IP address for the R-P Session.
- A10 Source IP Address - Synchronized - This is the PCF's A10 IP Address.
- Identification - Not synchronized - contains timestamp to protect against replay attacks.
- Mobile-Home Authentication Extension - Not synchronized, calculated per message.
- Registration Update Authentication Extension - Not synchronized, calculated per message.
- Session-Specific Extension - Synchronized - covers Key, MN_ID and SR-ID.
- C-VOSE - This contains multiple application types, Accounting, MEI and DAI. The accounting information will be synchronized. Details are in the accounting section.
- N-VOSE contents - ANID will be synchronized, both as part of the session establishment and when it changes as a result of handoff. Fast handoff is not supported, so PDSN Identifier and Identifiers are not relevant to the session redundancy discussion.
- RNPDIT - Synchronized - Radio Network Packet Data Inactivity Timer.
- The source UDP port for the A11 traffic will be synchronized.

PPP

All LCP options are synchronized. For IPCP, only the IP address and IPHC parameters are synchronized. DNS server IP address negotiated during IPCP negotiation is not synchronized to the standby unit. All per user attributes downloaded from AAA during authentication/authorization are synchronized to the standby unit.

Compression - Header and Payload

There is no synchronization of compression context for either header or payload compression. Fail-over to a standby PDSN results in the compression context being re-established.

Header compression - First packet for a session after switchover is dropped, and peer retries the packet after acknowledge timeout.

Payload compression - There is no compression history present after switchover on the standby. A CCP reset is automatically generated when decode fails. No special treatment is needed.

IP Address Assignment

When an IP address is dynamically assigned from a pool configured on the PDSN, it is necessary that the standby associates the same address with the session. The IP address will be synchronized as part of PPP state. If the IP address is received from AAA or a static IP address is used that does not come from a local pool, this address will also be associated with the session on the standby. Similarly, the address pool will be synced.

AAA - Authentication and Authorization

Table 2 lists the relevant Authentication and Authorization parameters. This is required on the standby to allow accurate recreation of AAA state.

Table 2 Standard AVPs Supported for Authentication and Authorization

Authentication and Authorization AVPs Supported By Cisco IOS Name	Synchronized	Description	Allowed In	
			Access Request	Access Accept
User-Name	Yes	User name for authentication and authorization.	Yes	No
User-Password	No	Password for authentication.	Yes	No
CHAP-Password	No	CHAP password.	Yes	No
NAS-IP-Address	No	IP address of the PDSN interface used for communicating with RADIUS server. A loopback address could be use for this purpose.	Yes	No
Service-Type	No	Type of service the user is getting. Supported values include: • "Outbound" for MSID based user access • "Framed" for other type of user access	Yes	Yes
Framed-Protocol	No	Framing protocol user is using. Supported values include: • PPP	Yes	Yes
Framed-IP-Address	Yes	IP address assigned to the user.	Yes	Yes
Session-Time-Out	Yes	Maximum number of seconds of service is to be provided to the user before session terminates. This attribute value becomes the per-user "absolute time-out."	No	Yes
Idle-Time-out	Yes	Maximum number of consecutive seconds of idle connection allowed to the user before the session terminates. This attribute value becomes the per-user "idle-time-out".	No	Yes
Calling-Station-ID	Yes	MSID identifier of the mobile user.	Yes	No
CHAP-Challenge (optional)	No	CHAP Challenge.	Yes	No

Table 2 Standard AVPs Supported for Authentication and Authorization (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Synchronized	Description	Allowed In	
			Access Request	Access Accept
Tunnel-Type	No	VPN tunneling protocol(s) used. Supported values include: • 1 for PPTP (not supported) • 3 for L2TP	No	Yes
Tunnel-Medium-Type	No. Not supported	Transport medium type to use for the tunnel.	No	Yes
Tunnel-Client- Endpoint	No. Not supported	Address of the client end of the tunnel. When you specify Tunnel-Client-Endpoint, Tunnel-Server is not supported. Use L2TP	No	Yes
Tunnel-Server- Endpoint	No. Not supported	Address of the server end of the tunnel.	No	Yes
Tunnel-Password	No. Not supported	Password to be used for authenticating remote server.	No	Yes
Tunnel-Assignment-ID	No. Not supported	Indicates to the initiator of the tunnel, identifier of the tunnel to which the session is assigned.	No	Yes
addr-pool	No. Not supported	Name of a local pool from which to obtain address. Used with service=ppp and protocol=ip. "addr-pool" works in conjunction with local pooling. It specifies the name of a local pool (which must have been pre-configured locally). Use the ip-local pool command for configuring local pools. For example: • ip address-pool local • ip local pool boo 10.0.0.1 10.0.0.10 • ip local pool moo 10.0.0.1 10.0.0.20	No	Yes
Inacl#<n>	Yes	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol =ipx. **Note** Per-user access lists do not currently work with ISDN interfaces.	No	Yes

Table 2 Standard AVPs Supported for Authentication and Authorization (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Synchronized	Description	Allowed In	
			Access Request	Access Accept
Inacl	Yes	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Contains an IP output access list for SLIP or PPP/IP (for example, intacl=4). The access list itself must be pre-configured on the router.	No	Yes
outacl#<n>	Yes	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx.	No	Yes
Outacl	Yes	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be pre-configured on the router.	No	Yes
interface-config	Yes	User-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command.	No	Yes
SPI	Yes	Carries authentication information needed by the home agent for authenticating a mobile user during MIP registration. Provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range. The information is in the same syntax as the **ip mobile secure host** *address* configuration command. Essentially, it contains the rest of the configuration command that follows that string, verbatim.	No	Yes

Table 2 Standard AVPs Supported for Authentication and Authorization (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Synchronized	Description	Allowed In	
			Access Request	Access Accept
IP-Pool-Definition	Yes	Defines a pool of addresses using the format: X a.b.c Z; where X is the pool index number, a.b.c is the pool's starting IP address, and Z is the number of IP addresses in the pool. For example, 3 10.0.0.1 5 allocates 10.0.0.1 through 10.0.0.5 for dynamic assignment.	No	Yes
Assign-IP-Pool	Yes	Assign an IP address from the identified IP pool.	No	Yes
Framed-Compression	Yes	Indicates a compression protocol used for the link. Supported values include: • 0: None • 1: VJ-TCP/IP header compression	No	Yes
Link-Compression	Yes	Link compression protocol to be used. Supported values include: • 0: None • 1: Stac • 2: Stac-LZS • 3: MS-Stac	No	Yes

GPP2 Packet Data Service Attributes

Table 3 lists the 3GPP2 Packet Data Service Attributes

Table 3 3GPP2 Packet Data Service Attributes

Name	Synchronized	Description	Allowed In	
			Access Request	Access Accept
mobileip-mn-lifetime	Yes	Defines lifetime used in Proxy MIP RRQ.	No	Yes
mobileip-mn-ipaddr	Yes	MN IP address for static address assignment. If this attribute is present, this address is used in Proxy MIP RRQ.	No	Yes
mobileip-mn- flags	Yes	Defines Flags used in Proxy MIP RRQ.	No	Yes

Table 3 3GPP2 Packet Data Service Attributes (Continued)

Name	Synchronized	Description	Allowed In	
CDMA-Realm	Yes	For MSID based access, "realm" information for construction of user name in the form MSID@realm. User names constructed this way are used for accounting purposes only. The format of realm information is: • ASCII string specifying realm of user's registered domain.	No	Yes
CDMA-User- Class	Yes	Type of service user is subscribed to. Supported values are: • 1 for Simple IP • 2 for Mobile IP	No	Yes
3GPP2-Reverse-Tunnel- Spec	Yes	Indicates whether reverse tunneling is required or not. Su.pported values are: • 0 for reverse tunneling not required. • 1 for reverse tunneling required.	No	Yes
3GPP2-Home-Agent- Attribute	Yes	Address of the Home Agent	Yes	Yes
3GPP2-IP-Technology	Yes	Indicates type of service user is subscribed to. Supported values are: • 1 for Simple IP • 2 for Mobile IP	No	Yes
3GPP2-Correlation-Id	Yes	Identifies all accounting records generated for a particular user flow.	Yes	Yes
3GPP2-Always-On	Yes	Indicates Always On Service. Supported values are: • 0 for non always on users • 1for always on users	No	Yes
3GPP2-Security Level	Yes	Indicates the type of security that the home network mandates on the visited network.	No	Yes
3GPP2- IKE Pre-shared Secret Request	No	Indicates that the PDSN needs a pre-shared secret for Phase 1 IKE negotiation with the HA.	Yes	No
3GPP2-Pre-shared secret	No	A pre-shared secret for IKE.	No	Yes
3GPP2-KeyID	No	Contains the KeyID parameter used during IKE exchange between the PDSN and the HA.	No	Yes

Table 3 3GPP2 Packet Data Service Attributes (Continued)

Name	Synchronized	Description	Allowed In	
3GPP2-Allowed DiffServ marking	No	Specifies if the user is able to mark packets with AF (A), EF (E). The Max Class (i.e., Max Selector Class), specifies that the user may mark packets with a Class Selector Code Point that is less than or equal to Max Class.	No	Yes
3GPP2-MN-AAA Removal Indication	Yes	When received in a RADIUS Access-Accept message, the PDSN shall not include the MN-AAA.	No	Yes
3GPP2-Foreign-Agent Address	No	The IPv4 address of the PDSN CoA contained in RRQ.	Yes	No
Service Option	Yes	Indicates the type of service being used.	Yes	No
DNS Update Required	No. Not supported	Indicates whether DNS update is required.	No	Yes
RN PDIT	Yes	Radio Network Packet Data Inactivity Timer.	No	Yes
Session Termination Capability	Yes	Indicates the nature of resource revocation supported.	Yes	Yes

AAA Accounting

GPP2 Accounting Records Fields

Table 4 identifies the GPP2 accounting records fields.

Table 4 GPP2 Accounting Records Fields

Item	Parameter	Description	Synchronized
A. Mobile Identifiers			
A1	MSID	MS ID (e.g., IMSI, MIN, IRM)	Yes
A2	ESN	Electronic Serial Number	Yes
A3	MEID	Mobile Equipment Identifier	Yes
B. User Identifiers			
B1	Source IP Address	IPv4 address of the MS.	Yes
B2	Network Access Identifier (NAI)	user@domain construct which identifies the user and home network of the MS.	Yes
B3	Framed-IPv6-Prefix	MS IPv6 prefix.	Not supported.
B4	IPv6 Interface ID	MS IPv6 interface identifier.	Not supported.
C. Session Identifiers			
C1	Account Session ID	The Account Session ID is a unique accounting ID created by the Serving PDSN that allows start and stop RADIUS records from a single R-P connection or P-P connection to be matched.	Yes

Table 4 GPP2 Accounting Records Fields (Continued)

Item	Parameter	Description	Synchronized
C2	Correlation ID	The Correlation ID is a unique accounting ID created by the Serving PDSN for each packet data session that allows multiple accounting events for each associated R-P connection or P-P connection to be correlated.	Yes
C3	Session Continue	This attribute when set to “true” means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. “False” means end of a session.	Yes
C4	Beginning Session	The attribute when set to “true” means new packet data session is established; “false” means continuation of previous packet data session. This attribute is contained in a RADIUS Accounting-Request (Start) record.	No
C5	Service Reference ID	This is the service instance reference ID received from the RN in an A11 Registration-Request message.	Yes
D. Infrastructure Identifiers			
D1	Home Agent	The IPv4 address of the HA.	Yes
D2	PDSN	The IPv4 address of the PDSN.	No. Should be configured to be the same on the active and standby.
D3	Address Serving PCF	The IP address of the serving PCF (the PCF in the serving RN).	Yes
D4	BSID	SID + NID + Cell Identifier type 2.	Yes
D5	IPv6 PDSN Address	The IPv6 address of the PDSN.	Not supported
D6	Foreign Agent Address	The IPv4 address of the FA-CoA.	Not supported
E. Zone Identifiers			
E1	User zone	Tiered Services user zone.	Yes
F. Session Status			
F1	Forward FCH Mux Option	Forward Fundamental Channel multiplex option.	Yes
F2	Reverse FCH Mux Option	Reverse Fundamental Channel multiplex option.	Yes
F5	Service Option	CDMA service option as received from the RN.	Yes
F6	Forward Traffic Type	Forward direction traffic type - either Primary or Secondary.	Yes
F7	Reverse Traffic Type	Reverse direction traffic type - either Primary or Secondary.	Yes
F8	FCH Frame Size	Specifies the FCH frame size.	Yes

Table 4 GPP2 Accounting Records Fields (Continued)

Item	Parameter	Description	Synchronized
F9	Forward FCH RC	The format and structure of the radio channel in the forward Fundamental Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates.	Yes
F10	Reverse FCH RC	The format and structure of the radio channel in the reverse Fundamental Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates.	Yes
F11	IP Technology	Identifies the IP technology to use for this call: Simple IP or Mobile IP.	Yes
F12	Compulsory Tunnel Indicator	Indicator of invocation of compulsory tunnel established on behalf of MS for providing private network and/or ISP access during a single packet data connection.	Yes
F13	Release Indicator	Specifies reason for sending a stop record.	Yes
F14	DCCH Frame Size	Specifies Dedicated Control Channel (DCCH) frame size.	Yes
F15	Always On	Specifies the status of Always On service.	Yes
F16	Forward PDCH RC	The Radio Configuration of the Forward Packet Data Channel. (This parameter can be used as an indication that the MS is 1xEV DV capable.)	Yes
F17	Forward DCCH Mux Option	Forward Dedicated Control Channel multiplex option.	Yes
F18	Reverse DCCH Mux Option	Reverse Dedicated Control Channel multiplex option	Yes
F19	Forward DCCH RC	The format and structure of the radio channel in the forward Dedicated Control Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates.	Yes
F20	Reverse DCCH RC	The format and structure of the radio channel in the reverse Dedicated Control Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates.	Yes
G. Session Activity			
G1	Data Octet Count (Terminating)	The total number of octets in IP packets sent to the user, as received at the PDSN from the IP network (i.e. prior to any compression and/or fragmentation).	Yes
G2	Data Octet Count (Originating)	The total number of octets in IP packets sent by the user.	Yes
G3	Bad PPP frame count	The total number of PPP frames from the MS dropped by the PDSN due to incorrect able errors.	Yes

Table 4 GPP2 Accounting Records Fields (Continued)

Item	Parameter	Description	Synchronized
G4	Event Time	This is an event timestamp which indicates one of the following: • The start of an accounting session if it is part of a RADIUS start message. • The end of an accounting session if it is part of a RADIUS stop message. • An Interim-Update accounting event if it is part of a RADIUS Interim-Update message.	Yes
G5	Remote IPv4 Address Octet Count	Contains the octet count associated with one or more remote IPv4 address; used for source/destination accounting.	Not supported
G6	Remote IPv6 Address Octet Count	Contains the octet count associated with one or more remote IPv6 address; used for source/destination accounting.	Not supported
G8	Active Time	The total active connection time on traffic channel in seconds.	Yes
G9	Number of Active Transitions	The total number of non-active to Active transitions by the user.	Not supported
G10	SDB Octet Count (Terminating)	The total number of octets sent to the MS using Short Data Bursts.	Yes
G11	SDB Octet Count (Originating)	The total number of octets sent by the MS using Short Data Bursts.	Yes
G12	Number of SDBs (Terminating)	The total number of Short Data Burst transactions with the MS.	Yes
G13	Number of SDBs (Originating)	The total number of Short Data Burst transactions with the MS.	Yes
G14	Number of HDLC layer octets received	The count of all octets received in the reverse direction by the HDLC layer in the PDSN.	Yes
G15	Inbound Mobile IP Signaling Octet Count	This is the total number of octets in registration requests and solicitations sent by the MS.	Yes
G16	Outbound Mobile IP Signaling Octet Count	This is the total number of octets in registration replies and agent advertisements sent to the MS prior to any compression and/or fragmentation.	Yes
G17	Last User Activity Time	This is a Timestamp (in number of seconds from Jan 1 1970 UTC) of the last known activity of the user.	Yes
I. Quality of Service			
I1	IP Quality of Service (QoS)	This attribute is deprecated.	Not supported
I2	Airlink Priority	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service.	Not supported
Y. Airlink Record Specific Parameters			

Table 4 GPP2 Accounting Records Fields (Continued)

Item	Parameter	Description	Synchronized
Y1	Airlink Record Type	3GPP2 Airlink Record Type.	No
Y2	R-P Connection ID	Identifier for the R-P Connection. This is the GRE key that uniquely identifies an R-P connection (an A10 connection) between the PCF and the PDSN.	Yes
Y3	Airlink Sequence Number	Sequence number for Airlink records. Indicates the sequence of airlink records for an R-P connection.	Yes
Y4	Mobile Originated / Mobile Terminated Indicator	Used only in SDB airlink records. Indicates whether the SDB is Mobile Originated or Mobile Terminated. (0=Mobile Originated and 1=Mobile Terminated).	Yes
Z. Container			
Z1	Container	3GPP2 Accounting Container attribute. This attribute is used to embed 3GPP2 AVPs.	Not supported

Radius Server Group Support

The IP address of the AAA server chosen will not be synchronized.

Mobile IP Signaling

For Mobile IP service, the parameters to be synchronized, per MIP flow, include the following:

- Mobile IP Registration Lifetime
- Mobile IP Flags indicated in the Registration Request
- MN-AAA Removal Indication received from AAA
- Home Agent IP address
- Mobile's IP Address
- Reverse Tunneling indication
- Care of Address from Mobile IP Registration Request
- FA-Challenge (used during Mobile Node reregistration)

Mobile IP tunneled traffic

This traffic is carried in either GRE tunnels or IP-in-IP tunnels. The only information that needs to be synchronized is the tunnel endpoint of the peer.

Locally Configured IPSec

For the PDSN on the Cat76xx, IPSec tunnels are terminated on the Macedon VPN Acceleration Module. The role of the PDSN is to retrieve parameters from AAA and, based on those parameters, trigger IPSec tunnel establishment. Synchronization of these parameters is sufficient to preserve IPSec tunnels in the event of PDSN fail-over for intra-chassis configurations. PDSN failover is not coupled with VPN Acceleration Module/SUP failover. Inter chassis configurations and intra-chassis Macedon/SUP failover does not currently support stateful IPSec.

FA-HA IPSec

FA-HA IPSec tunnels will be preserved when PDSN on 7600 fail-over occurs for intra-chassis configurations. They will not be preserved for inter chassis configurations.

AAA Accounting

Periodic Accounting Sync

Accounting information is optionally synchronized between the active and standby images. This synchronization occurs at the configured periodic accounting interval. The counters that are synchronized are g1 and g2, along with the packet counts. Sending an Interim Accounting record will trigger synchronization of the byte and packet counts. Setting the operator-defined periodic accounting interval determines the accuracy of the user-billing record as impacted by PDSN fail-over. It is possible that undercharging could occur; however, overcharging is not possible.

Accounting with VSA Approach

After a switchover takes place, the first interim or stop accounting record (as appropriate) includes a VSA (cdma-rfswact) indicating that a switchover has occurred. The inclusion of this VSA is controllable by issuing the **cdma pdsn redundancy accounting send vsa swact** command.

Note Please note that the G1 and G2 counters will not sync.

Here is a sample accounting debug with vsa:

```
Sep 13 18:23:10.179: RADIUS:   Cisco AVpair       [34]  16
Sep 13 18:23:10.179: RADIUS:   63 64 6D 61 2D 72 66 73 77 61 63 74 3D 31
[cdma-rfswact=1]
```

System Accounting

In a session redundancy setup, an accounting ON will be sent by the active unit only when the whole setup is brought up (accounting ON will not be sent by the newly active unit after a failover). The standby unit does not send any system accounting events under any scenarios. The events, however, are sent in a standalone mode.

A sys-off is sent if reload is issued on the active unit.

Configuring PDSN Session Redundancy

The following new commands have been introduced for PDSN Session Redundancy:

Enabling PDSN Session Redundancy

The active PDSN shall be able to synchronize the session and flow related data to its standby peer provided the redundancy capability has been enabled. By default this capability is disabled.

The commands syntax is as follows:

[**no**] **cdma pdsn redundancy**

When the above CLI is configured, session redundancy is enabled provided the underlying redundancy infrastructure has been configured. The redundancy functionality for PDSN is disabled when the above command with **no** is executed.

Periodic Accounting Counters Synchronization

The active PDSN by default will not try synchronizing accounting counters periodically. To enable periodic accounting counters synchronization, configure the following command:

[no] **cdma pdsn redundancy accounting update-periodic**

The **no** form of the command is used to go to the default behavior. When configured, the byte and packet counts for each flow are synced from the active to the standby unit (only if they undergo a change) at the configured periodic accounting interval (using **aaa accounting update periodic** xxx). If periodic accounting is not configured, the byte and packet counts will not be synced.

Debug Commands for PDSN-Session Redundancy

In order to facilitate the identification of problem areas of PDSN high availability, the following debug commands are introduced for debugging. All of these debug can be turned off using either undebug all or no debug all, if desired.

[no] **debug cdma attribute**

[no] **debug cdma pdsn redundancy packets**

To debug and collect any data pertaining to PDSN-SR, the above command is executed and the details pertaining to redundancy data is sent to the console.

[no] **debug cdma pdsn redundancy errors**

To debug the PDSN-SR redundancy errors the above command is executed and the details pertaining to A11 data is sent to the console.

[no] **debug cdma pdsn redundancy events**

To debug events for PDSN session redundancy events, above command is executed and the details pertaining to PDSN (e.g. RP) data is sent to the console.

Display of Redundancy Statistics

When a pair of PDSNs is operating in an active and a standby mode, it is desirable to show or display a variety of information about the sessions and its associated flows that have been synchronized to the standby. The following command shall allow the operator to view the session redundancy data for PDSN.

show cdma pdsn redundancy statistics

On execution the above command displays a number of data items; some of the examples are as follows:

- Number of sessions synchronized
- Number of SIP flows
- Number of MoIP flows
- Number of synchronized sessions up after a switch-over.
- Number of sessions failed to synchronize.

Note **show cdma pdsn redundancy statistics** will be hidden until **service internal** is configured.

show cdma pdsn redundancy

On execution of this command, in addition to existing data being displayed, it will also output “pdsn redundancy is enabled,” or “redundancy is not enabled,” depending on whether the redundancy feature for PDSN has been turned on, or not.

Clearing of PDSN Session Redundancy Statistics

clear cdma pdsn redundancy statistics

On execution of this command, all the data counters associated with the PDSN session redundancy will be actualized to initial value.

Other Debug Commands

In addition to the PDSN-SR debugging commands described above, the following commands associated with high availability are also useful debugging aid:

debug redundancy inter-device

debug ccm

Other Show Commands

In addition to the PDSN-SR show commands described above, the following commands associated with high availability are also useful:

show redundancy inter-device

Configuring PDSN Session Redundancy Infrastructure

The PDSN-SR feature uses the Cisco IOS Check-point Facility (CF) to send stateful data over Stream Control Transmission Protocol (SCTP) to a redundant PDSN. Additionally, in conjunction with Cisco IOS HSRP, the PDSN uses the Cisco IOS Redundancy Facility (RF) to monitor and report transitions on Active and Standby PDSNs.

Before you configure PDSN-SR, you need to configure the inter-device redundancy infrastructure.

Configuring HSRP

The Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts on networks without relying on the availability of any single router. HSRP is used in a group of routers for selecting an Active router and a Standby router. HSRP monitors both the inside and outside interfaces so that if any interface goes down, the whole device is deemed to be down and the Standby device becomes active and takes over the responsibilities of an Active device.

When configuring HSRP, note that the following recommendation and restrictions apply:

- At minimum, HSRP must be enabled and an HSRP a “master” group defined on one interface per PDSN instance. A “follow” group can be configured on all other PDSN interfaces using the standby interface configuration command with the follow keyword option specified. The advantages of using follow groups are:
  - The follow group feature enables all interfaces on which it is configured to share the HSRP parameters of the master group.
  - Interfaces that share the same group will follow the state of master interface and will use same priority as master interface. This will ensure that all interfaces are in the same HSRP state. Otherwise there is a possibility of one or more interfaces to assume another role than the master HSRP interface.
  - This optimizes HSRP group number and hence minimizes the configuration and maintenance overhead when having large configurations.
  - It eliminates unnecessary network traffic over all interfaces by eliminating HSRP Hello messages from follow groups, if configured.

- Do not configure a preemption delay on the Standby PDSN using the standby preempt interface configuration command.
- When the **standby use-bia** command is not used to allow bridge and gateways to learn the virtual MAC address, for optimization purposes, configure the **standby mac-refresh** command to a value greater than the default (hello messages are sent every 10 seconds) under the main interface (gig0/0). This value is used as the hello message interval.

Note If **standby use-bia** is configured, no hello messages are sent out of the follow group interfaces. We recommended that you use the default virtual MAC address with HSRP unless explicitly required not to.

- An ARP multicast packet is sent out when there is a HSRP state change to Active. ARP requests for follow group virtual IP address are responded if HSRP state is Active. Also an ARP multicast is sent on the follow group VLAN when a slave virtual IP address is configured and if the master group is Active.

Use the same group number for each PDSN follow group as is defined for the primary group. Using the same group number for the primary and follow groups facilitates HRSP group setup and maintenance in an environment that contains a large number of PDSN interfaces and HRSP groups.

More information on HSRP configuration and HSRP groups can be found here:

http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html

and

http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_configuration_example09186a0080094e90.shtml

Enabling HSRP and Configuring an HSRP Master Group

To enable HSRP on an interface and configure the primary group, use the following commands in interface configuration mode:

Step 1 Router(config-if)# **standby** [**group-number**] **ip** [**ip-address** [**secondary**]]

Enables the HSRP on the interface.

Step 2 Router(config-if)# **standby** [**group-number**] **priority** *priority*

Set the Hot Standby priority used in choosing the active router. The priority value range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. Specify that, if the local router has priority over the current active router, the local router should attempt to take its place as the active router.

Step 3 Router(config-if)# **standby** [**group-number**] **name** *name*

Specifies the name of the standby group.

Step 4 Router(config-if)# **standby use-bia** [**scope interface**]

(Optional) Configures HSRP to use the burned-in address of an interface as its virtual MAC address instead of the preassigned MAC address.

Configuring Follow Groups

HSRP follow groups are configured to share the HSRP parameters of the primary group by defining a follow group on the interface using the standby interface configuration command with the follow keyword option specified. Interfaces that share a group track states together and have the same priority.

To configure an interface to follow a primary group, use the following command in interface configuration mode:

Step 1 Router(config-if)# **standby** *group-number* **follow** *group-name*

Specifies the number of the follow group and the name of the primary group to follow and share status.

Note It is recommended that the group number specified is the same as the primary group number.

Step 2 Router(config-if)# **standby** *group-number* **ip** *virtual-ip-address*

Specifies the group number and virtual IP address of the follow group.

Note The group number specified above should be same as the master group number.

Enabling Inter-Device Redundancy

To enable inter-device redundancy, use the following commands beginning in global configuration mode.

Step 1 Router(config)# **redundancy inter-device**

Configures redundancy and enters inter-device configuration mode.

To remove all inter-device configuration, use the **no** form of the command.

Step 2 Router(config-red-interdevice)# **scheme standby** *standby-group-name*

Defines the redundancy scheme that is to be used. Currently, “standby” is the only supported scheme.

standby-group-name-Must match the standby name specified in the **standby name** interface configuration command (see the “Configuring HSRP” section). Also, the standby name should be the same on both PDSNs.

Step 3 Router(config-red-interdevice)# **exit**

Returns to global configuration mode.

Configuring the Inter-Device Communication Transport

Inter-device redundancy requires a transport for communication between the redundant PDSNs. This transport is configured using Interprocess Communication (IPC) commands.

To configure the inter-device communication transport between the two PDSNs, use the following commands beginning in global configuration mode:

Step 1 Router(config)# **ipc zone default**

Configures the Inter-device Communication Protocol (IPC) and enters IPC zone configuration mode.

Use this command to initiate the communication link between the Active device and the Standby device.

Step 2 Router(config-ipczone)# **association** *1*

Configures an association between two devices and enters IPC association configuration mode.

In IPC association configuration mode, you configure the details of the association, such as the transport protocol, local port and local IP addresses, and the remote port and remote IP addresses.

Valid association IDs range from 1 to 255. There is no default value.

Step 3 Router(config-ipczone)# **no shutdown**

Restarts a disabled association and its associated transport protocol. Note Shutdown of the association is required for any changes to the transport protocol parameters.

Step 4 Router(config-ipczone-assoc)# **protocol sctp**

Configures Stream Control Transmission Protocol (SCTP) as the transport protocol for this association and enables SCTP protocol configuration mode.

Step 5 Router(config-ipc-protocol-sctp)# **local-port** *local_port_num*

Defines the local SCTP port number to use to communicate with the redundant peer and enables IPC Transport-SCTP local configuration mode.

Valid port numbers range from 1 to 65535. There is no default value.

Note The local port number should be the same as the remote port number on the peer router.

Step 6 Router(config-ipc-local-sctp)# **local ip** *ip_addr*

Defines the local IP address that is used to communicate with the redundant peer. The local IP address must match the remote IP address on the peer router.

Step 7 Router(config-ipc-local-sctp)# **keepalive** [**period** [**retries**]]

Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets with a response before bringing down the interface or tunnel protocol for a specific interface.

Valid value for period is an integer value in seconds great than 0. The default is 10. Valid value for retries is an integer value greater than one and less than 355. The default is the previously used value or 5 if there was no value previously specified.

Step 8 Router(config-ipc-local-sctp)# **retransmit-timeout** *interval*

Configures the message retransmission time. Valid range is 300 to 60000 milliseconds. The minimum default is 1000. The maximum default is 60000.

Step 9 Router(config-ipc-local-sctp)# **path-retransmit** *number*

Configures the maximum number of keep-alive retries before the corresponding destination address is marked inactive. Valid range is 2 to 10. The default is 5.

Step 10 Router(config-ipc-local-sctp)# **assoc-retransmit** *number*

Defines the maximum number of retransmissions over all destination addresses before an association is declared failed. Valid range is 2 to 20. The default is 10.

Step 11 Router(config-ipc-local-sctp)# **exit**

Exits IPC transport - SCTP local configuration mode.

Step 12 Router(config-ipc-protocol-sctp)# **remote-port** *port_num*

Defines the remote SCTP port that is used to communicate with the redundant peer and enables IPC Transport-SCTP remote configuration mode. Valid port numbers range from 1 to 65535. There is no default.

Note The remote port number should be the same as the local port number on the peer device.

Step 13 Router(config-ipc-remote-sctp)# **remote-ip** *ip_addr*

Defines the remote IP address of the redundant peer that is used to communicate with the local device. All remote IP addresses must refer to the same device. To remove an association configuration, use the **no** form of the command.

Using the Loopback Interface For the PDSN-AAA Server Interface

To ensure that the AAA server views the active and standby units as a single NAS, the same NAS IP address should be used by both the units. Now, the NAS IP Address can be configured for the PDSN using the **ip radius source-interface** command. When configured, the IP address of that interface is used as the NAS IP Address.

However, the command does not support virtual IP addresses (HSRP). As a result, the only way to ensure that both the units appear as a single NAS is to configure a loopback interface, and use that interface as the source-interface. In short, the CLI would look something like:

ip radius source-interface Loopback1

Configuring Application Tracking to Handle Active-Active Situation

Step 1 Router(config) # **track** *object-id* **application pdsn**

Defines a tracking object for PDSN application.

Step 2 Router(config-if) # **standby track** *object-id* [**decrement** *priority*]

Associates the tracking object defined for PDSN with the HSRP config. HSRP would start tracking the state of this object. The configured **decrement** *priority* is used to change the HSRP priority based on the state of the tracking object. If the tracking object is "UP", HSRP will have the configured priority. If the tracking object is "DOWN", HSRP decrements its priority by the **decrement** *priority* specified in the **standby track** command.

Note If preemption is configured, the *priority* value should be greater than the difference in priorities of the active and standby PDSNs

Protocol Layering and RP Connections

Each mobile station has a single PPP connection with the PDSN, and for each PPP connection there is a corresponding R-P connection between the PDSN and the Base Station/ PCF. R-P connection-related information is maintained for the duration of the PPP connection.

Additionally, the PPP connection and the associated HDLC, LCP, CCP and IPCP state information is also maintained for the duration of the packet data session. One Simple IP flow and several Mobile IP flows can be supported over a single PPP connection.

Open RP Interface Connections

An R-P connection represents the logical tunnel between the PDSN and the Base Station/PCF. It enables bearer data for a PPP connection to be transported between the PDSN and the Base Station/PCF. R-P connection state information is maintained at the PDSN for the duration of the PPP connection. During handoff, the mobile station may connect the PDSN through another Base Station/PCF entity resulting in establishment of another R-P connection between the PDSN and the new Base Station/PCF. This results in the release of the R-P connection between the PDSN and the old Base Station/PCF.

R-P connection state information is maintained at the PDSN even during the dormant phase of the session. When a mobile station transitions to active state, this information allows the PDSN to associate the mobile station with an already available PPP connection. Loss of R-P state information results in the release of the PPP connection by the PDSN. As a result, a mobile station accessing packet data services following the loss of an R-P connection results in the establishment of a new PPP connection, and the reset and restart of user applications. Therefore, the PDSN retains the R-P connection state information to ensure minimal disruption of user applications during transitions between active and dormant session phases.

Note In PDSN Release 2.1, Dual RP Interface (Open RP and Closed RP) is not supported on the same PDSN instance.

PPP Connections

A PPP connection represents the link layer connectivity between the mobile station and the PDSN. It includes the HDLC state, negotiated LCP parameters, negotiated IP address and CCP compression state tables, etc. Peer PPP entities may re-negotiate LCP and CCP parameters during an active session without compromising continuity of user sessions; however, user identity, authentication-related information and negotiated IP addresses are retained, thus ensuring that applications established over the SimpleIP flow are unaware that renegotiation has occurred. PPP connection state information is retained at the PDSN during dormant phase of the session to ensure minimal disruption of user applications during transitions between active and dormant session phases.

Application Flows

One Simple IP and several Mobile IP flow instances can be supported over a single PPP connection. For each Simple IP flow, the state information includes the associated IP address, NAI and billing related user data records (UDRs), and other related information. For each Mobile IP flow, the state information includes the Mobile IP visitor list information, NAI and UDRs, and other related information.

Closed-RP/Open-RP Integration

Cisco PDSN Release 3.0 introduces the Closed-RP and Open-RP Integration feature, which includes the following details:

- Open RP and Closed RP handoff support on the same PDSN instance
- Open RP and Closed RP common clustering solution based on controller member architecture that already exist for Open RP

Handoff between Closed-RP and Open-RP

PDSN instance will be able to handoff the session between the Closed-RP and Open-RP PCF. During the handoff the PDSN will not re-negotiate the PPP for the session. Also in the accounting records for a Closed-RP PCF only the relevant parameters that are supported in the Closed-RP architecture are sent. For the Open-RP PCF all the 3GPP2 supported accounting parameters will be included records to the RADIUS.

Closed-RP/Open-RP Clustering Architecture

The controller module in the Open-RP clustering architecture supports Closed-RP clustering. In the dual mode, the controller module accepts Closed-RP connections from the Closed-RP PCF, and terminates the connection locally. After it successfully terminates the Closed-RP connection, the controller performs L2TP Tunnel switching on the session to one of the members. The following call control and call management capabilities of the Closed RP signaling interface are supported on the controller:

- Closed RP Tunnel setup procedures
- Closed RP Tunnel teardown procedures
- Closed RP Session setup procedures
- Closed RP Session release procedures
- Closed RP and Open RP handoff procedures

Closed-RP Tunnel Setup Procedures

The PCF establishes a Closed RP tunnel when it is brought into service, and PDSN IP addresses are statistically configured on it. PCF establishes a tunnel with each PDSN controller for which it has an IP address.

The following L2TP control messages are required to setup the tunnel in a Controller Closed RP Tunnel Setup

Step 1 Closed RP PCF sends SCCRQ (Start-Control-Connection-Request) to the PDSN controller which terminates the Closed RP tunnel.

Step 2 The PDSN controller in case accepts the tunnel request will reply with SCCRP (Start-Control-Connection-Reply) to the Closed RP PCF.

Step 3 Closed RP PCF responds with SCCCN (Start-Control-Connection-Connected) to the PDSN Controller.

Step 4 PDSN controller Acks the SCCCN message with ZLB (Zero Length Buffer) to the Closed RP PCF.

Closed RP Tunnel Clearing Procedures

Tunnel clearing can be initiated by the PDSN (Controller / Member) or by Closed RP PCF by sending a Stop Control Connection Notification Message, and ZLB is sent to Ack the message. The PDSN can be configured to initiate the Tunnel termination in the following scenarios

- There is no keepalive message
- There is no session.

Here is the Controller Closed RP Tunnel Clearing message flow:

Step 1 Closed RP PCF sends a Stop CCN to the PDSN controller, and the PDSN controller deletes the tunnel (including all the sessions on the tunnel) and responds with the ZLB Ack to the Closed RP PCF. All the Closed RP sessions that are switched to PDSN members are also locally cleared on the controller. If all the sessions are closed on the Closed RP tunnel between the controller and members, then Closed RP switched tunnel is also closed by sending a Stop CCN message to the member.

Step 2 The PDSN members can send Stop CCN to the PDSN controller, and the PDSN controller deletes the tunnel (including all the sessions on the tunnel) and responds with the ZLB Ack to the PDSN member. All the Closed RP session towards to the Closed RP PCF are locally cleared. If all the sessions are cleared, then Stop CCN is sent to the Closed RP PCF.

Closed RP Connection Setup Procedures

The following message flow depicts the Controller Closed RP Connection Setup:

Step 1 Closed RP PCF sends an ICRQ message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attributes, such as MSID.

Step 2 The PDSN controller sends an ICRP message to the Closed RP PCF. ICRP message is sent to the Closed RP PCF if, and only if, the PDSN controller is able to select a PDSN member for redirecting this particular session. Otherwise the ICRQ is rejected by the PDSN controller by sending a CDN message. Please refer to below note for selection for PDSN member

Step 3 Closed RP PCF sends an ICCN message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes, and for mandatory attributes.

Step 4 If the PDSN controller accepts the ICCN message, it sends a ZLB Ack message to the Closed RP PCF

Step 5 The PDSN controller sends a SCCRQ message to the PDSN member selected for redirecting the session.

Step 6 The PDSN member send a SCCRP message to the PDSN controller.

Step 7 The PDSN controller sends a SCCN message to the PDSN member.

Step 8 The PDSN member sends a ZLB Ack to the PDSN controller.

Step 9 The PDSN controller sends the ICRQ message to PDSN member. In the ICRQ, all the Closed RP AVP are included (similar to what was received from the Closed RP PCF). The PDSN controller includes 2 additional attributes in the ICRQ message (HopCount AVP set to 1 and Original NAS IP address AVP set to the original PCF IP address). By sending the PCF IP address in Original NAS IP address AVP allows the PDSN member to send the correct PCF IP address in the accounting information to the RADIUS

Step 10 The PDSN member sends ICRP to the PDSN controller if the ICRQ is accepted on the PDSN member.

Step 11 The PDSN controller sends ICCN to the PDSN member with the Closed RP AVP included.

Step 12 The PDSN member sends ZLB Ack to the PDSN controller.

Step 13 The PDSN member starts PPP negotiation with the mobile. Until the tunnel and session is established between the PDSN controller and PDSN member, the data packets (which are the PPP negotiation packets) from the mobile are dropped on the controller itself.

Note Steps 5 through 8 are performed only once for the tunnel to be setup between the Closed RP PDSN controller and the PDSN member.

Note Selection of the PDSN member is based on whether the PDSN controller already has the MSID information, or not. If the PDSN controller does not possess the MSID information, then member selection is based on the PDSN member selection criteria. If MSID information is already present, then the same member is selected.

Both 3GPP2 RP and Closed RP share a common MSID to the PDSN member table on the PDSN controller. This enables the PDSN controller to select the same PDSN member during the handoff between the RP technologies.

Closed RP Connection Release Procedure

The following message flow depicts the Controller Closed RP Connection Release procedure:

Step 1 The Closed RP PCF sends a CDN to the PDSN controller; the PDSN controller deletes the session on the tunnel and responds with the ZLB Ack to the Closed RP PCF. The PDSN controller also closes the Closed RP session with the PDSN member by sending a CDN message for the session to the member.

Step 2 The PDSN member sends a CDN to the PDSN controller; the PDSN controller deletes the session on the tunnel and responds with the ZLB Ack to the PDSN member. PDSN controller also closes the Closed RP session with the Closed RP PCF by sending a CDN message for the session to the Closed RP PCF.

Closed RP and Open RP Handoff Procedures

The following message flow depicts the Controller Closed RP Handoff Closed to Open RP PCF procedure:

Step 1 The Closed RP PCF sends an ICRQ message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attribute such as MSID.

Step 2 The PDSN controller sends an ICRP message to the Closed RP PCF. An ICRP message is sent to the Closed RP PCF if, and only if, the PDSN controller is able to select a PDSN member for redirecting this particular session. Otherwise the ICRQ is rejected by the PDSN controller by sending a CDN message. Please refer to the note below for selection for PDSN member.

Step 3 The Closed RP PCF sends an ICCN message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attributes.

Step 4 The PDSN controller, if it accepts the ICCN message, sends a ZLB Ack message to the Closed RP PCF

Step 5 The PDSN controller will send a SCCRQ message to the PDSN member selected for redirecting the session.

Step 6 The PDSN member will send a SCCRP message to the PDSN controller.

Step 7 The PDSN controller sends a SCCN message to the PDSN member.

Step 8 The PDSN member sends a ZLB Ack to the PDSN controller.

Step 9 The PDSN controller sends the ICRQ message to PDSN member. In the ICRQ all the Closed RP AVPs are included (similar to what was received from the Closed RP PCF).The PDSN controller includes 2 additional attributes in the ICRQ message (HopCount AVP set to 1 and Original NAS IP address AVP set to the original PCF IP address). By sending the PCF IP address in Original NAS IP address AVP allows the PDSN member to send the correct PCF IP address in the accounting information to the RADIUS.

Step 10 The PDSN member sends ICRP to the PDSN controller if the ICRQ is accepted on the PDSN member.

Step 11 The PDSN controller sends ICCN to the PDSN member with the Closed RP AVP included.

Step 12 The PDSN member sends ZLB Ack to the PDSN controller.

Step 13 The PDSN member starts PPP negotiation with the mobile.

Step 14 The Open RP PCF sends an A11 Registration request to the PDSN controller as part of the handoff.

Step 15 The PDSN controller rejects the Registration request with 88H (unknown PDSN) and provides the member IP address that holds the Closed RP session.

Step 16 The Open RP PCF sends the A11 registration request to the PDSN member.

Step 17 The PDSN member sends a A11 registration reply accept to the Open RP PCF.

Step 18 The PDSN member sends a CDN message to the Old PCF (PDSN controller) with message code 255 indicating handoff.

Step 19 The PDSN controller sends a ZLB Ack to the PDSN member.

Step 20 The PDSN controller sends a CDN message to the PCF with message code 255 indicating handoff.

Step 21 The PDSN receives a ZLB Ack for the CDN message from the PCF.

The following message flow depicts the Controller Closed RP Handoff Open to Close RP PCF procedure:

Step 1 The Open RP PCF sends an A11 Registration request to the PDSN controller as part of the handoff.

Step 2 The PDSN controller rejects the Registration request with 88H (unknown PDSN) and provides the member IP address that holds the Closed RP session.

