# Cisco Packet Data Serving Node (PDSN) Release 1.2

**Feature History**

| Release | Modification |
|---|---|
| 12.2(8)BY | This feature was introduced on the Cisco 7200 Series Router. |
| 12.2(8)ZB | This feature was introduced on the Cisco Catalyst 6500 Switch. |

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. 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, 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.

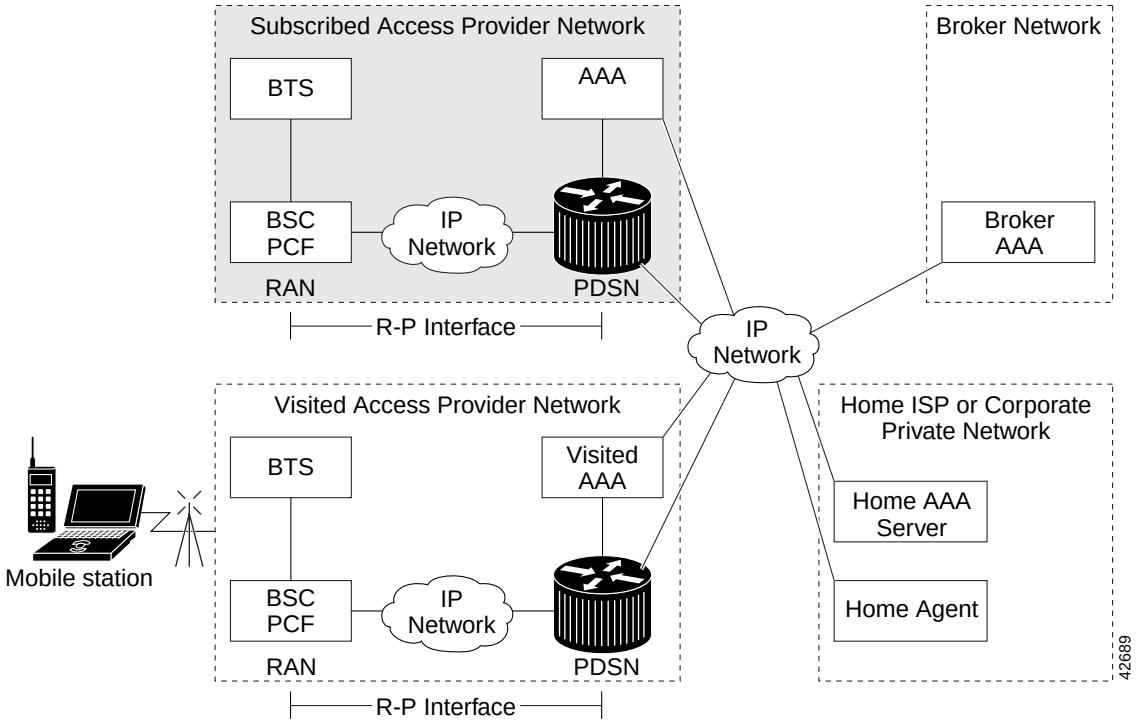
The Cisco PDSN supports all relevant 3GPP2 standards, including those that define the overall structure of a CDMA2000 network, and the interfaces between radio components and the PDSN.

# 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.

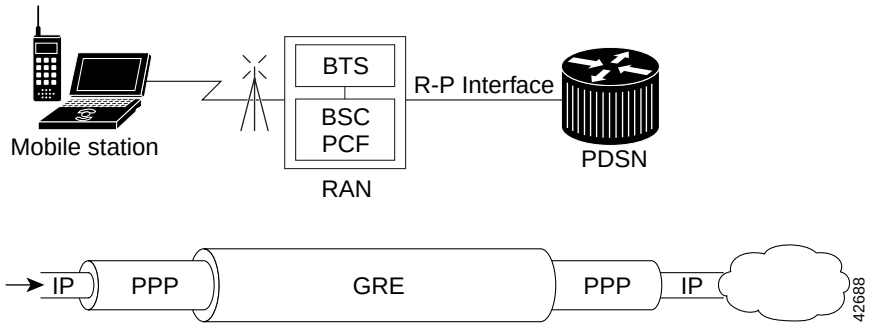
***Figure 1 The CDMA Network***




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 1.2, 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 1.2, 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 MobileIP Client