Step 3 The Open RP PCF sends the A11 registration request to the PDSN member.

Step 4 The PDSN member sends a A11 registration reply accept to the Open RP P.

Step 5 The PDSN member starts PPP negotiation with the mobile.

Step 6 The Closed RP PCF sends an ICRQ message to the PDSN controller as part of handoff. The PDSN controller checks for the Closed RP specific attributes and mandatory attributes, such as MSID.

Step 7 The PDSN controller sends an ICRP message to the Closed RP PCF. ICRP message is sent to the Closed RP PCF if and only if PDSN controller is able to select a PDSN member for redirecting this particular session. Otherwise the ICRQ is rejected by the PDSN controller by sending a CDN message. Please refer to below note for selection for PDSN member.

Step 8 The Closed RP PCF sends an ICCN message to the PDSN controller. PDSN controller checks for the Closed RP specific attributes and mandatory attributes.

Step 9 The PDSN controller, if it accepts the ICCN message, sends a ZLB Ack message to the Closed RP PCF.

Step 10 The PDSN controller sends a SCCRQ message to the PDSN member selected for redirecting the session.

Step 11 The PDSN member sends a SCCRP message to the PDSN controller.

Step 12 PDSN controller sends a SCCN message to the PDSN member.

Step 13 The PDSN member sends a ZLB Ack to the PDSN controller.

Step 14 The PDSN controller sends the ICRQ message to the PDSN member. In the ICRQ all the Closed RP AVPs are included (similar to what was received from the Closed RP PCF). The PDSN controller includes 2 additional attributes in the ICRQ message (HopCount AVP set to 1, and Original NAS IP address AVP set to the original PCF IP address). Sending the PCF IP address in Original NAS IP address AVP allows the PDSN member to send the correct PCF IP address in the accounting information to the RADIUS

Step 15 The PDSN member sends ICRP to the PDSN controller if the ICRQ is accepted on the PDSN member.

Step 16 The PDSN controller sends ICCN to the PDSN member with the Closed RP AVP included.

Step 17 The PDSN member sends ZLB Ack to the PDSN controller.

Step 18 The PDSN member sends A11 RP Update to the Old PCF.

Step 19 The PDSN member receives A11 RP Update Ack from the old PCF.

Step 20 The PDSN member receives A11 De registration request from the Old PCF.

Step 21 The PDSN member accepts the De registration request from the Old PCF.

The following message flow depicts the Controller Closed RP Handoff Closed to Closed RP PCF procedure:

Step 1 The Closed RP PCF sends an ICRQ message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attribute such as MSID.

Step 2 The PDSN controller sends an ICRP message to the Closed RP PCF. ICRP message is sent to the Closed RP PCF if, and only if, the PDSDN controller is able to select a PDSN member for redirecting this particular session. Otherwise, the ICRQ is rejected by the PDSN controller by sending a CDN message. Please refer to note below for selection for PDSN member.

Step 3 The Closed RP PCF sends an ICCN message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attribute.

Step 4 If the PDSN controller accepts the ICCN message, it sends a ZLB Ack message to the Closed RP PCF.

Step 5 The PDSN controller sends a SCCRQ message to the PDSN member selected for redirecting the session.

Step 6 The PDSN member sends a SCCRP message to the PDSN controller.

Step 7 The PDSN controller sends a SCCN message to the PDSN member.

Step 8 The PDSN member sends a ZLB Ack to the PDSN controller.

Step 9 The PDSN controller sends the ICRQ message to PDSN member. In the ICRQ all the Closed RP AVP are included (similar to what was received from the Closed RP PCF). PDSN controller includes 2 additional attributes in the ICRQ message (HopCount AVP set to 1, and Original NAS IP address AVP set to the original PCF IP address). Sending the PCF IP address in Original NAS IP address AVP allows the PDSN member to send the correct PCF IP address in the accounting information to the RADIUS.

Step 10 The PDSN member sends ICRP to the PDSN controller if the ICRQ is accepted on the PDSN member.

Step 11 The PDSN controller sends ICCN to the PDSN member with the Closed RP AVP included.

Step 12 The PDSN member sends ZLB Ack to the PDSN controller.

Step 13 The PDSN member starts PPP negotiation with the mobile.

Step 14 The Closed RP PCF sends an ICRQ message to the PDSN controller as part of handoff. The PDSN controller checks for the Closed RP specific attributes and mandatory attributes, such as MSID.

Step 15 The PDSN controller sends an ICRP message to the Closed RP PCF. ICRP message is sent to the Closed RP PCF if, and only if, the PDSN controller is able to select a PDSN member for redirecting this particular session. Otherwise, the ICRQ is rejected by the PDSN controller by sending a CDN message. Please refer to the note below for selection for PDSN member.

Step 16 The Closed RP PCF sends an ICCN message to the PDSN controller. The PDSN controller checks for the Closed RP specific attributes and mandatory attribute.

Step 17 The PDSN controller if accepts the ICCN message will send a ZLB Ack message to the Closed RP.

Step 18 The PDSN controller sends the ICRQ message to PDSN member. In the ICRQ all the Closed RP AVP are included (similar to what was received from the Closed RP PCF). The PDSN controller includes 2 additional attribute in the ICRQ message (HopCount AVP set to 1, and Original NAS IP address AVP set to the original PCF IP). Sending the PCF IP address in Original NAS IP address AVP allows the PDSN member to send the correct PCF IP address in the accounting information to the RADIUS.

Step 19 The PDSN member sends ICRP to the PDSN controller if the ICRQ is accepted on the PDSN member.

Step 20 The PDSN controller sends ICCN to the PDSN member with the Closed RP AVP included.

Step 21 The PDSN member sends ZLB Ack to the PDSN controller.

Step 22 The PDSN member sends a CDN message to the Old PCF (PDSN controller) with message code 255 indicating handoff.

Step 23 The PDSN controller sends a ZLB Ack to the PDSN member.

Step 24 The PDSN controller sends a CDN message to the PCF with message code 255 indicating handoff.

Step 25 The PDSN controller receives a ZLB Ack for the CDN message from the PCF.

Performance

In the solution controller that anchors the Closed RP session from the PCF, and does L2TP switching of these sessions to the PDSN member, the following performance measurements were found:

- The PDSN controller supports 20,000 Closed RP sessions and 140,000 Open RP sessions with 2 PDSN controllers (one being Active, and other Standby), with 8 PDSN member each supporting 20,000 sessions in total. These can be a mix of Closed RP and Open RP sessions.
- The PDSN controller supports approximately 10% of the Closed RP session that are active; 2,000 sessions will be able to send and receive traffic using this architecture. With 144Kbps required for each session, this translates to 300 Mbps of traffic support required on the PDSN controller for 10% of Closed RP session being active. CPU usage on the controller for a 20,000 Closed RP session open, and 2% of these session being active with 300Mbps of traffic is around 44%.
- The Open RP CPS on the controller is around 750 calls per second (for 140,000 sessions), with 300 Mbps traffic being sent on 2,000 closed RP session on the controller. The CPU usage during the period is 98%.

Mobility Management With Closed-RP

An important aspect of packet data services is mobility management. A user should be able to maintain an established service even when roaming within and beyond their service provider's coverage area. For such mobility management, the system supports handoffs that are transparent to user applications.

Handoffs

Handoffs occur as a result of user mobility. A CDMA2000 system supports three types of handoffs:

- **Inter-BTS Handoff**

  This type of handoff occurs when the mobile moves from one BTS coverage area to another BTS coverage area, generally within a BSC/PCF area. This type of handoff is not visible to the PDSN and is not discussed further.

- **Inter-PCF Handoff - Same PDSN**

  This type of handoff occurs when the mobile moves from the radio coverage area served by one BSC/PCF to a coverage area served by a different BSC/PCF, both connected to the same MSC. In this case, the new PCF can often connect to the same PDSN as the old PCF. However, this is not guaranteed.

  When a mobile with an active data session hands off from one PCF to another PCF, the target PCF sends an ICRQ with Session Inquiry AVP to all the PDSNs it is connected with. The PDSN that has the PPP session for the Mobile Node replies with ICRP and terminates the RP session with the Source PCF by sending a CDN with Cause Value 253. If none of the PDSNs, connected with the Target PCF has the PPP session for the Mobile Node, the PCF chooses the least loaded PDSN and proceeds with Call Setup.

- **Inter-PCF Handoff - Different PDSN**

  This type of handoff occurs when the mobile moves from the radio coverage area served by one BSC/PCF to a coverage area served by a different BSC/PCF and the new BSC/PCF is connected to a different MSC than the old BSC/PCF. In this case, the new and old PCFs are typically unable to connect to the same PDSN.

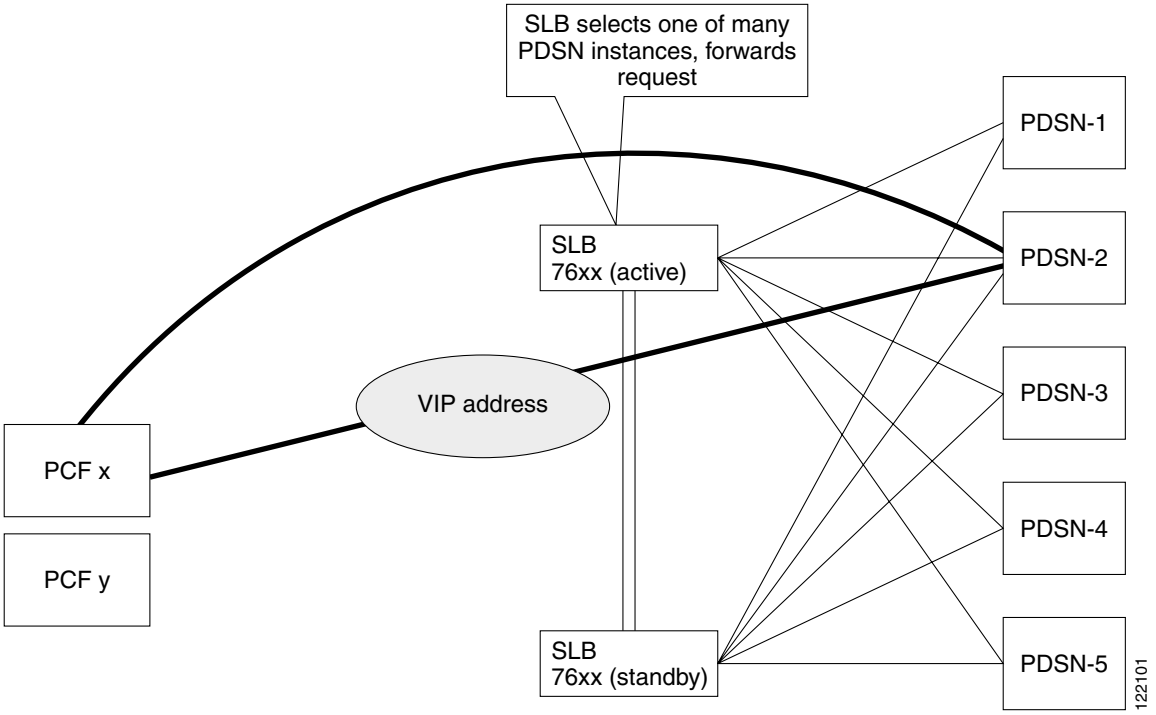
  This scenario is possible when the mobile moves to a different radio coverage area and the new BSC/PCF connects to a different MSC than the original BSC/PCF. In this case, it is unlikely that the same PDSN will be used. This results in Inter-PCF and Inter-PDSN handoff.

  When the target PCF learns that none of the PDSNs host the packet data session for the MN, the least loaded PDSN is selected and the session is set up using the same steps followed in initial call setup. This scenario is same as the new Closed RP connection setup.

IOS-SLB on the Supervisor card

One aspect of the Closed-RP feature requires that you configure Server Load Balancing on the Cisco Supervisor card. IOS-SLB on the Supervisor card provides loadbalancing for the Closed RP Tunnels between the PCFs and PDSNs. The Loadbalancing unit will direct the Closed RP tunnel to the appropriate PDSN instance. The IOS-SLB unit supports redundancy, so that there is no single point of failure for this system. Figure 6 illustrates this configuration.

Figure 6 Closed-RP Server Load Balancing Configuration



PPPoGRE RP Interface

The PDSN interfaces with the Radio Network/Base Station to provide a transmission path for the user data stream between the packet network and the radio access network. The PDSN interfaces to the Radio Network through the Packet Control Function (PCF) using the PPPoGRE RP interface.

The following list describes the transmission path between the Radio Network and the PDSN:

- The PDSN provides a media-independent physical link that supports IP packet transport capabilities.
- The PPPoGRE RP Interface supports both the signaling channel and the bearer data transport capabilities.

The PPPoGRE RP interface is based on 3GPP2 TIA/EIA/IS-835 standard for the control and bearer data transport capabilities. The following list describes the differences between the 3GPP2 standard and PPPoGRE RP Interface from the PDSN perspective:

- The PCF connecting the PDSN that supports PPPoGRE functionality sends the A11 Registration request with the GRE Protocol Type field set to 0x880B.
- Neither the PDSN, nor the mobile node requires AHDLC framing or de-framing for the PPPoGRE sessions.
- A10 bearer data packets are sent and received in the GRE Protocol field set to 0x880B (PPPoGRE).

A11 Session Update

This feature is based on Interoperability Specification (IOS) for *cdma2000 Access Network Interfaces* (*Part 7* (*A10 and A11 Interfaces*) (3G-IOSv4.3) Version 2.0.1 Date: July 2003) and Interoperability Specification (IOS) for *cdma2000 Access Network Interfaces* (*Part 3 Features* (3G-IOSv4.3) Version 2.0.1 Date: July 2003 standard). An A11 Session Update message is sent from the PDSN to the PCF to add, change, or update session parameters for an A10 connection. The following parameters are sent from the PDSN to PCF in an A11 Session Update message in a session parameters NVSE extension with Application Type 08H (Session Parameter). These session parameters NVSE extension will also be sent by the PDSN in the A11 Registration Reply messages.

- Radio Network Packet Data Inactivity Timer [01H]
  - Application Sub- Type 01H, the Application Data field contains the Radio Network Packet Data Inactivity Timer (RN-PDIT) value in seconds. This field is one octet in length and has range 01H-FFH, corresponding to timer values 1-255 seconds.
  - Supported for Service types Simple IP, Mobile IP, Proxy Mobile IP, MSID, and VPDN.
- Always On Indicator [02H]
  - For Application Sub Type 02H ((Always-on indicator), the Application Data is zero bytes in length.
  - Supported for Service types Simple IP and MSID.

As per the standard *cdma2000® Wireless IP Network Standard* TIA-835-C, AUGUST 2003, the PDSN will download the Always On Indicator VSA and RN-PDIT VSA from the Radius server (Visited/Home RADIUS) during the authentication phase. If a user initiates multiple packet data sessions, the PDSN may receive more than one RN PDIT VSA from different home domains. In this case, the largest RN PDIT value received from different home domains is sent from the PDSN to the RN. This update may happen during an ongoing packet data session when the PDSN receives a new RN PDIT value that is greater than the one previously sent to the RN. For Handoff scenario the RN-PDIT and Always-On indicator are sent the PCF in the A11 Registration Reply if the Airlink is not dormant.

SDB Indicator Marking

This feature supports short data burst (SDB) applications, such as SIP signaling for PTT applications, and proposes the interaction with the PDSN. SIP is used by PTT applications to signal a PTT call. The message is short and needs to be delivered to the end-user. The Short Data Burst support on the RAN can be used to send these to the end-user, especially when the messages are to be terminated to the mobile. This is especially important when the mobile user is actually dormant.

The proposal consists of two parts:

- Signalling of SDB indication, or other indications, on the GRE link between PDSN and PC.
- Identification of data packet suitable for payloads.

Note SDB Marking is only supported for service type Simple IP.

Signaling of SDB Indication

The SDB indication is based on the 3GPP2 Proposal Contribution (Ericsson/SKT) A30-20030818-006, where one of the reserved bits in the GRE header is used to indicate the SDB packets from the PDSN for dormant sessions. The PDSN definition of dormancy is Airlink Stop record A11 Registration request is received from the PCF and A11 Registration success reply is sent by the PDSN.

The PDSN may set the B bit to “1” if the GRE frame contains an IP packet suitable for transmission over the air interface in a Data Burst Message. In the PCF-to-PDSN direction, and on the A8 interface, the B bit is set to “0”.

Identification of Data Packets For SDB Indication

SDB indication is required for certain types of data only. Packets destined towards the mobiles that match the policy criteria will be chosen for SDB indication provided the mobile is in dormant mode

The local policy can be considered for an initial phase, if the selection of servers or signaling protocols is limited. For example, if there is only a single SIP server sending out SIP signaling message, a combination of port and source IP address may be used. In addition to this, the PDSN can also be configured with the min and max IP length.

On a Cisco PDSN, IOS MQC can be used to apply classification rules for matching packets that require SDB classification. For example, simple classification criteria can include port number, and source IP address range of the server. A more complex classification criterion can include a custom protocol inspection.

If packets pass the classification criteria and the user is dormant, the PDSN will signal SDB indication to the PCF.

To enable this feature, use the following command:

cdma pdsn compliance ios4.1 sdb

This command enables the PDSN to process an SDB record sent from PCF according to IOS4.1 Standard.

If deep classification is required for certain types of payloads such as RTP, or a custom application, IOS NBAR can be used for inspecting these packets. For a detailed description of how to configure IOS NBAR please refer to the documentation on NBAR.

A sample configuration for the classification function is shown here:

```
class-map match-all sdb-packets
     match packet length min 100 max 300
     match protocol <protocol>
     match access-group <access-group-number>
ip access-list <access-group-number> permit ip 192.0.2.0 0.0.0.255 any
```

(This example of access-list allows matching of a certain protocol from servers whose address range is 192.0.2.0/24)

The protocol and the access-group can be set to match the desired packet stream. The match criteria can also include a custom protocol inspection such as

ip nbar custom media_new 8 hex 0x60 **dest udp** 3001

The above statement classifies all packets with a UDP destination of port 3001, and contains the value 0x60 at offset 8. The protocol **media_new** can now be used in the **match protocol** *protocol* statement.

```
policy-map sdb-policy
     class sdb-packets
     set qos-group group-number
```

The policy map is then applied to the input interface. The group-number represents the classified match criteria. All packets that are set with the specific group-number will be flagged for SDB usage between the PCF and the PDSN. This is done with the following command:

cdma pdsn a11 dormant sdb-indication gre-flags *group-number*

The B bit (SDB indication) would be set for packets matching the sdb-indication group-number.

SDB Indicator Marking for PPP Control Packets

While data packets can be sent towards the mobile using SDBs as shown above, SDBs can also be used for delivering PPP control packets. This can be particularly helpful for Always-On sessions, where the session is dormant. Basically, with Always On configured, the PDSN sends out LCP echo requests (and waits for LCP echo replies) to keep the session alive. Hence, when such a session goes dormant, a data channel needs to be setup to deliver these LCP echo requests to the MN. The other option is to use SDBs to deliver the LCP echo requests without setting up a data channel.

Configure the following CLI in conjunction of the above CLIs to enable this feature:

cdma pdsn a11 dormant sdb-indication match-qos-group *group-number* **ppp-ctrl-pkts**

Resource Management

Resource management defines the mechanism to release packet data session related resources at the network elements like the PDSN and the HA. Resources may be released due to the session handoff or for administrative purposes.

IS-835-C defines two mechanisms for resource management:

- Packet of Disconnect (POD)
- Mobile IP Resource Revocation

While resource management based on Packet of Disconnect is applicable to Simple IP, Mobile IP and Proxy Mobile IP flows, resource management based on Mobile IP Resource revocation is applicable only to Mobile IP flows.

The Cisco PDSN supports resource management based on both Packet of Disconnect and Mobile IP resource revocation.

Resource Revocation for Mobile IP

Basic Mobile IP resource revocation is an IS-835-C initiative that defines the methods by which a mobility agent (one that provides Mobile IP services to a mobile node) can notify the other mobility agent of the termination of a registration due to administrative reasons or MIP handoff.

When configured on the PDSN/FA, the Mobility Agent Advertisement extension in the Agent advertisement will have the X bit set, thus advertising support for resource revocation on that link. A PDSN configured to support resource revocation in Mobile IPv4 will include a revocation support extension in all MIP RRQ including re-registrations. If the associated MIP RRP from the HA also includes a valid revocation support extension, then the PDSN will assume the associated registration as revocable.

For a registration that is revocable, if the PDSN/FA needs to terminate the session administratively, the PDSN/FA sends a resource revocation message to the HA and releases the resources held for that registration.

If the resource revocation ACK from the HA is not received within a configurable amount of time, the resource revocation message will be retransmitted.

On receipt of a resource revocation message from Home Agent, and a registration (identified by the home address, care-of address, and Home Agent address) is located, the resources held by that registration are freed, and a resource revocation ACK message is sent back to the Home Agent. If no other Mobile IP registrations are active on the PPP session associated with the revoked binding, then the PDSN will release the associated PPP and R-P sessions for the revoked registration.

Restrictions for Registration Revocation

The following restrictions for Registration Revocation on the PDSN apply:

- The STC VSA returned from AAA in access-accept message during FA-CHAP and HA-CHAP will be ignored, and local configuration on the PDSN and HA will take precedence.
- Revocation extension and messages, even if not protected by FHAE or IPSec, will be accepted and processed by both PDSN and HA. It is recommended that the user takes care of providing the security of the messages by either configuring FA-HA security association or by provisioning IPSec tunnel between the two agents.
- MobileIP MIB is not updated with the Registration revocation information.

- On the PDSN, all the **ip mobile foreign-service** commands need to be configured at the global level and not at the interface level.
- On the PDSN, for the I-bit support the local policy is to always negotiate I-bit and to always set it to 1 in the Revocation messages. Also the provision to set B-bit to 1 in the agent advertisement message while informing MN of the revoked data flow is not provided.
- Resource Revocation and Bind Update cannot be enabled simultaneously. Both are mutually exclusive of each other.

Packet of Disconnect

Radius Disconnect, or Packet of Disconnect (PoD) is a mechanism that allows the RADIUS server to send a Radius Disconnect Message to the PDSN to release Session related resources. Resources may be released due to the session handoff, or for administrative purposes. Some of the resources identified include PPP, RP sessions and Mobile IP bindings. Support for Radius Disconnect on the Cisco PDSN and Home Agent is TIA835C compliant.

The PDSN communicates its Resource management capabilities to the Home AAA in the Access Request message (sent for authentication/authorization procedure) by including a 3GPP2 Vendor Specific Session Termination Capability (STC) VSA. The value communicated in the STC VSA is obtained in the configuration. The PDSN also includes an NAS-Identifier attribute containing its Fully Qualified Domain Name (FQDN) in the Access Request.

The Home AAA server establishes a relationship between the user and the NAS Identifier/ NAS-IP address to detect a inter-PDSN handoff. If the NAS-Identifier/ NAS IP address received in the Access Request is different from the previously stored value (non-zero), an inter-PDSN handoff is detected.

The Disconnect Request contains the NAS-ID and the Username (NAI) attributes. It can optionally contain 3GPP2 Correlation ID Calling station ID (IMSI) and the Framed IP address—some session identification attributes. A Disconnect Reason VSA is included if a inter-PDSN handoff is detected. The session identification attributes supported by the PDSN are 3GPP2 Correlation ID and Calling station ID (IMSI).

If the 3GPP2 Correlation ID and Calling station ID (IMSI) attributes are received in the Disconnect Request, and the PDSN is able to find the session/flow corresponding to them, the PDSN will terminate the associated flow and send a Disconnect ACK message to RADIUS server. If session is not found for the received attributes, the PDSN will reply back with a Disconnect NACK message with error code “session context not found”. If the Disconnect request has invalid attributes (for example, an 8 digit IMSI), the PDSN will reply with a Disconnect NACK with error code “Invalid Request”.

The PDSN also supports processing Disconnect Requests that only contain the NAI attribute (if configured). In compliance with the standards, the PDSN terminates all sessions corresponding to the Username received.

The Ballot version mentions that a Disconnect Request can be received at the Home Agent (HA,) but details on the action to be taken in such an event is not detailed. Hence the approach followed is to terminate a specific binding if Framed-IP-Address attribute is received along with NAI, or terminate all bindings for the NAI, if only NAI attribute is received in the Disconnect Request.

The following restriction is present for this feature:

- All Dormant NVSE are not supported.

The command line interface for this feature will be standard AAA interfaces. The preferred method to configure POD in Release 2.0 and above is to use the **aaa server radius dynamic-author** command, which leads to a sub-configuration mode that has options to configure clients, security keys, and other variables.

The following NAS global AAA command is used to enable listening for POD packets:

- **aaa pod server key** *word,* where *word* is the shared key.

The full syntax for this command is:

- **aaa pod server [clients** *ipaddr1* **[***ipaddr2***] [***ipaddr3***] [***ipaddr4***]] [port** *port-number***] [auth-type {any | all | session-key}] server-key** [***encryption-type***] *string*

The following debug command is also available:

- **debug aaa pod**

Restrictions for RADIUS Disconnect

- All Dormant NVSE is not supported.
- MIB support is not currently planned.
- Processing of a RADIUS Disconnect message with only NAI present must be configured for compliance to IS 835-C.

Radius Enhancements

PDSN R3.0 includes the following RADIUS enhancements:

- Radius Server Load Balancing
- Selection of Radius Server based on realm.

Radius Server Load Balancing

The RADIUS Load-Balancing feature is a mechanism to share the load of RADIUS Authentication and Accounting transactions across a set of RADIUS servers. Currently, all transactions are sent to the first server considered to be alive in a server group. Only when this server stops responding and is marked dead, the PDSN fails over to the next one in the group. This mechanism of using only one server despite the presence of other usable servers in the group limits the overall throughput for call setup/teardown.

Thus, with Radius Server Load Balancing, the PDSN distributes the transaction load across multiple servers in a server group. It tracks the slower servers and reduces the transaction load on those servers and it adapts when a server is marked dead and when it comes back up again.

The transactions are grouped into batches (the size of which is configurable), and each server is assigned a batch to process. The feature then load-balances transactions based on these batches, one batch at a time. When the first transaction is received, the algorithm determines the server with the least outstanding transactions. This server is then assigned the next batch of transactions. Once a batch of transactions has been assigned, we again compute the server with the least outstanding transactions. This server gets assigned the next batch of transactions. Thus the server with the least outstanding transactions always gets assigned the next batch. This load-balancing scheme can be applied based on a server group. Thus, each server group defined on the IOS platform can have its own load-balancing scheme.

Care should be taken while configuring the batch size. The trade-off in large versus a small batch size is that of throughput versus CPU load. A large batch size results in lesser amount of computations hence a lower CPU load. However, it may cause a particular server within the server-group to be assigned transactions even though others in the group are idle. For very small batch sizes, the CPU load increases, as it computes outstanding load across servers more often. Lab simulations indicate that a batch size of 25 gives a decent throughput while not adversely affecting CPU load.

High Latency RADIUS servers

The algorithm adapts well to servers of varying response times. Servers that are quick will have a lower number of transactions outstanding and hence will be assigned larger number of the incoming transactions. Slower servers get proportionately lesser number of transactions.

Server Failovers

When a transaction fails over to the next server in the group after a failover, its outstanding count will be increased. Thus, failed-over transactions are also load-balanced. When the next batch of transactions is being assigned, this server's outstanding count will reflect it's load accurately - both new and failover transactions will be accounted for in the outstanding transaction count.

Dealing with Server Groups

Consider the following two server-groups:

Server-group SG1 with servers S1, S2, S3.

Server-group SG2 with servers S3, S4, S5.

Consider that SG1 is configured to be load-balanced, while SG2 is not. When requests are sent to SG2, these requests will be assigned to S3 as it is the first server in the group and its outstanding transaction count will increase. When requests are sent to SG1, these requests will be load-balanced across these servers. When sending transactions to S3, the outstanding transaction count for the server will be high due to the SG2 transactions being assigned directly to it. Hence it will receive a low proportion of transactions in SG1. This is the preferred behavior, since the goal is to send transactions to servers that are quicker and able to handle more load, where load is the total transactions a server is handling, not just those of the current server-group.

Preferred Servers

In certain cases, it is desirable to use the same server for the authentication and accounting phases of a session. With RADIUS server load balancing, however, there are no guarantees that the stop-record for a session will be sent to the same server as the start-record for that session. To avoid such situations a preferred-server indication is introduced in Release 3.0.

Note This indication is a preference/recommendation only.

The PDSN will try to use the server if possible, but if not, it will fall back to other servers in the group based on the load-balancing mechanism.

When this indicator is used, costs will not be considered in deciding the server to use. However, it might not be possible to always use the preferred server. The server may have been marked dead. Or the server may not be usable since it isn't part of the server-group that was used for a previous transaction for the session (for example, the Accounting server-group may be different from the authentication server-group). In this case, the algorithm is free to select an alternate server, based on the load-balancing scheme.

Incoming RADIUS requests

The RADIUS server load balancing feature is not applicable to incoming RADIUS requests (e.g. Packet of Disconnect). POD responses require that the server requesting service be the one that is responded too. Hence we shouldn't load-balance these requests across servers.

Subscriber Authorization Based on Domain

Cisco IOS provides a "Subscriber Authorization" mechanism to authorize subscribers based on their realm. You can find details of this feature at the following URL:

http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463

IS-835 Prepaid Support

The Cisco PDSN 2.0 software release provides real-time monitoring and rating of data calls for prepaid users. The prepaid billing solution for the PDSN is based on the RADIUS (AAA) server, and takes advantage of the existing flow-based accounting functionality. The prepaid billing feature requires the RADIUS server to interface with a Prepaid Billing Server (PBS) to relay real-time billing information between the PDSN and the PBS. A third-party Prepaid Billing Server controls the real-time rating of data calls and maintains balances in users' accounts. Cisco does not supply the PBS.

The following three types of Prepaid service are available in PDSN Release 2.1:

- Volume-based Prepaid data service
- Volume-based Prepaid data service with tariff switching
- Duration-based Prepaid data service

Prepaid functionality is supported on PDSN for the following type of data sessions:

- Simple IP sessions with authentication and authorization performed at AAA.
- VPDN sessions with authentication and authorization for the user performed at AAA.
- Mobile IP sessions with FA-CHAP performed for the session/NAI at AAA.
- Proxy mobile IP sessions with authentication and authorization for the user performed at AAA.

Prepaid service is also available for sessions opened with MSID-based authentication access.

Note Either Volume-based or Duration-based, but not both options in one prepaid flow, are supported on the PDSN. Multiple flows, each supporting either Volume or Duration based prepaid service, are allowed on the PDSN. The PDSN can be configured to support only Volume-based, or only Duration-based, or either type of Prepaid service per flow at any point in time.

Volume-based accounting for prepaid flows other than VPDN will count the bytes present in the PPP payload. For VPDN flows, it will count the bytes present in the PPP packet including the PPP packet header. A session that has multiple flows can have some of the flows with prepaid data service enabled, each either Volume-based or Duration-based, while other flows may not be prepaid enabled.

Tariff-based prepaid service is also supported for volume-based prepaid data service on the PDSN. To support tariff-based prepaid service, the Prepaid Billing Server should have the following capabilities:

- Charged by volume—different tariff for different time of day.
- The Billing server allocates a different quota (volume-based) for a user that is determined by a tariff for a different time-of-day (this ensures the two charging rates do not overlap).

Restrictions for Prepaid Support in Cisco PDSN Release 2.1

- Prepaid for remote address based accounting is not supported.
- Online Access Request messages are sent with Service-Type as “outbound” (instead of “Authorize Only”), and user password is included in the message.
- There is no Prepaid MIB support in the present release.
- Prepaid for the HA is not supported.

Prepaid Billing

When a user performs Simple IP access with AAA authentication, or Mobile IP access with FA-CHAP, the Prepaid capable PDSN sends a RADIUS Access-Request message for Authentication and Authorization. The Prepaid capable PDSN informs the Billing Server of its own Prepaid capabilities by including a PPAC VSA in the RADIUS Access-Request message.

The Home RADIUS performs Authentication and Authorization procedures as usual. If the HAAA identifies that a user is a prepaid user from its user profile, the HAAA interfaces with the Billing Server to retrieve prepaid related information for the user, and passes on the prepaid related information in the Access Request message. The Billing Server performs prepaid authorization for the user. The prepaid authorization procedure at HAAA and Billing Server consists of the following steps:

- Checking the PPAC VSA.
- Checking the home network policy.
- Checking the user’s account balance and state.

When the Billing Server successfully authorizes the user as a valid prepaid user, it notifies the HAAA that it supports prepaid service based on volume, or duration, or both, depending on the configuration at the Billing Server and capabilities as indicated by the PDSN. The HAAA encodes the information in a PPAC VSA to the PDSN, and indicates that volume-based or duration-based prepaid (or both) service is supported by the Billing Server.

HAAA sends the authorization response to the Prepaid capable PDSN using RADIUS Access-Accept/Reject messages. The authorization response includes a PPAQ VSA in the same RADIUS Access-Accept message stating an initial quota, quota-id and a threshold value of the quota for the prepaid flow corresponding to the user.

When the PDSN sends on-line Access Request messages to HAAA for prepaid related functionality, it does not set the User-Password (= 2) field in the message, and normal RADIUS message authentication is set and performed with Message Authenticator. Currently, the User-Password is set in online Access Requests to the default value of “cisco”.

If the PDSN does not receive the PPAC VSA from the HAAA in the initial RADIUS Access-Accept message, or the message is included but indicates that “Prepaid Accounting not used”, the PDSN will release the user’s prepaid flow if the RADIUS Access-Accept message includes a PPAQ VSA. The PDSN will send an Access Request to HAAA to return the quota allocated with Update-Reason VSA that indicates Client Service termination.

If the PDSN is capable of supporting prepaid service based on either volume or duration, then the PDSN will enable prepaid service for the flow based on the Billing server-indicated service that applies to the session in PPAC. If the Billing server also indicates that the PDSN can allocate either volume or duration, then the PDSN will enable prepaid service based on the type of quota (volume or duration) present in PPAQ from HAAA. If both types of quota are present in PPAQ, then prepaid flow is not opened on the PDSN.

If the PDSN is capable of supporting prepaid service based on volume, and Billing Server indicates that it will support prepaid service based on duration, then the PDSN will close the prepaid flow. The PDSN will send an Access Request message with Update-Reason VSA indicating “Client Service termination”. The same logic applies to the PDSN if it supports prepaid based on duration, and Billing Server returns prepaid service based on volume.

If the PDSN receives an Access-Accept message containing the PPAC VSA indicating prepaid service supported, but the initial quota is not included in the message, the PDSN will close the flow. Since no quota was received in the Access Accept, the PDSN will not send further RADIUS Access Request message to HAAA.

To ignore Billing Server interaction of HAAA for Access Requests sent by the PDSN during mobile IP re-registration for FA-CHAP, the PDSN will include the Session-Continue VSA set to “TRUE” in the on-line Access Request messages.

If multiple flows are present for the session that hosted the Prepaid flow, and a prepaid flow was stopped, and if it was the last flow for the session, then the session will be deleted by the PDSN. If one of mobile IP flows expires and it is not the last flow for the session, then the PDSN will close the flow locally. If the resource revocation mechanism is enabled on PDSN, the relevant resource revocation mechanism will be applied in this case.

If the Simple IP (SIP) flow is closed (for example, a PPP session is torn down or quota for the SIP flow expires), then all the other mobile IP flows, both prepaid and non-prepaid, will also get closed. If SIP flow is closing due to allocated quota expiry, it will send Access Request message with Update-Reason as “Quota Reached”. In other cases where the SIP session is closed, the Access Request will be sent with Update-Reason as “Client Service Termination”. All other prepaid flows for the PPP session will also send Access Request messages to close the prepaid service and return unused quota. The Update-Reason for all these flows will contain value for “Main SI Released”.

When threshold for the quota is reached, the PDSN sends an Access Request to HAAA to retrieve more quota for the flow. In case the values of threshold for the quota and the quota allocated are same, then on quota expiry (when Quota = Threshold), the PDSN will treat this as flow as closed, and send an Access Request with Update-reason as “Quota reached”.

When the quota expires for the flow, the PDSN sends an on-line Access Request to the HAAA to indicate that the prepaid flow is released. During this time the PDSN marks the flow as deleted, and stops switching any packets for the flow. On receipt of the Access Accept from the AAA server for this Access Request, the PDSN deletes the prepaid flow for the user and sends an Accounting Stop.

If resource revocation mechanism is enabled at the PDSN, then the PDSN will send a resource revocation to the HA to clear binding at the HA, and the PDSN will clear the visitor info for the flow.

Upon receiving a RADIUS Disconnect Request (POD) or Mobile IP revocation messages, the PDSN will send an on-line RADIUS Access-Request message containing the used quota and the Update-Reason Sub-Type set to “Remote forced disconnect”. The PDSN will delete the flow and send resource revocation message to the HA, and will send the existing RADIUS Accounting-Stop.

Volume-based Prepaid Data Service Flow

The metric for accounting volume based Prepaid service is total bytes flowing through the user flow in upstream and downstream direction.

Step 1 The Prepaid capable PDSN determines that Simple IP or Mobile IP setup requires a RADIUS Access-Request message to be sent to the Home RADIUS Server. For SIP sessions, the use has to be authenticated with AAA instead of local authentication. In case of Mobile IP users, FA-CHAP authentication is required.

The PDSN includes its own PPAC VSA to inform the HAAA/Billing Server that it supports Prepaid based on Volume (value = 1 or 3). If resource revocation is enabled on the PDSN, then it will send a SessionTerminationCapability (STC) attribute indicating that it can support resource revocation for Mobile IP sessions.

The Home RADIUS server performs the regular Authentication and Authorization of the Access Request sent by the user. If the user profile indicates the user is a Prepaid subscriber, HAAA interfaces with the Billing Server, and provides the Billing Server with the prepaid info for the user as received in the Access Request message.

Step 2 After the Billing Server receives the user's prepaid information, it checks the capabilities of PDSN (sent in the PPAC VSA). The Billing Server also checks that the user has a valid balance and account status. The Billing Server then indicates to the PDSN that it supports prepaid packet data service based on volume. It also assigns the initial quota for the user, which is typically a fraction of total available quota for the user. The quota allocated for the user is identified by a quota id assigned by Billing Server for the user for the current quota. The Billing Server interfaces with HAAA and provides this information to the HAAA.

The HAAA encapsulates the prepaid information received for the user in a RADIUS Access-Accept message and sends it to the PDSN. The RADIUS message includes:

- A PPAQ VSA that contains the following parameters:
  - Initialized quota for the user flow specified in VolumeQuota parameter
  - Quota ID for the quota allocated
  - A threshold value for the quota allocated in VolumeThreshold parameter
- A PPAC VSA indicating prepaid service is based on Volume.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. The PDSN stores the information present in the packet regarding the quota allocated for the flow and the threshold corresponding to the allocated flow. It also stores the Quota-ID allocated in the user flow present in the message. Once the flow for the user comes up (IP address assigned for Simple IP, or MIP RRP received from the HA and sent to the MS), the PDSN starts metering the user's traffic over the flow against the allocated quota.

Step 3 User data (IP datagrams) that flow through each Prepaid flow is accounted in both upstream and downstream directions. The bytes consumed are checked against the quota allocated for the flow by the Billing Server.

Step 4 Once the Volume Threshold value reaches the allocated quota for the prepaid flow, the PDSN sends an Access-Request Message to AAA to refresh quota for the user. This RADIUS packet contains a PPAQ VSA, which includes following parameters:

- Update-Reason Sub-Type that is set to indicate "Threshold reached" (= 3)
- Quota ID previously received
- Used volume in the VolumeQuota Sub-Type

HAAA authenticates the RADIUS packet and if authentication is successful, forwards the prepaid-related information present in the packet to the Billing Server.

Step 5 The Billing Server updates its database with the amount of quota the user utilizes. Since the user indicates quota renewal, the Billing Server apportions a fraction of prepaid account balance of the user. It also assigns a new Quota ID for the current allocated quota and a corresponding threshold value for the assigned quota. This information is passed on to HAAA.

The HAAA sends the information received from the Billing Server into a RADIUS Access-Accept message to be sent to PDSN. The attributes that are encapsulated into a PPAQ VSA include:

- Quota ID
- Allocated quota into VolumeQuota parameter
- Threshold corresponding to the assigned quota into VolumeThreshold parameter.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. The PDSN stores the information present in the packet and updates the quota allocated for the flow and the current threshold value corresponding to the allocated flow. It also stores the new Quota-ID allocated for the current quota.

Step 6 User data (IP datagrams) continues to flow through the Prepaid flow, and is accounted in both upstream and downstream directions. The bytes consumed are checked against the quota allocated for the flow.

Step 7 The PDSN decides to close the prepaid flow based on following criteria:

- Access-Request message was sent to renew the quota and corresponding Access-Accept message was not received from AAA after a configurable time value. This time is same as the RADIUS message timeout configured on PDSN.
- An Access-Accept was sent to retrieve quota and before Access-Accept can be received, the remaining VolumeQuota is consumed. This is when the VolumeQuota value and the VolumeThreshold values become same.

  In this case, PDSN sends an Access-Request message containing the PPAQ VSA that includes:

  - Update-Reason Sub-Type to indicate 'Quota reached' (= 4)
  - Amount of quota used by the user in VolumeQuota attribute.

At this time, the PDSN marks the prepaid flow as being marked for deleted, such that it does not switch any packets through it for the prepaid flow. It does not delete the prepaid flow immediately and waits for the response of the Access-Request or timeout of the Access-Request message.

Step 8 The Billing Server does not allocate a new quota when the user indicates “Quota reached” for the prepaid flow. The Billing Server terminates the prepaid flow and indicates the same to the HAAA. The HAAA sends an Access-Accept message to the PDSN acknowledging the termination of the Prepaid packet data session by encapsulating Update Reason Sub-type as “Quota is reached” inside PPAQ VSA.

After the PDSN receives the Access Accept message, it deletes the user flow for the Prepaid session. As part of the usual off-line accounting procedures, the PDSN sends an off-line RADIUS Accounting-Stop message upon successful release of the appropriate resources (normal operation).

Duration-based Prepaid Data Service Flow

The metric for accounting duration-based Prepaid service is session duration in seconds.

Step 1 The Prepaid capable PDSN determines that Simple IP or Mobile IP setup requires a RADIUS Access-Request message to be sent to the Home RADIUS Server. For SIP sessions, user authentication has to be performed with AAA rather than local authentication. In the case of Mobile IP users, FA-CHAP is required for authentication.

The PDSN includes its own PPAC VSA to inform the HAAA/Billing Server that it supports Prepaid based on Duration (value = 2 or 3). If resource revocation is enabled on the PDSN, the PDSN will send a SessionTerminationCapability (STC) attribute indicating that it can support resource revocation for Mobile IP sessions. The Event_Time attribute (G4, value = 55) will be included in the RADIUS Access-Request message.

The Home RADIUS server performs the regular Authentication and Authorization of the Access Request sent by the user. If the user profile indicates the user is a Prepaid subscriber, the HAAA interfaces with the Billing Server and provides the Billing Server with the prepaid related info for the user as received in the Access Request message.

Step 2 After the Billing Server receives the user's prepaid info, it checks the capabilities of the PDSN (sent in the PPAC VSA). The Billing Server also checks that the user has a valid balance and account status. The Billing Server informs the PDSN that it supports prepaid packet data service that is based on Duration. It also assigns the initial quota for the user, which is typically a fraction of total available quota for the user. The quota allocated for the user is identified by a quota id assigned by Billing Server for that user for the current quota. The Billing Server interfaces with the HAAA and provides this info to the HAAA.