## Cisco PDSN Simple IP

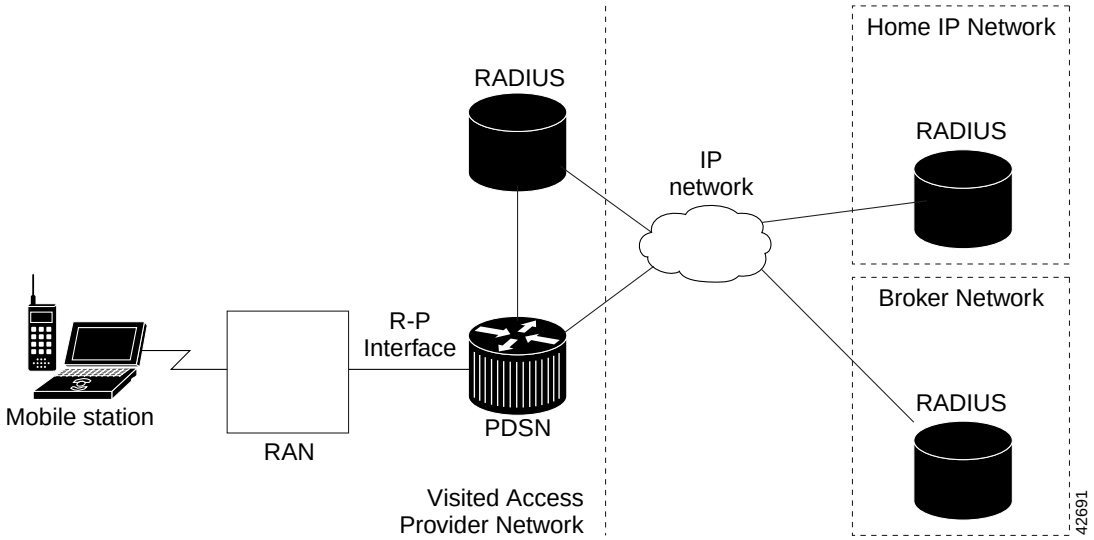
With Simple IP, a service provider's Cisco PDSN assigns a dynamic or static IP address to the mobile station during the PPP link setup. The mobile station retains this IP address as long as it is served by a radio network that has connectivity to the address-assigning PDSN.

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.

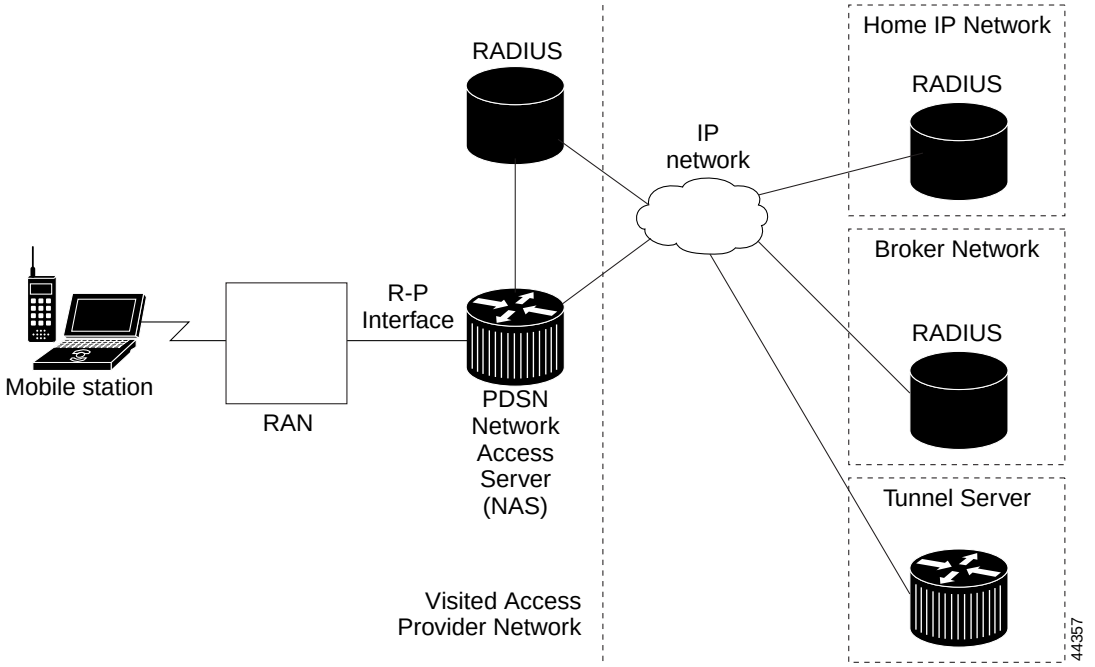
***Figure 3 CDMA Network - Simple IP Scenario***




## Cisco PDSN Simple IP with VPDN Scenario

A 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.

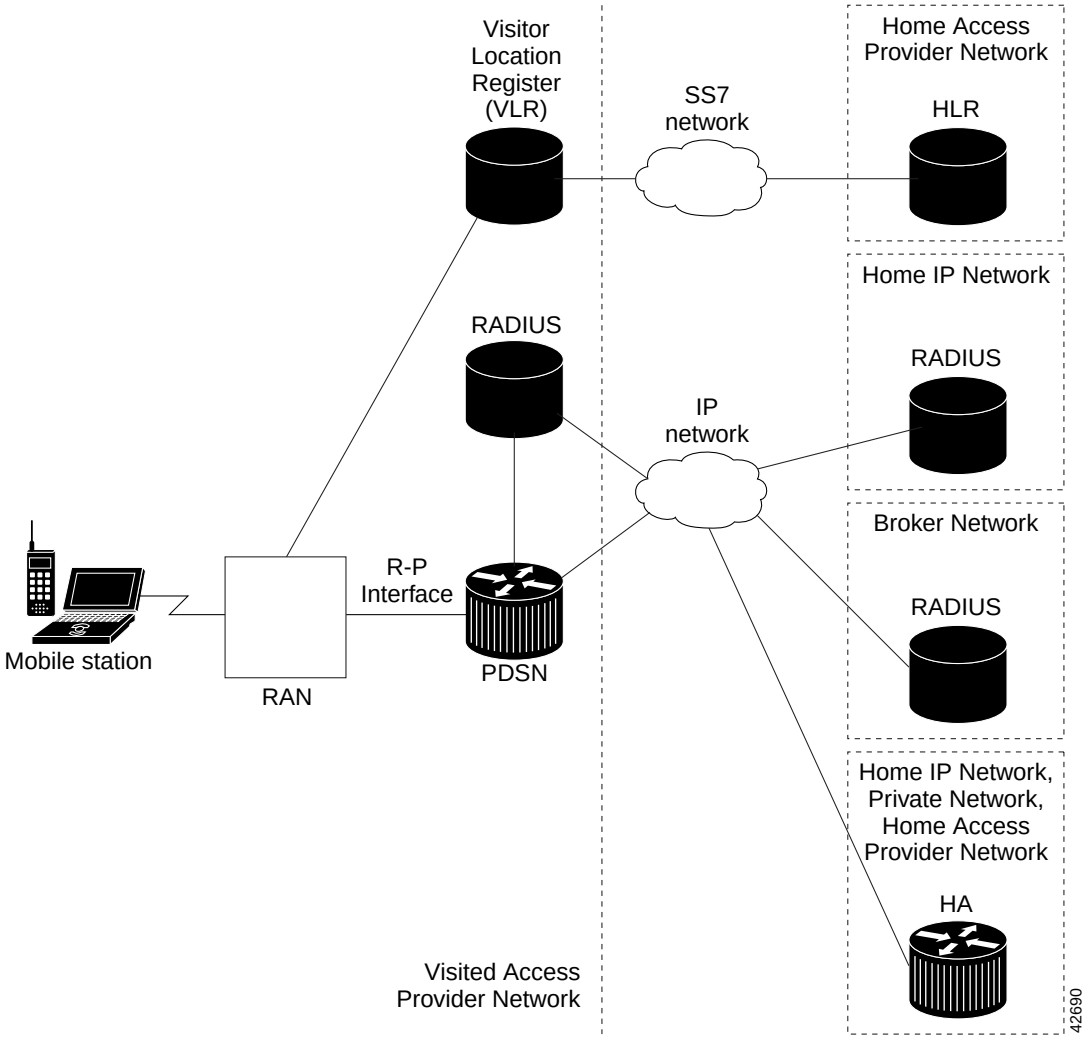
   The PPP client is forwarded through a Layer 2 Tunneling Protocol (L2TP) tunnel over User Datagram Protocol (UDP).
4. The PPP setup is completed and all frames exchanged between the client and tunnel server are sent through the NAS. The protocols running within PPP are transparent to the NAS.