The HAAA encapsulates the prepaid information received for the user in a RADIUS Access-Accept message and sends it to the PDSN. The RADIUS message includes:

A PPAQ VSA that contains the following parameters:

- Initialized quota for the user flow specified in DurationQuota parameter
- Quota ID for the quota allocated
- A threshold value for the quota allocated in DurationThreshold parameter

A PPAC VSA that indicates prepaid service is based on Volume.

For duration based Prepaid packet data service, the Event_Time attribute is used for DurationQuota/DurationThreshold allocation by the Billing Server.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. The PDSN stores information in the packet regarding the quota allocated for the flow, and threshold corresponding to the allocated flow. It also stores the Quota-ID allocated corresponding to the quota.

Once the flow for the user comes up (for example, an IP address assigned for Simple IP or MIP RRP received from the HA and sent to the MS), the PDSN starts the timer corresponding to the duration threshold value and duration quota value.

Once the timer expires for the threshold value of the allocated quota for the prepaid flow, the PDSN sends an Access-Request Message to AAA to refresh quota for the prepaid flow. This Access Request message contains a PPAQ VSA, which includes following parameters:

- Update-Reason Sub-Type that is set to indicate 'Threshold reached' (= 3)
- Quota ID previously received
- Used duration in the DurationQuota Sub-Type

The HAAA authorizes the RADIUS packet and, if successful, forwards the prepaid-related information in the packet to the Billing Server.

Step 3 The Billing Server updates its database with the amount of quota used by the user. Since the user indicates quota renewal, the Billing Server apportions a fraction of prepaid account balance of the user. It also assigns a new Quota ID for the current allocated quota and a corresponding threshold value for the assigned quota. This information is passed on to the HAAA.

The HAAA sends the information received from the Billing Server into a RADIUS Access-Accept message to be sent to the PDSN. The attributes that are encapsulated into a PPAQ VSA include:

- Quota ID
- Allocated quota into DurationQuota parameter
- Threshold corresponding to the assigned quota into DurationThreshold parameter.

After the PDSN receives the Access-Accept message from the AAA, it parses the RADIUS packet and retrieves the attributes inside it. The PDSN stores the information in the packet, updates it with the quota allocated for the flow and the current threshold value corresponding to the allocated flow. The PDSN restarts the duration quota timer with the new value received in the Accept-Accept message, and starts the threshold timer with the new threshold value received corresponding to the current quota. It also stores the new Quota-ID allocated for the current quota.

Step 4 The PDSN closes the prepaid flow based on following criteria:

- An Access-Request message was sent to renew the quota, and the corresponding Access-Accept message was not received from AAA after a configurable time value. This time value is same as the RADIUS message timeout configured on PDSN.
- An Access-Accept was sent to retrieve quota before the Access-Accept can be received, and the remaining DurationQuota is consumed and the timer corresponding to it expires. This event is when the DurationQuota value and the DurationThreshold values become the same.

  If this event occurs, the PDSN sends an Access-Request message containing the PPAQ VSA that includes:

  - Update-Reason Sub-Type to indicate ‘Quota reached’ (= 4)
  - Amount of quota used by the user in DurationQuota attribute.

The PDSN marks the prepaid flow for deletion, and does not switch any packets through it for the prepaid flow. The PDSN does not delete the prepaid flow immediately, and waits for the response of the Access-Request or timeout of the Access-Request message.

Step 5 The Billing Server does not allocate a new quota when the user indicates "Quota reached" for the prepaid flow. The Billing Server terminates the prepaid flow and indicates the same to the HAAA. HAAA sends an Access-Accept message to the PDSN acknowledging the termination of the Prepaid packet data session by encapsulating Update Reason Sub-type as "Quota is reached" inside PPAQ VSA.

When the PDSN receives the Access Accept message, it clears the user flow for the Prepaid session. As part of the usual off-line accounting procedures, the PDSN sends an off-line RADIUS Accounting-Stop message upon successful release of the appropriate resources.

Volume-based Prepaid Data Service with Tariff Switching

The PDSN and Billing Server support tariff switch, volume- based, Prepaid packet data service. The tariff switch trigger is controlled at the Billing Server. To support this capability, a new sub-Type PrepaidTariffSwitch (PTS) VSA attribute is sent by HAAA to PDSN. This attribute contains following key sub-types:

- QuotaId: Quota Id is same as present in PPAQ.
- VolumeUsedAfterTariffSwitch (VUATS): Volume switched after Tariff Switch
- TariffSwitchInterval (TSI): Interval in seconds between the time stamp (G4) of the corresponding on-line RADIUS Access-Request message and the next tariff switch condition

The following sequence describes the functionality of Prepaid data service when Tariff Switching is enabled.

Step 1 The Prepaid capable PDSN determines that Simple IP or Mobile IP setup requires a RADIUS Access-Request message to be sent to the Home RADIUS Server. For SIP sessions, authentication of the user with AAA has to be done instead of local authentication. In case of Mobile IP users, authentication via FA-CHAP is required.

PDSN includes its own PPAC VSA to inform the HAAA/Billing Server that it supports Prepaid based on Volume (value = 1 or 3). If resource revocation is enabled on the PDSN, then it will send a SessionTerminationCapability (STC) attribute indicating that it can support resource revocation for Mobile IP sessions.

The Home RADIUS server performs the regular Authentication and Authorization of the Access Request sent by the user. If the user profile indicates the user is a Prepaid subscriber, HAAA interfaces with the Billing Server and provides the Billing Server with the prepaid related info for the user as received in the Access Request message.

Step 2 After the Billing Server receives the user's prepaid info, it checks the capabilities of the PDSN that were sent in the PPAC VSA. It also checks that the user has a valid balance and account status. The Billing Server notifies the PDSN that it will support prepaid packet data service that is based on Volume. The Billing Server also assigns the initial quota for the user, which is typically fraction of total available quota for the user. The quota allocated for the user is identified by a quota id assigned by Billing Server for the user. The Billing Server interfaces with the HAAA and provides this info to the HAAA.

The Billing Server that supports Tariff Switching indicates the time (in seconds) remaining for the next tariff switch point, and passes the info to the HAAA server. Optionally, it can include the time after tariff switch point that the PDSN will send Access Request to the HAAA if the threshold value for the assigned quota is not reached.

The HAAA encapsulates the prepaid information received for the user from Billing Server in a RADIUS Access-Accept message and sends it to the PDSN. The RADIUS message includes:

- A PPAQ VSA that contains the following parameters:
  - Initialized quota for the user flow specified in VolumeQuota parameter
  - Quota ID for the quota allocated
  - A threshold value for the quota allocated in VolumeThreshold parameter
- A PTS VSA that contains the following parameters:
  - QuotaID as in PPAQ VSA attribute
  - TariffSwitchInterval indicating the time in seconds remaining before which the tariff switch condition will trigger
  - TimeIntervalafterTariffSwitchUpdate indicating the duration after tariff switch point when PDSN will send an on-line Access Request if threshold point is not reached.
- A PPAC VSA indicating prepaid service is based on Volume.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. It stores the information present in the packet regarding the quota allocated for the flow and threshold corresponding to the allocated flow. The PDSN also stores the Quota-ID allocated in the user flow present in the message.

Once the flow for the user comes up (the IP address assigned for Simple IP, or MIP RRP received from the HA and sent to the MS), the PDSN starts metering user's traffic over the flow against the allocated quota. It also starts the timer corresponding to the value received in TariffSwitchInterval attribute so that it is aware when the tariff switch condition is hit. The timer is started by the PDSN only if the timestamp of the Access Request + Tariff Switch Interval is more than the timestamp of the Access Accept message.

QuotaId present in the PTS attribute should be equal to the QuotaId present inside PPAQ. If the 2 values are unequal, the prepaid flow is closed by PDSN.

Step 3 User data (IP datagrams) that flows through each Prepaid flow is accounted in both upstream and downstream directions. The bytes consumed are checked against the quota allocated for the flow by the Billing Server.

Step 4 Once the VolumeThreshold value is reached for the allocated quota for the prepaid flow, the PDSN sends an Access-Request Message to AAA to refresh quota for the user. This RADIUS packet contains a PPAQ VSA, which includes following parameters:

- Update-Reason Sub-Type that is set to indicate ‘Threshold reached’ (= 3)
- Quota ID previously received
- Used volume in the VolumeQuota Sub-Type

The HAAA authorizes the RADIUS packet and if authorization is successful, forwards the prepaid-related information present in the packet to the Billing Server.

Step 5 The Billing Server updates its database with the amount of quota used by the user. Since the user indicates quota renewal, the Billing Server apportions a fraction of prepaid account balance of the user. It also assigns a new Quota ID for the current allocated quota and a corresponding threshold value for the assigned quota. This information is passed on to HAAA.

The Billing Server also indicates to the HAAA, the time remaining in seconds for the next Tariff Switch trigger point.

The HAAA sends the information received from the Billing Server into a RADIUS Access-Accept message to be sent to the PDSN. The attributes that are encapsulated into a PPAQ VSA include:

- Quota ID
- Allocated quota into VolumeQuota parameter
- Threshold corresponding to the assigned quota into VolumeThreshold parameter

The Attributes encapsulated inside PTS attribute includes:

- QuotaID, same as the PPAQ attribute
- TariffSwitchInterval that indicates the time (in seconds) remaining before which the tariff switch condition will trigger.
- TimeIntervalafterTariffSwitchUpdate that indicates the duration after tariff switch point when the PDSN will send an on-line Access Request if threshold point is not reached.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. It stores the information present in the packet updating with the quota allocated for the flow and the current threshold value corresponding to the allocated flow. It also stores the new Quota-ID allocated for the current quota.

Additionally, the PDSN re-starts the timer indicated in TariffSwitchInterval attribute. This time indicates the time remaining in seconds before the next tariff switch condition will be hit.

Step 6 User data (IP datagrams) continues to flow through the Prepaid flow, and is accounted in both upstream and downstream directions. The bytes consumed are checked against the quota allocated for the flow.

Step 7 The timer for the tariff switch interval expires, and indicates the tariff switch point for the flow is hit. The PDSN continues to count the total number of octets flowing through the session in upstream and downstream direction, and also the number of bytes switched by the PDSN after the tariff switch trigger point. If TimeIntervalafterTariffSwitchUpdate was sent by AAA, then the PDSN will start a timer with this value after the tariff switch point is reached.

Step 8 User data (IP datagrams) that flows through each Prepaid flow continues to be accounted in both upstream and downstream directions until the next threshold point is reached. The PDSN counts the total number of bytes switched till last quota update, and also the total number of bytes switched by PDSN after the Tariff Switch trigger point is hit. The bytes consumed are checked against the quota allocated for the flow.

Step 9 Once the VolumeThreshold value is reached for the quota allocated in VolumeQuota value for the flow or timer corresponding to TimeIntervalafterTariffSwitchUpdate expires, the PDSN sends quota update information in an Access Request Message to AAA and Billing Server. This on-line RADIUS Access-Request message contains following attributes in the PPAQ VSA:

- Update-Reason Sub-Type that is set to indicate “Threshold reached” (= 3) if threshold is reached. Otherwise, it is set to indicate “Tariff Switch Update” (=9) if TimeIntervalafterTariffSwitchUpdate expires
- The Quota ID previously received
- The utilized volume in the VolumeQuota Sub-Type

  The PTS attribute contains following subtypes:

  - Quota ID previously received
  - VolumeUsedAfterTariffSwitch (VUATS) attribute, that contains the total number of octets being switched by the PDSN after tariff switch trigger point.

The HAAA authorizes the RADIUS packet and, if authorization is successful, forwards the prepaid-related information present in the packet to the Billing Server.

The Billing Server updates its database with the amount of quota utilized by the user. Since the user indicates quota renewal, the Billing Server apportions a fraction of prepaid account balance of the user. It also assigns a new Quota ID for the current allocated quota and a corresponding threshold value for the assigned quota. This information is passed on to the HAAA.

The Billing Server also indicates to the HAAA the time remaining in seconds for the next Tariff Switch trigger point.

The HAAA sends the information received from the Billing Server into a RADIUS Access-Accept message to be sent to PDSN. The attributes that are encapsulated into a PPAQ VSA include:

- New Quota ID for the current quota
- Allocated quota into VolumeQuota parameter
- Threshold corresponding to the assigned quota into VolumeThreshold parameter

  The PTS attribute contains following subtypes:

  - Quota ID previously received
  - TariffSwitchInterval that indicates the time (in seconds) remaining before which the tariff switch condition will trigger.
  - Optionally TimeIntervalafterTariffSwitchUpdate that indicates the duration after the tariff switch point when the PDSN will send an on-line Access Request if threshold point is not reached.

After the PDSN receives the Access-Accept message from AAA, it parses the RADIUS packet and retrieves the attributes inside it. The PDSN stores the information present in the packet, and updates it with the quota allocated for the flow and the current threshold value corresponding to the allocated flow. It also stores the new Quota-ID allocated for the current quota.

Additionally, the PDSN re-starts the timer indicated in TariffSwitchInterval attribute. The PDSN starts the timer only if the timestamp of the Access Request + Tariff Switch Interval is more than the timestamp of the Access Accept message. This time indicates the time remaining in seconds before the next tariff switch condition will be hit.

Support for G17 Attribute in Acct-Stop and Interim Records

The G17 attribute is required to bill users based on when the last activity was detected rather than when the user is de-registered. The following scenario gives a brief on how the attribute is used and how AAA needs to identify the last user activity.

G17 is defined as last user activity to indicate the time when the last activity was detected by the user. The G17 attribute is sent in acct-stop and interim accounting update messages, and has the following usage guidelines:

- Configure support for the G17 attribute by issuing the **cdma pdsn attribute send g17** command
- The attribute is not included in acct-start record and included only in accounting stop/interim-update.
- The attribute is set to 0 when an airlink start record arrives.
- The attribute is set to the current time when airlink active stop arrives.
- The attribute is set to 0 once the acct-stop record is sent out.

The G17 attribute is useful under the following conditions:

- When the **cdma pdsn accounting send start-stop** command is not configured.
  - A session goes dormant. G17 is recorded with the current time. As the above CLI is not configured, there is no accounting stop generated.
  - The PDSN will continue to send interim update accounting records for this session. These messages will contain G17 with the value recorded with time when airlink-stop was received.
  - When the mobile finally deregisters (and receives an A11 RRQ with lft = 0, and w/o an airlink STOP), the PDSN sends an accounting stop with the G17 attribute that was recorded earlier when airlink-stop was received. This gives the real value of time when last user activity was detected.
- When the **cdma pdsn accounting send start-stop** command is configured.
  - The PDSN will generate an accounting stop when an airlink-stop is received from the PCF. This acct-stop will contain the G17 recorded with time when airlink-stop was received.
  - G17 is reset once the acct-stop is sent out. finally when the session ends, the accounting stop would have G17 as 0.
  - AAA server needs to use the previous value of G17 to find out the last user activity.

Mobile IP Call Processing Per Second Improvements

In previous Cisco PDSN Releases, the Mobile IP CPS rate was approximately 40—comparatively low to that of Simple IP CPS which around 125. Mobile IP CPS was low because some of the Mobile IP configurations are interface specific. When these configurations are applied to the virtual-template interface (which is typical for the PDSN software), it takes considerable time to clone the virtual-access from the Virtual-Template because of the presence of the Mobile IP configuration, and this directly affects the CPS for Mobile IP service. The virtual-access are cloned when the calls are setup. To reduce virtual-access cloning time, PDSN Release 2.1 supports commonly used per-interface configurations in global configuration mode, and supports per-interface for backward compatibility.

IS-835-B Compliant Static IPSec

An IPSec Security Association is a unidirectional logical connection between two IPSec systems, and is uniquely identified by Security Parameter Index (SPI), IP Destination Address, and the Security Protocol (where the Security Protocol is Authenticate Header (AH) or Encapsulating Security Payload (ESP). The Security Association has two types: Transport and Tunnel.

IPSec based security may be applied on tunnels between the PDSN and HA depending on parameters received from Home AAA server. A single tunnel may be established between each PDSN-HA pair. A single tunnel between a PDSN-HA pair can have three types of traffic streams: Control Messages, Data with IP-in-IP encapsulation, and Data with GRE-in-IP encapsulation. All traffic carried in the tunnel has the same level of protection provided by IPSec.

The IS835 standard defines MobileIP service as described in RFC 2002; the Cisco PDSN provides Mobile IP service and Proxy Mobile IP service.

In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy on the MN's behalf to the HA. Once Security-Osculations (tunnels) are established, they remain active until there is traffic (user traffic or user binding) on the tunnel, or the lifetime of the security association expires.

IS-835 B specification describes three mechanisms to provide IP Security: 1) Certificates, 2) Dynamically distributed Pre-Shared secret, and 3) Statically configured Pre-Shared secret.

Once security associations (tunnels) are established, they remain active till there is traffic (user traffic or user bindings) on the tunnel, or until the lifetime of the association expires.

The IS835 standard specifies support for the following IPSec modes:

- IKE & Public Certificate(X.509)
- Dynamic pre-shared IKE secret distributed by Home Radius Server.
- Statically configured IKE pre-shared secret.

Note IS835B Static IPSec feature is available only on the Cisco 7200 Internet router platform. The Cisco IOS IPSec feature is available on the Cisco 7200 7200 Internet router, Cisco 6500 Catalyst switch, and Cisco 7600 switch platforms. PDSN Release 2.1 only supports Statically configured Pre-Shared secret.

The level of IPsec protection on a tunnel between the PDSN and HA is determined by a "security level" parameter: whether to provide IPSec protection on control messages, data, control message plus data, or no protection. The security level attribute is received from the Home Radius server in an Access-Accept Message by the PDSN. On the HA, this attribute has to be configured for each Foreign Agent because there is no provision to pass security-level from the Home AAA server to the Home Agent.

PDSN Release 2.1 supports the following values:

- IPSec for Mobile Control and Data traffic
- No IPSec

Once a Security Association is established, it will be periodically refreshed by the PDSN until the tunnel expires.

If reverse tunneling is supported by the HA (as indicated by the RADIUS server), and IPSec security is authorized for the tunneled data, and a mobile requests reverse tunneling, then the PDSN will provide security on the reverse tunnel.

The HA determines which type of security association (if any) is required with a PDSN. The HA uses the same security policy that is specified in the Home RADIUS server and returned to the PDSN in the 3GPP2 security level attribute. All MN will receive the same security level while accessing the same PDSN.

Configuring IPSec in Cisco IOS

To employ IS835-B IPSec on the PDSN requires that you configure the following commands:

- **[no] ip mobile cdma ipsec**—enables or disables the CDMA IPSec feature. This command is only present in crypto images for the Cisco 7200 Series Internet Router, and in non-crypto images for the Cisco MWAM.
- **[no] ip mobile cdma ipsec profile** *profile-tag*—This command is only present in crypto images for the Cisco 7200 Series Internet Router.
- **show ip mobile cdma ipsec**—This command shows if the feature is enabled.
- **show ip mobile cdma ipsec profile**—This command shows the crypto profile configured.
- **[no] debug ip mobile cdma ipsec**—This turns on the debug on this feature.

Here is a sample configuration:

```
Router(config)#crypto isakmp policy 1
                        authentication pre-share
Router(config)#crypto isakmp key cisco address 7.0.0.2
Router(config)#crypto ipsec transform-set mobile-set1 esp-3des
Router(config)#crypto ipsec profile testprof
                        set transform-set mobile-set1
Router(config)#crypto identity pdsntest
Router(config)#ip mobile cdma ipsec
Router(config)# ip mobile cdma ipsec profile testprof
Router(config)#ip mobile foreign-agent reg-wait 30
```

Additionally, to employ Cisco IOS IPSec on the PDSN you must configure “Transform” and “CryptoMap,” and apply Cryptomap to the interface.

The Transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting particular data flow. Use the **crypto ipsec transform-set mobile-set1 esp-3des** command to configure the transforms set.

The Crypto map entries created for IPSec pull together the various parts used to set up IPSec security associations, including the following:

- Which traffic should be protected by IPSec (per a crypto access list).
- The granularity of the flow to be protected by a set of security associations.
- The location IPSec-protected traffic should be sent (remote IPSec peer).
- The local address used for IPSec traffic (applying Crypto map to interface).
- The type of IPSec security that should be applied to this traffic (selected from a list of one or more transform sets).
- Whether security associations are manually established, or established with IKE.
- The parameters that might be necessary to define an IPSec security association.

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. These Crypto map sets are applied to interface; then all traffic passing through the interface is evaluated against the applied crypto map set.

The policy described in the crypto map entries is used during the negotiation of security association, for IPSec to succeed between two IPSec peers, both peers’ crypto map entries must a contain compatible configuration statement.

Only one crypto map set is applied to single interface; Multiple interfaces can share the same crypto map set.

Multiple Crypto map entries can be created for interface; the sequence number of each map-entry is used to rank the map-entries.

Multiple Crypto map entries must be created for a given interface if different data flows are handled by separate IPSec peers. If different IPSec security is required for different types of traffic, create a separate access list for each type of traffic, and create a separate crypto map entry for each access list.

The following configuration example illustrates the minimum requirement to establish Crypto map entries that use IKE.

```
Router(config)# access-list mobile-example permit ip 10.0.0.0  0.0.0.255
Router(config)# crypto ipsec transform-set mobile-set1 esp-3des
Router(config)# crypto map map-mobile-example 10 ipsec-isakmp
                                  match mobile-example
                                  set transform-set transform-set mobile-set1
                                  set peer 10.0.0.34
```

```
Router(config)# interface FastEthernet0/1
                                  ip address 10.0.0.32
                                  crypto map map-mobile-example
```

Cisco employs two additional mechanisms to define cryptomaps:

- Dynamic Crypto-maps: these are crypto-maps with fe fields that relate to policy. They are only suitable for applications that do not require initiating IKE, but only respond to IKE.
- IPSec Profiles: is a mechanism to convert a Crypto Map into a template that can be used to dynamically set up an identical policy.

```
Router(config)# access-list mobile-example permit ip 10.0.0.0  0.0.0.255
Router(config)# crypto ipsec transform-set mobile-set1 esp-3des
Router(config)# crypto  map map-mobile-example 10 ipsec-isakmp profile example-profile
                               match mobile-example
                               set transform-set transform-set mobile-set1
                               set peer 10.0.0.34
```

The following example illustrates the minimum Crypto configuration for IS835-based IPSec:

```
Router(config)# crypto isakmp policy 1
                hash md5
                authentication pre-share
Router(config)# crypto isakmp key <cisco> address <peer ip address7.0.0.10>
Router(config)# crypto ipsec transform-set testtrans esp-3des
Router(config)#crypto ipsec profile testprof
                                 description new cli
                               set transform-set testtrans
```

On-Demand Address Pools (ODAP)

A PDSN Cluster can consist of up to ten MWAM cards, with one Cluster Controller and a Backup Cluster Controller, and 48 PDSN IOS application image instances.

While MWAM cards provide a higher density of PDSNs, they make it necessary to allocate IP addresses from a central source. This simplifies configuration so users will not have to configure a local pool of IP addresses in each PDSN. With on-demand address pools, a DHCP/ODAP server manages a block of addresses for each ODAP client application. The ODAP clients will request subnets from the ODAP Subnet Allocation Server. These pools of subnetted IP addresses can dynamically increase or decrease in size depending on the utilization of the IP addresses. A pool can be divided into subnets of various sizes and the server assigns these subnets to routers running ODAP clients upon request. The PDSN will run the ODAP client and use OSPF to aggregate the routes. The DHCP/ODAP Server can either be an external Cisco AR, or run on a Cisco IOS image.

Note To use the ODAP feature, you must have Cisco IOS Release 12.2(15)T or later.

In this case, either the PDSN Cluster controller, or the backup cluster controller on one of the MWAM cards, will be configured as the DHCP/ODAP Server. The local IP pools used for PDSN Home Agent applications can also use the DHCP/ODAP Server for a subnet pool. A different name for the mobile IP pools would be used in the configurations.

Pool Sizing Information

The PDSN configuration dictates that either the PDSN Cluster Controller or the PDSN Backup Cluster Controller on one of the MWAM cards is configured as the DHCP Server with the ODAP Subnet Allocation Server. These processors will have more capacity because they provide PDSN Clustering functionality, and do not process the actual PDSN sessions. The ODAP clients reside on each of the PDSN images.

You must decide how large to make the ODAP subnet pools based on the following variables:

- Number of MWAMs and number of PDSNs per MWAM
- How many total PDSN sessions will be required
- Incoming call rates
- Number of available IP addresses for the ODAP pool.

Use the following information to size the ODAP Subnet Allocation Server pool and to determine how many IP addresses are required for all the PDSN applications.

- Each PDSN IOS application can support up to 20,000 PDSN sessions.
- Each MWAM contains:
  - Either a PDSN Cluster Controller or Backup Cluster Controller and up to 4 PDSN IOS images, so each MWAM can support up to 80,000 sessions (4 * 20000).

Note If a Cluster Controller or Backup Cluster Controller is not configured, then 5 PDSN images can be used allowing up to 100,000 sessions (5 * 20000).

- A Catalyst 6500 chassis contains up to 6 MWAM cards. The total number of local IP addresses needed in the pool for each chassis:
  - 6 MWAMs * 80,000 sessions = 480,000 IP addresses in the PDSN ODAP pool.

In order to configure an ODAP subnet pool for Mobile IP PDSN applications, determine the number IP addresses needed for each PDSN. Use the following formula to determine the Mobile IP pool size:

- PDSN Subnet IP Pool size = (number of PDSNs x number of sessions)

Always On Feature

The PDSN supports Always On service to maintain the subscriber's packet data session in the local network. Always On support dictates that the PDSN will not release a subscriber's packet data session due to PPP idle timer expiry unless the PDSN determines the user is no longer reachable.

The Always On service maintains a subscriber's packet data session irrespective of PPP inactivity timer value for the user. At the same time, by making use of a finite PPP inactivity timer value, this feature provides a way to keep a session only as long as the user is reachable. The PDSN uses LCP Echos (as per rfc1661 and IS835B) to determine if the user is reachable.

Always On service is enabled for a user only when the F15 "Always On" attribute is received and set to a value of **1** in the access accept message from the AAA server.

The PDSN supports the ability to configure the Echo-Reply-Timeout timer and Echo-Request-Attempts counter. There is no extra configuration required on the PDSN to enable the Always On feature itself; however, you can disable the feature by configuring the Echo-Request-Attempts to **0**. The PPP inactivity timer will be started for a session entering IPCP open state, if is configured or retrieved from AAA, for the user.

For always on users:

1. Upon expiration of the inactivity timer, Echo-Request-Attempts counter is initialized to the configured value.
2. If the Echo-Request-Attempts counter is zero, PPP session is torn down. If the Echo-Request-Attempts counter is nonzero, an LCP Echo-Request message will be sent, Echo-Request-Attempts counter is decremented, and Echo-Reply-Timeout timer is started.
3. Upon receipt of corresponding LCP Echo-Reply message, Echo-Reply-Timeout timer is stopped and PPP inactivity timer is restarted.
4. Upon expiration of Echo-Reply-Timeout timer, repeat from 2 above.

This feature is not supported for VPDN users, and is not applicable to Mobile IP users.

For Always-on users, a value of "1" will be sent for F15 attribute in the accounting start/stop/interim records. For non-always-on users, the F15 attribute will only be sent in the accounting records if configured.

Restrictions for the Always On Feature:

- The Always On implementation follows the IS835B standard; the IS835C specific additions are not available in this release of PDSN.
- Echo-Reply is the only packet that will stop always-on timer.

  Basically it means even if there is upstream/downstream data received, the session will be teared down unless Echo-reply received within configured number of retries and configured time interval.
- Always-on feature is not applicable for mobileip users.
- Always-on feature is not supported for VPDN users.
- Aging of Dormant PPP sessions feature works independent of always-on users. The aging of dormant PPP sessions feature does not care for the always-on property of a session.

NPE-G1 Platform Support

PDSN Release 2.0 and above, introduces support for the NPE-G1 router platform. The maximum number of sessions supported on the NPE G1 platform is 20,000. A faster processor will provide higher throughput rates compared the VXR NPE-400. The throughput is expected to be 2 times better than the VXR NPE-400 platform.

The supported configuration on a Cisco 7206VXR NPE-G1 processor is with 1Gigabyte of DRAM and one PA-2FE-TX FE port adaptor. The Cisco 7206VXR NPE-G1 processor has three 10/100/1000 based Ethernet Ports.

For IPSec support, a service adaptor SA-VAM2 is required.

PDSN MIB Enhancement

The following sub-sections highlight the MIBs that are added in R3.0:

PPP Counters in Release 3.0

Objects have been added under the following existing MIB subgroups:

- cCdmaPppSetupStats
- cCdmaPppReNegoStats
- cCdmaPppAuthStats
- cCdmaPppReleaseStats
- cCdmaPppMiscStats

The below table describes the list of PPP counters that have been added in R3.0.

Table 5 PPP Counters in Release 3.0

CDMA PPP MIB Subgroup	Counter Description
cCdmaPppSetupStats	
PPP stats - LCP Failure - option issue	Total number of PPP calls failed by LCP option negotiation failure.
PPP stats - IPCP failure option-issue	Total number of PPP calls failed by IPCP option negotiation failure.
PPP stats - Authentication aborted	Total number of PPP calls failed by authentication max-retry.
Session Disc - no remote-ip address:	Total number of sessions released because MN rejects IP address allocated by PDSN.
PPP stats - Lower layer disconnected:	Total number of calls released by RP layer.
PPP stats - TermReq-From-MN-IPCP:	LCP Term-Req received from MS During IPCP
PPP stats - TermReq-From-PDSN-IPCP:	LCP Term-Req Sent from PDSN During IPCP
PPP stats - TermReq-From-PDSN-Auth:	LCP Term-Req Sent from PDSN During Authentication
PPP stats - TermReq-From-MN-Auth:	LCP Term-Req received from MS During Authentication
PPP stats - TermReq-From-PDSN-LCP :	LCP Term-Req Sent from PDSN During LCP
PPP stats - TermReq-From-MN-LCP :	LCP Term-Req received from MS During LCP
PPP stats - A10Release-PCF-preLCP :	A10 Released by PCF before LCP stage
PPP stats - A10Release-PDSN-preLCP :	A10 Release by PDSN before LCP stage
PPP stats - A10Release-PCF-LCP :	A10 Released by PCF During LCP stage without LCP Term-Req
PPP stats - A10Release-PDSN-LCP :	A10 Released by PDSN During LCP stage without LCP Term-Req
PPP stats - A10Release-PCF-Auth:	A10 Released by PCF During Authentication without LCP Term-Req

Table 5 PPP Counters in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
PPP stats - A10Release-PDSN-Auth	A10 Released by PDSN During Authentication without LCP Term-Req
PPP stats - A10Release-PCF-IPCP :	A10 Released by PCF During IPCP stage without LCP Term-Req
PPP stats - A10Release-PDSN-IPCP :	A10 Released by PDSN During IPCP stage without LCP Term-Req
PPP stats - LCP - success :	PPP connections that finished LCP successfully
PPP stats - auth - success :	PPP connections that finished AUTH successfully
PPP stats - IPCP - success :	PPP connections that finished IPCP successfully
cCdmaPppReNegoStats	
Session Reneg - Lower layer handoff:	Total number of sessions renegotiated due to PANID/CANID comparison during handoff.
cCdmaPppAuthStats	
Session Authen- CHAP auth timeout:	MN does not respond for CHAP request.
Session Authen- PAP auth timeout:	PDSN does not receive PAP request from MN.
Session Authen- MSCHAP auth timeout:	MN does not respond for MSCHAP request.
Session Authen- sessions skipped PPP Auth:	Total number of sessions skipped PPP authentication.
cCdmaPppReleaseStats	
PPP stats - release - pcf deregister:	PPP connections released as PCF sends deregistration
PPP stats - release - lifetime expiry:	PPP connections released due to life timer expiry
cCdmaPppMiscStats	
Session Data Compress - CCP negotiation failures:	Total number of sessions failed CCP negotiation.
LCP Echo Stats - total LCP Echo Req. sent:	Total transmission of LCP Echo Request.
LCP Echo Stats - LCP Echo Req. resent:	Total retransmission of LCP Echo Request.
LCP Echo Stats - LCP Echo Reply received:	Total received LCP Echo Reply.
LCP Echo Stats - LCP Echo Request timeout:	Total LCP Echo Request timeout.
Receive Errors - unknown protocol errors:	Total packets which protocol value cannot be identified out of packets received at PPP stack.
Receive Errors - bad pkt length:	Total bytes discarded with reasons above.

RP Counters in Release 3.0

The following list identifies new MIB subgroups in Release 3.0:

- cCdmaRPRegReqErrors
- cCdmaRPRegUpdAckErrors
- cCdmaRPSessUpdAckErrors

- cCdmaRPRegReplyErrors
- cCdmaRPRegUpdErrors
- cCdmaRPSessUpdErrors
- cCdmaRpSessUpdStats
- cCdmaPcfSoRpSessUpdStats

The following list identifies existing MIB subgroups, under which objects are added:

- cCdmaTrafficStats
- cCdmaPcfSoRpRegStats
- cCdmaPcfSoRpUpdStats
- cCdmaSystemInfo
- cCdmaRpRegStats

Table 6 indicates the additional RP counters supported in Release 3.0:

Table 6 RP Counters Supported in Release 3.0

CDMA PPP MIB Subgroup	Counter Description
cCdmaSystemInfo	
sysInfo - PPPoGREsessions	The total number of PPPoGRE sessions currently established with this system.
sysInfo-HDLC-GREsessions	The total number of HDLCoGRE sessions currently established with this system.
sysInfo-totalSessions	The total number of sessions established since system was last restarted.
sysInfo-totalReleases	The total number of sessions released since system was last restarted.
sysInfo-totalMSIDFlow	The total number of flows currently using MSID service.
sysInfo-totalVPDNFlow	The total number of flows currently using VPDN service.
cCdmaRpRegStats	
RegStats-Reqs	The number of Initial A11 Registration requests received since system was last restarted.
RegStats-Disc	The number of Initial A11 Registration requests silently discarded since system was last restarted.
RegStats-RegReqs	The number of A11 Re-Registration requests received since system was last restarted.
RegStats-RegDisc	The number of A11 Re-Registration requests silently discarded since system was last restarted.
RegStats-DeregReqs	The number of A11 De-Registration requests received since system was last restarted.
RegStats-DeregDisc	The number of A11 De-Registration requests silently discarded since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
RegStats-HandoffReqs	The number of A11 Handoff Registration requests received since system was last restarted.
RegStats-HandoffAccepted	Total number of accepted handoff A11 Registration Requests meant for already existing session, since the system was last restarted.
RegStats-HandoffDenied	Total number of denied handoff A11 Registration Requests meant for already existing session, since the system was last restarted.
RegStats-HandoffDisc	The number of handoff A11 Registration requests silently discarded since system was last restarted.
RegStats-RegAirlinkStart	The number of A11 Re-Registration requests containing Airlink Start since system was last restarted.
RegStats-RegAirlinkStop	The number of A11 Re-Registration requests containing Airlink Stop since system was last restarted.
RegStats-DeregAirlinkStop	The number of Inter PCF active handoff since system was last restarted.
RegStats-HandoffInterPCFActive	The number of A11 De-Registration requests containing Airlink Stop since system was last restarted.
RegStats-HandoffInterPCFDormant	The number of Inter PCF dormant handoff since system was last restarted.
cCdmaRpSessUpdStats	
SessUpdStats-TransReqs	Total number of A11 Session Updates transmitted since system was last restarted.
SessUpdStats-AcceptedReqs	Total number of A11 Session Update Acknowledgements received with the Status field set to zero (indicating that the corresponding Registration Update was accepted), since system was last restarted.
SessUpdStats-DeniedReqs	Total number of A11 Session Update Acknowledgements received with the Status field set to non-zero indicating that the corresponding Registration Update was denied, since system was last restarted.
SessUpdStats-NotAckedReqs	Total number of A11 Session Update Updates sent, for which no corresponding A11 Registration Acknowledgements received, since system was last restarted.
SessUpdStats-TransReqs	Total number of initial A11 Session Updates sent, excluding the re-transmitted A11 Registration Updates, since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
SessUpdStats-RetransReqs	Total number of re-transmitted A11 Session Updates, since system was last restarted.
SessUpdStats-RecAcks	Total number of A11 Session Update Acknowledgements received, since system was last restarted.
SessUpdStats-DiscAcks	Total number of A11 Session Update Acknowledgements discarded, since system was last restarted.
SessUpdStats-AlwaysON	Total number of initial A11 Session Updates sent due to Always On since system was last restarted. Note that this count does not include any retransmissions.
SessUpdStats-RNPDIT	Total number of initial A11 Registration Updates sent due to RNPDIT value downloaded, since system was last restarted. Note that this count does not include any retransmissions.
SessUpdStats-UnSpecFail	The number of session update registrations failed for unspecified reason since system was last restarted.
SessUpdStats-ParamNotUpd	The number of session update registrations failed for session parameters not updated reason since system was last restarted.
SessUpdStats-MNAuthenFail	The number of session update registrations failed due to MN authentication failure since system was last restarted.
SessUpdStats-IdentMismatchFail	The number of session update registrations failed due to registration identity mismatch since system was last restarted.
SessUpdStats-BadReqsFail	The number of session update registrations failed due to poorly formed request since system was last restarted.
cCdmaTrafficStats	
trafficStats-SDBPaks	Total number of SDB marked data packets sent to PCF from PDSN since system was last restarted.
trafficStats-SDBOctets	Total number of SDB marked data octets sent to PCF from PDSN since system was last restarted.
cCdmaPcfSoRpRegStats	
PcfSoRegStats-InitRegReqs	The number of Initial A11 Registration requests received since system was last restarted.
PcfSoRegStats-InitRegDisc	The number of Initial A11 Registration requests silently discarded since system was last restarted.
PcfSoRegStats-RegReqs	The number of A11 Re-Registration requests received since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
PcfSoRegStats-ReregDisc	The number of A11 Re-Registration requests silently discarded since system was last restarted.
PcfSoRegStats-DeregReqs	The number of A11 De-Registration requests received since system was last restarted.
PcfSoRegStats-DiscardedReqs	The number of A11 De-Registration requests silently discarded since system was last restarted.
PcfSoRegStats-RcvdReqs	The number of A11 Handoff Registration requests received since system was last restarted.
PcfSoRegStats-AcptdReqs	Total number of accepted handoff A11 Registration Requests meant for already existing session, since the system was last restarted.
PcfSoRegStats-DeniedReqs	Total number of denied handoff A11 Registration Requests meant for already existing session, since the system was last restarted.
PcfSoRegStats-Disc	The number of handoff A11 Registration requests silently discarded since system was last restarted.
PcfSoRegStats-ReregAirlinkStart	The number of A11 Re-Registration requests containing Airlink Start since system was last restarted.
PcfSoRegStats-ReregAirlinkStop	The number of A11 Re-Registration requests containing Airlink Stop since system was last restarted.
PcfSoRegStats-DeregAirlinkStop	The number of A11 De-Registration requests containing Airlink Stop since system was last restarted.
cCdmaPcfSoRpUpdStats	
PcfSoHandoffUpdStats	The number of update registrations sent as a result of inter pcf handoffs, since system was last restarted.
PcfSoHandoffUpdStats-NotAckedReqs	Total number of A11 Registration Updates (sent as the result of inter PCF handoffs), for which no corresponding A11 Registration Acknowledgements received, since system was last restarted.
PcfSoHandoffUpdStats-RecAcks	Total number of A11 Registration Acknowledgements received for the A11 Registration Updates sent as the result of inter PCF handoffs, since system was last restarted.
PcfSoHandoffUpdStats-AcceptReqs	Total number of A11 Registration Acknowledgements received with the Status field set to zero (indicating that the corresponding Registration Update was accepted), since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
PcfSoHandoffUpdStats-DeniedReqs	Total number of A11 Registration Acknowledgements received with the Status field set to non-zero indicating that the corresponding Registration Update was denied, since system was last restarted.
PcfSoHandoffUpdStats-DiscAcks	Total number of A11 Registration Acknowledgements discarded, since system was last restarted.
PcfSoHandoffUpdStats-TxdReqs	Total number of initial A11 Registration Updates sent as the result of inter PCF handoffs, excluding the re-transmitted A11 Registration Updates, since system was last restarted.
PcfSoHandoffUpdStats-RetxdReqs	Total number of re-transmitted A11 Registration Updates as the initial Registration Update (sent as a result of inter PCF handoffs) was not acked or denied, since system was last restarted.
PcfSoHandoffUpdStats-UnknownFail	The number of update registrations failed for unspecified reason since system was last restarted. The update is sent as a result of inter PCF handoff.
PcfSoHandoffUpdStats-AdminProhibitFail	The number of update registrations failed due to administrative prohibition since system was last restarted. The update is sent as a result of inter PCF handoff.
PcfSoHandoffUpdStats-MNAuthenFail	The number of update registrations failed due to MN authentication failure since system was last restarted. The update is sent as a result of inter PCF handoff.
PcfSoHandoffUpdStats--IdMismatch	The number of registrations failed due to registration identity mismatch since system was last restarted. The update is sent as a result of inter PCF handoff.
PcfSoHandoffUpdStats-BadReqs	The number of update registrations failed due to poorly formed request since system was last restarted. The update is sent as a result of inter-PCF handoff.
cCdmaRPRegReqErrors	
RegReqErr-PakLen	Invalid Registration request packet length while parsing since system was last restarted.
RegReqErr-Protocol	Invalid Protocol value in the Registration Request Session Specific Extension since system was last restarted.
RegReqErr-Flags	Invalid Flags value in the Registration Request since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
RegReqErr-MHAEKey	Invalid Authentication key in the Registration Request Mobile-Home Authentication extension since system was last restarted.
RegReqErr-SPIMismatch	Mismatch in SPI in the Registration Request Mobile-Home Authentication extension since system was last restarted.
RegReqErr-SPI	Invalid SPI in the Registration Request Mobile-Home Authentication extension since system was last restarted.
RegReqErr-ConnId	Invalid Connection ID in the Registration Request since system was last restarted.
RegReqErr-MNID	Invalid MN ID in the Registration Request since system was last restarted.
RegReqErr-MNIDType	Invalid MN ID type in the Registration Request since system was last restarted.
RegReqErr-MSIDLen	Invalid MSID length in the Registration Request since system was last restarted.
RegReqErr-SSE	Session Specific extension missing in the Registration Request since system was last restarted.
RegReqErr-MHAE	Mobile-Home Authentication extension missing in the Registration Request since system was last restarted.
RegReqErr-Order	Invalid order of the extensions in the Registration Request since system was last restarted.
RegReqErr-VSE	Invalid Vendor specific extensions in the Registration Request since system was last restarted.
RegReqErr-AppType	Invalid Application type in Vendor specific extensions in the Registration Request since system was last restarted.
RegReqErr-DupAppType	Duplicate Application type in Vendor specific extensions in the Registration Request since system was last restarted.
RegReqErr-AppSubType	Invalid Sub Application type in Vendor specific extensions in the Registration Request since system was last restarted.
RegReqErr-VendorId	Invalid Vendor ID in Vendor specific extensions in the Registration Request since system was last restarted.
RegReqErr-CVSE	Duplicate Critical Vendor extension in the Registration Request since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
RegReqErr-UnknownAttr	Unknown Accounting attribute in the Registration Request since system was last restarted.
RegReqErr-LenAttr	Invalid accounting attribute length in the Registration Request since system was last restarted.
RegReqErr-DupAttr	Duplicate accounting attribute received in the Registration Request since system was last restarted.
RegReqErr-AcctRecRetrans	Same accounting sequence number and record type in the Registration Requests airlink record not updated since system was last restarted.
RegReqErr-SeqNum	Invalid sequence number in the airlink accounting record Registration Requests silently discarded since system was last restarted.
RegReqErr-DupGREKey	Duplicate GRE Key received in the Registration Request for different MSID from the same PCF since system was last restarted.
RegReqErr-SameGREKey	Same GRE Key and Airlink setup received in the Registration Request for existing session since system was last restarted.
RegReqErr-GREKeyChangeNoSetup	GRE changed without airlink setup received in the Registration Request for existing session since system was last restarted.
RegReqErr-InitNoSetup	Airlink Setup record not received in the Initial Registration Request since system was last restarted.
RegReqErr-StartBeforeSetup	Airlink Start record received before the Airlink setup in the Registration Request since system was last restarted.
RegReqErr-StartOnClose	Airlink Start record received in the De-Registration Request since system was last restarted.
RegReqErr-StartOnActive	Airlink Start record received in the Registration Request for already active session since system was last restarted.
RegReqErr-StopOnDormant	Airlink Stop record received in the Registration Request for already dormant session since system was last restarted.
RegReqErr-InitStop	Airlink Stop record received in the Initial Registration Request since system was last restarted.
RegReqErr-InitSDB	Airlink SDB received in the Initial Registration Request since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
RegReqErr-airlinkRec	Invalid Accounting Airlink record type in the Registration Request since system was last restarted.
RegReqErr-DeregNoSession	De-Registration Request for non existing session registration request is discarded since system was last restarted.
RegReqErr-ReregInDisc	Re-Registration Request received for the session in the disconnecting or deleting state, therefore the registration request is discarded since system was last restarted.
RegReqErr-Memfail	Registration Request discarded due to memory allocation failure during processing since system was last restarted.
RegReqErr-MaxSessions	Registration request rejected because of maximum limit or configured number of session reached since system was last restarted.
cCdmaRPRegUpdAckErrors	
RegUpdAckErr-PakLen	Invalid Registration Update Ack packet length while parsing since system was last restarted.
RegUpdAckErr-Protocol	Invalid Protocol value in the Registration Update Ack Session Specific Extension since system was last restarted.
RegUpdAckErr-RUAEKey	Invalid Authentication key in the Registration Update Ack Registration Update Authentication extension since system was last restarted.
RegUpdAckErr-SPI	Invalid SPI in the Registration Update Ack Registration Update Authentication extension since system was last restarted.
RegUpdAckErr-ConnId	Invalid Connection ID in the Registration Update Ack since system was last restarted.
RegUpdAckErr-MNID	Invalid MN ID in the Registration Update Ack since system was last restarted.
RegUpdAckErr-MNIDType	Invalid MN ID type in the Registration Update Ack since system was last restarted.
RegUpdAckErr-MSIDLen	Invalid MSID length in the Registration Update Ack since system was last restarted.
RegUpdAckErr-SSE	Session Specific extension missing in the Registration Update Ack since system was last restarted.
RegUpdAckErr-RUAE	Registration Update Authentication extension missing in the Registration Update Ack since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
RegUpdAckErr-Order	Invalid order of the extensions in the Registration Update Ack since system was last restarted.
RegUpdAckErr-VSE	Invalid Vendor specific extensions in the Registration Update Ack since system was last restarted.
RegUpdAckErr-NoSession	De-Registration Update Ack for non existing session Registration Update Ack is discarded since system was last restarted.
RegUpdAckErr-MemFail	Registration Update Ack discarded due to memory allocation failure during processing since system was last restarted.
cCdmaRPSessUpdAckErrors	
SessUpdAckErr-PakLen	Invalid Session Update Ack packet length while parsing since system was last restarted.
SessUpdAckErr-Protocol	Invalid Protocol value in the Session Update Ack Session Specific Extension since system was last restarted.
SessUpdAckErr-RUAEKey	Invalid Authentication key in the Session Update Ack Registration Update Authentication extension since system was last restarted.
SessUpdAckErr-SPI	Invalid SPI in the Session Update Ack Session Update Authentication extension since system was last restarted.
SessUpdAckErr-ConnId	Invalid Connection ID in the Session Update Ack since system was last restarted.
SessUpdAckErr-MSID	Invalid MN ID in the Session Update Ack since system was last restarted.
SessUpdAckErr-MSIDType	Invalid MN ID type in the Session Update Ack since system was last restarted.
SessUpdAckErr-MSIDLen	Invalid MSID length in the Session Update Ack since system was last restarted.
SessUpdAckErr-SSE	Session Specific extension missing in the Session Update Ack since system was last restarted.
SessUpdAckErr-RUAE	Session Update Authentication extension missing in the Session Update Ack since system was last restarted.
SessUpdAckErr-Order	Invalid order of the extensions in the Session Update Ack since system was last restarted.
SessUpdAckErr-VSE	Invalid Vendor specific extensions in the Session Update Ack since system was last restarted.
SessUpdAckErr-NoSession	De-Session Update Ack for non existing session Session Update Ack is discarded since system was last restarted.