## 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 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.

## PMTU Discovery by MobileIP 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 will support the feature set of PDSN R1.2. The funtionality remains the same as it would on the Cisco 7200 platforms. The significant difference between PDSN on the 7200 and on the MWAM is that a Catalyst 6500 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 each increment of 200,000 sessions. Each 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

This section describes the following key features of the Cisco PDSN Release 1.2:

- PDSN Cluster Controller / Member Architecture
- PDSN MIB Enhancement
- Prepaid Billing
- Support for R-P Registration Messages
- 3 DES Encryption
- Mobile IP IPSec
- Hardware IPSec Acceleration Using IPSec Acceleration Module—Static IPSec
- 1xEV-DO Support
- Integrated Foreign Agent (FA)
- AAA Support
- Packet Transport for VPDN
- Proxy Mobile IP
- Multiple Mobile IP Flows
- PDSN Clustering Peer-to-Peer and Controller / Member Architecture

**Note** The Cisco PDSN 1.2 software release 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 Feature Matrix"in Table 1 lists the available images for PDSN 1.2, and identifies the features available on each image.

***Table 1 PDSN Feature Matrix***

| Feature Name | c7200-c5is-mz | c7200-c5ik9s-mz | c7200-c6is-mz | c7200-c6ik9s-mz | svcmwam-c6is-mz | svcmwam-c6ik9s-mz |
|---|---|---|---|---|---|---|
| 8000 Sessions | X | X | | | X | X |
| 20000 Sessions | | | X | X | | |
| Prepaid Billing | | | X (Optional) | X (Optional) | X (Optional) | X (Optional) |
| PDSN Controller / Member Clustering | | | X | X | X | X |
| PDSN Peer-to-Peer Clustering | X | X | X | X | | |
| PDSN MIB Enhancements | X | X | X | X | X | X |
| 1xEV-DO Support | X | X | X | X | X | X |
| ESN in Billing | X | X | X | X | X | X |
| 3DES Encryption Mobile IP IPSec | | X | | X | | X |
| PPP Optimization | X | X | X | X | X | X |

**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 Cluster Controller / Member Architecture

Release 1.2 introduces a new controller-member architecture that improves cluster capacity by reducing the resource utilization on the PDSN cluster member.

This new 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.

**Note** PDSNs in controller-member mode and peer-to-peer mode cannot co-exist in the same cluster. They are mutually exclusive.

For information on redundancy and load balancing in the PDSN Release 1.2, see the "PDSN Clustering Peer-to-Peer and Controller / Member Architecture" section on page 21.

**Note** This feature is a variant of the PDSN Release 1.2 software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN 1.2.

# PDSN MIB Enhancement

The PDSN 1.2 software release allows you to 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 also supports the following features

- New 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 new TRAP threshold group added to support different severity levels. Agent generates notifications only if the serverity level of the affected service is higher than the configured severity level. The severity level can be configured using the following methods:
  a. The CLI using the **cdma pdsn mib trap level** 1-4, or by
  b. Using SNMP, set the object cCdmaNotifSeverityLevel.

# Prepaid Billing

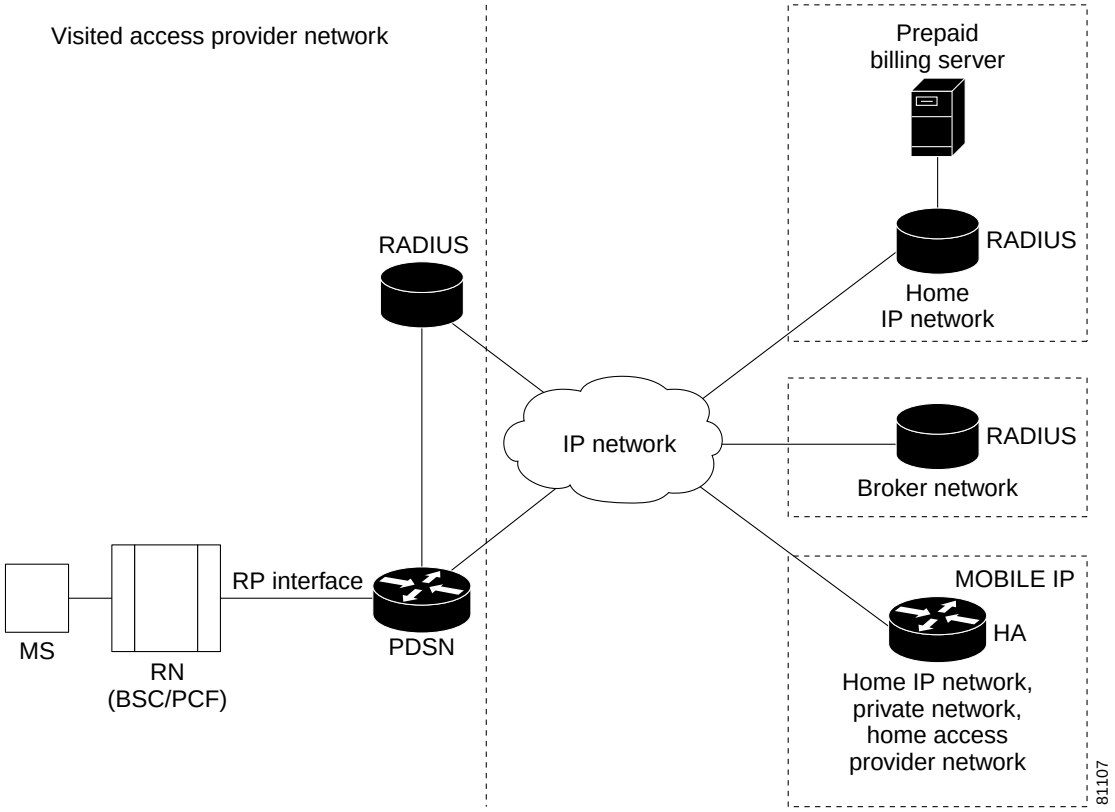
The Cisco PDSN 1.2 software release provides real-time monitoring and rating of data calls for prepaid users. The prepaid billing solution for the PDSN is based on the RADIUS (AAA) server, and takes advantage of the existing flow-based accounting functionality. The prepaid billing feature requires the 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 prepaid billing feature provides the following services:

- Simple IP-based service metering in real time. See the "Prepaid Simple IP Call Flow" section on page 13 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 14 for more information.
- Rating based on per-flow data volume, octet or packet count, and call duration.

Figure 6 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 6 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 3.

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 1.2 software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN 1.2.

# 3 DES Encryption

The Cisco PDSN 1.2 release 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 Release 1.2 software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN 1.2.

# 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 1.2 on the Cisco 6500 platform requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500. 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://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin09186a0080129ead.html

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.

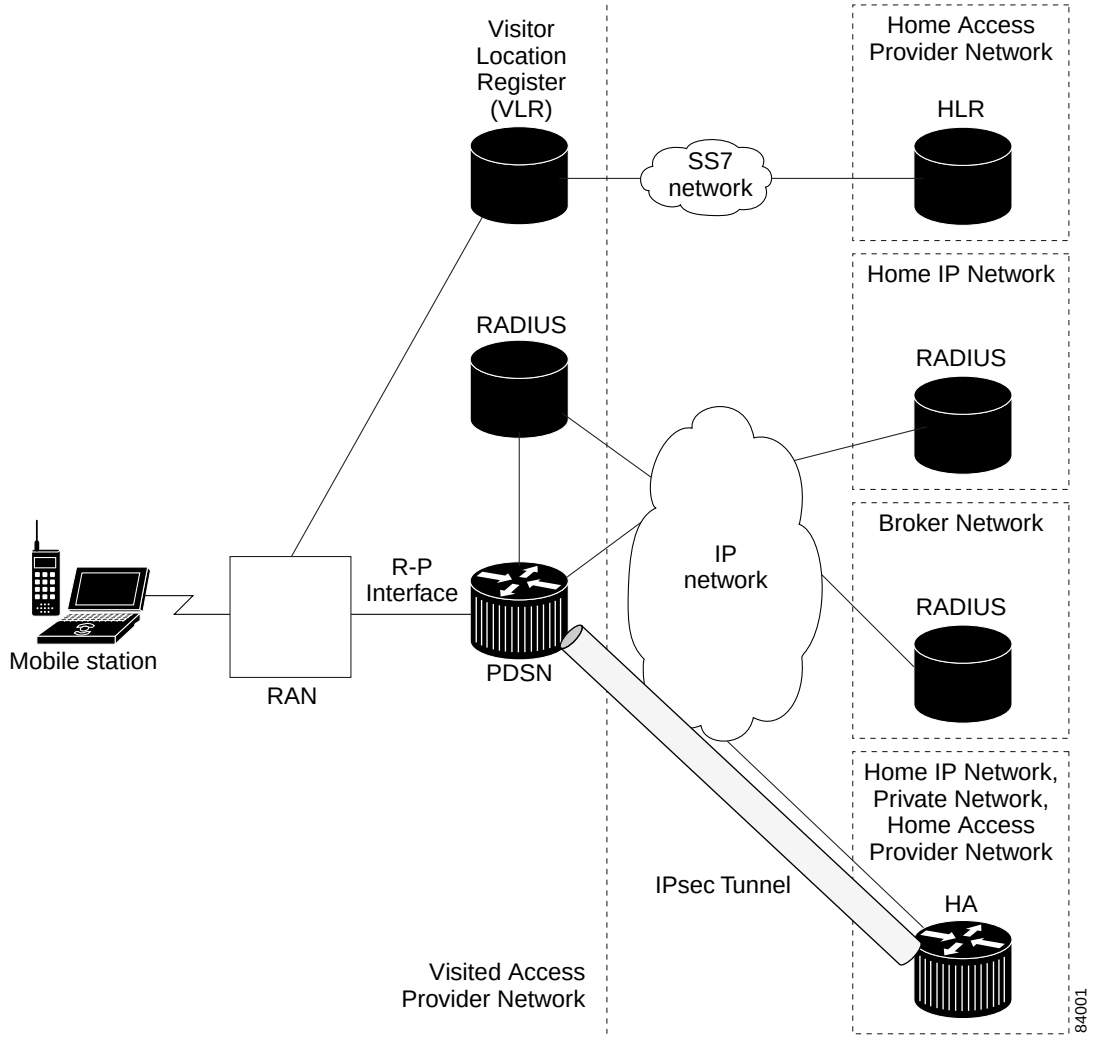
IS-835-B defines MobileIP service as described in RFC 2002; the Cisco PDSN provides Mobile IP service and Proxy Mobile IP service.