Table 6 RP Counters Supported in Release 3.0 (Continued)

CDMA PPP MIB Subgroup	Counter Description
SessUpdAckErr-MemFail	Session Update Ack discarded due to memory allocation failure during processing since system was last restarted.
cCdmaRPRegReplyErrors	
RegRplyErr-Internal	Registration reply not sent due to internal error during processing since system was last restarted.
RegRplyErr-MemFail	Registration reply not sent due to memory allocation failure during processing since system was last restarted.
RegRplyErr-NoSecOrParse	Cannot send Reply to PCF because security association not found for the PCF or Parse error of Request since system was last restarted.
cCdmaRPRegUpdErrors	
RegUpdErr-Internal	Registration update not sent due to internal error during processing since system was last restarted.
RegUpdErr-MemFail	Registration update not sent due to memory allocation failure during processing since system was last restarted.

The following MIB enhancements are included in the Cisco PDSN Release 2.1:

PPP Counter Objects have been added under the following existing MIB subgroups:

- cCdmaPppSetupStats
- cCdmaPppReNegoStats
- cCdmaPppAuthStats
- cCdmaPppReleaseStats
- cCdmaPppMiscStats

In PDSN Release 2.1 a new MIB CISCO-CDMA-PDSN-CRP-MIB is defined to reflect the support of Closed RP interface on PDSN.

The MIB has two groups, SystemInfo and PerPCF Stats. SystemInfo group has the system level info like Total number of Closed RP sessions while the PerPCF stats group details call management statistics per PCF.

CDMA PDSN System Information

ccpcEnabled OBJECT-TYPE

"An indication of whether Closed RP feature is enabled."

::= { ccpcSystemInfo 1 }

ccpcSessionTotal OBJECT-TYPE

"The total number of Closed RP sessions currently established with this system."

::= { ccpcSystemInfo 2 }

CDMA PDSN Closed RP Registration Statistics per PCF

The PDSN PCF table maintains reference about the PCF in the RAN currently interacting with the PDSN.

An entry is created when an L2TP tunnel is established with the PCF. An entry is deleted when the tunnel is deleted.

Statistics Objects maintained per PCF include the following:

ccpcPcfIpAddressType OBJECT-TYPE

"Represents the type of the address specified by ccpcPcfIpAddress."

::= { ccpcPcfPerfStatsEntry 1 }

ccpcPcfIpAddress OBJECT-TYPE

"The IP address of the PCF that serves the mobile node."

::= { ccpcPcfPerfStatsEntry 2 }

ccpcPcfRcvdIcrqs OBJECT-TYPE

"Total number of Incoming-Call-Requests received to establish a L2TP session since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 3 }

ccpcPcfAcptdIcrqs OBJECT-TYPE

"Total number of Incoming-Call-Requests accepted since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 4 }

ccpcPcfDroppedIcrqs OBJECT-TYPE

"Total number of Incoming-Call-Requests denied since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 5 }

ccpcPcfSentIcrps OBJECT-TYPE

"Total number of Incoming-Call-Replies sent since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 6 }

ccpcPcfRcvdIccns OBJECT-TYPE

"Total number of Incoming-Call-Connected messages received since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 7 }

ccpcPcfAcptdIccns OBJECT-TYPE

"Total number of Incoming-Call-Connected messages accepted since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 8 }

ccpcPcfDroppedIccns OBJECT-TYPE

"Total number of Incoming-Call-Connected messages accepted since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 9 }

ccpcPcfRcvdCdns OBJECT-TYPE

"Total number of Call-Disconnect-Notify messages received to tear down L2TP session since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 10 }

ccpcPcfSentCdns OBJECT-TYPE

"Total number of Call-Disconnect-Notify messages sent to PCF to tear down L2TP session since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 11 }

ccpcPcfDroppedCdns OBJECT-TYPE

"Total number of Call-Disconnect-Notify messages dropped since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 12 }

ccpcPcfRcvdZlbs OBJECT-TYPE

"Total number of Zero-Length-Buffer messages received since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 13 }

ccpcPcfSentZlbs OBJECT-TYPE

"Total number of Zero-Length-Buffer messages sent since the L2TP tunnel was established with PCF."

::= { ccpcPcfPerfStatsEntry 14 }

In PDSN Release 2.0 and above, the MIB CISCO-CDMA-PDSN-MIB module is modified to provide the following statistics by PCF plus Service Option:

- PCF and Service Option based RP Registration Statistics
- PCF and Service Option based RP Update Statistics
- PCF and Service Option based PPP Statistics

PCF/Service Option-based RP Statistics

In Release 1.2, the PDSN MIB provided RP registration statistics that offer box level information. These statistics are defined under the group "cCdmaRpRegStats." In Release 2.0 and above, in addition to box level information, the PCF/SO-based RP statistics will also be provided, and the MIB objects pertaining to these statistics is defined under the following group:

cCdmaPcfSoRpRegStats OBJECT IDENTIFIER

::= { cCdmaPerformanceStats 10 }

PCF/Service Option-based RP Update Statistics

The Release 1.2 MIB provides RP update statistics at box level; the MIB objects pertaining to these statistics are defined under the group cCdmaRpUpdStats. In addition to these statistics, the Release 2.0 MIB will provide PCF/SO based RP update statistics. These new MIB objects are defined under the following group.

cCdmaPcfSoRpUpdStats OBJECT IDENTIFIER

::= { cCdmaPerformanceStats 11 }

PCF/Service Option-based PPP Statistics

In Release 1.2, the MIB objected defined under the group "cCdmaPppStats" provides box level information about PPP negotiation between the PDSN and the MN. In Release 2.0, the MIB will provide the following PPP stats based on PCF/SO.

cCdmaPcfSoPppCurrentConns,

cCdmaPcfSoPppConnInitiateReqs,

cCdmaPcfSoPppConnSuccesses,

cCdmaPcfSoPppConnFails,

cCdmaPcfSoPppConnAborts

These objects are grouped under the following MIB group.

cCdmaPcfSoPppSetupStats OBJECT IDENTIFIER

::= { cCdmaPerformanceStats 12 }

As with previous releases, you can manage the Cisco PDSN with Cisco Works 2000 network management system using SNMP. In addition to the standard 7200 and 6500 MIBS, the Cisco CDMA PDSN MIB (CISCO_CDMA_PDSN_MIB.my) is part of the PDSN solution. The Cisco PDSN MIB continues to support the following features:

- Statistics groups
  - Handoff statistics: include inter-PCF success and failure, inter-PDSN handoff
  - Service option based success and failure statistics
  - Flow type based failure statistics
  - MSID authentication statistics
  - Addressing scheme statistics: static or dynamic mobile IP/simple IP
- A TRAP threshold group to support different severity levels. Agent generates notifications only if the severity level of the affected service is higher than the configured severity level. The severity level can be configured using the following methods:
  - The CLI using the **cdma pdsn mib trap level** 1-4, or by
  - Using SNMP, set the object cCdmaNotifSeverityLevel.

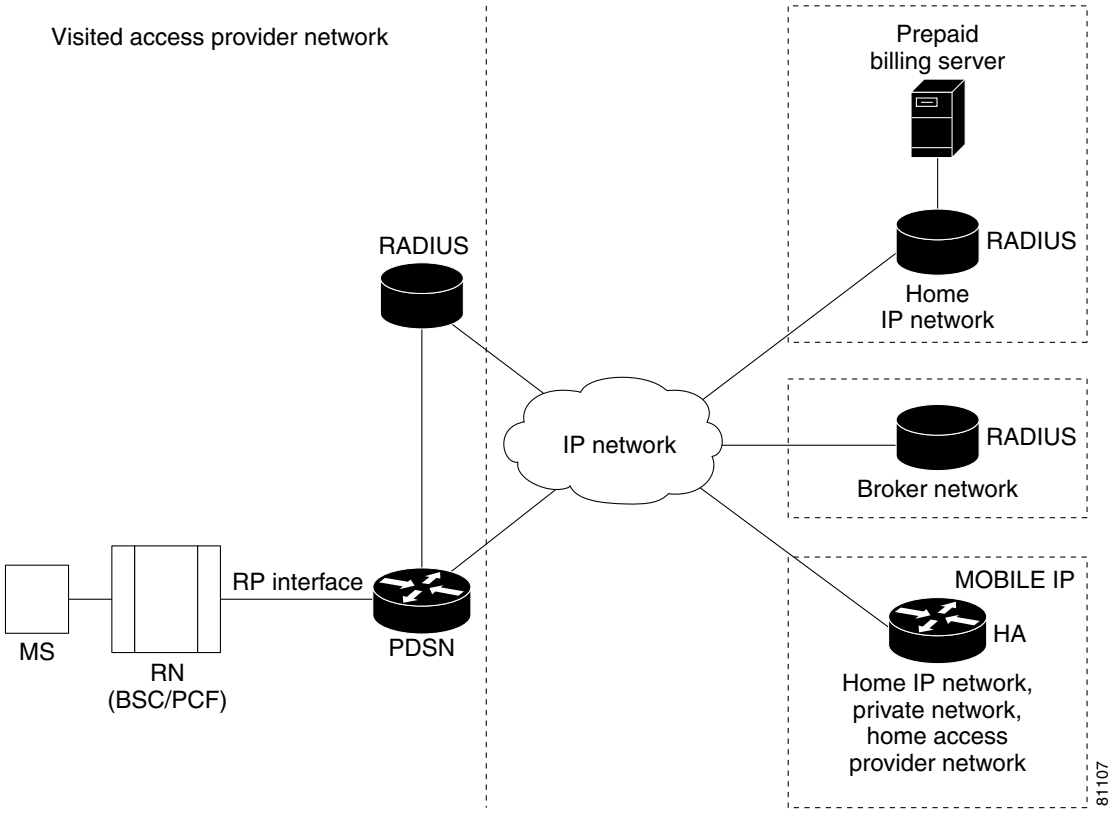
Cisco Proprietary Prepaid Billing

PDSN Release 2.1 supports Cisco's proprietary prepaid billing features, that provide the following services:

- Simple IP-based service metering in real time. See the "Prepaid Simple IP Call Flow" section on page 95 for more information.
- Undifferentiated Mobile IP service in real-time, with support for multiple Mobile IP flows per user. See the "Prepaid Mobile IP Call Flow" section on page 96 for more information.
- Rating based on per-flow data volume, octet or packet count, and call duration.

Figure 7 shows the network reference architecture for prepaid service. The PBS resides in the mobile station's home network and is accessed by the home RADIUS server. A Cisco Access Registrar (AR) with prepaid functionality can be used as the home RADIUS server to provide service to prepaid and non-prepaid users.

Figure 7 PDSN Prepaid Billing Architecture



For roaming users, the local RADIUS server in the visited network forwards AAA requests to the home RADIUS server, using a broker RADIUS server if required. For roaming prepaid users, this requires that the local and broker AAA servers forward the new vendor specific prepaid accounting attributes transparently to the home RADIUS server.

In existing networks, where the home RADIUS server does not support the interface to the Prepaid Billing Server, AR can be placed in front of the home RADIUS server to act as a proxy. In this case AR forwards all authorization and accounting messages to /from the home RADIUS server and communicates with the PBS. This scenario is relevant if an operator already has a RADIUS server.

While this architecture does impose some additional requirements on the RADIUS server, the interface towards the PDSN does not change.

It is possible that an operator may want to use an existing WIN or IN based prepaid billing server. In this situation, the PBS will interface to the external prepaid billing server.

Accounting Records

The PDSN will continue to generate per flow accounting records in the same way as it does for non-prepaid users. However, the last Accounting Stop Request for a flow will contain the new prepaid Vendor Specific Attributes (VSAs) for reporting the final usage.

How Prepaid Works in PDSN

When a prepaid mobile user makes a data service call, the MS establishes a Point-to-Point Protocol (PPP) link with the Cisco PDSN. The Cisco PDSN authenticates the mobile station by communicating with the AAA server. The AAA server verifies that the user is a valid prepaid subscriber, determines what services are available for the user, and tracks usage for billing.

The methods used to assign an IP address and the nature of the connection are similar to those discussed in the "How PDSN Works" section on page 5.

The following sections describe the IP addressing and communication levels in the prepaid environment for each respective topic:

- Prepaid Simple IP Call Flow
- Prepaid Mobile IP Call Flow

Prepaid Simple IP Call Flow

In the following scenario, the prepaid user has sufficient credit and makes a Simple IP data call. The user disconnects at the end of the call.

Step 1 The MS originates a call by sending an origination message. A traffic channel is assigned, and the MS is authenticated using CHAP.

Step 2 The PDSN determines that a Simple IP flow is requested and sends an Access Request to the RADIUS server.

Step 3 The RADIUS Server looks up the user's profile and determines that user has prepaid service. It sends an initial authentication request to the billing server.

Step 4 The billing server checks that the user has sufficient quota to make a call, and returns the result.

Step 5 The RADIUS Server sends an Access Accept message to PDSN indicating that this is a prepaid user.

Step 6 The PDSN completes the PPP connection, and an IP address is assigned to the MS.

Step 7 PDSN sends an Accounting Request (Start) as normal, and sends an Access Request to AR for initial quota authorization. The request contains the Service Id VSA that indicates the call is Simple IP.

Step 8 The RADIUS Server, knowing that this is a prepaid user, sends an initial quota authorization request to the billing server, which returns the quota information to the RADIUS Server. The RADIUS Server includes the quota information in the Access Accept message and sends it to the PDSN.

Step 9 The PDSN saves the received quota information and monitors user data against this. When the quota is used up, the PDSN sends an Access Request to AR indicating the usage and reason "Quota Depleted."

Step 10 The RADIUS Server then sends a re-authorization request to PBS, which updates the user's account, allocates additional quota, and returns the new quota information to the RADIUS Server.

Step 11 The RADIUS Server includes the new quota information in the Access Accept message and sends it to the PDSN. The PDSN updates the new quota information in its tables, and adjusts the usage to allow for quota that was used since the Access Request was sent. The PDSN then continues to monitor the user data. Steps 9 - 11 are repeated as long as the user has sufficient quota.

Step 12 When the user disconnects, the MS initiates release of the call and the traffic channel is released. The PDSN clears the session and sends an Accounting Request Stop record. The record includes the prepaid VSAs to report final usage.

Step 13 The RADIUS Server updates its own records and sends final usage report to PBS. The PBS updates the user's account and replies to the AR. And the AR sends the Accounting Response to PDSN.

Prepaid Mobile IP Call Flow

In the following scenario, the prepaid user makes a Mobile IP data call. The user runs out of quota during the mobile IP data session and the PDSN disconnects the call. The call flow shows a single Mobile IP flow; however, additional flows are established and handled in a similar manner when the MS sends additional Mobile IP Registration Requests.

Step 1 The MS originates a call by sending an Origination message. A traffic channel is assigned, but the MS skips CHAP.

Step 2 The PDSN completes the PPP connection. Since the MS skips IP address assignment during IPCP the PDSN assumes Mobile IP.

Step 3 The PDSN sends an Agent Advertisement with a FA-CHAP challenge, and the MS initiates a Mobile IP Registration Request with FA-CHAP response.

Step 4 The PDSN sends the Access Request with FA-CHAP to the AR. The AR looks up the user's profile and determines that the user has prepaid service. It the sends an authentication request to the billing server.

Step 5 The billing server checks that the user has sufficient quota to make a call and returns an **ok**. The RADIUS Server sends an Access Accept message to the PDSN that indicates a prepaid user.

Step 6 The PDSN forwards the mobile IP Registration Request to the Home Agent and receives a Registration Reply. The PDSN forwards the reply to the MS.

Step 7 The PDSN sends an Access Request for initial quota authorization. The request contains Service Id VSA that indicates this is a Mobile IP call. The AR, knowing that this is a prepaid user, sends the initial quota authorization request to the PBS. The billing server returns the quota information to the AR, who includes the quota information in the Access Accept message and sends it to the PDSN.

Step 8 The PDSN saves the received quota information and monitors the user data against this. When the quota is used up, the PDSN sends an Access Request to AR indicating the usage and reason "Quota Depleted."

Step 9 The AR sends re-authorization request to the PBS, who updates the user's account, allocates additional quota, and returns the new quota information to the AR.

Step 10 The AR includes the new quota information in the Access Accept message and sends it to the PDSN. The PDSN updates the new quota information in its tables, and adjusts usage to allow for quota used since the Access Request was sent. The PDSN then continues to monitor the user data. Steps 8-10 are repeated as long as the user has sufficient funds.

Step 11 If the PDSN requests an additional quota but the user has run out, the PBS rejects the request with reason "Exceeded Balance," and the AR sends an Access Reject to PDSN.

Step 12 The PDSN deletes the Mobile IP flow, determines that this is the last flow, and requests release of the A10 connection by sending A11-Registration Update to the PCF. The PCF sends an ack message and initiates release of the traffic channel.

Step 13 The PDSN clears the session and sends an Accounting Request Stop record. The record includes the prepaid VSAs to report final usage.

Step 14 The AR updates its own records and sends final usage report to PBS, who updates the user's account and replies to the AR.

Step 15 The AR finally sends the Accounting Response to PDSN.

Note This feature is a variant of the PDSN Release 2.1 software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN 2.0.

3 DES Encryption

The Cisco PDSN include 3DES encryption, which supports IPSec on PDSN. To accomplish this on the 7200 platform, Cisco supplies an SA-ISA card for hardware provided IPsec. IPSec on the MWAM platform requires you to use a Cisco VPN Acceleration Module.

This feature allows VPDN traffic and Mobile IP traffic (between the PDSN Home Agent) to be encrypted. In this release the PDSN requires you to configure the parameters for each HA before a mobile ip data traffic tunnel is established between the PDSN and the HA.

Note This feature is only available with hardware support.

Note This feature is a variant of the PDSN software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN.

Mobile IP IPSec

The Internet Engineering Task Force (IETF) has developed a framework of open standards called IP Security (IPSec) that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IS-835-B specifies three mechanisms for providing IPSec security:

- Certificates
- Dynamically distributed pre-shared secret
- Statically configured pre-shared secret.

Note IS-835-B Statically configured pre-shared secret is not supported in PDSN Release 1.2. Only CLI-configured, statically configured pre-shared-secret of IKE will be implemented and supported.

Hardware IPSec Acceleration Using IPSec Acceleration Module—Static IPSec

Note The Cisco PDSN Release on the Cisco 6500 and 7600 platforms requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500 switch and the Cisco 7600 Internet Router. VPNSM does not have any physical WAN or LAN interfaces, and utilizes VLAN selectors for its VPN policy. For more information on Catalyst 6500 Security Modules visit http://wwwin.cisco.com/issg/isbu/products/6000/6500security.shtml. For more information on the Cisco 7600 Internet Router visit http://wwwin.cisco.com/rtg/routers/products/7600/techtools/index.shtml.

IPSec-based security may be applied on tunnels between the PDSN and the HA depending on parameters received from Home AAA server. A single tunnel may be established between each PDSN-HA pair. It is possible for a single tunnel between the PDSN-HA pair to have three types of traffic streams: Control Messages, Data with IP-in-IP encapsulation, and Data with GRE-in-IP encapsulation. All Traffic carried in the tunnel will have the same level of protection provided by IPSec.

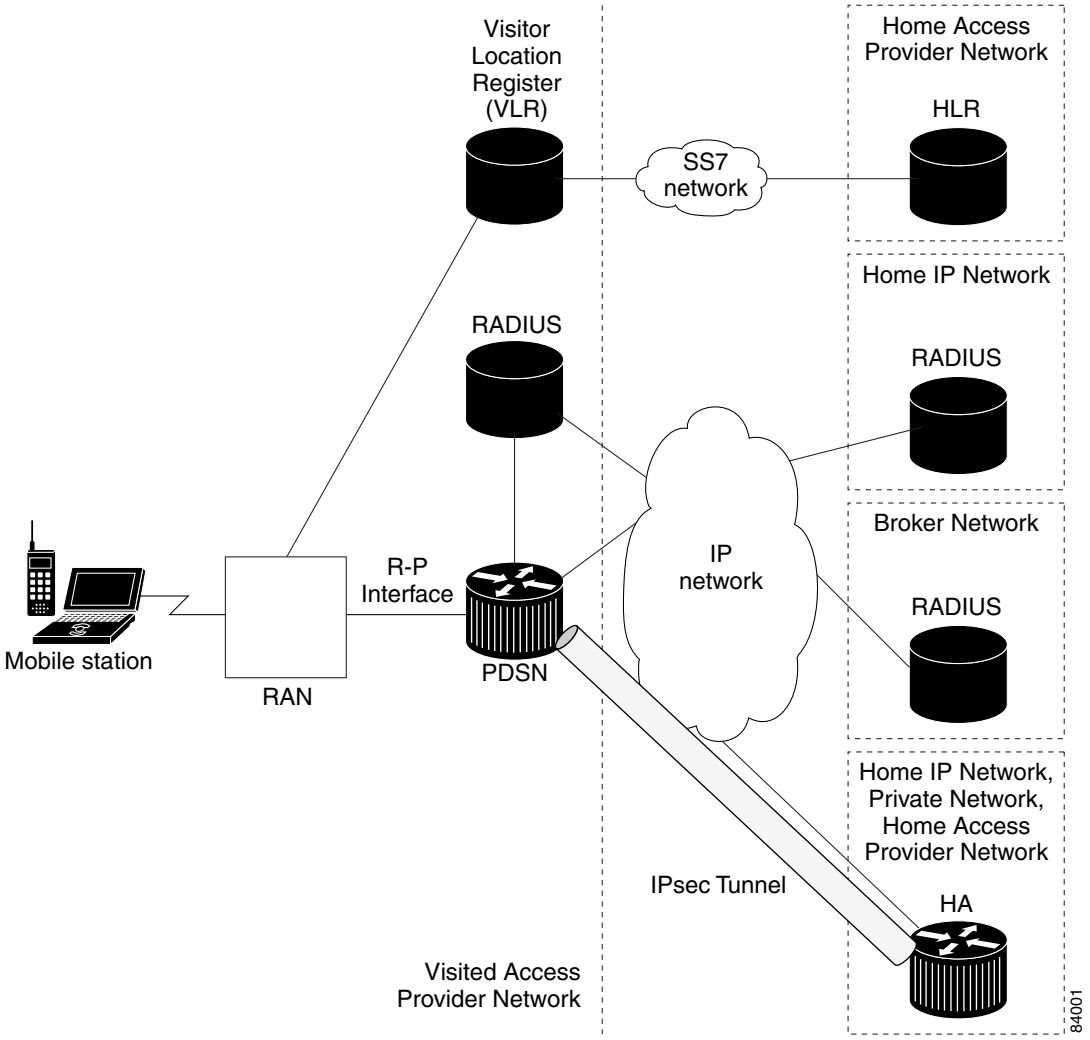
IS-835-B defines MobileIP service as described in RFC 2002; the Cisco PDSN provides Mobile IP service and Proxy Mobile IP service.

In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy for the MN to the HA.

Once Security Associations (SAs, or tunnels) are established, they remain active until there is traffic on the tunnel, or the lifetime of the SAs expire.

Figure 8 illustrates the IS-835-B IPSec network topology.

Figure 8 IS-835-B IPSec Network



Hardware IPSec acceleration of 8000 IPSec tunnels per chassis is available through the use of the Cisco VPN Acceleration Module. Refer to the *xxxxx* for more information.

Note This feature is a variant of the PDSN software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN.

Conditional Debugging Enhancements

Trace Functionality in Release 3.0

While conditional debugging has been a useful tool to limit the displayed debugs to a particular user, the output can still be a bit misleading if a few users are traced together. Therefore, the following capabilities are added in R3.0:

- The PDSN currently supports display of the MNID/username with every line printed from the CDMA debugs. A similar mechanism is also added for a few other subsystems, like MoIP, PPP, and AAA. Some of the commonly used debugs that are enhanced with the trace functionality are:
  - **debug ppp negotiation**
  - debug aaa id
  - debug aaa accounting
  - debug aaa authentication
  - debug aaa authorization
  - debug ip mobile
  - debug cdma pdsn a11 events
  - debug cdma pdsn accounting
  - debug cdma pdsn service-selection
  - debug cdma pdsn session events
  - cdma pdsn redundancy debugs
- When the debug conditions match, every line of the debug message is pre-pended with either the username or the IMSI (not both), depending on the condition set.

Note Pre-pending of Username/IMSI is not supported for a11 cluster debugs.

Note Pre-pending of Username/IMSI is not supported for **cdma pdsn redundancy** debugs.

Note GRE debugs are not pre-pended with IMSI for the first few lines.

Note **debug cdma pdsn a11 errors** are not printed for matching conditions.

Note **debug aaa accounting** does not get pre-pended with username.

- The above behavior is controlled through the **cdma pdsn debug show-condition** and **ip mobile debug include username** commands. If conditional debugging is enabled without these CLI being configured, the username/IMSI will not be displayed in the debugs. However, if the above CLIs are configured without configuring conditional debugging, the username/IMSI is printed along with the debugs.

Enhancements Prior to Release 3.0

PDSN Release 2.1 supports additional conditional debugging for Mobile IP components. Mobile IP conditional debugging is supported based on NAI as well as the MN's home address.

Currently, when multiple conditional debugging is enabled, the debug output does not individually display the condition for which the debugs are printed for all the CDMA related debugs.

Check Condition

A condition is set using the **debug condition username** command.

Delete Condition

The debugging conditions can be removed using the following commands:

- **no debug condition username**—removes all the conditions based on **username**
- **no debug condition username** *username*—removes the condition for the specified *username*

When a condition is removed using the above CLI, the IOS Conditional Debugging Subsystem, which maintains a list of conditions and the TRUE conditions, resets the flag. When all the conditions are removed, the debugging information will appear without any filter applied.

The PDSN software also utilizes conditional debugging based on the Mobile Subscriber ID (MSID) into the CDMA subsystem by using the existing IOS debug condition of the Cisco CLI. The calling option of the CLI is used to specify the MSID (for example, debug condition calling 00000000011124).

The following debug commands are supported for conditional debugging based on NAI. The NAI is a name like foo@bar.com.

- **debug ip mobile**
- **debug ip mobile host**
- **debug ip mobile proxy**

The following debug commands are not impacted by NAI-based conditional debugging:

- **debug ip mobile local-area**
- **debug ip mobile router**

This release provides conditional debugging support for the following PDSN CLI commands:

- **debug cdma pdsn accounting**
- **debug cdma pdsn accounting flow**
- **debug cdma pdsn session** [**errors** | **events**]
- **debug ip mobile**
- **debug condition username**

The a11 debugs additionally support msid-based debugging using the following individual CLI commands:

- **debug cdma pdsn a11 events mnid**
- **debug cdma pdsn a11 errors mnid**
- **debug cdma pdsn a11 packet mnid**

Conditional debugging is an IOS feature, and the following CLI are available across all images.

```
router# debug condition ?
  application  Application
  called       called number
  calling      calling
  glbp         interface group
  interface    interface
  ip           IP address
  mac-address  MAC address
  match-list   apply the match-list
  standby      interface group
  username     username
  vcid         VC ID
```

The options **calling**, **username**, and **ip** are used by the CDMA/Mobile IP subsystems.

```
PDSN#debug condition username ?
  WORD  Username for debug filtering

PDSN#debu condition calling ?
  WORD  Calling number

PDSN#debu condition ip ?
  A.B.C.D  IP address
```

Refer to the debug commands in the Command Reference for more information about conditional debugging in PDSN Release 2.1.

Electronic Serial Number (ESN) in Billing

The ESN is a unique identifier for a piece of equipment, such as of a mobile device, and is used during the authentication process. The ESN is parameter a2 of the R-P Session Setup airlink record, and parameter A2 in the PDSN Usage Data Record (UDR). Both parameters are introduced in this release.

The PDSN accepts the parameter a2, and puts it as A2 into a User Data Record.

This feature is supported in the Cisco Access Registrar.

Support for Mobile Equipment Indentifier (MEID)

The MEID is a new attribute introduced in IS-835D, and will eventually replace the ESN AVP. In the interim period, both attributes are supported on the PDSN.

To include the MEID in Access Request, FA-CHAP, or Mobile IP RRQ, use the **cdma pdsn attribute send a3** command.

1xEV-DO Support

The Cisco PDSN supports Evolution-Data Optimized (1xEV-DO). 1xEV-DO offers high performance, high-speed, high-capacity wireless Internet connectivity, and is optimized for packet data services. It can transport packet data traffic at forward peak rates of 2.4 Mbps, which is much higher than the current 1xRTT peak rate of 144 kbps.

PDSN support for 1xEV-DO technology includes the following enhancements:

- PDSN recognizes a new Service Option value of 59 (decimal) for 1xEV-DO in Active Start Airlink Record.
- The PDSN CLI commands are enhanced to show sessions—**show cdma pdsn session**—so that packet service options are displayed (1xRTT, 1xEV-DO, or undefined).

Features Available From Previous PDSN Releases

The following features were introduced in previous PDSN software releases, and are still supported in Release 2.0.

Integrated Foreign Agent (FA)

The FA is an essential component to mobility, because it allows a mobile station to remotely access services provided by the station's home network. The Cisco PDSN provides an integrated FA. The FA communicates with any standard HA including the Cisco IOS-based HA.

AAA Support

The Cisco PDSN provides an authentication client that communicates with any standard AAA server, including Cisco Access Registrar, to authenticate the mobile station. It uses the mobile stations' name (NAI) for authentication of the user with the local AAA server.

- The Cisco PDSN supports the following AAA services for Simple IP:
  - Password Authentication Protocol (PAP) and CHAP authentication.
  - Accounting information.
  - IP address allocation for the mobile user.

Note The Cisco PDSN supports the assignment of IP addresses and the mapping of MSID to NAI for special configuration users. Typically, this includes MSID-based access users who skip the authentication process during the PPP establishment, and who want just the Simple IP routing service.

- The Cisco PDSN supports the following AAA services for VPDN:
  - PAP and CHAP authentication.
  - Accounting information.
- The Cisco PDSN supports the following AAA services for Proxy Mobile IP:
  - PAP and CHAP authentication.
  - Accounting information.
  - Assignment of IP address (as received from HA, in the Registration Reply message) during the IPCP phase.
- The Cisco PDSN supports the following AAA services for Mobile IP:
  - Optionally skip authentication during PPP upon receiving REJ from the mobile station.

- FA Challenge/Response as defined in TIA/EIA/IS-835-B through Mobile IP registration.
- FA-HA and FA-mobile station authentications as described under Mobile IP section.
- Verification of the FA challenge response in a Mobile IP registration request corresponding to a recent advertisement.

The Cisco PDSN also supports service provisioning using AAA servers and a user service profile. This profile is defined by the user's home network. It is referenced by the NAI. It is typically stored in the AAA server in the user's home network, along with the user authentication information, and is retrieved as part of authorization reply.

Packet Transport for VPDN

The Cisco PDSN supports the transport of VPDN packets. If the operator offers VPDN services, the mobile station can securely access private resources through a public Internet or dedicated links. The VPDN tunnel extends from the PDSN/FA to the home IP network. The home IP network is the IP network associated with the NAI.

Proxy Mobile IP

With Proxy Mobile IP as part of the PPP link initiation, the PDSN registers with a HA on behalf of the mobile station. It obtains an address from the HA and forwards that address to the mobile station as part of IPCP during PPP initialization.

Multiple Mobile IP Flows

The Cisco PDSN allows multiple IP access points from the same mobile station, as long as each IP flow registers individually (each IP flow requires a unique NAI). This enables multiple IP hosts to communicate through the same mobile access device and share a single PPP connection to the operator's network. For accounting purposes, it is important that the PDSN generate separate usage data records (UDRs) for each flow to the AAA server.

Redundancy and Load Balancing

This section provides information about Intelligent PDSN Selection and Load Balancing for the Controller - Member cluster model.

PDSN Cluster Controller / Member Architecture

The PDSN Controller member architecture was designed to support 8 members with redundant Active/Standby controllers. This controller-member mode designates certain nodes as controllers responsible for performing PDSN selection, and for maintaining the global session tables. Each member node maintains information only about the sessions that are terminated on that node. Controllers can be redundant with all session information synchronized between them, and they monitor the state of all nodes to detect the failure of a member or another controller.

When a PDSN cluster operates in the controller-member mode, controllers are dedicated to the PDSN selection function, and do not terminate bearer sessions.

PDSN Release 2.1 supports the following enhancements:

- Cluster scalability to support 48 members with bulk-update of session information
- Conditional debugging support for MSID under clustering feature
- Controller Show command enhancements
- Clear command under clustering feature to clear clustering statistics

When a Registration Request (RRQ) arrives from the PCF to the active controller, the controller uses the MSID as an index to look up the session-table. If a session record entry is present, the controller forwards the RRQ to the PDSN that hosts the session for the MSID. If the session entry is not present in the controller session-table, the controller chooses a member based on a configured selection algorithm, and replies to the PCF with an RRP that suggests the member IP address in the message.

When the session comes up, the member sends a Session-Up message from the member for that session (MSID) to the controller. On receipt of this message from the member, the controller creates the Session Record for that MSID in the controller to establish MSID-member association on the controller. On receipt of Session-Down message from member, the controller flushes the Session Record from the controller.

The controller does not create a Session Record for the MSID when it redirects the RRQ, but only on the receipt of a Session-Up message from the member on which the session has come up

To support a large number of members (28~48) per Controller, processing overhead is reduced when members send one bulk-update packet to the controller for every configured periodic update time interval with multiple pairs of Session-Up/Session-Down. The packet contains concatenated multiple MSIDs with one Session-Up/Session-Down flag, thereby saving bytes in the packet. The controller will process these bulk-update packets and send a bulk-update-ack packet to the members.

Conditional Debugging Support Under Clustering Feature

The Cisco PDSN 2.0 Clustering feature adds additional support for the conditional debugging with the following clustering debug command on both controller and member:

- **Debug cdma pdsn cluster controller message** {**event** | **error** | **packet**}

Note PDSNs in controller-member mode and peer-to-peer mode cannot co-exist in the same cluster. They are mutually exclusive.

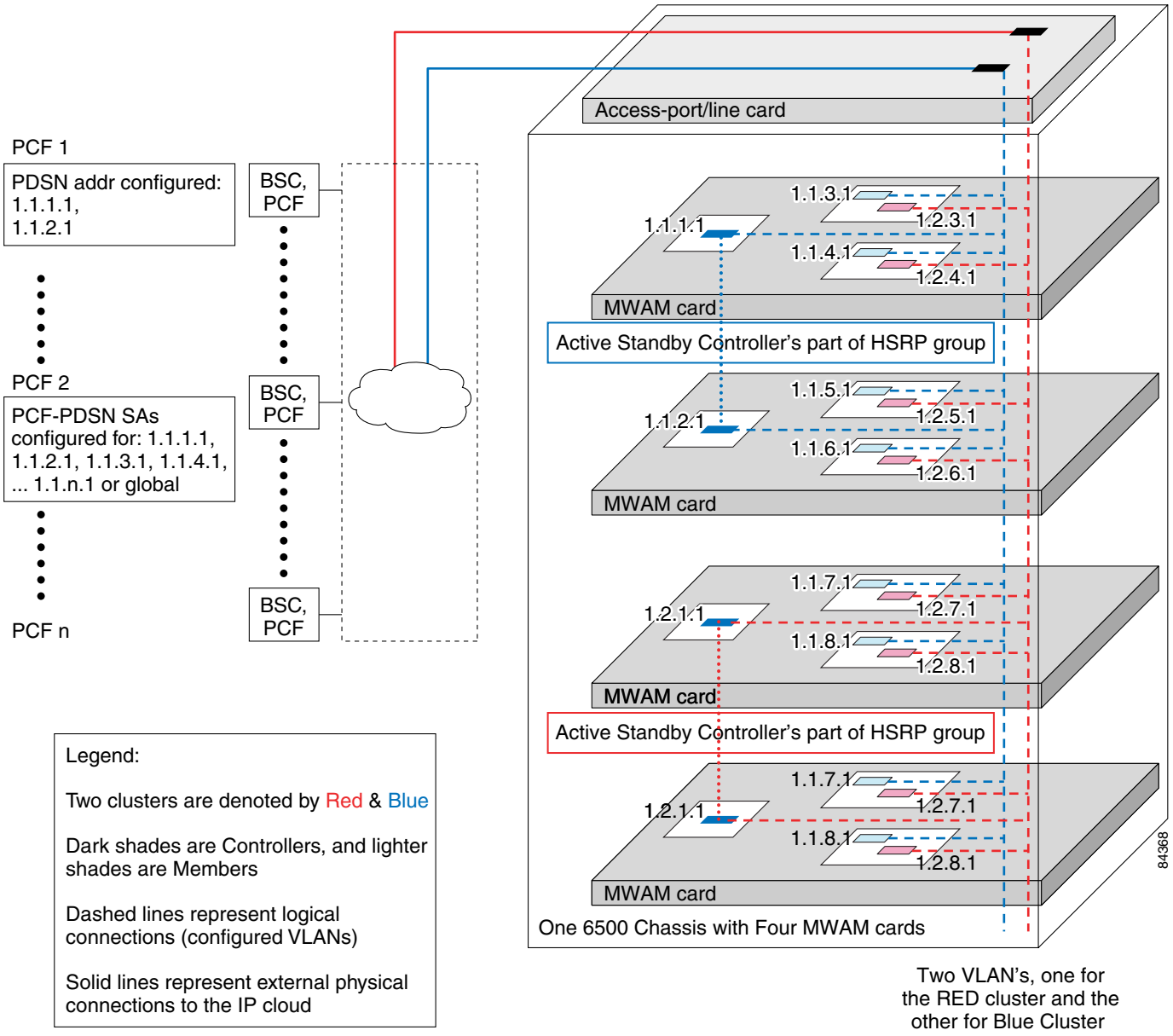
PDSN Controller-Member Clustering

In Controller-Member clustering, a controller maintains load and session (such as A10 connection) information for each member in the cluster, and performs member selection for load-balancing or inter-PDSN handoff avoidance. The controller identifies the operational state of each member and detects the failure of a member, or the failure of another controller. A member notifies the controller about its load and session information.

Note The new PDSN Controller-Member clustering feature is only available on the **-c6is-mz**, and **-c6ik9s-mz** images.

Figure 9 illustrates the Controller-Member architecture on the 6500 or 7600-based MWAM platform. This illustration depicts two PDSN clusters with two primary and two backup controllers, and their corresponding members.

Figure 9 PDSN Controller -Member Architecture for MWAM on the Catalyst 6500



PDSNs that are designated as controllers, perform member PDSN selection and load balancing. The following list describes the major functions of the controllers:

- Controllers maintain the load information for all members—they obtain the load information by seeking the cluster members. Alternatively, the members send the load value at configurable intervals inside a session origination or termination message. Controllers synchronize by exchanging information as needed.
- The link on which controllers exchange information is an HSRP-based state information exchange (HA redundancy is based on this type of implementation).
- The link on which the active controller and members exchange information is a unicast HSRP address for the active controller, but must be configured on the members.