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 7 illustrates the IS-835-B IPSec network topology.

*Figure 7 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 Release 1.2 software. Refer to the Feature Matrix to see which features are available on a specific image of PDSN 1.2.

# Conditional Debugging

PDSN Release 1.2 software introduces 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).

To enable conditional debugging, set the condition and enable the required IOS debugs. Some conditional debugging based on the Network Access Identifier (NAI) is already supported by various IOS modules (for example, PPP using the username option). To enable conditional debugging for a specific NAI, use the following command:

**debug condition username** *username*

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**]

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**

Refer to Appendix A, "Using Debug Commands for PDSN Release 1.2" for more information about conditional debugging in PDSN Release 1.2.

# 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.

## 1xEV-DO Support

The Cisco PDSN 1.2 release 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 R1.2 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 1.2.

## 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 both the Controller - Member cluster model, and for the Peer-to-Peer cluster model.

# PDSN Clustering Peer-to-Peer and Controller / Member Architecture

The PDSN Clustering Peer-to-Peer Architecture (or PDSN Intelligent Selection and Load Balancing feature), implemented in the PDSN R1.1 software release, functions in a peer-to-peer model. All the PDSNs in the cluster share their load and served MSID, and multicast their load and MSID to all other PDSNs in the cluster. This drains resources because large MSID tables need to be stored on all the PDSNs, and because a large amount of traffic is generated to exchange the information among the cluster members. This results in constraints on the cluster size.