- The actual PDSN selection and load-balancing procedures are similar to the R1.1 implementation; however, different record tables are used.
- Auto-configuration of a new PDSN controller added to the cluster—The new controller must be configured as such, and must be configured as a member of the HSRP group of routers. As a consequence, the new controller (standby) automatically downloads member and session records from the active controller. The active controller updates the standby as needed, so that records are synchronized.
- Auto-configuration of the controllers when a new member is added to the cluster—The new member registers with the active controller, which updates the standby controller.
- Redundancy—All controllers in the cluster maintain session and load information for all members. This provides redundancy for availability, and, in case of a controller failure, session and load-balancing information is not lost.

Redundancy

Cluster redundancy is based on the premise that only one PDSN might fail at any given time. Two controllers are configured as an HSRP group: One controller is active, the other standby. Controllers have redundancy and members have load sharing.

Load Sharing

Cluster member loadsharing is an N+1 scheme. If a member fails, the established sessions will be lost, but the overall group capacity allows sessions to be re-established with the other group members. Additionally, redundancy is also enhanced because cluster members no longer have to be network neighbors.

Controllers exchange information over an ethernet link. Controllers and members exchange information over a unicast interface link where members address messages to the HSRP group address of the controllers. The members in a PDSN cluster do not need to be network neighbors; they can be attached anywhere in the IP network.

Adding an additional controller to a cluster is simplified by auto-configuration of the controller in the cluster. This is possible by configuring the additional controller for HSRP. The newly-added controller will automatically synchronize with the active controller. Similarly, when a new member is added to the cluster, auto-configuration for the member occurs in all cluster controllers.

PDSN Cluster Member Selection

Selection of a cluster member by the controller is based on a *load factor*. Load factor is a computed value by session load and CPU load on a member. The controller attempts to assign sessions to a member that has smallest load factor so that data connections are evenly distributed over members in the cluster as much as possible.

If an A11 Registration Request is received indicating a handoff, a member that is already serving the session is selected by the controller.

Load Balancing

A controller maintains load information for all members in the cluster in order to perform PDSN Cluster Member selection. This load information is transferred from the members to the controller under the following conditions:

- at periodic intervals.
- when a session is established or dismantled in a member. In this case, the periodic timer is restarted.
- requested from the members by the controller.

The session and member records are synchronized between the active and standby controllers as needed. Since both active and standby controller maintain session and load information for all the members of that cluster, failure of a controller does not result in the loss of any session or load information.

Upgrading the Controller PDSN Software from R1.2 to R2.0

To upgrade the PDSN controller to Release 2.0, perform the following tasks:

Step 1 Reload either the Active/Standby controller so that at least one of the controllers is operating to take care new incoming calls.

Step 2 Load Release 2.0 software. Once the controller with Release 2.0 software is operational, ensure both controllers have synched session information using the following command:

 # show cdma pdsn cluster controller configuration

Step 3 Issue the following command to make use of the scalable bulk-synch mechanism of session information between Controller and member PDSN introduced in Release 2.0 PDSN Software.

config# **cdma pdsn cluster controller member periodic-update**

Follow the same procedure as above to upgrade the other PDSN controller to Release 2.0.

Upgrading the Member PDSN Software from R1.2 to R2.0 and Above

To upgrade a member PDSN to Release 2.0 or 2.1, perform the following tasks:

Step 1 Separate a member PDSN out of the cluster by configuring the following command on the member PDSN:

config# **cdma pdsn cluster member prohibit administratively**

The status of the member will be updated to the controller in a subsequent periodic keepalive reply message that the member sends to the controller. The controller, upon reception of this message, does not select this member for any of the new incoming calls.

Step 2 Display the member PDSNs which are prohibited administratively by issuing the following command:

#show cluster controller member prohibited administratively

The calls, which are already connected to the member, will be alive until the mobile node disconnects the call. Alternatively, the calls can be forcibly cleared on the prohibited member using the following command:

#clear cdma pdsn session all

Step 3 When all the calls are brought down, upgrade the software to Release 2.0 and above, or shutdown this member without disrupting the operation of the PDSN cluster. When the member comes online you can configure it to rejoin the cluster by issuing the following command:

config# **no cdma pdsn cluster member prohibit administratively**

Once the controller is updated with the status the new member PDSN will be selected for new incoming calls.

Step 4 Configure the following command to use the scalable bulk-synch mechanism of session information between Controller and member PDSN:

config# **cdma pdsn cluster member periodic-update 300**

Scalability

In this release the PDSN uses a new scalability feature that allows PPP sessions to run on virtual-access subinterfaces that can support up to 20000 sessions.

Note When using the virtual-access subinterfaces, not more than 20 percent (or a maximum of 4000) of the sessions should be compression sessions.

Note If you are using the Cisco PDSN with a AAA server, ensure that the attribute “compression=none” is not present in your user profiles. If it is, the Cisco PDSN will use the full virtual- access interface instead of the virtual-access sub-interface.

Note To increase the call setup performance, use the **no virtual-template snmp** global configuration command. This prevents the virtual-access subinterfaces from being registered with the SNMP functionality of the router, and reduces the amount of memory used.

High Availability

Overview

High availability allows you to minimize the switchover time from the active supervisor engine to the standby supervisor engine if the active supervisor engine fails.

Prior to this feature, fast switchover ensured that a switchover to the standby supervisor engine happened quickly. However, with fast switchover, because the state of the switch features before the switchover was unknown, you had to re-initialize and restart all the switch features when the standby supervisor engine assumed the active role.

High availability removes this limitation; high availability allows the active supervisor engine to communicate with the standby supervisor engine, keeping feature protocol states synchronized. Synchronization between the supervisor engines allows the standby supervisor engine to take over in the event of a failure.

In addition, high availability provides a versioning option that allows you to run different software images on the active and standby supervisor engines.

For high availability, a system database is maintained on the active supervisor engine and updates are sent to the standby supervisor engine for any change of data in the system database. The active supervisor engine communicates and updates the standby supervisor engine when any state changes occur, ensuring that the standby supervisor engine knows the current protocol state of supported features. The standby supervisor engine knows the current protocol states for all modules, ports, and VLANs; the protocols can initialize with this state information and start running immediately.

The active supervisor engine controls the system bus (backplane), sends and receives packets to and from the network, and controls all modules. Protocols run on the active supervisor engine only.

The standby supervisor engine is isolated from the system bus and does not switch packets. But it does receive packets from the switching bus to learn and populate its Layer 2 forwarding table for Layer 2-switched flows. The standby supervisor engine also receives packets from the switching bus to learn and populate the Multilayer Switching (MLS) table for Layer 3-switched flows. The standby supervisor engine does not participate in forwarding any packets and does not communicate with any modules.

If you enable high availability when the standby supervisor engine is running, image version compatibility is checked and if found compatible, the database synchronization starts. High availability compatible features continue from the saved states on the standby supervisor engine after a switchover.

When you disable high availability, the database synchronization is not done and all features must restart on the standby supervisor engine after a switchover.

If you change high availability from enabled to disabled, synchronization from the active supervisor engine is stopped and the standby supervisor engine discards all current synchronization data.

If you change high availability from disabled to enabled, synchronization from the active to standby supervisor engine is started (provided the standby supervisor engine is present and its image version is compatible).

NVRAM synchronization occurs irrespective of high availability being enabled or disabled (provided there are compatible NVRAM versions on the two supervisor engines).

If you do not install a standby supervisor engine during system bootup, the active supervisor engine detects this and the database updates are not queued for synchronization. Similarly, when you reset or remove the standby supervisor engine, the synchronization updates are not queued and any pending updates in the synchronization queue are discarded. When you hot insert or restart a second supervisor engine that becomes the standby supervisor engine, the active supervisor engine downloads the entire system database to the standby supervisor engine. Only after this global synchronization is completed, the active supervisor engine queues and synchronizes the individual updates to the standby supervisor engine.

Note When you hot insert or restart a second supervisor engine, it might take a few minutes for the global synchronization to complete.

For more information about High Availability, including configuration details, and information about power management, refer to the "PDSN Controller-Member Clustering" section on page 105, as well as the documents at the following urls:

- *Catalyst 6500 Series Software Configuration Guide* (6.1.1a), with special attention to the "Configuring Redundancy" chapter at:
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/index.htm
- *Catalyst 6000 Family IOS Software Configuration Guide, Release 12.2(9)YO* at:
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122yo/swcg/supcfg.htm
  - http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122yo/swcg/pwr_envr.htm

Related Features and Technologies

- Mobile IP
- PPP (Point-to-Point Protocol)
- AAA (Authentication, Authorization, and Accounting)
- VPDN (Virtual Private Data Network) using L2TP
- RADIUS (Remote Authentication Dial-In User Service)

Related Documents

For additional information about the Cisco PDSN Release 2.1 software, refer to the following documents:

- *Release Notes for the Cisco PDSN 2.1 Feature in Cisco IOS Release 12.3(11)YF*

For more information about:

- MWAM hardware and software information, refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note.*
- The IP Sec configuration commands included in this document, refer to the "IP Security and Encryption" section in the *Cisco IOS Security Configuration Guide*.
- The AAA configuration commands included in this document, refer to the Cisco IOS Release 12.3 documentation modules *Cisco IOS Security Command Reference* and *Cisco IOS Security Configuration Guide*.
- The PPP and RADIUS configuration commands included in this document, refer to the Cisco IOS Release 12.3 documentation module *Cisco IOS Dial Services Command Reference*.
- Mobile IP, refer to the Cisco Release 12.3 documentation modules *Cisco IOS IP Command Reference* and *Cisco IOS IP Configuration Guide*.
- Virtual Private Networks, refer to the Cisco IOS Release 12.3 documentation modules *Cisco IOS Dial Services Configuration Guide, Network Services* and *Cisco IOS Dial Services Command Reference*.

Supported Platforms

The Cisco PDSN for MWAM release is a feature enhancement for the Cisco 7206 router and the Multi-Processor WAN Application Module (MWAM) card that resides on the Cisco Catalyst 6500 switch or Cisco 7600 Internet Router. Refer to the following document for more information regarding the respective platforms:

- *Release Notes for the Cisco PDSN 3.0 Feature in Cisco IOS Release 12.3(14)YX* for information about the supported platforms.

Supported Standards, MIBs, and RFCs

Standards

- TIA/EIA/IS-835-B, Wireless IP Network Standard
- TIA/EIA/IS-2001-B, Interoperability Specification (IOS) for CDMA 2000 Access Network Interfaces (Also known as 3GPP2 TSG-A and as TR45.4)
- TIA/EIA/TSB-115, Wireless IP Network Architecture Based on IETF Protocols

MIBs

- CISCO_CDMA_PDSN_MIB.my
- CISCO_PROCESS_MIB.my
- CISCO_MOBILE_IP_MIB.my
- CISCO_AHDLC_MIB.my
- CISCO_AAA_CLIENT_MIB.my
- CISCO_AAA_SERVER_MIB.my
- CISCO_VPDN_MGMT_MIB.my
- CISCO_VPDN_MGMT_EXT_MIB.my

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

- RFC 791, *Internet Protocol*
- RFC 1144, *Compressing TCP/IP Headers for Low-speed Serial Links*
- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1334, *PPP Authentication Protocols*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*
- RFC 1962, *The PPP Compression Control Protocol (CCP)*
- RFC 1974, *PPP Stac LZS Compression Protocol*
- RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 2002, *IP Mobility Support*
- RFC 2003, *IP Encapsulation within IP*
- RFC 2005, *Applicability Statement for IP Mobility Support*
- RFC 2006, *The Definitions of Managed Objects for IP Mobility Support using SMIv2*
- RFC 2118, *Microsoft Point-To-Point Compression (MPPC) Protocol*

- RFC 2344, *Reverse Tunneling for Mobile IP*
- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*
- RFC 3012, *Mobile IPv4 Challenge/Response Extension*

Configuration Tasks

This section describes the steps for configuring the Cisco PDSN software on both the 7200 and MWAM platforms. Prior to configuring instances of the PDSN on MWAM application cards, you must create a base Catalyst 6500 or 7600 configuration. Refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note* for more information.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(11)T:

Memory Requirements

Table 7 shows the memory requirements for the PDSN Software Feature Set that supports the Cisco 7206VXR router, the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform, and the Cisco NPE-G1 router. The table also lists the memory requirements for the IP Standard Feature Set (for the Home Agent [HA]).

Table 7 Memory Requirements for the Cisco 7206VXR Router and MWAM on the 6500 Catalyst Switch and 7600 Router

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7206VXR Router	PDSN Software Feature Set	c7200-c6is-mz.123-14.YX c7200-c6ik9s-mz.123-14.YX	20 MB	512 MB	RAM
Cisco 6500 Catalyst Switch	PDSN Software Feature Set	c6svc5fmwam-c6is-mz (This is a bundled image)	40MB	512MB	RAM

Table 7 Memory Requirements for the Cisco 7206VXR Router and MWAM on the 6500 Catalyst Switch and 7600 Router (Continued)

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7600 Internet Router	PDSN Software Feature Set	c6svc5fmwam-c6is-mz (This is a bundled image)	40MB	512MB	RAM
Cisco NPE-G1 Router	PDSN Software Feature Set	c7200-c6is-mz.123-14.YX c7200-c6ik9s-mz.123-14.YX	40MB	512MB	RAM

Hardware Supported

Cisco IOS Release 12.4(11)T is optimized for PDSN Release 3.0 on the Cisco 7206VXR router, the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform, and the Cisco NPE-G1 router.

A Hardware-Software Compatibility Matrix is available on CCO for users with CCO login accounts. This matrix allows users to search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is available at the following URL:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Software Compatibility

Cisco IOS Release 12.4(11)T is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(11)T supports the same features that are in Cisco IOS Release 12.4, with the addition of the PDSN Release 3.0 feature.

Note We recommend that you use the Cisco SXE3 Supervisor image with Release 3.0

Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version** EXEC command:

```
Router#show version
mwt5-6509a-06-4#sh ver
Cisco IOS Software, MWAM Software (MWAM-C6IS-M), Version 12.3(11)YF4, RELEASE SOFTWARE
(fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by Cisco
Systems, Inc.
Compiled Mon 25-Jul-05 15:24 by ssearch

ROM: System Bootstrap, Version 12.2(11)YS2 RELEASE SOFTWARE

mwt5-6509a-06-4 uptime is 2 hours, 9 minutes System returned to ROM by reload at 07:35:31
UTC Wed Jul 6 2005 System restarted at 02:31:05 UTC Tue Jul 26 2005 System image file is
"svcmwam-c6is-mz"

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2
```

```
Last reset from power-on
1 Gigabit Ethernet interface
511K bytes of non-volatile configuration memory.

Configuration register is 0x4

mwt5-6509a-06-4#
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

Upgrading PDSN Image from YF-based Image to R3.0-based Image

If you are upgrading the PDSN from a YF-based image to a R3.0-based image, you first need to upgrade the SUP image from a SXB-based image to the recommended SXE-based image.

Note We recommend that you upgrade to the Cisco IOS Supervisor Engine 720, Release 12.2(18)SXE3.

For more information on the 12.2(18)SXE3 Supervisor image, please refer to the following URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

After you upgrade the SUP image, you can then upgrade the PDSN image.

Upgrading the Supervisor Image:

To upgrade the Supervisor image, perform the following procedure:

Step 1 Copy the SUP image to the disks (disk0: / slavedisk0:).

Step 2 Add the following command to the running config boot system disk0: *SUP image name*. Here is an example:

```
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXE3.bin
```

Note This step may require you to unconfigure previously configured instances of this CLI in order to enable the image to properly reload.

Step 3 Perform a “write memory” so that running configuration is saved on both active and standby SUP.

Step 4 Issue **reload** command on the active SUP.

Both active and standby SUP will reload simultaneously and come up with the SXE3-based image.

Note Issuing the **reload** command on the active SUP will cause both the active and standby Supervisors to reload simultaneously, thus causing some downtime during the upgrade process.

Upgrading the PDSN Image on MWAM:

To upgrade an image on the Cisco MWAM, you will need a compact flash card that has the MP partition from the current image or later, and a recent supervisor image. To locate the images, please go to the Software Center at Cisco.com (http://www.cisco.com/public/sw-center/)

Upgrading the Controller PDSN on MWAM:

To upgrade to the R3.0-based image on the PDSN controller, perform the following procedure:

Step 1 Bring down the Standby PDSN Controller Loaded with YF based image, by issuing the **hw-module module** *slot #* **reset cf:1** command on Supervisor. The active PDSN Controller will continue to service the incoming requests.

Log onto the supervisor and boot the MP partition on the PC.

```
SUP-PDSN#hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-HA#
SUP-HA#
Nov 10 18:01:29.624: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:01:29.624: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:01:55.252: SP: PC shutdown completed for module 8
Nov 10 18:01:55.256: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:04:00.195: SP: OS_BOOT_STATUS(8) MP OS Boot Status: finished booting
Nov 10 18:04:42.299: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:04:42.271: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:04:43.143: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
SUP-PDSN#
```

Step 2 Once the module is online, copy the R3.0 image to pclc# slot file system by issuing the following command:

copy tftp: *tftp file location* **pclc#** *linecard* *#***-fs:**

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
SUP-PDSN#$/10.77.155.10/pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005  pclc#8-fs:
Destination filename [c6svc5fmwam-h1is-mz.R30_11092005]?
Accessing tftp://10.77.155.10/pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005...
Loading pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005 from 10.77.155.10 (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
[OK - 24168088 bytes]
```

```
24168088 bytes copied in 192.376 secs (125629 bytes/sec)
SUP-PDSN#
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has started>
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till upgrade
completes!!>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has succeeded>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>
SUP-PDSN#
```

Step 3 Now boot the MWAM card back to partition 4, the processor comes back as standby unit, and you have an upgraded image on standby PDSN controller.

```
SUP-PDSN#hw-module module 8 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-PDSN#
Nov 10 18:10:34.831: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:10:34.831: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:10:57.387: SP: PC shutdown completed for module 8
Nov 10 18:10:57.391: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:12:13.370: SP: OS_BOOT_STATUS(8) MWAM
Nov 10 18:14:30.447: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:14:30.434: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:14:31.293: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
```

Step 4 Verify that all the bindings serviced by the active PDSN controller running the YF image have been synched with the newly brought up standby PDSN controller running R3.0 PDSN image. The same can be verified by issuing the following show command on Active and Standby PDSN controller.

```
7600a-cont2# show cdma pdsn cluster controller member load

Secs until   Seq seeks         Member
(past) seek    no reply      IPv4 Addr      State   Load   Sessions
-------------------------------------------------------------------
          2       0         20.20.10.2      ready      0          15
          8       0         20.20.10.1      ready      0          15
-------------------------------------------------------------------
                   Controller IPv4 Addr   20.20.101.105


7600a-cont2# show cdma pdsn cluster controller session count
         30 session records
```

Step 5 Bring down the active PDSN Controller with the YF-based image. The newly upgraded standby PDSN controller (running R3.0-based PDSN image) becomes the active unit.

Step 6 Perform steps 1 through 3 as described above.

Step 7 Verify that all the bindings serviced using the active PDSN controller running R3.0 image have been synced with the newly enabled standby PDSN controller running R3.0 PDSN image. The same can be verified by issuing the following show command on active and standby PDSN controller.

```
7600a-cont1#show cdma pdsn cluster controller member load

Secs until   Seq seeks         Member
(past) seek    no reply      IPv4 Addr      State   Load   Sessions
---------------------------------------------------------------------
          2       0         20.20.10.2      ready      0          15
          8       0         20.20.10.1      ready      0          15
---------------------------------------------------------------------
                    Controller IPv4 Addr   20.20.101.105


7600a-cont1# show cdma pdsn cluster controller session count
        30 session records
```

Note We recommend that you remove the "HSRP Preemption" configuration between the active and standby PDSN Controller before proceeding with the Upgade/Downgrade Procedure.

Note The downgrade process is similar to the upgrade process, where the SUP image should be downgraded first, followed by the PDSN image.

Note If config-on-SUP mode (mwam config-mode supervisor) is used on MWAM, the startup configuration is written on the SUP. This will assist you in upgrading/downgrading the images without losing the PDSN configuration between the YF and R3.0 images.

Upgrading the Member PDSN on MWAM:

To upgrade to the R3.0-based image on the PDSN, perform the following procedure:

Step 1 In PDSN cluster environment you can segregate a member PDSN out of the cluster by configuring the following command on the member PDSN, so that no new request from mobile node are entertained by this member:

```
7600a-pdsn1(config)# cdma pdsn cluster member prohibit administratively
```

The calls, which are already connected to the member, will be alive until the mobile node disconnects the call. Alternatively, the calls can be forcibly cleared on the prohibited member using the following command:

```
7600a-pdsn1(config)# clear cdma pdsn session all
```

Step 2 Now bring down the PDSN Loaded with YF based image, by issuing the **hw-module module** *slot #* reset **cf:1** command on Supervisor.

Log onto the supervisor and boot the MP partition on the PC.

```
SUP-PDSN# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-HA#
```

```
SUP-HA#
Nov 10 18:01:29.624: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:01:29.624: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:01:55.252: SP: PC shutdown completed for module 8
Nov 10 18:01:55.256: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:04:00.195: SP: OS_BOOT_STATUS(8) MP OS Boot Status: finished booting
Nov 10 18:04:42.299: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:04:42.271: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:04:43.143: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
SUP-PDSN#
```

Step 3 Once the module is online, copy the R3.0 image to pclc# slot file system by issuing the following command:

copy tftp: *tftp file location* pclc# linecard #-fs:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
SUP-PDSN#$/10.77.155.10/pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005  pclc#8-fs:
Destination filename [c6svc5fmwam-h1is-mz.R30_11092005]?
Accessing tftp://10.77.155.10/pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005...
Loading pdsn/images/c6svc5fmwam-h1is-mz.R30_11092005 from 10.77.155.10 (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
[OK - 24168088 bytes]

24168088 bytes copied in 192.376 secs (125629 bytes/sec)
SUP-PDSN#
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has started>
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till upgrade
completes!!>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has succeeded>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>
SUP-PDSN#
```

Step 4 Now boot the MWAM card back to partition 4, the processor comes back online, and you have an upgraded image on PDSN.

```
SUP-PDSN#hw-module module 8 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-PDSN#
Nov 10 18:10:34.831: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:10:34.831: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:10:57.387: SP: PC shutdown completed for module 8
Nov 10 18:10:57.391: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:12:13.370: SP: OS_BOOT_STATUS(8) MWAM
Nov 10 18:14:30.447: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
```

```
Nov 10 18:14:30.434: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:14:31.293: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
```

Step 5 Join the member PDSN with the cluster environment by configuring the following command on the member PDSN, so that the controller can direct new incoming request to this member PDSN as well.

```
7600a-pdsn1(config)# no cdma pdsn cluster member prohibit administratively
```

Note The downgrade process is similar to the upgrade process, where the SUP image should be downgraded first followed by the PDSN image. Additionally, ensure all session redundancy specific configuration on PDSN was removed before downgrading to the YF-based image.

Note If config-on-SUP mode (mwam config-mode supervisor) is used on MWAM, the startup configuration is written on SUP. This will assist you in upgrading/downgrading the images without losing the PDSN configuration between YF and R3.0 images.

Changing Configuration on R3.0 PDSN in a Live Network:

If you need to change the working configuration on a PDSN in a live network environment, perform the following procedure:

Step 1 Bring the standby PDSN out of service. An example would be to unconfigure the **cdma pdsn redundancy** command on the standby PDSN. This isolates the standby PDSN from the session redundancy setup.

```
7600a-Stdy(config)# no cdma pdsn redundancy
```

Step 2 Perform a “write memory” so that running configuration is saved.

Step 3 Now make the necessary configuration changes on the standby PDSN, and save the configuration.

Step 4 Re-configure the **cdma pdsn redundancy** command, and save the configuration.

Step 5 Issue the **reload** command to bring the standby PDSN back into the session redundancy setup with the changed configuration. Verify the processor comes back in the SR setup using the following show commands:

```
7600a-Stdy#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Gi0/0.101   300 110    Standby  20.20.101.10    local           20.20.101.101

7600a-Stdy# show cdma pdsn redundancy
CDMA PDSN Redundancy is enabled

CDMA PDSN Session Redundancy system status
  PDSN state = STANDBY HOT
  PDSN-peer state = ACTIVE

CDMA PDSN Session Redundancy Statistics
  Last clearing of cumulative counters never
                       Total              Current
                 Synced from active      Connected
  Sessions                15                   15
```

```
  SIP Flows               15                    15
  MIP Flows               0                     0
PMIP Flows               0                     0

7600a-Stdy#show redundancy inter-device
Redundancy inter-device state: RF_INTERDEV_STATE_STDBY
  Scheme: Standby
      Groupname: pdsn-rp-sr1 Group State: Standby
  Peer present: RF_INTERDEV_PEER_COMM
  Security: Not configured

7600a-Stdy#show redundancy states
my state = 8  -STANDBY HOT
     peer state = 13 -ACTIVE
           Mode = Duplex
        Unit ID = 0

     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 9
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

7600a-Stdy#
```

Step 6 Now make the standby PDSN to takeover as active by reloading the current active PDSN.

Note Some outage might occur while performing this step concerning existing calls on the active PDSN (which is being taken out of service), when synched with newly active unit because of change in configuration.

Step 7 Perform Step 1 to Step 5 on current standby PDSN.

Note Configurations on the active and standby should be the same for PDSN SR to work properly.

Note We recommend that you disable the "HSRP preemption" configuration on the active and standby PDSN before proceeding with the configuration changes.

Loading the IOS Image to the MWAM

The image download process automatically loads an IOS image onto the three Processor complexes on the MWAM. All three complexes on the card run the same version of IOS, so they share the same image source. The software for MWAM bundles the images it needs in flash memory on the PC complex. For more information, refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note*.

Limitations

There are specific limitations and restrictions when loading an IOS image on the MWAM; please find them at the following URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_release_note09186a00803b8dd5.html#wp70466

Configuring the PDSN Image

The Cisco PDSN can provide four classes of user services: Simple IP, Simple IP with VPDN, Mobile IP, and proxy Mobile IP. The following sections describe the configuration tasks for implementing Cisco PDSN. Each category of tasks indicates whether the tasks are optional or required.

R-P Interface Configuration Tasks (Required for all classes of user services)

The following tasks establish the R-P interface, also referred to as the A10/A11 interface. Configuring the R-P interface is required in all 7200 platform configuration scenarios.

To configure the R-P interface, complete the following tasks:

- Enabling PDSN Services
- Creating the CDMA Ix Interface
- Creating a Loopback Interface
- Creating a Virtual Template Interface and Associating It With the PDSN Application
- Enabling R-P Interface Signaling

User Session Configuration Tasks (Optional)

To configure the user session, complete the following task.

- Configuring User Session Parameters

Session Redundancy Configuration Tasks

To configure Session Redundancy on the PDSN, complete the following tasks:

- Configuring HSRP
- Enabling HSRP and Configuring an HSRP Master Group
- Configuring Follow Groups
- Enabling Inter-Device Redundancy
- Configuring the Inter-Device Communication Transport
- Using the Loopback Interface For the PDSN-AAA Server Interface

AAA and RADIUS Configuration Tasks (Required for All Scenarios)

To configure the AAA and RADIUS in the PDSN environment, complete the following tasks.

- Configuring AAA in the PDSN Environment
- Configuring RADIUS in the PDSN Environment

Prepaid Configuration Tasks

- Configuring Prepaid in the PDSN Environment

VPDN Configuration Tasks (Required for Simple IP with VPDN Scenario)

To configure the VPDN in the PDSN environment, complete the following task:

- Enabling VPDN in a PDSN Environment

Mobile IP Configuration Tasks (Required for Mobile IP)

To configure Mobile IP on the PDSN, complete the following task:

- Configuring the Mobile IP FA
- Configuring IS835-B IPSec for the Cisco PDSN
- Configuring Mobile IP Security Associations
- Enabling Network Management

PDSN Selection Configuration Tasks (Optional)

To configure PDSN selection, complete the following tasks:

- Configuring PDSN Cluster Controller
- Configuring PDSN Cluster Member
-

Network Management Configuration Tasks (Required for Network Management in Any Scenario)

To configure network management, complete the following task:

- Enabling Network Management

Other Configuration Tasks

The following tasks are optional on the PDSN:

- Configuring Always On Service
- Configuring A11 Session Updates
- Configuring SDB Indicator Marking
- Configuring SDB Indicator Marking for PPP Control Packets
- Configuring On Demand Address Pools
- Configuring PoD on the PDSN (RADIUS Disconnect)
- Configuring Mobile IP Resource Revocation on the PDSN
- Configuring Closed-RP Interfaces
- Configuring Short Data Burst Flagging
- Configuring PDSN Accounting Events
- Configuring CDMA RADIUS Attributes

Tuning, Verification, and Monitoring Tasks (Optional)

To tune, verify, and monitor PDSN elements, complete the following tasks:

- Monitoring and Maintaining the PDSN

Enabling PDSN Services

To enable PDSN services, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# service cdma pdsn`	Enables PDSN services.

Creating the CDMA Ix Interface

To create the CDMA Ix interface, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# interface cdma-Ix1`	Defines the CDMA virtual interface for the R-P interface.
`Router(config-if)# ip address` *ip-address mask*	Assigns an IP address and mask to the CDMA-Ix virtual interface. This IP address will be used by the RAN to communicate with the PDSN.

Creating a Loopback Interface

We recommend that you create a loopback interface and then associate the loopback interface IP address to the virtual template, rather than directly configuring an IP address on the virtual template.

To create a loopback interface, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# interface loopback` *number*	Creates a loopback interface. A loopback interface is a virtual interface that is always up.
`Router(config-if)# ip address` *ip-address mask*	Assigns an IP address to the loopback interface.

Creating a Virtual Template Interface and Associating It With the PDSN Application

Creating a virtual template interface allows you to establish an interface configuration and apply it dynamically.

To create a virtual template interface that can be configured and applied dynamically, use the following commands in global configuration mode:

Command	Purpose
`Router(config) interface virtual-template` *number*	Creates a virtual template interface.
`Router(config-if)# ip unnumbered loopback` *number*	Assigns the previously defined loopback IP address to the virtual template interface.
`Router(config-if)# ppp authentication chap pap optional`	Enables PPP authentication.
`Router(config-if)# ppp accounting none`	Disables PPP accounting to enable 3GPP2 accounting.

Command	Purpose
Router(config-if)# **ppp accm** *0*	Specifies the transmit ACCM table value. The value must be specified as 0.
Router(config-if)# **ppp timeout idle** *value*	Specifies the PPP idle timeout.
Router(config-if)# **exit**	Exit interface configuration mode.
Router(config)# **cdma pdsn virtual-template** *virtual-template-num*	Associates a virtual template with the PDSN application.

Enabling R-P Interface Signaling

To enable the R-P interface signaling, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **cdma pdsn secure pcf** *lower_addr* [*upper_addr*] **spi** {*spi_val* | [**inbound** *in_spi_val* **outbound** *out_spi_val*]} **key** {**ascii** | **hex**} *string*	Defines the PCF security association on the PDSN.
Router(config)# **cdma pdsn a10 max-lifetime** *seconds*	Specifies the maximum lifetime the PDSN accepts in A11 registration requests from the PCF.
Router(config)# **cdma pdsn a10 gre sequencing**	Enables inclusion of per-session Generic Routing Encapsulation (GRE) sequence numbers in the outgoing packets on the A10 interface. (This is the default behavior.)
Router(config)# **cdma pdsn retransmit a11-update** *number*	Specifies the maximum number of times an A11 Registration Update message will be re-transmitted.
Router(config)# **cdma pdsn timeout a11-update** *seconds*	Specifies A11 Registration Update message timeout value.
Router(config)# **cdma pdsn maximum pcf** *number*	Specifies the maximum number of packet control functions (PCF) that can be connected to the PDSN at one time.

Configuring User Session Parameters

To configure user session parameters, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **cdma pdsn maximum sessions** *maxsessions*	Specifies the maximum number of mobile sessions allowed on a PDSN.
Router(config)# **cdma pdsn ingress-address-filtering**	Enables ingress address filtering.
Router(config)# **cdma pdsn msid-authentication** [**imsi** *number*] [**min** *number*] [**irm** *number*] [**profile-password** *password*]	Enables provision of Simple IP service using MSID-based authentication.
Router(config)# **cdma pdsn timeout mobile-ip-registration** *timeout*	Specifies the number of seconds before which Mobile IP registration should occur for a user who skips PPP authentication.

Configuring PDSN Session Redundancy Infrastructure

The PDSN-SR feature uses the Cisco IOS Check-point Facility (CF) to send stateful data over Stream Control Transmission Protocol (SCTP) to a redundant PDSN. Additionally, in conjunction with Cisco IOS HSRP, the PDSN uses the Cisco IOS Redundancy Facility (RF) to monitor and report transitions on Active and Standby PDSNs.

Before configuring PDSN-SR, you need to configure the inter-device redundancy infrastructure.

Configuring HSRP

The Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts on networks without relying on the availability of any single router. HSRP is used in a group of routers for selecting an Active router and a Standby router. HSRP monitors both the inside and outside interfaces so that if any interface goes down, the whole device is deemed to be down and the Standby device becomes active and takes over the responsibilities of an Active device.

When configuring HSRP, note that the following recommendation and restrictions apply:

- At minimum, HSRP must be enabled and an HSRP a “master” group defined on one interface per PDSN instance. A “follow” group can be configured on all other PDSN interfaces using the **standby interface** configuration command with the **follow** keyword option specified. The advantages of using follow groups are:
  - The follow group feature enables all interfaces on which it is configured to share the HSRP parameters of the master group.
  - Interfaces that share the same group will follow the state of master interface and will use same priority as master interface. This will ensure that all interfaces are in the same HSRP state. Otherwise there is a possibility of one or more interfaces to assume another role than the master HSRP interface.
  - This optimizes HSRP group number and minimizes the configuration and maintenance overhead when having large configurations.
  - It eliminates unnecessary network traffic over all interfaces by eliminating HSRP Hello messages from follow groups, if configured.

Note Do not configure a preemption delay on the Standby PDSN using the **standby preempt** interface configuration command.

- When the **standby use-bia** command is not used to allow bridge and gateways to learn the virtual MAC address, for optimization purposes, configure the **standby mac-refresh** command to a value greater than the default (hello messages are sent every 10 seconds) under the main interface (gig0/0). This value is used as the hello message interval.

Note If **standby use-bia** is configured, then there will be no hello messages sent out of follow group interfaces. It is recommended to use **standby use-bia** unless explicitly required not to configure.

- An ARP multicast packet is sent out when there is a HSRP state change to Active. ARP requests for follow group virtual IP address are responded if HSRP state is Active. Also an ARP multicast is sent on the follow group VLAN when a slave virtual IP address is configured and if the master group is Active.

Use the same group number for each PDSN follow group as is defined for the primary group. Using the same group number for the primary and follow groups facilitates HRSP group setup and maintenance in an environment that contains a large number of PDSN interfaces and HRSP groups.

More information on HSRP configuration and HSRP groups can be found here:

http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html

and

http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_configuration_example09186a0080094e90.shtml

Enabling HSRP and Configuring an HSRP Master Group

To enable HSRP on an interface and configure the primary group, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# standby [group-number] ip [ip-address [secondary]]`	Enables the HSRP on the interface.
`Router(config-if)# standby [group-number] priority priority`	Sets the Hot Standby priority used in choosing the active router. The priority value range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. Specify that, if the local router has priority over the current active router, the local router should attempt to take its place as the active router.
`Router(config-if)# standby [group-number] name name`	Specifies the name of the standby group.
`Router(config-if)# standby use-bia [scope interface]`	(Optional) Configures HSRP to use the burned-in address of an interface as its virtual MAC address instead of the preassigned MAC address.

Configuring Follow Groups

HSRP follow groups are configured to share the HSRP parameters of the primary group by defining a follow group on the interface using the standby interface configuration command with the follow keyword option specified. Interfaces that share a group track states together and have the same priority.

To configure an interface to follow a primary group, use the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# standby group-number follow group-name`	Specifies the number of the follow group and the name of the primary group to follow and share status. **Note** It is recommended that the group number specified is the same as the primary group number.
`Router(config-if)# standby group-number ip virtual-ip-address`	Specifies the group number and virtual IP address of the follow group. **Note** The group number specified above should be same as the master group number.

Enabling Inter-Device Redundancy

To enable inter-device redundancy, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# redundancy inter-device`	Configures redundancy and enters inter-device configuration mode. To remove all inter-device configuration, use the **no** form of the command.
`Router(config-red-interdevice)# scheme standby standby-group-name`	Defines the redundancy scheme that is to be used. Currently, **standby** is the only supported scheme. *standby-group-name*-Must match the standby name specified in the standby name interface configuration command (see the "Configuring HSRP" section). Also, the standby name should be the same on both PDSNs.
`Router(config-red-interdevice)# exit`	Returns to global configuration mode.

Configuring the Inter-Device Communication Transport

Inter-device redundancy requires a transport for communication between the redundant PDSNs. This transport is configured using Interprocess Communication (IPC) commands.

To configure the inter-device communication transport between the two PDSNs, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ipc zone default`	Configures the Inter-device Communication Protocol (IPC) and enters IPC zone configuration mode. Use this command to initiate the communication link between the Active device and the Standby device.
`Router(config-ipczone)# association 1`	Configures an association between two devices and enters IPC association configuration mode. In IPC association configuration mode, you configure the details of the association, such as the transport protocol, local port and local IP addresses, and the remote port and remote IP addresses. Valid association IDs range from 1 to 255. There is no default value.
`Router(config-ipczone)# no shutdown`	Restarts a disabled association and its associated transport protocol. **Note** Shutdown of the association is required for any changes to the transport protocol parameters.
`Router(config-ipczone-assoc)# protocol sctp`	Configures Stream Control Transmission Protocol (SCTP) as the transport protocol for this association and enables SCTP protocol configuration mode.
`Router(config-ipc-protocol-sctp)# local-port` *local_port_num*	Defines the local SCTP port number to use to communicate with the redundant peer and enables IPC Transport-SCTP local configuration mode. Valid port numbers range from 1 to 65535. There is no default value. **Note** The local port number should be the same as the remote port number on the peer router.
`Router(config-ipc-local-sctp)# local ip` *ip_addr*	Defines the local IP address that is used to communicate with the redundant peer. The local IP address must match the remote IP address on the peer router.

Command	Purpose
`Router(config-ipc-local-sctp)# keepalive [period [retries]]`	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets with a response before bringing down the interface or tunnel protocol for a specific interface. Valid value for period is an integer value in seconds great than 0. The default is 10. Valid value for retries is an integer value greater than one and less than 355. The default is the previously used value or 5 if there was no value previously specified.
`Router(config-ipc-local-sctp)# retransmit-timeout interval`	Configures the message retransmission time. Valid range is 300 to 60000 milliseconds. The minimum default is 1000. The maximum default is 60000.
`Router(config-ipc-local-sctp)# path-retransmit number`	Configures the maximum number of keep-alive retries before the corresponding destination address is marked inactive. Valid range is 2 to 10. The default is 5.
`Router(config-ipc-local-sctp)# assoc-retransmit number`	Defines the maximum number of retransmissions over all destination addresses before an association is declared failed. Valid range is 2 to 20. The default is 10.
`Router(config-ipc-local-sctp)# exit`	Exits IPC transport - SCTP local configuration mode.
`Router(config-ipc-protocol-sctp)# remote-port port_nun`	Defines the remote SCTP port that is used to communicate with the redundant peer and enables IPC Transport-SCTP remote configuration mode. Valid port numbers range from 1 to 65535. There is no default. **Note** The remote port number should be the same as the local port number on the peer device.
`Router(config-ipc-remote-sctp)# remote-ip ip_addr`	Defines the remote IP address of the redundant peer that is used to communicate with the local device. All remote IP addresses must refer to the same device. To remove an association configuration, use the **no** form of the command.

Using the Loopback Interface For the PDSN-AAA Server Interface

To ensure that the AAA server views the active and standby units as a single NAS, the same NAS IP address should be used by both the units. Now, the NAS IP Address can be configured for the PDSN using the **ip radius source-interface** command. When configured, the IP address of that interface is used as the NAS IP Address.

However, the CLI does not support virtual IP addresses (HSRP). As a result, the only way to ensure that both the units appear as a single NAS is to configure a loopback interface, and use that interface as the source-interface. In short, the CLI would look something like:

ip radius source-interface Loopback1

Configuring Application Tracking to Handle active-active Situation

Command	Purpose
`Router(config) # track` *object-id* **application pdsn**	Defines a tracking object for PDSN application.
`Router(config-if) # standby track` *object-id* [**decrement** *priority*]	Associates the tracking object defined for PDSN with the HSRP config. HSRP would start tracking the state of this object. The configured decrement priority is used to change HSRP priority based on the state of the tracking object. If the tracking object if "UP", HSRP will have the configured priority. When the tracking object is "DOWN", HSRP decrements its priority by the **decrement** *priority* specified in the **standby track** command.

Configuring AAA in the PDSN Environment

Access control is the way you manage who is allowed access to the network server and the services they are allowed to use. AAA network security services provide the primary framework through which you set up access control on your router or access server. For detailed information about AAA configuration options, refer to the "Configuring Authentication," and "Configuring Accounting" chapters in the *Cisco IOS Security Configuration Guide*.

To configure AAA in the PDSN environment, use the following commands in global configuration mode:

Command	Purpose
`Router(config)#` **aaa new-model**	Enables AAA access control.
`Router(config)#` **aaa authentication ppp default group radius**	Enables authentication of PPP users using RADIUS.
`Router(config)#` **aaa authorization configuration default group radius**	Enables Network Access Identifier (NAI) construction in the absence of CHAP.
`Router(config)#` **aaa authorization config-commands**	Re-establishes the default created when the **aaa authorization commands** *level method1* command was issued.

Command	Purpose
`Router(config)# aaa authorization network if-authenticated default group radius`	Restricts network access to a user. Runs authorization for all network-related service requests. Uses the group radius authorization method as the default method for authorization.
`Router(config)# aaa accounting update periodic` *minutes*	Enables an interim accounting record to be sent periodically to the accounting server. The recommended period of time is 60 minutes.
`Router(config)# aaa accounting network pdsn start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

Configuring RADIUS in the PDSN Environment

RADIUS is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information. For detailed information about RADIUS configuration options, refer to the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*.

To configure RADIUS in the PDSN environment, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# radius-server host` *ip-addr* `key` *sharedsecret*	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.
`Router(config)# radius-server vsa send accounting 3gpp2`	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor-specific attributes to only accounting attributes.
`Router(config)# radius-server vsa send authentication 3gpp2`	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor-specific attributes to only authentication attributes.
`Router(config)# radius-server attribute 55 include-in-acct-req`	Enables sending G4 (Event Time) Accounting-Start from PDSN.

Configuring Prepaid in the PDSN Environment

For the 1.2 release of the Cisco PDSN software, to configure prepaid, ensure that you include crb-entity-type=1 in the user profile.

In Cisco PDSN release 2.0 and above, to configure IS835C Prepaid, use the following commands in global configuration mode:

Command	Purpose

`router (config)# cdma pdsn accounting prepaid ?`
`  duration`
`  threshold`
`  volume`
	
	Prepaid service based on duration.
	Configure threshold percentage per quota.
	Prepaid service based on volume.

Enabling VPDN in a PDSN Environment

To configure VPDN in the PDSN environment, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# vpdn enable`	Enables VPDN.
`Router(config)# vpdn authen-before-forward`	Specifies to authenticate a user locally before tunneling.

For more information about VPDNs, refer to the Cisco IOS Release 12.3 documentation modules *Cisco IOS Dial Services Configuration Guide: Network Services* and *Cisco IOS Dial Services Command Reference*.

Configuring the Mobile IP FA

Mobile IP operation (as specified by TR-45.6) requires the ability to authenticate a mobile station through a challenge/response mechanism between the PDSN (acting as an FA) and the mobile station.

To configure the Mobile IP FA, use the following commands in global and interface configuration modes:

Command	Purpose
`Router(config)# router mobile`	Enables Mobile IP. This and other Mobile IP commands are used here to enable R-P signaling. They are required regardless of whether you implement Simple IP or Mobile IP.
`Router(config)# cdma pdsn send-agent-adv`	Enables agent advertisements to be sent over a newly formed PPP session with an unknown user class that negotiates IPCP address options.
`Router(config) interface virtual-template number`	Creates a virtual template interface.
`Router(config-if)# cdma pdsn mobile-advertisement-burst {[number value] | [interval msec]}`	Configures the number of FA advertisements to send and the interval between them when a new PPP session is created.
`Router(config-if)# ip mobile foreign-service challenge {[timeout value] | [window num]}`	Configure the challenge timeout value and the number of valid recently-sent challenge values.
`Router(config-if)# ip mobile foreign-service challenge forward-mfce`	Enables the FA to send mobile foreign challenge extensions (MFCE) and mobile node-AAA authentication extensions (MNAE) to the HA in registration requests.
`Router(config-if)# ip mobile registration-lifetime seconds`	Configures the maximum Mobile IP registration lifetime.
`Router(config-if)# ip mobile foreign-service [reverse-tunnel [mandatory]]`	Enables Mobile IP FA service on this interface.
`Router(config-if)# ip mobile foreign-service registration`	Sets the R bit in an Agent Advertisement.

To reduce the virtual-access cloning time in order to increase the CPS rate on a standalone PDSN on a Cisco 7200 router, use the following per interface configurations in global configuration mode:

Command	Purpose
`Router(config)# ip mobile foreign-service`	Enables foreign agent service on an interface if care-of addresses are configured
ip mobile prefix-length	Appends the prefix-length extension to the advertisement.
ip mobile registration-lifetime	Sets the registration lifetime value advertised.
`Router(config)# ip mobile foreign-service challenge`	(Optional) Configures the foreign agent challenge parameters.
home-access allowed	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99.
limit	(Optional) Number of visitors allowed on the interface. The Busy (B) bit will be advertised when the number of registered visitors reaches this limit.
registration-required	(Optional) Solicits registration from the mobile node even if it uses collocated care-of addresses. The Registration-required (R) bit will be advertised.
reverse-tunnel	(Optional) Enables reverse tunneling on the foreign agent. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

The CPS on a standalone PDSN on a Cisco 7200 Internet Router should improve to 100 CPS from the current number of 40.

Configuring IS835-B IPSec for the Cisco PDSN

To configure IS835-B IPSec for the PDSN, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# Router(config)# ip mobile cdma ipsec`	Enables or disables the CDMA IPSec feature. This is only present in crypto images for the Cisco 7200 Series Internet router, and non-crypto images for the Cisco MWAM. The Crypto Map definition is not complete until: 1. ACL associated with it is defined, and 2. The Crypto-Map applied on Interface. You can configure Crypto MAP for different HAs by using a different sequence number for each HA in one crypto-map set.
`Router(config)# ip mobile cdma ipsec profile` *profile-tag*	Converts Crypto Map into a template that can be used to setup an identical policy dynamically. This command is only present in crypto images for the Cisco 7200 Series Internet router. It is assumed that crypto-profile has been created earlier. Basically, crypto-map has been marked as profile by the **crypto map** *Tag_1 Seq_No* **ipsec-isakmp profile** *Tag_2* command. In this command *Tag_2* is profile name, and this will be entered using this CLI.

Here is an example configuration for the IS835-B based IPSec feature:

```
Router(config)#crypto isakmp policy 1
                        authentication pre-share
Router(config)#crypto isakmp key cisco address 7.0.0.2
Router(config)#crypto ipsec transform-set mobile-set1 esp-3des
Router(config)#crypto ipsec profile testprof
                        set transform-set mobile-set1
Router(config)#crypto identity pdsntest
Router(config)#ip mobile cdma ipsec
Router(config)# ip mobile cdma ipsec  profile testprof
Router(config)#ip mobile foreign-agent reg-wait 30
```

Configuring Proxy Mobile IP Attributes Locally

As an alternative to true Mobile IP, which is not supported by all mobile devices, you can configure the Cisco PDSN to provide many of the benefits of Mobile IP through the use of proxy Mobile IP. All proxy Mobile IP attributes can be retrieved from the AAA server. To configure proxy Mobile IP attributes locally, use the following command in global configuration mode:

Command	Purpose
Router(config)# **ip mobile proxy-host nai** *username@realm* [**flags** *rrq-flags*] [**ha** *homeagent*] [**homeaddr** *address*] [**lifetime** *value*] [**local-timezone**]	Specifies proxy Mobile IP attributes locally on the PDSN.

Configuring Mobile IP Security Associations

To configure security associations for mobile hosts, FAs, and HAs, use one of the following commands in global configuration mode:

Command	Purpose
Router(config)# **ip mobile secure** {**aaa-download** | **visitor** | **home-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key** {**hex** | **ascii**} *string* [**replay timestamp** [*number*] **algorithm md5 mode prefix-suffix**]	Specifies the security associations for IP mobile users.
Router(config)# **ip mobile secure proxy-host nai** *string* **spi** *spi* **key** {**ascii** | **hex**} *string*	Specifies the security associations for proxy Mobile IP users.

Configuring PDSN Cluster Controller

To configure the PDSN Cluster Controller attributes locally, use the following commands in global configuration mode.

Note These commands have no effect if the router supports PDSN member functionality from a prior configuration.

Command	Purpose
Router(config)# **cdma pdsn secure cluster default spi** *spi number* [**key** ascii | hex *value*]	Configures one common security association for all PDSNs in a cluster.
Router #cdma **pdsn cluster controller interface** *interface name*	Enables the controller functionality for PDSN Controller/Member clustering, specifies which interface to send messages to and from
Router# **cdma pdsn cluster controller standby** *cluster-name*	Configures the PDSN to operate as a cluster controller in standby.

Configuring PDSN Cluster Member

To configure the PDSN Cluster Member attributes locally, use the following commands in global configuration mode:

Note These commands have no effect if the router supports PDSN member functionality from a prior configuration.

Configuring Peer-to-Peer PDSN Selection

Command	Purpose
`Router(config)# cdma pdsn secure cluster default spi` *spi_index* [**key ascii** | **hex** *value*]	Configures one common security association for all PDSNs in a cluster.
`Router(config)# cdma pdsn cluster member controller` *ipaddr*	Configures the PDSN to operate as a cluster member.
`Router(config)# cdma pdsn cluster member interface` *interface name*	Configures the PDSN to operate as a cluster member.

A group of Cisco PDSNs can be configured to exchange session information with one another when needed. When a session request is received by the PDSN, it not only checks its own session list for the existence of a session, it also checks the lists of the PDSNs within its group. If a session exists in the group, the Mobile IP registration message for the session is rejected, and an alternate PDSN is recommended. The BSC/PCF can then establish session with the recommended PDSN.

To configure PDSN selection and PDSN load balancing, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# cdma pdsn selection interface` *interface_name*	Configures the interface be used to send and receive PDSN selection messages.
`Router(config)# cdma pdsn selection session-table-size` *size*	Enables the PDSN selection feature and defines the size of the session table.[1]
`Router(config)# cdma pdsn selection load-balancing` [**threshold** *val* [**alternate**]]	Enables the load balancing function of PDSN selection. The Alternate option alternately suggests two other PDSNs with the least load.
`Router(config)# cdma pdsn selection keepalive` *value*	Specifies the length of time to track a PDSN that is not responding.
`Router(config)# cdma pdsn secure cluster default spi` {*spi_val* | [**inbound** *inspi_val* **outbound** *outspi_val*]} **key** {**ascii**|**hex**} *string*	Specifies the default mobility security associations for all PDSNs in a cluster, as well as inbound and outbound spi values.

1. You must issue the **cdma pdsn selection session-table-size** command before you issue the **cdma pdsn selection load-balancing** command.

Enabling Network Management

To enable SNMP network management for the PDSN, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **snmp-server community** *string* [**ro** | **rw**]	Specifies the community access string to permit access to the SNMP protocol.
Router(config)# **snmp-server enable traps cdma**	Enables network management traps for CDMA.
Router(config)# **snmp-server host** *host-addr* **traps version** {**1** | **2** | **3** [**auth** | **noauth** | **priv**]}	Specifies the recipient of an SNMP notification operation.
Router(config)# **cdma pdsn failure-history** *entries*	Specifies the maximum number of entries that can be maintained in the SNMP session failure table.
Router(config)#**no virtual-template snmp**	Prevents the virtual-access subinterfaces from being registered with the SNMP functionality of the router and reduces the amount of memory being used, thereby increasing the call setup performance.

Configuring Always On Service

Always On service maintains the subscriber's packet data session in the local network. The PDSN will not initiate release of the subscriber's packet data session due to PPP idle timer expiry, unless the PDSN determines the user is no longer reachable. The Always On feature is enabled by default. To change the default parameters related to this feature, use following command:

Command	Purpose
Router(config)# **cdma pdsn a10 always-on keepalive** {**interval** *1-65535* [**attempts** *0-255*] | **attempts** *0-255*}	Configures always-on service parameters on the PDSN. The **keepalive interval** is the duration in seconds, for which the PDSN waits for the LCP echo response from peer before sending next LCP echo. The default value is 3seconds. The **no** form of this command will return to the default value. **attempts** is the number of times LCP echo must be sent before declaring an always-on user is not reachable for tearing down the session after the idle timer expires. The default value is 3. Configuring this variable to 0 is similar to ignoring the always-on property for the user.

Configuring A11 Session Updates

A11 Session Update messages are sent from the PDSN to the PCF to add, change, or update session parameters for an A10 connection. To enable the A11 Session Update feature, perform the following tasks:

Command	Purpose
Router(config)# **cdma pdsn a11 session-update** {[**always-on**] *1-10* [**rn-pdit**] *0-9*}	Enables the A11 Session update feature on the PDSN, and sends an A11 session update for either the Always On, or RNPDIT (or both) attributes that are downloaded from the AAA during the authentication phase. The default timeout value is 3 seconds. The default retransmit number is 3.
Router#**cdma pdsn retransmit a11-update** *number*	Specifies the maximum number of times an A11 Registration Update message is retransmitted. Possible values are 0 through 9. The default is 5 retransmissions.

Configuring SDB Indicator Marking

This feature supports short data burst applications, such as SIP signaling for PTT applications, and proposes the interaction with the PDSN. SIP is used by PTT applications to signal a PTT call. The message is short and needs to be delivered to the end-user. The Short Data Burst support on the RAN can be used to send these to the end-user, especially when the messages are to be terminated to the mobile. This is especially important when the mobile user is actually dormant. Use the following command to configure SDB Indicator Marking:

Command	Purpose
Router(config)# **cdma pdsn a11 dormant sdb-indication gre-flags** *group-number*	The *group-number* represents the classified match criteria. All packets that are set with the specific group-number will be flagged for SDB usage between the PCF and the PDSN. The B bit (SDB indication) would be set for packets matching the sdb-indication group-number.

Configuring SDB Indicator Marking for PPP Control Packets

While data packets can be sent towards the mobile using SDBs as shown above, SDBs can also be used for delivering PPP control packets. This can be particularly helpful for Always-On sessions, where the session is dormant. Basically, with Always On configured, the PDSN sends out LCP echo requests (and waits for LCP echo replies) to keep the session alive. Hence, when such a session goes dormant, a data channel needs to be setup to deliver these LCP echo requests to the MN. The other option is to use SDBs to deliver the LCP echo requests without setting up a data channel.

Use the following CLI in conjunction of the above CLI to enable this feature:

Command	Purpose
`Router(config)# cdma pdsn a11 dormant sdb-indication match-qos-group` *group-number* `ppp-ctrl-pkts`	The *group-number* represents the classified match criteria.

Configuring On Demand Address Pools

To configure the DHCP Server with the ODAP Subnet Allocation Server, perform the following configuration tasks. This configuration can be either on a PDSN Cluster Controller or a Backup Cluster Controller.

Command	Purpose

`Router(config)# ip dhcp pool` *pdsn-pool*
 	
`network 13.0.0.0 255.248.0.0`
 	
`subnet prefix-length 20`
	Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode (identified by the config-dhcp# prompt).
	
	Specifies the subnet network number and mask of the DHCP address pool.
	
	The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
	
	Configures a subnet allocation pool and determine the size subnets that are allocated from the pool. The range is from 1 to 31.

`Router(config)# ip dhcp pool` *pdsn-pool-2*
`network 14.0.0.0 255.255.0.0`
`subnet prefix-length 24`
	Defines a second address pool.

Command	Purpose
interface GigabitEthernet 0/0.101 **encapsulation dot1Q** 101 **ip address** 10.10.1.96 255.255.255.0 **standby** 1 ip 10.10.1.16 **standby** 1 preempt **standby** 1 name 6509-cluster	Configures a Gigabit Ethernet interface and enter interface configuration mode. **encapsulation dot1Q** enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs (VLANs). **standby ip** activates the Hot Standby Router Protocol (HSRP). **standby preempt** configures Hot Standby Router Protocol (HSRP) preemption and preemption delay. **standby name** configures the name of the standby group.
router ospf *100* **log-adjacency-changes** **network** 10.10.1.0 0.0.0.255 area 0	**router ospf** configures an OSPF routing process. The *process id* is internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. Configures the router to send a syslog message when an OSPF neighbor goes up or down

The IOS DHCP Server feature is enabled by default in IOS. If it becomes disabled, use the global **service dhcp** command to re-enable the feature.

For the i**p dhcp pool pdsn-pool** command, the subnet is 13.0.0.0 and the mask defines the size of the pool. The **subnet prefix-length** defines the size of the subnet chunks using standard CIDR bit count notation to determine the number of addresses that are configured in each subnet lease. Here is a sample of the **show dhcp ip pool** command output:

```
Pool pdsn-pool :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 524288
 Leased addresses               : 4096
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 13.0.48.0            13.0.0.0  - 13.7.255.255                 4096
```

In this example, one subnet of 4096 addresses has been leased out. It is leased to PDSN1 in this example.

In the following example, a second PDSN pool is shown for reference, pdsn-pool-2. This shows different values used for the pool size and the subnet chunks. Nothing is presently leased.

```
Pool pdsn-pool-2 :
 Utilization mark (high/low)         : 100 / 0
 Subnet size (first/next)            : 0 / 0
 Total addresses                     : 65536
 Leased addresses                    : 0
 Pending event                       : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 14.0.0.0             14.0.0.0  - 14.0.255.255                 0
```

OSPF is configured to log adjacency changes for network 10.10.1.0, which is the GigEthernet 0/0.101 interface.

Currently, the ODAP Subnet Allocation Server only allows one **network** command under the **ip dhcp pool name-of-pool** command. To support disjointed subnets, you must define a pool that is large enough to contain all assigned IP addresses. You can use the following global configuration command:

ip dhcp excluded-address low-address [**high-address**]

This command informs the ODAP Subnet Allocation Server to not lease these addresses to the ODAP client. Issuing this command help some configurations with disjointed IP address space, but may not work in other cases, depending on the range of IP addresses.

Configure the following ODAP client and OSPF commands on the PDSN:

Command	Purpose
`Router(config)# ip dhcp ping packets 0 <<< disables ping test (range 0-10)`	Specifies the number of packets a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server sends to a pool address as part of a ping operation.
`ip dhcp ping timeout 100 <<< reduces ping time (range 100-10000 ms)`	Specifies how long a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server waits for a ping reply from an address pool.
`Router(config)# ip address-pool dhcp-pool <<< enables ODAP client`	Enables the ODAP client.
`ip dhcp pool pdsn-pool`	Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode (identified by the config-dhcp# prompt).
`utilization mark high`	Configures the high utilization mark of the current address pool size.
`utilization mark low 5`	Configures the low utilization mark of the current address pool size
`origin dhcp subnet size initial /20 autogrow /20 <<< config address pool as ODAP`	Configures an address pool as an on-demand address pool (ODAP).
`Router (config)# ip dhcp-server 7.0.0.96`	Specifies which Dynamic Host Configuration Protocol (DHCP) servers to use on your network.

Additionally, perform the following configuration details on the PDSN:

```
interface Loopback1
 ip address 10.11.2.92 255.255.255.255

interface CDMA-Ix1
 ip address 10.11.1.92 255.255.255.255

interface GigabitEthernet0/0.1
 encapsulation dot1Q 20
 ip address 10.0.1.1 255.255.0.0

interface GigabitEthernet0/0.301
 encapsulation dot1Q 301
 ip address 7.0.0.92 255.255.255.0
```

```
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address dhcp-pool pdsn-pool <<name of ODAP pool to use
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none

router ospf 100
 log-adjacency-changes
 redistribute connected subnets route-map MAP <<advertises CDMA-Ix interface
 redistribute static subnets <<advertises the ODAP subnets
 passive-interface Virtual-Template1 <<no OSPF updates out here
 network 10.10.1.0 0.0.0.255 area 0

access-list 11 permit 10.11.1.92
access-list 12 deny 128.0.0.0 0.0.0.255
access-list 12 permit any

route-map MAP permit 10 <<only the CDMA-Ix update gets out
 match ip address 11
 set tag 9

route-map DENY-MAP permit 10 <<blocks 128.x.x.x internal network between
 match ip address 12 <<the PC and sibytes on the MWAM card
 set tag 9
```

or

```
summary-address 128.0.0.0 255.0.0.0 not-advertise <<also blocks the 128 network
```

The **ip dhcp ping packets** 0 command will disable the ODAP client from sending a ping to determine if an address is available. The ODAP default time is 2 seconds to wait for an ICMP echo reply. This will reduce the address allocation time at the risk of detecting duplicate addresses. The **ip address-pool dhcp-pool** command enables the ODAP client on the PDSN. The pool for the PDSN to use is called *pdsn-pool*. The **origin** command tells that it is DHCP, and gives an initial size for the pool to use and a size to grow by. In this case, both the **initial** and **autogrow** are set for a subnet size of 4096. The **utilization mark** (high/low) command can be used to set a percentage of pool usage before the router will schedule a subnet request for a new subnet, or to free a subnet that is no longer being used. The name of the pool must also be configured on the Virtual-Template1 interface. Here is the output of the show command.

```
PDSN#show ip dhcp pool

Pool pdsn-pool :
 Utilization mark (high/low)     : 95 / 5
 Subnet size (first/next)        : 20 / 20 (autogrow)
 Total addresses                 : 4094
 Leased addresses                : 0
 Pending event                   : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 13.0.64.1            13.0.64.1        - 13.0.79.254       0
```

The **ip dhcp-server** *7.0.0.96* command causes DHCP requests to go to this particular DHCP Server. Otherwise Broadcast messages are sent to discover the DHCP Servers.

For OSPF, the **redistribute static subnets** command is used to aggregate the ODAP subnet routes on the SUP. The **redistribute connected subnets route-map** *MAP* command uses an access-list functionality to only allow the CDMA-Ix1 IP address to be known to the SUP. All other “connected subnets” routing updates are not sent out.

Alternatively, the **summary-address** *128.0.0.0 255.0.0.0* **not-advertise** command can be used instead of the **route-map** *DENY-MAP permit 10* command to prevent the 128.0.0.0 route from being seen. The **route-map** is similar to an access-list, so the **summary-address** command may be preferable and have less impact on processor performance.

There are additional configuration details for the Catalyst 6500 Series Switch, as well as additional commands that will assist you in configuring ODAP on the PDSN. For more information, refer to the following Cisco 12.3 IOS documentation:

- 12.3 IOS Documentation, *DHCP Server - On-Demand Address Pool Manager*
- 12.3 IOS Documentation, *Configuring DHCP (IOS IP configuration guide)*
- 12.3 IOS Documentation, *DHCP ODAP Server Support*

Configuring PoD on the PDSN

To enable the Packet of Disconnect (RADIUS Disconnect) feature on the PDSN, perform the following tasks:

Command	Purpose
`Router(config)# cdma pdsn radius disconnect`	Enables the RADIUS disconnect feature on the PDSN.
`Router(config)# aaa pod server [clients ipaddr1 [ipaddr2] [ipaddr3] [ipaddr4]] [port port-number] [auth-type {any | all | session-key}] server-key [encryption-type] string`	AAA command that enables listening for POD packets.

`Router(config)# aaa server radius dynamic-author`
`Router(config-locsvr-radius)#?`
`RADIUS Application commands:`
`  auth-type  Specify the server authorization type`
`  client  Specify a RADIUS client`
`  default  Set a command to its defaults`
`  exit  Exit from RADIUS application configuration mode`
`  ignore  Override behavior to ignore certain parameters`
`  no  Negate a command or set its defaults`
`  port  Specify port on which local radius server listens`
`  server-key  Encryption key shared with the radius clients`
	Enters RADIUS application configuration mode, and presents the user with several configuration options.

Configuring Mobile IP Resource Revocation on the PDSN

To enable resource revocation support on PDSN, perform the following task:

Command	Purpose
`Router(config)# ip mobile foreign-service revocation [timeout value] [retransmit value] [timestamp]`	**timeout** *value* is the time interval in seconds between re-transmission of resource revocation message. The wait time is between 0-100, and the default value is 3 seconds. **retransmit** *value* is the number of maximum re-transmissions of MIPv4 resource revocation messages. The number of retries for a transaction is 0-100. The default value is 3. **Note** All foreign-service configurations should be done globally and not under the virtual-template interface. **Timestamp** specifies the unit of timestamp field for revocation. The unit of timestamp value for revocation is in milliseconds.

Configuring Closed-RP Interfaces

To enable the Closed-RP feature on the PDSN, perform the following tasks:

Command	Purpose
`Router(config)# cdma pdsn pcf default closed-rp`	Enables the Closed-RP feature on the PDSN. All the PCFs connecting to the PDSN will be treated as Closed-RP PCFs. When this command is configured the 3GPP2 (Open) RP interface will be disabled on the PDSN.
`Router(config)# cdma pdsn a10 ahdlc trailer`	Enables the PDSN such that AHDLC frames are expected to contain the trailer byte. When the **no** version of the command is configured, each AHDLC frame will be considered a full AHDLC fragment, and the PDSN will start processing the packet.

VPDN Configuration
`----------`
`Router(config)#vpdn enable`
`Router(config)#vpdn authen-before-forward`
`Router(config)#vpdn ip udp ignore checksum`
`!`
`Router(config)#vpdn-group CDMA`
`Router(config-vpdn)#accept-dialin`
`Router(config-vpdn-acc-in)#protocol l2tp`
`Router(config-vpdn)#source-ip` *`CDMA-Ix IP address`*
`Router(config-vpdn)#l2tp tunnel hello` *`value`*
`Router(config-vpdn)#no l2tp tunnel authentication`
`Router(config-vpdn)#l2tp tunnel timeout no-session never`
	Enables the virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway).
	
	Configures various Layer 2 Tunneling Protocol (L2TP) tunnel variables.

`ip slb serverfarm PDSN-FARM`
 	
`ip slb vserver PDSN-SLB`
`virtual 150.150.0.100 udp 1701`
`serverfarm PDSN-FARM`
`sticky 65535 group 1 netmask 255.255.254.0`
`idle 10`
`inservice`
`!`
	Identifies a server farm, and enters server farm configuration mode.
	
	Configures the virtual server.
	
	Sticky forwards requests coming in from each subnet (PCF complex) to the same real server (PDSN instance).

Here is a sample configuration for the Closed-RP feature on the PDSN:

```
Router#sh run
Building configuration...

Current configuration : 3450 bytes
!
! Last configuration change at 04:23:40 UTC Tue May 27 2003
! NVRAM config last updated at 04:24:03 UTC Tue May 27 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname Router
!
```

```
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
ip dhcp ping packets 0
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.3 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.173 255.255.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.3 255.0.0.0
!
interface GigabitEthernet0/0.47
 encapsulation dot1Q 47
 ip address 47.0.0.43 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
```

```
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool mobilenodes 30.0.0.2 30.0.0.255
ip local pool pdsn-pool 122.3.0.1 122.3.16.1
ip local pool pdsn-pool 122.4.0.1 122.4.16.1
ip local pool pdsn-pool 122.5.0.1 122.5.16.1
ip local pool pdsn-pool 122.1.0.1 122.1.16.1
ip local pool pdsn-pool 122.2.0.1 122.2.16.1
ip default-gateway 9.15.0.1
ip classless
ip route 7.0.0.1 255.255.255.255 16.1.1.60
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.6
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
ip route 150.150.10.3 255.255.255.255 47.0.0.11
no ip http server
!
!
!
!
radius-server host 10.76.86.62 auth-port 1645 acct-port 1646 key cisco
radius-server key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
```

Note You will also have VPDN configuration tasks, Layer 2 Tunneling Protocol (L2TP) tunnel configuration tasks, and Load Balancing configuration tasks to perform. Please refer to the appropriate documentation for more specific information.

For information regarding VPDN configuration details, please refer to the following URL:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7e8f.html#wp1167095

For information regarding Layer 2 Tunneling Protocol (L2TP) tunnel configuration details, please refer to the following URL:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7e90.html

For information regarding IOS Server Load Balancing, please refer to the following URL:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/products_feature_guide09186a008020b9f3.html#wp3601032

Configuring Short Data Burst Flagging

This feature adds support for short data burst applications such as SIP signaling for PTT applications, and proposes the interaction with PDSN. SIP is used by PTT applications to signal a PTT call. The message is short and needs to be delivered to the end-user. The Short Data Burst support on the RAN can be used to send these over to the end-user, especially when the messages are to be terminated to the mobile.

To configure SDB on the PDSN so that all packets that are set with the specific group-number will be flagged for SDB usage between the PCF and the PDSN, use the following command in global configuration:

Command	Purpose
`Router(config)# cdma pdsn a11 dormant sdb-indication gre-flags group-number`	Configures SDB so that all packets that are set with the specific group-number will be flagged for SDB usage between the PCF and the PDSN.

Configuring PDSN Accounting Events

To configure attributes of PDSN accounting events, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# clock timezone zone hours-offset [minutes-offset]`	Sets the time zone for display purposes.
`Router(config)# cdma pdsn accounting local-timezone`	Sets the local time stamp for PDSN accounting events.
`Router(config)# cdma pdsn accounting time-of-day`	Sets triggers for accounting information for different times of day.
`Router(config)# cdma pdsn accounting send start-stop`	Enables the PDSN to send: • An Accounting Stop record when it receives an active stop airlink record (dormant state) • An Accounting Start record when it receives an active start airlink record (active state)

Configuring CDMA RADIUS Attributes

To configure both authentication and accounting requests on the PDSN, perform the following tasks:

Command	Purpose
Router(config)# **cdma pdsn attribute send {a1 { fa-chap | mip-rrq} | a2 {auth-req | fa-chap | mip-rrq} | a3 {auth-req | fa-chap | mip-rrq} | {c5 {acct-reqs} | f15 {acct-reqs} | f16 {acct-reqs} | f5 {fa-chap} | g1 {acct-start} | g2 {acct-start} | g17 | esn-optional | meid-optional | is835a}**	Enables both authentication and accounting requests on the PDSN.

Monitoring and Maintaining the PDSN

To monitor and maintain the PDSN, use the following commands in privileged EXEC mode:

Command	Purpose
Router# **clear cdma pdsn cluster controller session records age** *days*	Clears session records of a specified age.
Router# **clear cdma pdsn cluster controller session record all**	Clears all the session records of the PDSN cluster controller.
Router# **clear cdma pdsn cluster controller statistics**	Clears PDSN cluster controller statistics.
Router# **clear cdma pdsn cluster member statistics**	Clears PDSN cluster member statistics.
Router# **clear cdma pdsn selection** [**pdsn** *ip-addr* | **msid** *octet-stream*]	Clears the PDSN selection tables.
Router# **clear cdma pdsn session** {**all** | **pcf** *ip-addr* | **msid** *octet-stream*} {**send** {**all-update** | **termreq**}}	Clears the session.
Router# **clear cdma pdsn statistics**	Clears the RAN-to-PDSN interface (RP) or PPP statistics on the PDSN.
Router# **clear ip mobile binding** {**all** [**load** *standby-group-name*] | *ip-address* | **nai** *string ip_address*}	Removes mobility bindings.
Router# **clear ip mobile visitor** [*ip-address* | **nai** *string ip_address*]	Clears visitor information.
Router#**clear vpdn tunnel l2tp ?** all All L2TP tunnels hostname Based on the hostnames id Based on the tunnel ID ip Based on IP address	Clears VPDN L2TP Tunnel information for the Closed-PR feature.
Router# **show cdma pdsn**	Displays the status and current configuration of the PDSN gateway.
Router# **show cdma pdsn accounting**	Display the accounting information for all sessions and the corresponding flows.
Router# **show cdma pdsn accounting detail**	Displays detailed accounting information for all sessions and the corresponding flows.
Router# **show cdma pdsn accounting session** *msid*	Displays the accounting information for the session identified by the msid.
Router# **show cdma pdsn accounting session** *msid* **detail**	Displays the accounting information (the counter names) for the session identified by the msid.

Command	Purpose
Router# **show cdma pdsn accounting session** *msid* **flow** {**mn-ip-address** *IP_address*}	Displays the accounting information for a specific flow that is associated with the session identified by the msid.
Router# **show cdma pdsn accounting session** *msid* **flow user** *username*	Displays accounting information for a flow with username that is associated with the session identified by the msid.
Router# **show cdma pdsn ahdlc** *slot_number* **channel** [*channel_id*]	Displays Asynchronous High-Level Data Link Control (AHDLC) engine information.
Router# **show cdma pdsn cluster controller** [**configuration** | **statistics**]	Displays configuration and statistics for the PDSN cluster controller.
Router# **show cdma pdsn cluster controller config**	Displays the IP addresses of the members that are registered with a specific controller.
Router# **show cdma pdsn cluster controller member** [**load** | **time** | *ipaddr*]	Displays either the load reported by every PDSN cluster member, or the time until (or past) the seek time of the member, or for detailed information related to the member of the specified ip address.
Router# **show cdma pdsn cluster controller queueing**	Displays statistics associated with controller queueing feature.
Router# **show cdma pdsn cluster member queueing**	Displays statistics associated with member queueing feature.
Router# **show cdma pdsn cluster controller session** [**count** [**age** *days*] | **oldest** [**more** *1-20 records*] | **imsi** *BCDs* [**more** *1-20 records*]	Displays session count, or count by age, or one or a few oldest session records, or session records corresponding to the IMSI entered.
Router# **show cdma pdsn cluster controller statistics**	Displays the IP addresses of the members that are registered with a specific controller.
Router# **show cdma pdsn cluster member** [**configuration** | **statistics**]	Displays configuration and statistics for the PDSN cluster member.
Router# **show cdma pdsn flow {mn-ip-address** *ip_address* | **msid** *string* | **service-type** | **user** *string*}	Displays flow-based summary of active sessions, and the flows and IP addresses assigned to the mobile numbers in each session.
Router# **show cdma pdsn pcf** [**brief** | *ip-addr*]	Displays the PCF information for those PCFs that have R-P tunnels to this PDSN.
Router# **show cdma pdsn pcf secure**	Displays security associations for all PCFs configured on this PDSN.
Router# **show cdma pdsn resource** [*slot_number* [**ahdlc-channel** [*channel_id*]]]	Displays AHDLC resource information.
Router# **show cdma pdsn selection** {**summary** | **msid** *octet_stream*}	Displays the PDSN selection session table.
Router# **show cdma pdsn session** [**brief** | **dormant** | **mn-ip-address** *address* | **msid** *msid* | **user** *nai*]	Displays the session information on the PDSN.
Router# **show cdma pdsn statistics** [**ahdlc** | **rp** [**pcf** *ip address*] | **error**] [**ppp** [*pcf ip address*]]	Displays VPDN, PPP, RP interface, prepaid, RADIUS, and error statistics for the PDSN.
Router# **show compress detail-ccp**	Displays the compression information for all users.

Command	Purpose
Router# **show diag** [*slot*]	Displays diagnostic information about the controller, interface processor, and port adapters associated with a specified slot of a Cisco router.
Router# **show interfaces virtual-access** *number*	Displays a description of the configuration of the virtual access interface.
Router# **show ip mobile cdma ipsec profile**	Displays the configured IPSec profiles.
Router# **show ip mobile cdma ipsec security-level**	Displays a list of FAs and their security levels.
Router# **show ip mobile globals**	Displays MIPv4 Registration Revocation support in MIP subsystem.
Router# **show ip mobile proxy** [**host** [**nai** *string*] | **registration** | **traffic**]	Displays information about a proxy Mobile IP host.
Router# **show ip mobile secure**	Displays mobility security associations for Mobile IP.
Router# **show ip mobile traffic**	Displays MIPv4 Registration Revocation message related statistics
Router# **show ip mobile visitor**	Displays a list of visitors.
Router# **show ip mobile violation**	Displays information about security violations.
Router# **show mwam module** *slot_num port_num*	Displays connectivity information regarding the individual processors on the MWAM card.
Router# **show tech-support cdma pdsn**	Displays PDSN information that is useful to Cisco Customer Engineers for diagnosing problems.
Router#**show vpdn** Router#**show vpdn session** Router#**show vpdn tunnel**	Displays VPDN information relevant to the Closed-RP Interface.

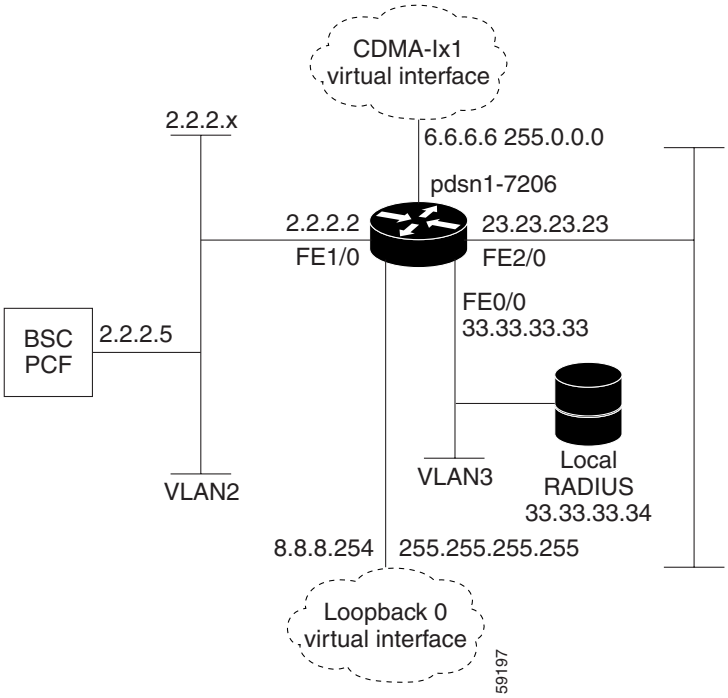
Configuration Examples

This section provides the following configuration examples:

Cisco PDSN Configuration for Simple IP

Figure 10 and the information that follows is an example of PDSN architecture for Simple IP and its accompanying configuration.

Figure 10 PDSN for Simple IP—A Network Map




```
service cdma pdsn
!
hostname PDSN1-7206
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization config-commands

aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 60
aaa accounting network pdsn start-stop group radius
!
no ip gratuitous-arps
!
interface Loopback0
ip address 8.8.8.254 255.255.255.255
!
interface CDMA-Ix1
ip address 6.6.6.6 255.0.0.0
!
interface FastEthernet0/0
! Interface for communication with RADIUS server and NMS
ip address 33.33.33.33 255.255.255.0
!
!
!
```

```
interface FastEthernet1/0
! Interface to PCF -  R-P
ip address 2.2.2.2 255.255.255.0
half-duplex
no cdp enable
!
interface FastEthernet2/0
! Interface to external network - Pi
ip address 23.23.23.23 255.255.0.0
!
!
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool pdsn-pool
ppp accm 0
ppp authentication chap pap optional
ppp accounting none
ppp timeout idle 2000
!
ip local pool pdsn-pool 8.8.8.1 8.8.8.253
ip classles
!
!
radius-server host 33.33.33.34 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn virtual-template 1
cdma pdsn maximum sessions 16000
cdma pdsn a10 max-lifetime 36000
cdma pdsn msid-authentication
cdma pdsn secure pcf 2.2.2.5 spi 100 key ascii cisco
!
!
!
end
```

Cisco PDSN Configuration for Simple IP with VPDN

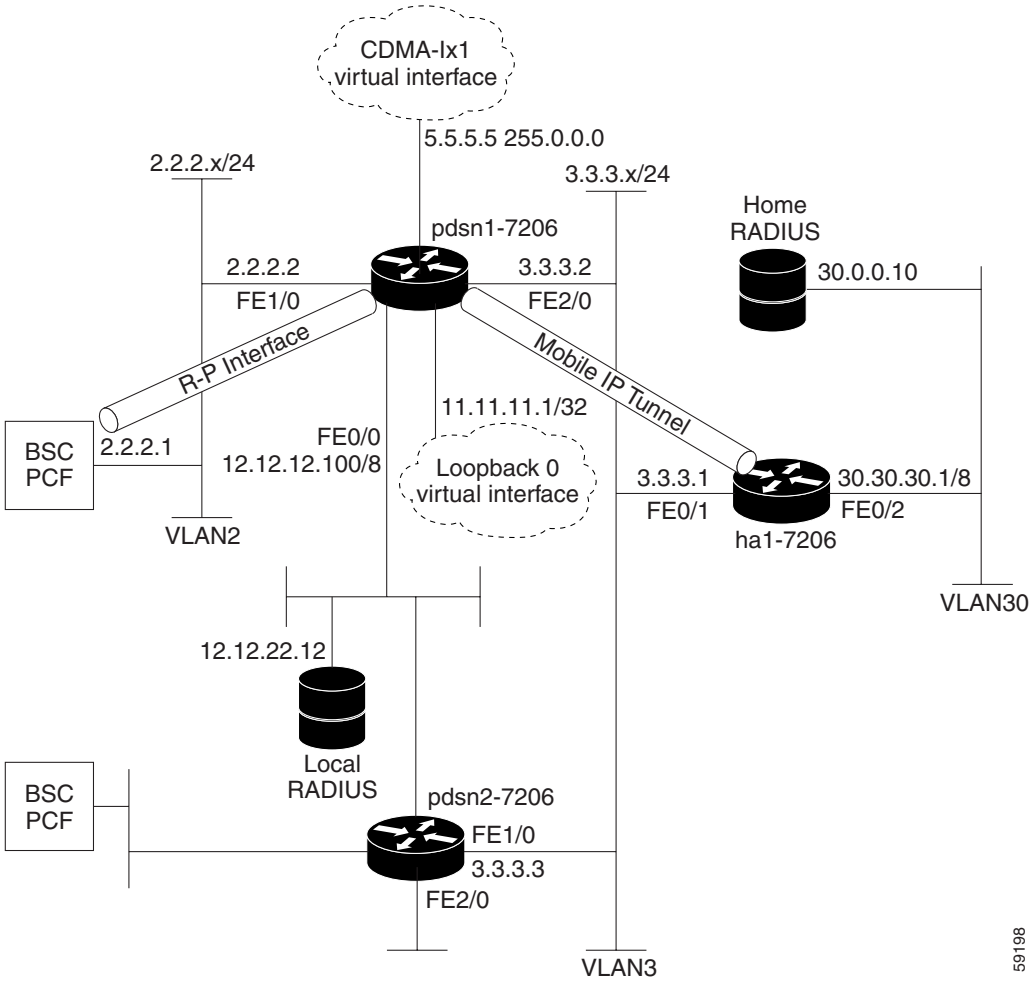
The configuration Simple IP with VPDN is identical to the configuration for Simple IP with two additional lines:

```
vpdn enable
vpdn authen-before-forward
```

Cisco PDSN Configuration for Mobile IP

Figure 11 and the information that follows is an example of PDSN architecture for Mobile IP service and its accompanying configuration. The example shows the configuration of PDSN1.

Figure 11 PDSN for Mobile IP—A Network Map




```
service cdma pdsn
!
hostname PDSN1-7206
!
aaa new-model
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
!
interface Loopback0
ip address 11.11.11.1 255.255.255.255
!
interface CDMA-Ix1
```

```
ip address 5.5.5.5 255.0.0.0
!
interface FastEthernet0/0
description AAA NMS interface
ip address 12.12.12.100 255.0.0.0
!
interface FastEthernet1/0
description R-P interface
ip address 2.2.2.2 255.255.255.0
full-duplex
!
!
interface FastEthernet2/0
description Pi interface
ip address 3.3.3.2 255.255.255.0
full-duplex
!
interface Virtual-Template1
ip unnumbered loopback0
no ip route-cache
no keepalive
ppp authentication chap pap optional
ppp timeout idle 2000
!
router mobile
!
ip classless
no ip http server
ip mobile foreign-agent care-of FastEthernet2/0
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
!
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn secure pcf 2.2.2.1 spi 100 key ascii cisco
cdma pdsn virtual-template 1
cdma pdsn msid-authentication
!
!
end
```

Combined Configuration for Cisco PDSN

The following example illustrates a PDSN configured for all scenarios: Simple IP, Simple IP with VPDN, Mobile IP, Proxy Mobile IP, and peer-to-peer PDSN selection.

```
service cdma pdsn
!
hostname PDSN1
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 60
aaa accounting network pdsn start-stop group radius
!
```

```
vpdn enable
vpdn authen-before-forward
virtual-profile aaa
username HA password 0 rosebud
username LNS password 0 cisco
username PDSN password 0 cisco
no ip gratuitous-arps
!
interface Loopback0
ip address 8.8.8.254 255.255.255.255
!
interface CDMA-Ix1
ip address 6.6.6.6 255.0.0.0
!
interface FastEthernet0/0
! Interface for communication with RADIUS server and NMS
ip address 33.33.33.33 255.255.255.0
!
!
!
interface FastEthernet1/0
! Interface to PCF -  R-P
ip address 2.2.2.2 255.255.255.0
!
interface FastEthernet2/0
! Interface to external network - Pi
ip address 23.23.23.23 255.255.0.0
!
!
!
interface Virtual-Template1
ip unnumbered Loopback0
no keepalive
peer default ip address pool pdsn-pool
ppp accm 0
ppp authentication chap pap optional
ppp accounting none
ppp timeout idle 2000
!
router mobile
!
ip local pool pdsn-pool 8.8.8.1 8.8.8.253
ip classless
ip mobile foreign-agent care-of FastEthernet2/0
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
!
!
radius-server host 33.33.33.34 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn virtual-template 1
cdma pdsn maximum sessions 16000
cdma pdsn a10 max-lifetime 36000
cdma pdsn msid-authentication
cdma pdsn secure pcf 2.2.2.5 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
cdma pdsn selection interface FastEthernet0/0
!
!
!
end
```

PDSN Cluster Configuration

The following configuration illustrates 3 MWAMs in a 6500 configuration:

```
Verify hardware configuration on Cat6K:
cat6500 router#sh module
Mod Ports Card Type
---------------------------------------------
  1    2  Catalyst 6000 supervisor 2 (Active)
  3   48  SFM-capable 48-port 10/100 Mbps RJ45
  4    2  IPSec VPN Accelerator
  5   16  SFM-capable 16 port 1000mb GBIC
  7    3  MWAM Module
  8    3  MWAM Module (MP)
  9    3  MWAM Module

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  0005.7485.8494 to 0005.7485.8495   3.5   6.1(3)       6.2(2.108)   Ok
  3  0001.63d7.2352 to 0001.63d7.2381   4.2   6.3(1)       6.2(2.108)   Ok
  4  0008.7ca8.1386 to 0008.7ca8.1389   0.200 7.2(1)       6.2(2.108)   Ok
  5  0001.63d6.cd92 to 0001.63d6.cda1   4.1   6.3(1)       6.2(2.108)   Ok
  7  0001.0002.0003 to 0001.0002.000a   0.203 7.2(1)       1.0(0.1)     Ok
  8  00e0.b0ff.3a10 to 00e0.b0ff.3a17   0.201 7.2(1)       1.2(0.12)    ShutDown
  9  0002.0002.0003 to 0002.0002.000a   0.203 7.2(1)       1.0(0.1)     Ok

Mod Sub-Module                    Hw     Status
--- ------------------------- ------- -------
  1 Policy Feature Card          2 3.2    Ok
  1 Cat6k MSFC 2 daughterboard     2.2    Ok
cat6500 router#

Controller configuration:
cat6500 router#session slot 7 processor 6
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.76 ... Open


Press RETURN to get started!


S76>
S76>
S76>
S76>en
S76#sh run
S76#sh running-config
Building configuration...

Current configuration : 1489 bytes
!
! No configuration change since last restart
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
!
hostname S76
!
!
```

```
ip subnet-zero
ip cef
!
!
!
interface Loopback1
 no ip address
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.401
 encapsulation dot1Q 401
 ip address 10.121.68.76 255.255.255.0
 standby 1 ip 10.121.68.98
 standby 1 priority 120
 standby 1 preempt
 standby 1 name 6509-cluster
!
router mobile
!
ip classless
ip route 10.10.72.1 255.255.255.255 10.121.68.72
ip route 10.10.73.1 255.255.255.255 10.121.68.73
ip route 10.10.74.1 255.255.255.255 10.121.68.74
ip route 10.10.75.1 255.255.255.255 10.121.68.75
ip route 10.10.92.1 255.255.255.255 10.121.68.92
ip route 10.10.93.1 255.255.255.255 10.121.68.93
ip route 10.10.94.1 255.255.255.255 10.121.68.94
ip route 10.10.95.1 255.255.255.255 10.121.68.95
ip route 128.0.0.0 255.255.255.0 GigabitEthernet0/1
no ip http server
ip pim bidir-enable
!
!
!
cdma pdsn secure pcf 10.121.68.62 10.121.68.66 spi 100 key ascii cisco
cdma pdsn secure pcf 10.121.68.82 10.121.68.86 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii user
cdma pdsn cluster controller interface GigabitEthernet0/0.401
cdma pdsn cluster controller standby 6509-cluster
cdma pdsn cluster controller timeout 10
cdma pdsn cluster controller window 3
!
line con 0
line vty 0
 no login
line vty 1 4
 login
line vty 5 15
 login
!
end

router#
cat6500 router#session slot 9 processor 6
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.96 ... Open

router>
Press RETURN to get started!
```

```
router 96#show running-config
Building configuration...

Current configuration : 1182 bytes
!
! No configuration change since last restart
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
!
hostname router96
!
!
ip subnet-zero
ip cef
!
!
!
!
interface Loopback1
 no ip address
!
interface CDMA-Ix1
 no ip address
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.401
 encapsulation dot1Q 401
 ip address 10.121.68.96 255.255.255.0
 standby 1 ip 10.121.68.98
 standby 1 priority 120
 standby 1 preempt
 standby 1 name 6509-cluster
!
router mobile
!
ip classless
ip route 10.10.72.1 255.255.255.255 10.121.68.72
ip route 128.0.0.0 255.255.255.0 GigabitEthernet0/2
no ip http server
ip pim bidir-enable
!
!
!
cdma pdsn secure pcf 10.121.68.62 10.121.68.66 spi 100 key ascii cisco
cdma pdsn secure pcf 10.121.68.82 10.121.68.86 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii user
cdma pdsn cluster controller interface GigabitEthernet0/0.401
cdma pdsn cluster controller standby 6509-cluster
cdma pdsn cluster controller timeout 10
cdma pdsn cluster controller window 3
!
line con 0
line vty 0
 no login
line vty 1 4
 login
line vty 5 15
 login
```

```
!
end

router96#

Verify active controller and standby controller
router76#show standby
GigabitEthernet0/0.401 - Group 1
  State is Active
    2 state changes, last state change 00:27:09
  Virtual IP address is 10.121.68.98
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.112 secs
  Preemption enabled, min delay 0 sec, sync delay 0 sec
  Active router is local
  Standby router is 10.121.68.96, priority 120 (expires in 9.064 sec)
  Priority 120 (configured 120)
  IP redundancy name is "6509-cluster"
router76#

router96#sh standby
GigabitEthernet0/0.401 - Group 1
  State is Standby
    1 state change, last state change 00:26:57
  Virtual IP address is 10.121.68.98
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.532 secs
  Preemption enabled, min delay 0 sec, sync delay 0 sec
  Active router is 10.121.68.76, priority 120 (expires in 9.580 sec)
  Standby router is local
  Priority 120 (configured 120)
  IP redundancy name is "6509-cluster"
router96#

Members configuration:
cat6500 router#session slot 7 processor 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.73 ... Open

router73>

Press RETURN to get started!


router73#sh run
router73#sh running-config
Building configuration...

Current configuration : 3192 bytes



! Last configuration change at 04:10:06 UTC Sun Sep 15 2002
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
```

```
!
hostname router73
!
aaa new-model
!
!
aaa group server radius CSCO-30
 server 10.1.1.244 auth-port 1645 acct-port 1646
 server 10.1.1.200 auth-port 2812 acct-port 2813
!
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network pdsn start-stop group radius
aaa session-id common
!
username root nopassword
username cisco password 0 cisco
username pdsn password 0 cisco
ip subnet-zero
ip gratuitous-arps
ip cef
!
!
!
interface Loopback1
 ip address 10.10.173.1 255.255.255.0
!
interface CDMA-Ix1
 ip address 10.10.73.1 255.255.255.0
 tunnel source 10.10.73.1
 tunnel key 16404
 tunnel sequence-datagrams
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.310
 encapsulation dot1Q 310
 ip address 10.1.1.73 255.255.255.0
!
interface GigabitEthernet0/0.401
 encapsulation dot1Q 401
 ip address 10.121.68.73 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback1
no keepalive
 peer default ip address pool pdsn-pool
 ppp accm 0
 ppp authentication chap pap optional
 ppp ipcp address unique
 cdma pdsn mobile-advertisement-burst interval 500 number 3
!
router mobile
!
router ospf 100
 log-adjacency-changes
 summary-address 7.3.0.0 255.255.0.0
 redistribute connected subnets route-map MAP-DENY
 network 10.10.73.1 0.0.0.0 area 73
 network 10.10.73.0 0.0.0.255 area 73
 network 10.10.173.1 0.0.0.0 area 0
 network 10.121.68.0 0.0.0.255 area 0
!
```

```
ip local pool pdsn-pool 7.3.1.0 7.3.16.255
ip local pool pdsn-pool 7.3.17.0 7.3.32.255
ip local pool pdsn-pool 7.3.33.0 7.3.48.255
ip local pool pdsn-pool 7.3.49.0 7.3.64.255
ip local pool pdsn-pool 7.3.65.0 7.3.78.255
ip local pool pdsn-pool 7.3.79.0 7.3.79.31
ip mobile foreign-agent care-of GigabitEthernet0/0.310
ip classless
ip route 128.0.0.0 255.255.255.0 GigabitEthernet0/1
no ip http server
ip pim bidir-enable
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service reverse-tunnel
cdma pdsn mobile-advertisement-burst interval 500 number 3
!
!
access-list 9 deny   128.0.0.0 0.0.255.255
access-list 9 permit any
!
route-map MAP-DENY permit 10
 match ip address 9
 set tag 9
!
radius-server host 10.1.1.244 auth-port 1645 acct-port 1646 key foo
radius-server host 10.1.1.200 auth-port 2812 acct-port 2813 key foo
radius-server retransmit 3
radius-server deadtime 1
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
cdma pdsn accounting local-timezone
cdma pdsn virtual-template 1
cdma pdsn send-agent-adv
cdma pdsn secure pcf 10.121.68.62 10.121.68.66 spi 100 key ascii cisco
cdma pdsn secure pcf 10.121.68.82 10.121.68.86 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii user
cdma pdsn cluster member controller 10.121.68.98
cdma pdsn cluster member interface GigabitEthernet0/0.401
cdma pdsn cluster member timeout 10
cdma pdsn cluster member window 2
!
line con 0
line vty 5 15
!
end

Show commands on Controllers
PDSN-CONTROLLER#show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.1
no R-P signaling proxy
timeout to seek member = 10 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default:  spi 100, Timestamp +/- 0, key ascii clustering
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
  group: cluster
Controller maximum number of load units = 1000
```

```
PDSN-CONTROLLER#show cdma pdsn cluster controller member load
 Secs until   Seq seeks         Member
(past) seek    no reply      IPv4 Addr      State   Load   Sessions
---------------------------------------------------------------------
          6       0          20.6.84.1      ready      0          0
          5       0          20.6.62.1      ready      0          0
          1       0          20.6.64.1      ready      0          0
---------------------------------------------------------------------
                   Controller IPv4 Addr      20.3.68.60


PDSN-CONTROLLER#show cdma pdsn cluster controller member  20.6.84.1
PDSN cluster member 20.6.84.1 state      ready
 registered with PDSN controller 20.3.68.60
 reported load 0 percent, will be sought in 7 seconds

  Member 20.6.84.1 statistics:
  Controller seek rcvd 1, Member seek reply rcvd 554
  Member state changed 0 time to ready
  Member state changed 0 time to Admin prohibited
  Session-Up message rcvd 0, Session-Down message received 0
  Member seek not replied in sequence 0


PDSN-CONTROLLER#show cdma pdsn cluster controller statistics
Controller-Member Interface:
  Cluster Reg Request rcvd 858, accepted 852, discarded 6
  Cluster Reg Request sent 1425
  Cluster Reg Reply rcvd 1427, accepted 1424, discarded 3

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 6
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 3
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0

  Controller seek requests rcvd 852, replies sent 852
  Member seek requests sent 1425, replies rcvd 1424
  Member state transition msgs rcvd 0, replies sent 0
    ready 0, Administratively prohibited 0
  Total A11 Reg Requests forwarded 0
    A11 Reg Requests orig forwarded 0, retry forwarded 0
    Session-Up from member 0, Session-Down from member 0
    No Acknowledgement from member 0

Controller Redundancy Interface:
    Update rcvd 0 sent 2330 orig sent 2276 fail 18
    UpdateAck rcvd 2330 sent 0
    DownloadReq rcvd 0 sent 20 orig sent 19 fail 0
    DownloadReply rcvd 20 sent 0 orig sent 0 fail 0 drop 0
    DownloadAck rcvd 0 sent 20 drop 0

    Errors: Authentication failed 0 ID mismatch 0
            Ignored due to no redundancy configuration 0

router76#sh cdma pdsn cluster controller session ?
  count   Count of session records
  imsi    Session record for International Mobile Subscriber Identity
  oldest  Oldest session record
```

```
router76#sh cdma pdsn cluster controller session ol
router76#sh cdma pdsn cluster controller session oldest ?
  more  The oldest and a few more session records to show
  |     Output modifiers
  <cr>

router76#sh cdma pdsn cluster controller session oldest
           IMSI   Member IPv4 Addr   Age [days]   Anchor changes
----------------------------------------------------------------
62000015434         10.10.73.1
----------------------------------------------------------------

router76#sh cdma pdsn cluster controller session imsi 62000015434
           IMSI   Member IPv4 Addr   Age [days]   Anchor changes
----------------------------------------------------------------
62000015434         10.10.73.1
----------------------------------------------------------------

router76#


Show commands on member:

PDSN-MEMBER#show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.1
IP address of controller is 20.3.68.60
no prohibit administratively
timeout to resend status or seek controller = 250 sec or less, randomized
resend a msg for 6 timeouts sequentially if no reply, then inform operator
default:  spi 100, Timestamp +/- 0, key ascii clustering
this PDSN cluster member is configured


PDSN-MEMBER#show cdma pdsn cluster member statistics
Controller-Member Interface:
  Cluster Reg Request rcvd 593, accepted 593, discarded 0
  Cluster Reg Request sent 3
  Cluster Reg Reply rcvd 1, accepted 1, discarded 0

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0

  Controller seek requests rcvd 593, replies sent 593
  Member seek requests sent 3, replies rcvd 1
  Member state transition msgs sent 0, replies rcvd 0
    ready 0, Administratively prohibited 0
  Session-Up msg sent 0, Session-Down msg sent 0
  Session-Up msg Ack rcvd 0, Session-Down msg Ack rcvd 0
  Controller seek not replied in sequence 0
  Member state not replied in sequence 0

Cat6k SUP configuration
cat6500 router#sh running-config
Building configuration...
```

```
Current configuration : 9838 bytes
!
! Last configuration change at 00:21:56 UTC Sat Sep 14 2002 by root
! NVRAM config last updated at 14:10:00 UTC Fri Sep 13 2002 by root
!
version 12.2
service timestamps debug uptime
service timestamps log datetime localtime
no service password-encryption
!
hostname cat6500 router
!
boot system slot0:c6sp222-jk9sv-mz
boot device module 4 cf:3
boot device module 5 cf:4
boot device module 6 cf:4
boot device module 7 cf:4
boot device module 8 cf:4
boot device module 9 cf:4
aaa new-model
aaa authentication login default local
aaa authorization exec default local
enable secret level 1 5 $1$T17C$7icHsiM4vHj6nIE6medGj.
enable secret level 6 5 $1$wB/9$.ML91zZopFpYp12VNxA1p.
enable password lab
!
username u0 privilege 0 password 0 cisco
username root nopassword
username u1 password 0 cisco
username u6 privilege 6 password 0 cisco
username u8 privilege 8 password 0 cisco
username cisco password 0 cisco
username u2 privilege 2 nopassword
username u15 privilege 15 nopassword
username u10 privilege 10 nopassword
username v1 nopassword user-maxlinks 1
!
monitor session 1 source interface Fa3/24
monitor session 1 destination interface Fa3/12
redundancy
 main-cpu
  auto-sync standard
ip subnet-zero
!
!
no ip domain-lookup
!
mls flow ip destination
mls flow ipx destination
!
!
no spanning-tree vlan 310
!
!
!
interface Loopback1
 ip address 10.10.10.10 255.255.255.0
!
interface Port-channel1
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
```

```
interface GigabitEthernet1/1
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 309
 switchport mode access
!
interface GigabitEthernet1/2
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
 switchport mode access
!
interface GigabitEthernet2/1
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
 switchport mode access
!
interface GigabitEthernet2/2
 no ip address
 shutdown
!
interface FastEthernet3/1
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 222
!
interface FastEthernet3/2
 no ip address
 shutdown
!
interface FastEthernet3/3
 no ip address
 shutdown
!
interface FastEthernet3/4
 no ip address
 shutdown
!
interface FastEthernet3/5
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 66
 switchport mode access
!
interface FastEthernet3/6
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 66
 switchport mode access
!
interface FastEthernet3/7
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 66
 switchport mode access
!
```

```
interface FastEthernet3/8
 ip address 1.1.1.1 255.255.255.0
 shutdown
!
interface FastEthernet3/9
 no ip address
 shutdown
!
interface FastEthernet3/10
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
 channel-group 1 mode on
!
interface FastEthernet3/11
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
 channel-group 1 mode on
!
interface FastEthernet3/12
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/13
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/14
 no ip address
 shutdown
!
interface FastEthernet3/15
 ip address 3.3.3.3 255.255.255.0
 shutdown
!
interface FastEthernet3/16
 no ip address
 shutdown
!
interface FastEthernet3/17
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 311
 switchport mode access
!
interface FastEthernet3/18
 no ip address
 shutdown
!
interface FastEthernet3/19
 no ip address
 shutdown
!
interface FastEthernet3/20
 no ip address
 shutdown
```

```
!
interface FastEthernet3/21
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/22
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/23
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/24
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/25
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/26
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 401
!
interface FastEthernet3/27
 no ip address
 shutdown
!
interface FastEthernet3/28
 no ip address
 shutdown
!
interface FastEthernet3/29
 no ip address
 shutdown
!
interface FastEthernet3/30
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/31
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/32
 no ip address
 snmp trap link-status
```

```
 switchport
 switchport access vlan 310
!
interface FastEthernet3/33
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/34
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/35
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/36
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/37
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/38
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/39
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/40
 no ip address
 shutdown
 snmp trap link-status
 switchport
 switchport access vlan 333
!
interface FastEthernet3/41
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/42
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
```

```
interface FastEthernet3/43
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/44
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/45
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/46
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 310
!
interface FastEthernet3/47
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 333
!
interface FastEthernet3/48
 no ip address
 snmp trap link-status
 switchport
 switchport access vlan 333
!
interface GigabitEthernet4/1
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet4/2
 no ip address
 snmp trap link-status
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 flowcontrol receive on
 cdp enable
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
```

```
interface GigabitEthernet5/3
 no ip address
 shutdown
!
interface GigabitEthernet5/4
 no ip address
 shutdown
!
interface GigabitEthernet5/5
 no ip address
 shutdown
!
interface GigabitEthernet5/6
 no ip address
 shutdown
!
interface GigabitEthernet5/7
 no ip address
 shutdown
!
interface GigabitEthernet5/8
 no ip address
 shutdown
!
interface GigabitEthernet5/9
 no ip address
 shutdown
!
interface GigabitEthernet5/10
 no ip address
 shutdown
!
interface GigabitEthernet5/11
 no ip address
 shutdown
!
interface GigabitEthernet5/12
 no ip address
 shutdown
!
interface GigabitEthernet5/13
 no ip address
 shutdown
!
interface GigabitEthernet5/14
 no ip address
 shutdown
!
interface GigabitEthernet5/15
 no ip address
 shutdown
!
interface GigabitEthernet5/16
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan222
 ip address 172.19.23.16 255.255.254.0
 ip nat outside
!
```

```
interface Vlan309
 no ip address
!
interface Vlan310
 ip address 10.1.1.222 255.255.255.0
 ip nat inside
!
interface Vlan401
 ip address 10.121.68.200 255.255.255.0
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.10 0.0.0.0 area 0
 network 10.121.68.0 0.0.0.255 area 0
 default-information originate
!
ip nat inside source list 100 interface Vlan222 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.26.1
ip route 0.0.0.0 0.0.0.0 172.19.22.1
ip route 5.5.5.0 255.255.255.0 10.1.1.92
ip route 10.10.113.1 255.255.255.255 10.1.1.221
ip route 10.10.116.1 255.255.255.255 10.1.1.221
ip route 10.10.195.1 255.255.255.255 10.1.1.95
no ip http server
ip pim bidir-enable
!
!
ip access-list extended VRZ-101
 permit ip host 10.10.195.1 host 10.10.116.1
access-list 100 permit ip 5.0.0.0 0.255.255.255 any
arp 127.0.0.22 0000.2200.0000 ARPA
arp 127.0.0.12 0000.2100.0000 ARPA
!
route-map MAP deny 10
 match ip address 100
!
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps casa
snmp-server enable traps vtp
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server host 10.1.1.199 public
!
privilege configure level 8 snmp-server community
privilege configure level 8 username
privilege configure level 8 username u10 privilege 10 nopassword
privilege exec level 6 show running
privilege exec level 8 config terminal
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
```

```
 password lab
 transport input lat pad mop telnet rlogin udptn nasi
line vty 5 10
 exec-timeout 0 0
!
ntp master 3
end
```

Closed RP IOS SLB Load Balancing Configuration

The following configuration example illustrates the IOS Server Load Balancing for the Closed-RP feature on the PDSN. This example includes 6 instances of the PDSN.

Supervisor Configuration

```
SLB-6500#show running-config
Building configuration...

Current configuration : 6422 bytes
!
! Last configuration change at 00:37:57 UTC Thu Jun 5 2003
! NVRAM config last updated at 02:54:07 UTC Wed May 28 2003
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SLB-6500
!
logging snmp-authfail
!
clock calendar-valid
mwam module 5 port 1 allowed-vlan 1-1000
mwam module 5 port 2 allowed-vlan 1-1000
mwam module 5 port 3 allowed-vlan 1-1000
mwam module 7 port 1 allowed-vlan 1-1000
mwam module 7 port 2 allowed-vlan 1-1000
mwam module 7 port 3 allowed-vlan 1-1000
vtp mode transparent
ip subnet-zero
!
!
no ip domain-lookup
!
!
ip slb serverfarm PDSN-FARM
 real 37.0.0.2
  weight 1
  inservice
 !
 real 37.0.0.3
  weight 1
  inservice
 !
 real 37.0.0.4
  weight 1
  inservice
 !
```

```
 real 37.0.0.5
  weight 1
  inservice
 !
 real 37.0.0.6
  weight 1
  inservice
!
ip slb vserver PDSN-SLB
 virtual 150.150.0.100 udp 1701
 serverfarm PDSN-FARM
 sticky 65535 group 1 netmask 255.255.254.0
 idle 10
 inservice
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
mls verify ip length minimum
mls verify ipx length minimum
!
!
!
!
!
!
spanning-tree mode pvst
no spanning-tree vlan 24
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
vlan internal allocation policy ascending
!
vlan 4-5,7-9,11,16,20,24-25,36-37,47,99-100,199-200,300
!
!
interface GigabitEthernet2/1
 no ip address
 switchport
 switchport access vlan 4
 switchport mode access
!
interface GigabitEthernet2/2
 no ip address
 switchport
 switchport access vlan 7
!
interface FastEthernet3/1
 ip address 10.76.86.60 255.255.255.192
!
interface FastEthernet3/2
 no ip address
 shutdown
!
interface FastEthernet3/3
 no ip address
 shutdown
!
```

```
interface FastEthernet3/4
 no ip address
 switchport
 switchport access vlan 4
!
interface FastEthernet3/5
 no ip address
 speed 100
 duplex full
 switchport
 switchport access vlan 4
!
interface FastEthernet3/6
 no ip address
 switchport
 switchport access vlan 4
!
interface FastEthernet3/7
 no ip address
 switchport
 switchport access vlan 8
!
interface FastEthernet3/8
 no ip address
 switchport
 switchport access vlan 8
!
interface FastEthernet3/9
 no ip address
 switchport
 switchport access vlan 9
!
interface FastEthernet3/10
 no ip address
 shutdown
!
interface FastEthernet3/11
 no ip address
 switchport
 switchport access vlan 100
!
interface FastEthernet3/12
 no ip address
 switchport
 switchport access vlan 47
!
interface FastEthernet3/13
 no ip address
 speed 100
 duplex half
 switchport
 switchport access vlan 100
!
interface FastEthernet3/14
 no ip address
 switchport
 switchport access vlan 100
!
interface FastEthernet3/15
 no ip address
 shutdown
!
interface FastEthernet3/16
 no ip address
```

```
 switchport
 switchport access vlan 4
!
interface FastEthernet3/17
 no ip address
 shutdown
!
interface FastEthernet3/18
 no ip address
 shutdown
!
interface FastEthernet3/19
 no ip address
 switchport
 switchport access vlan 199
!
interface FastEthernet3/20
 no ip address
 switchport
 switchport access vlan 20
!
interface FastEthernet3/21
 no ip address
 shutdown
!
interface FastEthernet3/22
 no ip address
 shutdown
!
interface FastEthernet3/23
 no ip address
 shutdown
!
interface FastEthernet3/24
 no ip address
 duplex half
 switchport
 switchport access vlan 7
!
interface FastEthernet3/25
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/26
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/27
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/28
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/29
 no ip address
 switchport
 switchport access vlan 25
!
```

```
interface FastEthernet3/30
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/31
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/32
 no ip address
 shutdown
!
interface FastEthernet3/33
 no ip address
 shutdown
!
interface FastEthernet3/34
 no ip address
 shutdown
!
interface FastEthernet3/35
 no ip address
 switchport
 switchport access vlan 25
!
interface FastEthernet3/36
 no ip address
 switchport
 switchport access vlan 36
!
interface FastEthernet3/37
 no ip address
 shutdown
!
interface FastEthernet3/38
 no ip address
 shutdown
!
interface FastEthernet3/39
 no ip address
 shutdown
!
interface FastEthernet3/40
 no ip address
 shutdown
!
interface FastEthernet3/41
 no ip address
!
interface FastEthernet3/42
 no ip address
 switchport
 switchport access vlan 200
!
interface FastEthernet3/43
 no ip address
 switchport
 switchport access vlan 16
!
interface FastEthernet3/44
 no ip address
 switchport
```

```
 switchport access vlan 16
!
interface FastEthernet3/45
 no ip address
 shutdown
!
interface FastEthernet3/46
 no ip address
 shutdown
!
interface FastEthernet3/47
 no ip address
 shutdown
!
interface FastEthernet3/48
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan4
 ip address 150.150.0.2 255.255.254.0
!
interface Vlan5
 no ip address
!
interface Vlan7
 ip address 7.0.0.111 255.0.0.0
!
interface Vlan9
 no ip address
!
interface Vlan16
 ip address 16.1.1.1 255.0.0.0
!
interface Vlan20
 ip address 15.1.1.50 255.0.0.0
!
interface Vlan25
 ip address 9.15.50.4 255.255.0.0
!
interface Vlan36
 ip address 36.0.0.20 255.0.0.0
!
interface Vlan37
 ip address 37.0.0.1 255.0.0.0
!
interface Vlan47
 ip address 47.0.0.111 255.0.0.0
!
interface Vlan99
 ip address 99.99.11.1 255.0.0.0
!
interface Vlan100
 ip address 20.1.1.50 255.0.0.0
!
ip default-gateway 9.15.0.1
ip classless
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 64.0.0.0 255.0.0.0 10.76.86.1
no ip http server
!
!
```

```
!
!
!
dial-peer cor custom
!
!
!
alias exec cls clear ip slb sessions
alias exec clr clear counters
alias exec cpu show proc cpu | inc CPU
alias exec hist show proc cpu history
alias exec clss clear ip slb sessions
alias exec clsc clear ip slb counters
alias exec clc clear counters
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 no login
!
!
monitor session 1 source interface Fa3/6
ntp clock-period 17179954
ntp master
ntp server 9.15.50.4
end

SLB-6500#
```

PDSN Configuration

```
MWAM-PDSN2#sh run
Building configuration...

Current configuration : 3872 bytes
!
! Last configuration change at 00:34:06 UTC Thu Jun 5 2003
! NVRAM config last updated at 00:35:49 UTC Thu Jun 5 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname MWAM-PDSN2
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username MWAM-PDSN2 password 0 cisco
username HA password 0 cisco
```

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
ip dhcp ping packets 0
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.1 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
 tunnel sequence-datagrams
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.172 255.255.0.0
!
interface GigabitEthernet0/0.7
 encapsulation dot1Q 7
 ip address 7.0.0.1 255.0.0.0
!
interface GigabitEthernet0/0.8
 encapsulation dot1Q 8
 ip address 8.0.0.11 255.0.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.2 255.0.0.0
!
interface GigabitEthernet0/0.47
```

```
 encapsulation dot1Q 47
 ip address 47.0.0.42 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool pdsn-test 13.2.0.1 13.2.0.100
ip local pool pdsn-pool 121.1.0.1 121.1.16.1
ip local pool pdsn-pool 121.2.0.1 121.2.16.1
ip local pool pdsn-pool 121.3.0.1 121.3.16.1
ip local pool pdsn-pool 121.4.0.1 121.4.16.1
ip local pool pdsn-pool 121.5.0.1 121.5.16.1
ip default-gateway 9.15.0.1
ip classless
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.32
ip route 150.150.6.2 255.255.255.255 47.0.0.6
ip route 150.150.6.3 255.255.255.255 47.0.0.33
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
ip route 150.150.10.3 255.255.255.255 47.0.0.11
ip mobile foreign-agent care-of GigabitEthernet0/0.7
no ip http server
!
!
!
!
radius-server host 10.76.86.62 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
alias exec cls clear cdma pdsn session all
alias exec cpu show proc cpu | i CPU
alias exec crad clear radius statistics
alias exec tclear clear vpdn tunnel l2tp all
alias exec cstats clear cdma pdsn statistics
alias exec sip show cdma pdsn | i Simple
alias exec hist sh proc cpu hist
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
```

```
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
!
!
end

MWAM-PDSN2#
```

```
MWAM-PDSN3#sh run
Building configuration...

Current configuration : 3479 bytes
!
! Last configuration change at 00:34:36 UTC Thu Jun 5 2003
! NVRAM config last updated at 00:34:38 UTC Thu Jun 5 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname MWAM-PDSN3
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
ip dhcp ping packets 0
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
```

```
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.3 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.173 255.255.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.3 255.0.0.0
!
interface GigabitEthernet0/0.47
 encapsulation dot1Q 47
 ip address 47.0.0.43 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool mobilenodes 30.0.0.2 30.0.0.255
ip local pool pdsn-pool 122.3.0.1 122.3.16.1
ip local pool pdsn-pool 122.4.0.1 122.4.16.1
ip local pool pdsn-pool 122.5.0.1 122.5.16.1
ip local pool pdsn-pool 122.1.0.1 122.1.16.1
ip local pool pdsn-pool 122.2.0.1 122.2.16.1
ip default-gateway 9.15.0.1
ip classless
ip route 7.0.0.1 255.255.255.255 16.1.1.60
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.6
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
```

```
ip route 150.150.10.3 255.255.255.255 47.0.0.11
no ip http server
!
!
!
!
radius-server host 10.76.86.62 auth-port 1645 acct-port 1646 key cisco
radius-server key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
alias exec cls clear cdma pdsn session all
alias exec cpu show proc cpu | i CPU
alias exec crad clear radius statistics
alias exec tclear clear vpdn tunnel l2tp all
alias exec cstats clear cdma pdsn statistics
alias exec sip show cdma pdsn | i Simple
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
!
!
end

MWAM-PDSN3#


MWAM-PDSN4#sh running-config
Building configuration...

Current configuration : 3387 bytes
!
! Last configuration change at 00:34:26 UTC Thu Jun 5 2003
! NVRAM config last updated at 00:34:28 UTC Thu Jun 5 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname MWAM-PDSN4
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
```

```
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.2 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.174 255.255.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.4 255.0.0.0
!
interface GigabitEthernet0/0.47
 encapsulation dot1Q 47
 ip address 47.0.0.44 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
```

```
ip local pool pdsn-pool 123.1.0.1 123.1.16.1
ip local pool pdsn-pool 123.2.0.1 123.2.16.1
ip local pool pdsn-pool 123.3.0.1 123.3.16.1
ip local pool pdsn-pool 123.4.0.1 123.4.16.1
ip local pool pdsn-pool 123.5.0.1 123.5.16.1
ip classless
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.32
ip route 150.150.6.2 255.255.255.255 47.0.0.6
ip route 150.150.6.3 255.255.255.255 47.0.0.33
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
ip route 150.150.10.3 255.255.255.255 47.0.0.11
no ip http server
!
!
!
!
radius-server host 9.15.50.5 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
alias exec cls clear cdma pdsn session all
alias exec cpu show proc cpu | i CPU
alias exec crad clear radius statistics
alias exec tclear clear vpdn tunnel l2tp all
alias exec cstats clear cdma pdsn statistics
alias exec sip show cdma pdsn | i Simple
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
!
!
end

MWAM-PDSN4#
```

```
MWAM-PDSN5#sh running-config
Building configuration...

Current configuration : 3389 bytes
!
! Last configuration change at 00:34:48 UTC Thu Jun 5 2003
! NVRAM config last updated at 00:34:50 UTC Thu Jun 5 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname MWAM-PDSN5
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.5 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
 tunnel bandwidth transmit 0
```

```
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.175 255.255.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.5 255.255.0.0
!
interface GigabitEthernet0/0.47
 encapsulation dot1Q 47
 ip address 47.0.0.45 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
ip local pool pdsn-pool 124.1.0.1 124.1.16.1
ip local pool pdsn-pool 124.2.0.1 124.2.16.1
ip local pool pdsn-pool 124.3.0.1 124.3.16.1
ip local pool pdsn-pool 124.4.0.1 124.4.16.1
ip local pool pdsn-pool 124.5.0.1 124.5.16.1
ip classless
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.32
ip route 150.150.6.2 255.255.255.255 47.0.0.6
ip route 150.150.6.3 255.255.255.255 47.0.0.33
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
ip route 150.150.10.3 255.255.255.255 47.0.0.11
no ip http server
!
!
!
!
radius-server host 9.15.50.5 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
alias exec cls clear cdma pdsn session all
alias exec cpu show proc cpu | i CPU
alias exec crad clear radius statistics
alias exec tclear clear vpdn tunnel l2tp all
```

```
alias exec cstats clear cdma pdsn statistics
alias exec sip show cdma pdsn | i Simple
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
!
!
end

MWAM-PDSN5#
```

```
MWAM-PDSN6#sh running-config
Building configuration...

Current configuration : 3387 bytes
!
! Last configuration change at 00:35:03 UTC Thu Jun 5 2003
! NVRAM config last updated at 00:35:44 UTC Thu Jun 5 2003
!
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service cdma pdsn
!
hostname MWAM-PDSN6
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa accounting network pdsn start-stop group radius
!
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
vpdn enable
vpdn authen-before-forward
```

```
vpdn ip udp ignore checksum
!
vpdn-group CDMA
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 150.150.0.100
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 87.0.0.6 255.0.0.0
!
interface CDMA-Ix1
 ip address 150.150.0.100 255.255.254.0
 tunnel source 150.150.0.100
 tunnel key 1
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 25
 ip address 9.15.50.176 255.255.0.0
!
interface GigabitEthernet0/0.37
 encapsulation dot1Q 37
 ip address 37.0.0.6 255.0.0.0
!
interface GigabitEthernet0/0.47
 encapsulation dot1Q 47
 ip address 47.0.0.46 255.0.0.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
ip local pool pdsn-pool 125.1.0.1 125.1.16.1
ip local pool pdsn-pool 125.2.0.1 125.2.16.1
ip local pool pdsn-pool 125.3.0.1 125.3.16.1
ip local pool pdsn-pool 125.4.0.1 125.4.16.1
ip local pool pdsn-pool 125.5.0.1 125.5.16.1
ip classless
ip route 9.100.0.0 255.255.0.0 9.15.0.1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.76.86.41 255.255.255.255 9.15.0.1
ip route 10.76.86.62 255.255.255.255 9.15.0.1
ip route 150.150.2.2 255.255.255.255 47.0.0.2
ip route 150.150.2.3 255.255.255.255 47.0.0.3
ip route 150.150.4.2 255.255.255.255 47.0.0.4
ip route 150.150.4.3 255.255.255.255 47.0.0.5
ip route 150.150.6.2 255.255.255.255 47.0.0.32
ip route 150.150.6.2 255.255.255.255 47.0.0.6
```

```
ip route 150.150.6.3 255.255.255.255 47.0.0.33
ip route 150.150.6.3 255.255.255.255 47.0.0.7
ip route 150.150.8.2 255.255.255.255 47.0.0.8
ip route 150.150.8.3 255.255.255.255 47.0.0.9
ip route 150.150.10.2 255.255.255.255 47.0.0.10
ip route 150.150.10.3 255.255.255.255 47.0.0.11
no ip http server
!
!
!
!
radius-server host 9.15.50.5 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting 3gpp2
cdma pdsn pcf default closed-rp
cdma pdsn virtual-template 1
no cdma pdsn a10 ahdlc trailer
!
control-plane
!
alias exec cls clear cdma pdsn session all
alias exec cpu show proc cpu | i CPU
alias exec crad clear radius statistics
alias exec tclear clear vpdn tunnel l2tp all
alias exec cstats clear cdma pdsn statistics
alias exec sip show cdma pdsn | i Simple
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line vty 0 4
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 exec-timeout 0 0
 transport preferred all
 transport input all
 transport output all
!
!
end

MWAM-PDSN6#
```

Open-Closed RP Configuration Example

Controller Configuration

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service cdma pdsn
!
hostname ctlr76
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
no aaa new-model
!
resource policy
!
clock timezone IST 5 30
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 41.0.0.41
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
vpdn-group MEMBERS
 request-dialin
  protocol l2tp
 source-ip 41.0.0.41
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 no ip address
!
interface CDMA-Ix1
 no ip address
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.110
 description PCF
 encapsulation dot1Q 110
 ip address 41.0.0.76 255.0.0.0
 no snmp trap link-status
 no cdp enable
 standby 1 ip 41.0.0.41
 standby 1 priority 110
```

```
 standby 1 preempt
 standby 1 name SSP-CTLR
!
ip classless
ip route 5.0.0.82 255.255.255.255 41.0.0.82
no ip http server
!
!
!
!
!
no cdma pdsn a10 gre sequencing
cdma pdsn timeout a11-update 5
cdma pdsn secure pcf default spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
cdma pdsn cluster controller interface GigabitEthernet0/0.110
cdma pdsn cluster controller standby SSP-CTLR
cdma pdsn cluster controller member periodic-update
cdma pdsn cluster controller queueing
cdma pdsn cluster controller closed-rp MEMBERS
!
control-plane
!
line con 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
line vty 1 4
line vty 5 15
!
!
end
```

Member Configuration

```
! Last configuration change at 10:46:54 IST Fri Nov 11 2005
! NVRAM config last updated at 14:17:44 IST Thu Nov 10 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service cdma pdsn
!
hostname mem82a
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby PDSN-SSP-SR
!
!
redundancy
enable password lab
!
aaa new-model
!
!
```

```
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting network pdsn start-stop group radius
!
!
aaa session-id common
!
resource policy
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 2000
    local-ip 41.0.1.82
   remote-port 2000
    remote-ip 41.0.2.82
!
clock timezone IST 5 30
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
!
subscriber redundancy rate 500 1
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 5.0.0.82
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
interface Loopback0
 ip address 82.82.82.82 255.255.255.0
!
interface Loopback1
 ip address 7.0.0.82 255.255.255.0
!
interface CDMA-Ix1
 ip address 5.0.0.82 255.255.255.0
 tunnel source 5.0.0.82
 tunnel key 107036
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
```

```
!
interface GigabitEthernet0/0.51
 description AAA
 encapsulation dot1Q 51
 ip address 51.0.0.82 255.0.0.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.71
 description PI
 encapsulation dot1Q 71
 ip address 71.0.1.82 255.0.0.0
 no snmp trap link-status
 standby 182 ip 71.0.0.82
 standby 182 follow PDSN-SSP-SR
!
interface GigabitEthernet0/0.110
 description RP
 encapsulation dot1Q 110
 ip address 41.0.1.82 255.0.0.0
 no snmp trap link-status
 standby 82 ip 41.0.0.82
 standby 82 name PDSN-SSP-SR
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool ispabc-pool1
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool ispabc-pool1 82.0.1.0 82.0.16.255
ip local pool ispabc-pool1 82.0.17.0 82.0.32.255
ip local pool ispabc-pool1 82.0.33.0 82.0.48.255
ip local pool ispabc-pool1 82.0.49.0 82.0.64.255
ip local pool ispabc-pool1 82.0.65.0 82.0.79.31
ip classless
ip route 72.0.0.0 255.0.0.0 71.0.0.254
no ip http server
ip mobile foreign-agent care-of Loopback1
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
ip mobile registration-lifetime 65535
!
!
!
snmp-server community public RO
!
!
radius-server host 51.0.0.2 auth-port 1645 acct-port 1646 key cisco
cdma pdsn pcf default closed-rp
cdma pdsn accounting send start-stop
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
no cdma pdsn a10 gre sequencing
cdma pdsn timeout a11-update 5
cdma pdsn secure pcf default spi 100 key ascii cisco replay 200
cdma pdsn secure cluster default spi 100 key ascii cisco
cdma pdsn cluster member controller 41.0.0.41
cdma pdsn cluster member interface GigabitEthernet0/0.110
cdma pdsn cluster member queueing
cdma pdsn redundancy
```

```
!
control-plane
!
line con 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
line vty 1 4
line vty 5 15
!
!
end
```

Session Redundancy Configuration Examples

Supervisor Configuration

```
!
! Last configuration change at 14:50:14 IST Tue Dec 13 2005
! NVRAM config last updated at 17:20:23 IST Wed Nov 30 2005
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 10
!
hostname mwtbc11-7609a
!
boot system flash disk0:
logging snmp-authfail
enable password lab
!
no aaa new-model
clock timezone IST 5 30
mwam module 7 port 1 allowed-vlan 1-4094
mwam module 7 port 2 allowed-vlan 1-4094
mwam module 7 port 3 allowed-vlan 1-4094
mwam module 8 port 1 allowed-vlan 1-4094
mwam module 8 port 2 allowed-vlan 1-4094
mwam module 8 port 3 allowed-vlan 1-4094
ip subnet-zero
ip rcmd rcp-enable
!
!
no ip domain-lookup
!
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
no scripting tcl init
no scripting tcl encdir
!
!
redundancy
 mode rpr-plus
```

```
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface FastEthernet1/1
 no ip address
 shutdown
!
interface FastEthernet1/2
 no ip address
 shutdown
!
interface FastEthernet1/3
 switchport
 switchport access vlan 71
 switchport mode access
 no ip address
!
interface FastEthernet1/4
 no ip address
 shutdown
!
interface FastEthernet1/5
 no ip address
 shutdown
!
interface FastEthernet1/6
 no ip address
 shutdown
!
interface FastEthernet1/7
 no ip address
 shutdown
!
interface FastEthernet1/8
 no ip address
 shutdown
!
interface FastEthernet1/9
 switchport
 switchport access vlan 51
 switchport mode access
 no ip address
!
interface FastEthernet1/10
 no ip address
 shutdown
!
interface FastEthernet1/11
 no ip address
 shutdown
!
interface FastEthernet1/12
 no ip address
 shutdown
```

```
!
interface FastEthernet1/13
 no ip address
 shutdown
!
interface FastEthernet1/14
 no ip address
 shutdown
!
interface FastEthernet1/15
 no ip address
 shutdown
!
interface FastEthernet1/16
 no ip address
 shutdown
!
interface FastEthernet1/17
 no ip address
 shutdown
!
interface FastEthernet1/18
 no ip address
 shutdown
!
interface FastEthernet1/19
 no ip address
 shutdown
!
interface FastEthernet1/20
 no ip address
 shutdown
!
interface FastEthernet1/21
 no ip address
 shutdown
!
interface FastEthernet1/22
 no ip address
 shutdown
!
interface FastEthernet1/23
 no ip address
 shutdown
!
interface FastEthernet1/24
 no ip address
 shutdown
!
interface FastEthernet1/25
 no ip address
 shutdown
!
interface FastEthernet1/26
 no ip address
 shutdown
!
interface FastEthernet1/27
 no ip address
 shutdown
!
interface FastEthernet1/28
 no ip address
 shutdown
```

```
!
interface FastEthernet1/29
 no ip address
 shutdown
!
interface FastEthernet1/30
 no ip address
 shutdown
!
interface FastEthernet1/31
 no ip address
 shutdown
!
interface FastEthernet1/32
 no ip address
 shutdown
!
interface FastEthernet1/33
 no ip address
 shutdown
!
interface FastEthernet1/34
 no ip address
 shutdown
!
interface FastEthernet1/35
 no ip address
 shutdown
!
interface FastEthernet1/36
 no ip address
 shutdown
!
interface FastEthernet1/37
 no ip address
 shutdown
!
interface FastEthernet1/38
 no ip address
 shutdown
!
interface FastEthernet1/39
 no ip address
 shutdown
!
interface FastEthernet1/40
 no ip address
 shutdown
!
interface FastEthernet1/41
 no ip address
 shutdown
!
interface FastEthernet1/42
 no ip address
 shutdown
!
interface FastEthernet1/43
 no ip address
 shutdown
!
interface FastEthernet1/44
 no ip address
 shutdown
```

```
!
interface FastEthernet1/45
 no ip address
 shutdown
!
interface FastEthernet1/46
 no ip address
 shutdown
!
interface FastEthernet1/47
 no ip address
 shutdown
!
interface FastEthernet1/48
 no ip address
 shutdown
!
interface GigabitEthernet2/1
 switchport
 switchport access vlan 110
 switchport mode access
 no ip address
!
interface GigabitEthernet2/2
 switchport
 switchport access vlan 73
 switchport mode access
 no ip address
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 shutdown
!
interface GigabitEthernet2/5
 no ip address
 shutdown
!
interface GigabitEthernet2/6
 no ip address
 shutdown
!
interface GigabitEthernet2/7
 no ip address
 shutdown
!
interface GigabitEthernet2/8
 no ip address
 shutdown
!
interface GigabitEthernet2/9
 no ip address
 shutdown
!
interface GigabitEthernet2/10
 no ip address
 shutdown
!
interface GigabitEthernet2/11
 no ip address
 shutdown
```

```
!
interface GigabitEthernet2/12
 no ip address
 shutdown
!
interface GigabitEthernet2/13
 no ip address
 shutdown
!
interface GigabitEthernet2/14
 no ip address
 shutdown
!
interface GigabitEthernet2/15
 no ip address
 shutdown
!
interface GigabitEthernet2/16
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 no ip address
 shutdown
!
interface GigabitEthernet9/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 mtu 4500
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet9/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 4500
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 shutdown
!
```

```
interface Vlan71
 description PI Interface
 ip address 71.0.0.254 255.0.0.0
!
interface Vlan73
 description To the Sup on the HA chassis
 ip address 73.0.0.2 255.255.255.0
standby 73 ip 73.0.0.73
 standby 73 name PDSN-SUP
!
interface Vlan110
 description RP Interface
 ip address 41.0.0.252 255.0.0.0
!
ip classless
ip route 7.0.0.82 255.255.255.255 71.0.0.82
ip route 72.0.0.0 255.0.0.0 73.0.0.1
ip route 82.0.0.0 255.0.0.0 71.0.0.82
!
no ip http server
!
snmp-server community public RO
!
!
control-plane
!
!
dial-peer cor custom
!
!
alias exec sia show crypto ipsec sa
alias exec cec show crypto engine connections active
alias exec csa clear crypto sa
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password cisco
 login
line vty 5 15
 exec-timeout 0 0
 privilege level 15
 password cisco
 login
!
!
monitor event-trace timestamps
no cns aaa enable
end
```

PDSN 1 Configuration

```
!
! Last configuration change at 10:46:54 IST Fri Nov 11 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
```

```
service cdma pdsn
!
hostname mem82a
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby PDSN-SSP-SR
!
!
redundancy
enable password lab
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting network pdsn start-stop group radius
!
!
aaa session-id common
!
resource policy
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 2000
    local-ip 41.0.1.82
   remote-port 2000
    remote-ip 41.0.2.82
!
clock timezone IST 5 30
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
!
subscriber redundancy rate 500 1
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 5.0.0.82
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
```

```
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 82.82.82.82 255.255.255.0
!
interface Loopback1
 ip address 7.0.0.82 255.255.255.0
!
interface CDMA-Ix1
 ip address 5.0.0.82 255.255.255.0
 tunnel source 5.0.0.82
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.51
 description To AAA Server
 encapsulation dot1Q 51
 ip address 51.0.0.82 255.0.0.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.71
 description PI Interface
 encapsulation dot1Q 71
 ip address 71.0.1.82 255.0.0.0
 no snmp trap link-status
 standby 182 ip 71.0.0.82
 standby 182 follow PDSN-SSP-SR
!
interface GigabitEthernet0/0.110
 description RP Interface
 encapsulation dot1Q 110
 ip address 41.0.1.82 255.0.0.0
 no snmp trap link-status
 standby 82 ip 41.0.0.82
 standby 82 name PDSN-SSP-SR
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool pdsn-pool 82.0.1.0 82.0.16.255
ip local pool pdsn-pool 82.0.17.0 82.0.32.255
ip local pool pdsn-pool 82.0.33.0 82.0.48.255
ip local pool pdsn-pool 82.0.49.0 82.0.64.255
ip local pool pdsn-pool 82.0.65.0 82.0.79.31
ip classless
ip route 72.0.0.0 255.0.0.0 71.0.0.254
no ip http server
ip mobile foreign-agent care-of Loopback1
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
ip mobile registration-lifetime 65535
!
```

```
!
!
snmp-server community public RO
!
!
radius-server host 51.0.0.2 auth-port 1645 acct-port 1646 key cisco
cdma pdsn pcf default closed-rp
cdma pdsn accounting send start-stop
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
no cdma pdsn a10 gre sequencing
cdma pdsn timeout a11-update 5
cdma pdsn secure pcf default spi 100 key ascii cisco replay 200
cdma pdsn secure cluster default spi 100 key ascii cisco
cdma pdsn cluster member controller 41.0.0.41
cdma pdsn cluster member interface GigabitEthernet0/0.110
cdma pdsn cluster member queueing
cdma pdsn redundancy
!
control-plane
!
line con 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
line vty 1 4
line vty 5 15
!
!
end
```

PDSN 2 Configuration

```
!
! Last configuration change at 12:35:50 IST Thu Nov 10 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service cdma pdsn
!
hostname mem82b
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby PDSN-SSP-SR
!
!
redundancy
enable password lab
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
```

```
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting network pdsn start-stop group radius
!
!
aaa session-id common
!
resource policy
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 2000
    local-ip 41.0.2.82
   remote-port 2000
    remote-ip 41.0.1.82
!
clock timezone IST 5 30
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
!
subscriber redundancy rate 500 1
vpdn enable
vpdn authen-before-forward
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 source-ip 5.0.0.82
 l2tp tunnel hello 0
 no l2tp tunnel authentication
 l2tp tunnel timeout no-session never
!
no virtual-template snmp
!
!
!
interface Loopback0
 ip address 82.82.82.82 255.255.255.0
!
interface Loopback1
 ip address 7.0.0.82 255.255.255.0
!
interface CDMA-Ix1
 ip address 5.0.0.82 255.255.255.0
 tunnel source 5.0.0.82
 tunnel bandwidth transmit 0
 tunnel bandwidth receive 0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.51
 description To AAA Server
```

```
 encapsulation dot1Q 51
 ip address 51.0.0.182 255.0.0.0
 no snmp trap link-status
!
interface GigabitEthernet0/0.71
 description PI Interface
 encapsulation dot1Q 71
 ip address 71.0.2.82 255.0.0.0
 no snmp trap link-status
 standby 182 ip 71.0.0.82
 standby 182 follow PDSN-SSP-SR
!
interface GigabitEthernet0/0.110
 description RP Interface
 encapsulation dot1Q 110
 ip address 41.0.2.82 255.0.0.0
 no snmp trap link-status
 standby 82 ip 41.0.0.82
 standby 82 name PDSN-SSP-SR
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pdsn-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool pdsn-pool 82.0.1.0 82.0.16.255
ip local pool pdsn-pool 82.0.17.0 82.0.32.255
ip local pool pdsn-pool 82.0.33.0 82.0.48.255
ip local pool pdsn-pool 82.0.49.0 82.0.64.255
ip local pool pdsn-pool 82.0.65.0 82.0.79.31
ip classless
ip route 72.0.0.0 255.0.0.0 71.0.0.254
no ip http server
ip mobile foreign-agent care-of Loopback1
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
ip mobile registration-lifetime 65535
!
!
!
snmp-server community public RO
!
!
radius-server host 51.0.0.1 auth-port 1645 acct-port 1646 key cisco
cdma pdsn pcf default closed-rp
cdma pdsn accounting send start-stop
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
no cdma pdsn a10 gre sequencing
cdma pdsn timeout a11-update 5
cdma pdsn secure pcf default spi 100 key ascii cisco replay 200
cdma pdsn secure cluster default spi 100 key ascii cisco
cdma pdsn cluster member controller 41.0.0.41
cdma pdsn cluster member interface GigabitEthernet0/0.110
cdma pdsn cluster member queueing
cdma pdsn redundancy
!
control-plane
!
```

```
line con 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
line vty 1 4
line vty 5 15
!
!
end
```

Simple IPV6 Configuration Example

```
PDSN:
pdsn2#sh run
Building configuration...

Current configuration : 4595 bytes
!
version 12.3
no service pad
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service cdma pdsn
!
hostname mwtcc21-pdsn2
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby pdsn-sr0
!
!
redundancy
no logging queue-limit
enable password lab
!
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 1
aaa accounting network pdsn start-stop group radius
!
!
aaa session-id common
!
resource manager
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 4.0.0.103
```

```
   remote-port 5000
    remote-ip 4.0.0.101
!
ip subnet-zero
!
!
ip cef
ip cef accounting per-prefix non-recursive
ip domain name cisco.com
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
ipv6 unicast-routing
ipv6 cef
!
no virtual-template snmp
!
!
username pdsn2 password 0 cisco
!
!
interface Loopback0
 ip address 6.0.0.1 255.0.0.0
!
interface Loopback2
 ip address 77.0.0.1 255.0.0.0
!
interface Loopback3
 ip address 3.0.0.1 255.0.0.0
!
interface CDMA-Ix1
 ip address 5.0.0.1 255.0.0.0
 tunnel source 5.0.0.1
 tunnel key 1
 tunnel sequence-datagrams
!
interface FastEthernet0/0
 ip address 10.77.154.236 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 86.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 22.22.22.3 255.0.0.0
 duplex full
 no cdp enable
!
interface FastEthernet2/0
 ip address 88.0.0.4 255.0.0.0
 duplex half
 standby delay minimum 30 reload 60
 standby 12 ip 88.0.0.251
 standby 12 name pdsn-sr2
!
interface FastEthernet3/0
 ip address 4.0.0.103 255.0.0.0
 duplex auto
 speed auto
 standby delay minimum 30 reload 60
```

```
 standby 10 ip 4.0.0.254
 standby 10 name pdsn-sr0
!
interface FastEthernet3/1
 ip address 7.0.0.4 255.0.0.0
 duplex auto
 speed auto
 standby delay minimum 30 reload 60
 standby 11 ip 7.0.0.254
 standby 11 name pdsn-sr1
!
interface Ethernet4/0
 no ip address
 duplex half
 ipv6 enable
!
interface Ethernet4/1
 ip address 66.0.0.2 255.0.0.0
 duplex half
 ipv6 address 2001::1/64
 ipv6 enable
!
interface Ethernet4/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet4/3
 no ip address
 shutdown
 duplex half
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ipv6 enable
 ipv6 nd ra-interval 1000
 ipv6 nd ra-lifetime 5000
 no ipv6 nd suppress-ra
 no peer default ip address
 peer default ipv6 pool pdsn-ipv6-pool
 no keepalive
 compress stac
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool pdsn-pool 11.0.0.1 11.0.0.255
ip default-gateway 10.77.154.193
ip classless
ip route 9.0.0.2 255.255.255.255 86.0.0.1
ip route 15.0.0.0 255.0.0.0 7.0.0.2
ip route 19.0.0.0 255.0.0.0 7.0.0.2
ip route 17.19.21.34 255.255.255.255 88.0.0.3
ip mobile foreign-agent care-of Loopback2
ip mobile foreign-service challenge forward-mfce timeout 10
ip mobile foreign-service reverse-tunnel
ip mobile registration-lifetime 60000
!
no ip http server
no ip http secure-server
!
!
ip radius source-interface Loopback3
```

```
ipv6 local pool pdsn-ipv6-pool 2001:420:10::/48 64
!
!
radius-server host 9.0.0.2 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
cdma pdsn accounting send start-stop
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdlc engine 0 usable-channels 8000
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn send-agent-adv
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii cisco
cdma pdsn secure pcf 4.0.0.2 spi 100 key ascii cisco
cdma pdsn ipv6
cdma pdsn redundancy
cdma pdsn redundancy accounting update-periodic
!
control-plane
!
!
gatekeeper
 shutdown
!
alias dhcp hu util ma hi
alias dhcp lu util ma lo
alias dhcp o30 origin dhcp subnet size initial /30 autogrow /30
alias dhcp o29 origin dhcp subnet size initial /29 autogrow /29
alias dhcp sp30 subnet prefix-length 30
alias dhcp sp subnet prefix-length
alias dhcp sp29 subnet prefix-length 29
alias dhcp sp28 subnet prefix-length 28
alias configure nopl no ip dhcp pool ispabc-odappool
alias configure cpool ip dhc poo ispabc-odappool
alias configure cpl ip dhc poo ispabc-odappool
alias exec shpl sh ip dhc poo
alias exec shb sh ip dhc bin
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 5 15
!
!
end
```

PDSN Accounting

The CDMA2000 packet accounting model is divided into radio specific parameters collected by the radio network elements, and the IP network specific parameters collected by the serving PDSN. In conformance with the packet accounting procedures specified in TIA/EIA/IS-835-B, the PDSN merges the radio specific parameters for a given user session with the IP network specific ones to form a Usage Data Record (UDR). After merging the parameters, the PDSN sends the UDR to the local RADIUS server at trigger events specified. The PDSN maintains the UDR until it receives positive acknowledgment from the RADIUS server indicating that the RADIUS server has correctly received the UDR.

Flow Based Accounting

The Cisco PDSN supports multiple user sessions per mobile station. Each of these user sessions is termed a flow. For each mobile station, one Simple IP based flow and one or more Mobile IP based flows can be supported. Each flow is identified by a unique IP address. Accounting procedures for generating a separate UDR for each flow is called flow based accounting.

The Cisco PDSN supports flow based accounting. As per TIA/EIA/IS-835-B specifications, each flow is identified by a unique Correlation-ID. Accounting start/stop message pair for each flow is correlated by unique Accounting-Session-ID.

While creating UDRs for flow based accounting, radio specific accounting parameters are common to all flows. IP network specific parameters, such as uplink and downlink octet counts are specific to each flow and are identified by the unique IP address assigned to that flow. The PDSN creates UDR for each flow by merging the radio specific parameters and the IP network specific parameters. These UDRs are forwarded to the RADIUS server via accounting-request (start, stop, interim) messages.

The following RADIUS attributes are contained in the UDR sent by PDSN.

Table 8 In Accounting Start Record

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44
Framed-Protocol		7
Framed-IP-Address	B1	8
Event-Timestamp	G4	55
CDMA-Correlation-ID	C2	26/44

Table 8 In Accounting Start Record

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MSC-Add	D4	26/10
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	11	26/36
CDMA-Airlink-QoS	14	26/39
CDMA-RP-Session-ID	Y2	26/41
CDMA-ESN	A2	26/52
CDMA-MEID	A3	26/116

Table 9 In Accounting Stop Record

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44

Table 9 In Accounting Stop Record (Continued)

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
Framed-Protocol		7
Framed-IP-Address	B1	8
Event-Timestamp	G4	55
Acct-Output-Octets	G1	43
Acct-Input-Octets	G2	42
Acct-Input-Packets		47
Acct-Output-Packets		48
Acct-Session-Time		46
Acct-Input-Giga-Words		52
Acct-Output-Giga-Words		53
DHHC-Frame-Format	F14	26/50
CDMA-Active-Time	G8	26/49
CDMA-Correlation-ID	C2	26/44
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MSC-Add	D4	26/10
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	11	26/36
CDMA-Mobile-IP-Signaling-In-Bound Count	G15	26/46
CDMA-Mobile-IP-Signaling-Out-Bound-Count	G16	26/47
CDMA-Airlink-QoS	14	26/39
CDMA-RP-Session-ID	Y2	26/41
CDMA-Bad-Frame-Count	G3	26/25

Table 9 In Accounting Stop Record (Continued)

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
CDMA-HDLC-Layer-Bytes-In	G14	26/43
CDMA-SDB-Input-Octets	G10	26/31
CDMA-SDB-Output-Octets	G11	26/32
CDMA-NumSDB-Input	G12	26/33
CDMA-NumSDB-Output	G13	26/34
CDMA-last-user-activity	G17	
CDMA-Reason-Ind	F13	26/24
CDMA-Session-Continue	C3	26/48
CDMA-ESN	A2	26/52
CDMA-MEID	A3	26/116

The following list identifies the prepaid VSAs that can be included in the RADIUS attributes contained in the Accounting Stop Record:

- crb-auth-reason
- crb-duration
- crb-total-volume
- crb-uplink-volume
- crb-downlink-volume
- crb-total-packets
- crb-uplink-packets
- crb-downlink-packets
- crb-session-id

Table 10 In Interim-accounting Record

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44
Framed-Protocol		7

Table 10 In Interim-accounting Record (Continued)

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
Framed-IP-Address	B1	8
Event-Timestamp	G4	55
Acct-Output-Octets	G1	43
Acct-Input-Octets	G2	42
Acct-Input-Packets		47
Acct-Output-Packets		48
Acct-Input-Giga-Words		52
Acct-Output-Giga-Words		53
CDMA-Active-Time	G8	26/49
CDMA-Correlation-ID	C2	26/44
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MSC-Add	D4	26/10
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	11	26/36
CDMA-Airlink-QoS	14	26/39
CDMA-RP-Session-ID	Y2	26/41
CDMA-HDLC-Layer-Bytes-In	G14	26/43
CDMA-Bad-Frame-Count	G3	26/25
CDMA-SDB-Input-Octets	G10	26/31
CDMA-SDB-Output-Octets	G11	26/32
CDMA-NumSDB-Input	G12	26/33

Table 10 In Interim-accounting Record (Continued)

Attribute Name	TIA/EIA/IS-835-B	Type/Subtype
CDMA-NumSDB-Output	G13	26/34
CDMA-last-user-activity	G17	

AAA Authentication and Authorization Profile

This section describes User Profiles to be configured at the AAA server for authentication and authorization of users for various service types (Simple IP, Mobile IP, etc.). It also describes the minimal configuration required for the same.

1. Client router should be authorized to access Cisco Access Registrar

The client profile contains the ip address of the router and the shared key. The following example illustrates a client profile:

```
[ //localhost/Radius/Clients/username ]
    Name = username
    Description =
    IPAddress = 9.15.68.7
    SharedSecret = lab
    Type = NAS
    Vendor =



    IncomingScript~ =
    OutgoingScript~ =
    UseDNIS = FALSE
    DeviceName =
    DevicePassword =
```

2. A User should have a profile configured at AAA (this is applicable to an NAI as well, in case of MoIP).

A user profile contains username, password, and the base profile where attributes retrieved during authorization can be configured.

The following example illustrates a user profile:

```
[ //localhost/Radius/UserLists/Default/username ]
    Name = username
    Description =
    Password = <encrypted>
    AllowNullPassword = FALSE
    Enabled = TRUE
    Group~ =
    BaseProfile~ = username-sip
    AuthenticationScript~ =
    AuthorizationScript~ =
    UserDefined1 =
```

3. A Base Profile contains attributes applied for the user during authorization.

The following example illustrates a base profile :

```
[ //localhost/Radius/Profiles/username-sip ]
    Name = username-sip
    Description =
    Attributes/
```

4. cd attributes

```
[ //localhost/Radius/Profiles/username-sip/Attributes ]
    CDMA-IP-Technology = x
```

AAA Profiles for Various Service Types

The following examples document AAA profiles for various service types such as SIP, MoIP, and others. The mandatory/optional attributes, and the attributes required to be configured for enabling different features, are specified.

Simple IP

CDMA-IP-Technology = x

The following attributes are optional and are needed only for specific scenarios:

- IP address assignment is done through AAA:

  Framed-IP-Address = 8.1.0.2

- Download pool name:

  cisco-avpair = ip:addr-pool=pdsn-pool

- Enable compression:

  cisco-avpair = “lcp:interface-config=compress stac”

  cisco-avpair = “lcp:interface-config=compress mppc”

  cisco-avpair = “lcp:interface-config=compress predictor”

- Other Optional Parameters

  Framed-Protocol = PPP

  Framed-Routing = None

  Service-Type = Framed

VPDN

cisco-avpair = vpdn:tunnel-type=l2tp

cisco-avpair = vpdn:ip-addresses=5.5.5.1

cisco-avpair = vpdn:l2tp-tunnel-password=cisco

The following configuration is optional at AAA contacted by LNS:

cisco-avpair = ip:addr-pool=pdsn-pool

MSID based Authentication

- (a)Simple IP case :

  cisco-avpair = cdma:cdma-realm=cisco.com

  CDMA-IP-Technology = x
- (b)Proxy Mobile IP Case :

  cisco-avpair = lcp:cdma-user-class=3

  cisco-avpair = cdma:cdma-realm=cisco.com

  cisco-avpair = “lcp:spi#0 = spi 100 key ascii cisco”

  cisco-avpair = lcp:cdma-ha-ip-addr=5.5.5.1

Proxy Mobile IP

cisco-avpair = lcp:cdma-ha-ip-addr=5.5.5.1

cisco-avpair = “lcp:spi#0 = spi 100 key ascii cisco”

cisco-avpair = lcp:cdma-user-class=3

Mobile IP

- cisco-avpair = lcp:cdma-user-class=2

  The following attributes are optional, and are only needed for specific scenarios:
  - Dynamic Home Agent Assignment :

    CDMA-HA-IP-Addr = 6.0.0.2
  - Download Security Association and static IP addresses (at Home Agent):

    cisco-avpair = “mobileip:spi#0=spi 100 key ascii cisco”

    cisco-avpair = “mobileip:static-ip-addresses=20.0.0.1 20.0.0.2 20.0.0.3 20.0.0.4”
  - Download Static ip pool name (at Home Agent):

    cisco-avpair = “mobileip:spi#0=spi 100 key ascii cisco”

    cisco-avpair = “mobileip:static-ip-pool=mypool”

Prepaid (Optional)

- cisco-avpair = “crb-entity-type=1”

Attributes

This section lists several of the various Accounting and Authentication attributes for the Cisco PDSN.

Authentication and Authorization RADIUS Attributes

The PDSN, Home Agent, and the RADIUS server support RADIUS attributes listed in Table 11 and Table 12 for authentication and authorization services.

Table 11 Authentication and Authorization AVPs Supported by Cisco IOS

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
User-Name	1	NA	64	string	User name for authentication and authorization.	Yes	No
User-Password	2	NA	>=18 && <=130	string	Password for authentication	Yes	No
CHAP-Password	3	NA	19	string	CHAP password	Yes	No
NAS-IP-Address	4	NA	4	IP address	IP address of the PDSN interface used for communicating with RADIUS server.	Yes	No
Service Type	6	NA	4	integer	Type of service the user is getting. Supported values: • Outbound for MSID based user access • Framed for other type of user access	Yes	Yes
Framed-Protocol	7	NA	4	integer	Framing protocol user is using. Supported values: • PPP	Yes	Yes
Framed-IP-Address	8	NA	4	integer	IP address assigned to user.	Yes	Yes
Vendor-Specific	26	NA			Vendor Specific Attributes	Yes	Yes
Session-Time-out	27	NA	4	integer	Maximum number of seconds service is to be provided to the user before session terminates. This attribute value becomes the per-user “absolute time-out”.	No	Yes
Idle-Time-out	28	NA	4	integer	Maximum number of consecutive seconds of idle connection allowed to the user before the session terminates. This attribute value becomes the per-user “idle-time-out”.	No	Yes
Calling-Station-ID	31	15	NA	string	MSID identifier of the mobile user.	Yes	No
CHAP-Challenge (optional)	60	NA	>=7	string	CHAP Challenge	Yes	No

Table 11 Authentication and Authorization AVPs Supported by Cisco IOS (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
Tunnel-Type	64	NA	6		VPN tunneling protocol(s) used. Supported values: • 1 for PPTP (not supported) • 3 for L2TP	No	Yes
Tunnel-Medium- Type	65	NA			Transport medium type to use for the tunnel.	No	Yes
Tunnel-Client- Endpoint	66	NA	4	ip-addr	Address of the client end of the tunnel.	No	Yes
Tunnel-Server- Endpoint	67	NA	4	ip-addr	Address of the server end of the tunnel.	No	Yes
Tunnel-Password	69	NA	>=5	string	Password to be used for authenticating remote server.	No	Yes
Tunnel-Assignment- ID	82	NA	>=3	string	Indicates to the initiator of the tunnel, identifier of the tunnel to which the session is assigned.	No	Yes
addr-pool	26/1	Cisco	>=3	string	Name of a local pool from which to obtain address. Used with service=ppp and protocol=ip. "addr-pool" works in conjunction with local pooling. It specifies the name of a local pool (which must have been pre-configured locally). Use the ip-local pool command for configuring local pools. For example: • ip address-pool local • ip local pool boo 10.0.0.1 10.0.0.10 • ip local pool moo 10.0.0.1 10.0.0.20	No	Yes
Inacl#<n>	26/1	Cisco	>=3	string	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol =ipx. **Note** Per-user access lists do not currently work with ISDN interfaces.	No	Yes

Table 11 Authentication and Authorization AVPs Supported by Cisco IOS (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
Inacl	26/1	Cisco	>=3	string	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Contains an IP output access list for SLIP or PPP/IP (for example, intacl=4). The access list itself must be pre-configured on the router.	No	Yes
outacl#<n>	26/1	Cisco	>=3	string	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx.	No	Yes
outacl	26/1	Cisco	>=3	string	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be pre-configured on the router.	No	Yes
interface-config	26/1	Cisco	>=3	string	User-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command.	No	Yes

Table 11 Authentication and Authorization AVPs Supported by Cisco IOS (Continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
spi	26/1	Cisco	>=3	string	Carries authentication information needed by the home agent for authenticating a mobile user during MIP registration. Provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range. The information is in the same syntax as the **ip mobile secure host** *addr* configuration command. Essentially, it contains the rest of the configuration command that follows that string, verbatim.		
IP-Pool-Definition	26/217	Cisco	>=3	string	Defines a pool of addresses using the format: X a.b.c Z; where X is the pool index number, a.b.c is the pool's starting IP address, and Z is the number of IP addresses in the pool. For example, 3 10.0.0.1 5 allocates 10.0.0.1 through 10.0.0.5 for dynamic assignment.	No	Yes
Assign-IP-Pool	26/218	Cisco	4	integer	Assign an IP address from the identified IP pool.	No	Yes
Link-Compression	26/233	Cisco	4	integer	Link compression protocol to be used. Supported values are: • 0: None • 1: Stac • 2: Stac-LZS • 3: MS-Stac	No	Yes

Table 12 Table 6.Authentication and Authorization AVPs For Packet Data Services

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
mobileip-mn-lifetime	26/1	Cisco	>=3	string	Defines lifetime used in Proxy MIP RRQ	No	Yes
mobileip-mn-ipaddr	26/1	Cisco	>=3	string	MN IP address for static address assignment. If this attribute is present, this address is used in Proxy MIP RRQ	No	Yes
mobileip-mn-flags	26/1	Cisco	>=3	string	Defines Flags used in Proxy MIP RRQ.	No	Yes
static-ip-addresses	26/1	Cisco	>=3	string	IP address list for static addresses for same NAI but multiple flows. • Used at Home Agent	No	Yes
static-ip-pool	26/1	Cisco	>=3	string	IP address pool name for static address for same NAI with multiple flows. • Used at Home Agent	No	Yes
ip-addresses	26/1	Cisco	>=3	string	IP address list used for dynamic address assignment. • Used at Home Agent	No	Yes
ip-pool	26/1	Cisco	>=3	string	IP address pool name used for dynamic address assignment. • Used at the Home Agent	No	Yes
CDMA-Realm	26/34	Cisco	>=3 && <=64	string	For MSID based access, “realm” information for construction of user name in the form MSID@realm. User name so constructed is used for accounting purposes only. Format of realm information is: • ASCII string specifying “realm” of user’s	No	Yes
CDMA-User-Class	26/35	Cisco	1	integer	Type of service user is subscribed to. Supported values are: • 1 for Simple IP • 2 for Mobile IP	No	Yes

Table 12 Table 6.Authentication and Authorization AVPs For Packet Data Services (Continued)

3GPP2-Reverse-Tunnel-Spec	26/4	3GPP2	4	integer	Indicates whether reverse tunneling is required or not. Supported values are: • 0 for reverse tunneling not required. • 1 for reverse tunneling required.	No	Yes
3GPP2-Home-Agent-Attribute	26/7	3GPP2	4	ip address	Address of the Home Agent	Yes	Yes
3GPP2-IP-Technology	26/22	3GPP2	4	integer	Indicates type of service user is subscribed to. Supported values are: • 1 for Simple IP • 2 for Mobile IP	No	Yes
3GPP2-Correlation-Id	26/44	3GPP2	8	string	Identifies all accounting records generated for a particular user flow.	Yes	Yes
3GPP2-Always-On	26/78	3GPP2	4	integer	Indicates Always On Service. Supported values are: • 0 for non always on users • 1for always on users	No	Yes

Accounting Services RADIUS Attributes

The PDSN and the RADIUS server support the RADIUS attributes listed in Table 13 for accounting services. The inclusion of the various attributes in each of the accounting messages is detailed in the table. The inclusion, or not, of attributes in a message is not configurable.

Table 13 Accounting AVPs For Packet Data Services

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
User-Name	B2	1	NA	64	string	Network Access Identifier (NAI) of the mobile user.	RFC 2865	Yes	Yes	Yes
NAS-IP-Address	D2	4	NA	4	IP addr	PDSN/FA address	RFC 2865	Yes	Yes	Yes
NAS-Port	NA	5	NA	4	integer	Port number on the PDSN used for communicating with the RADIUS server	RFC 2865	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
Service-Type	NA	6	NA	4	integer	Type of service the user is getting. Supported values: • "Outbound" for MSID based user access • "Framed" for other type of user access	RFC 2865	Yes	Yes	Yes
Framed-Protocol	NA	7	NA	4	integer	Framing protocol user is using. Supported values: • PPP	RFC 2865	Yes	Yes	Yes
Framed-IP-Address	B1	8	NA	4	IP addr	IP address assigned to the user.	RFC 2865	Yes	Yes	Yes
Calling-Station-Id	A1	31	NA	15	string	MSID identifier of the mobile user.	RFC 2865	Yes	Yes	Yes
Acct-Status-Type	NA	40	NA	4	integer	Accounting record type Supported Values: • 1 for Start • 2 for Stop • 3 for Interim-Update • 7 for Accounting-On • 8 for Accounting-Off	RFC 2866	Yes	Yes	Yes
Acct-Delay-Time	NA	41	NA	4	integer	Number of seconds PDSN has been trying to send this accounting record.	RFC 2866	Yes	Yes	Yes
Acct-Input-Octets	G2	42	NA	4	integer	Total number of octets in IP packets send by the mobile user (verify)	RFC 2866	Yes	Yes	Yes
Acct-Output-Octets	G1	43	NA	4	integer	Total number of octets in IP packets send to the mobile user (verify)	RFC 2866	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
Acct-Session- Id	C1	44	NA	4	string	A unique accounting ID created by the PDSN that allows stop and start records to be matched in a log file.	RFC 2866	Yes	Yes	Yes
Acct- Authentic	NA	45	NA	4	integer	Method of authenticating the user Supported values: • 1 for RADIUS • 2 for local • 3 for remote	RFC 2866	Yes	Yes	Yes
Acct-Session Time	NA	46	NA	4	integer	Number of seconds user has received service.	RFC 2866	Yes	Yes	Yes
Acct-Input-Packets	NA	47	NA	4	integer	Number of packets sent from the mobile user (verify).	RFC 2866	Yes	Yes	Yes
Acct-Output-Packets	NA	48	NA	4	integer	Number of packets sent to the mobile user (verify).	RFC 2866	Yes	Yes	Yes
EventTime stamp	G4	55	NA	4	integer	Indicates start of accounting session or stop of accounting session if part of a RADIUS start message or stop message, respectively. It is also used in a RADIUS interim message to indicate the time of the event which triggered the interim message.	RFC 2869	Yes	Yes	Yes
NAS-Port- Type	NA	61	NA	4	integer	Type of physical port on the PDSN.	RFC 2865	Yes	Yes	Yes
Source Ipv6 Prefix	B#	97	NA	4-20	Ipv6-prefix	Carries the IPv6 prefix of the MS. The length includes the reserved byte as well as the prefix length field byte (see RFC 3162, section 2.3).	RFC3162	Yes	Yes	Yes
Ipv6 Interface ID	B4	96	NA	10	string	Interface ID of the mobile flow	RFC 3162	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
3GPP2-ESN	A2	26/52	3GPP2	15	string	ASCII string of ESN	IS-835-B	Yes	Yes	Yes
3GPP2-MEID	A3	26/116	3GPP2	14	string	ASCII string of MEID	IS-835-D	Yes	Yes	Yes
3GPP2-HA-IP-Addr	D14	26/7	3GPP2	4	ip-addr	IP address of the Home Agent	IS-835-B	Yes	Yes	Yes
3GPP2-PCF-IP-Addr	D3	26/9	3GPP2	4	ip-addr	IP address of the serving PCF	IS-835-B	Yes	Yes	Yes
3GPP2-BSID	D4	26/10	3GPP2	12	string	Base station ID	IS-835-B	Yes	Yes	Yes
3GPP2-User-Zone-ID	E1	26/11	3GPP2	4	integer	Tiered services user zone	IS-835-B	Yes	Yes	Yes
3GPP2-Forward-Mux-Option	F1	26/12	3GPP2	4	integer	Forward direction multiplex option	IS-835-B	Yes	Yes	Yes
3GPP2-Reverse-Mux-Option	F2	26/13	3GPP2	4	integer	Reverse direction multiplex option	IS-835-B	Yes	Yes	Yes
3GPP2- Service-Option	F5	26/16	3GPP2	4	integer	CDMA air interface service option Supported values: • 07H, • 0fH • 1007H • 016H • 017H • 018H • 019H, 25 decimal • 021H, 33 decimal • 03BH, 59 decimal	IS-835-B	Yes	Yes	Yes
3GPP2-Forward-Traffic-Type	F6	26/17	3GPP2	4	integer	Forward traffic type Supported values: • 0 for Primary • 1 for Secondary	IS-835-B	Yes	Yes	Yes
3GPP2-Reverse-Traffic-Type	F7	26/18	3GPP2	4	integer	Forward traffic type Supported values: • 0 for Primary • 1 for Secondary	IS-835-B	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
3GPP2-Fundamental-Frame-Size	F8	26/19	3GPP2	4	integer	Fundamental channel Frame Size Supported values: • 0 for No Fundamental • 1 for 5ms frame • 2 for 20ms frame	IS-835-B	Yes	Yes	Yes
3GPP2-Forward-Fundamental-RC	F9	26/20	3GPP2	4	integer	Forward Fundamental RC Use is not yet specified in the specs.	IS-835-B	Yes	Yes	Yes
3GPP2-Reverse-Fundamental-RC	F10	26/21	3GPP2	4	integer	Reverse Fundamental RC. Use is not yet specified in the specs.	IS-835-B	Yes	Yes	Yes
3GPP2-IP-Technology	F11	26/22	3GPP2	4	integer	Specifies Simple IP, Mobile IP, or other technology Supported values: • 1 for Simple IP • 2 for Mobile IP Other values are configurable, but the defaults are as follows: • 2 for Proxy Mobile IP • 1 for VPDN	IS-835-B	Yes	Yes	Yes
3GPP2-Comp-Tunnel-Flag	F12	26/23	3GPP2	4	integer	Indicator of invocation of compulsory tunnel established on behalf of MS for providing private network and/or ISP access during a single packet data connection. Supported values: • 0 for no tunnel • 1 for non-secure tunnel • 2 for secure tunnel	IS-835-B	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
3GPP2-Release-Indicator	F13	26/24	3GPP2	4	integer	Specifies reason for sending a Stop record. Supported values: • 0 for unknown • 1 for PPP/service time-out • 2 for Handoff • 3 for PPP termination • 4 for MIP registration failure	IS-835-B	Yes	Yes	Yes
3GPP2-Bad-PPP-Frame-Count	G3	26/25	3GPP2	4	integer	Number of PPP frames from the mobile station dropped by PDSN due to un-correctable errors.	IS-835-B	Yes	Yes	Yes
3GPP2-Num-Active-Transitions	G9	26/30	3GPP2	4	integer	Number of dormant to active transitions by the user.	IS-835-B	Yes	Yes	Yes
3GPP2-SDB-Octet-Count-Terminating	G10	26/31	3GPP2	4	integer	Total number of octets sent to the user via Short Data Bursts.	IS-835-B	Yes	Yes	Yes
3GPP2-SDB-Octet-Count-Originating	G11	26/32	3GPP2	4	integer	Total number of octets sent by the user via Short Data Bursts.	IS-835-B	Yes	Yes	Yes
3GPP2-Num-SDB-Terminating	G12	26/33	3GPP2	4	integer	Total number of Short Data Burst transactions sent to the user	IS-835-B	Yes	Yes	Yes
3GPP2-Num-SDB-Originating	G13	26/34	3GPP2	4	integer	Total number of Short Data Burst transactions sent by the user.	IS-835-B	Yes	Yes	Yes
3GPP2-IP- QOS	l1	26/36	3GPP2	4	integer	Differentiated Services Code Points associated with the user data Use is not yet specified in the specs.	IS-835-B	Yes	Yes	Yes
3GPP2-Airlink-QOS	l4	26/39	3GPP2	4	integer	Identifies airlink QoS associated with the user data. Use is not yet specified in the specs.	IS-835-B	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
3GPP2-RP-Session-ID	Y2	26/41	3GPP2	4	integer	RP Session ID associated with user session	IS-835-B	Yes	Yes	Yes
3GPP2-Num-Bytes-Received- Total	G14	26/43	3GPP2	4	integer	Count of all bytes received in the reverse direction by the HDLC layer in PDSN.	IS-835-B	Yes	Yes	Yes
3GPP2-Correlation-ID	C2	26/44	3GPP2	8	integer	Identifies all the accounting sessions authorized for this NAI at a PDSN.	IS-835-B	Yes	Yes	Yes
3GPP2-MobileIP-InBound-Signaling-Count	G15	26/46	3GPP2	4	integer	Total number of octets in Registration Requests and Solicitations sent by the mobile.	IS-835-B	Yes	Yes	Yes
3GPP2-MobileIP-OutBound-Signaling-Count	G16	26/47	3GPP2	4	integer	Total number of octets in Registration Replies and advertisements sent to the mobile.	IS-835-B	Yes	Yes	Yes
3GPP2- Session-Continue	C3	26/48	3GPP2	4	integer	Session Continue Indicator to the RADIUS server. Supported values: • 0 for End of a Session • 1 for Session to Continue	IS-835-B	Yes	Yes	Yes
3GPP2-Active-Time	G8	26/49	3GPP2	4	integer	Total active connection time on traffic channel in seconds.	IS-835-B	Yes	Yes	Yes

Table 13 Accounting AVPs For Packet Data Services (Continued)

Name	3GPP2 Type	AVP Type	Vendor	Length	Format	Description	Reference Specs	Attribute Present In		
								start	stop	interim
3GPP2- DCCH-Frame-Format	F14	26/50	3GPP2	4	integer	Frame sizes on DCCH channel Supported values: • 0 (no DCCH) • 1 (5 ms and 20 ms) • 2 (20ms) • 3 (5 ms)	IS-835-B	Yes	Yes	Yes
3GPP2-Always-On	F15	26/78	3GPP2	4	integer	Always On Service Indication. Supported values: • 0 when not enabled • 1 when enabled	IS-835-B	Yes[1]	Yes[2]	Yes[3]

1. F15 will be sent only when Always On service enabled for the user. However configuration option is provided to send it for all users.
2. F15 will be sent only when Always On service enabled for the user. However configuration option is provided to send it for all users.
3. F15 will be sent only when Always On service enabled for the user. However configuration option is provided to send it for all users.

Prepaid RADIUS Attributes

The following table describes the Prepaid specific attributes:

Table 14 Prepaid Specific Standard Attributes

Name	Length	Format	Description	Attribute Present In		
				Access Request	Access Accept	Access Reject
PPAC	>2	Octet String	• PDSN capability • Prepaid mechanism authorized for user	Yes, mandatory	Yes, mandatory	
PPAQ	>8	Octet String	• Prepaid quota authorized for the user • Prepaid quota utilized by the user	Yes, mandatory	Yes, mandatory	
PTS	>8	Octet String	• Prepaid tariff switch capability • Prepaid quota utilized by the user after tariff switch	Yes, mandatory	Yes, optional	

Acronyms

1XRTT—Single Carrier, Radio Transmission Technology

1xEV-DO—Evolution-Data Optimized

3GPP2—3rd Generation Partnership Project 2

A10—3GPP2 TSG-A defined interface for user data

A11—3GPP2 TSG-A defined interface for control messages

AAA—Authentication, Authorization and Accounting

AH—Authentication Header

AHDLC—Asynchronous High-Level Data Link Control

APN—Access Point Name

BG—Border Gateway

BSC—Base Station Controller

BSS—Base Station Subsystem

BTS—Base Transceiver Station

CDMA—Code Division Multiple Access

CHAP—Challenge Handshake Authentication Protocol

CN—Corresponding Node

CoA—Care-Of-Address

CRB—Cisco Radius Billing (part of the VSA)

DES—Data Encryption Standard

DNS—Domain Name Server

EAP—Extensible Authentication Protocol

EIA—Electronic Industries Alliance

ESN—Electronic Serial Number

FA—Foreign Agent

FAC—Foreign Agent Challenge (also FA-CHAP)

GRE—Generic Routing Encapsulation

HA—Home Agent

HDLC—High-Level Data Link Control

HSRP—Hot Standby Router Protocol

IMSI—International Mobile Subscriber Identifier

IP—Internet Protocol

IPCP—IP Control Protocol

IS-835B—Specification of the CDMA2000 Wireless Data Architecture

ISP—Internet Service Provider

ITU—International Telecommunications Union

L2TP—Layer 2 Tunneling Protocol

LAC—L2TP Access Controller

LCP—Link Control Protocol

LNS—L2TP Network Server

MAC—Medium Access Control

MEID—Mobile Equipment Identifier

MIB—Management Information Base

MIN—Mobile Identification Number

MIP—Mobile IP

MS—Mobile Station (= TE + MT)

MSID—Mobile Station Identification

MT—Mobile Termination

MWAM—Multi-processor WAN Application Module

NAI—Network Access Identifier

NAS—Network Access Server

P-MIP—Proxy-Mobile IP

PAP—Password Authentication Protocol

PCF—Packet Control Function

PDSN—Packet Data Serving Node

PPP—Point-to-Point Protocol

PPTP—Point-to-Point Tunneling Protocol

RADIUS—Remote Authentication Dial-in User Service

RAN—Radio Access Network

RP—Radio-PDSN Interface

SDB—Short Data Burst

SIP—Simple IP

SNMP—Simple Network Management Protocol

SPI Value—Security Parameter Index Value

TE—Terminal Equipment

TIA—Telecommunications Industry Association

TID—Tunnel Identifier

UDR—Usage Data Record

UDP—User Datagram Protocol

VPDN—Virtual Packet Data Network

VSA—Vendor Specific Attribute

WAP—Wireless Application Protocol