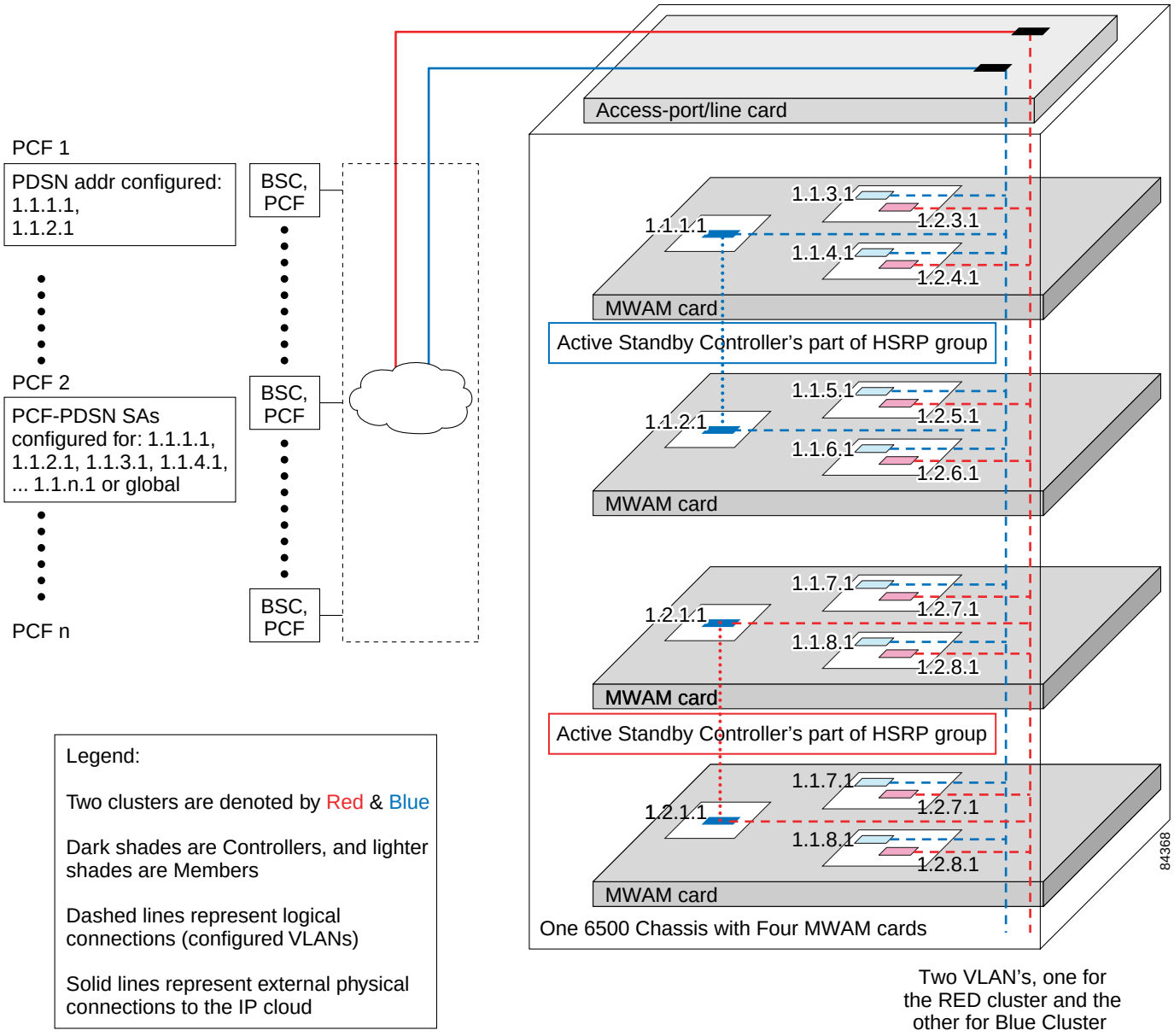
In the Cisco PDSN 1.2 release, you can choose between Peer-to-Peer clustering, or Controller-Member clustering. In Controller-Member clustering, a controller maintains load and session (such as A10 connection) information for each member in the cluster, and performs member selection for load-balancing 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** It is not possible to configure Peer-to-Peer clustering for PDSN on the MWAM. This feature is only supported on the Cisco 7200 platform.

**Note** The new PDSN Controller-Member clustering feature is only available on the **-c6is-mz**, and **-c6ik9s-mz** images.

Figure 8 illustrates the Controller-Member architecture on the 6500-based MWAM platform. This illustration depicts two PDSN clusters with two primary and two backup controllers, and their corresponding members.

*Figure 8 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.

# Intelligent PDSN Selection and Load Balancing (Peer-to-Peer)

The Cisco Intelligent PDSN Selection (Peer-to-Peer) feature in Release 1.2 allows you to group a number of Cisco PDSNs into clusters that can exchange session information for performance and load-balancing purposes. Each Cisco PDSN in a group maintains a table that contains information for the entire group. Using PDSN clusters, minimizes inter-PDSN handoff, provides intelligent load-balancing, and ensures high availability.

To distribute session information, each PDSN sends a broadcast to the Mobile IP multicast address when a session is created or ended. The IP address of the originating PDSN and the MSID are encoded in the Mobile IP messages. Each PDSN in a group updates its session table upon receiving the broadcast.

When a session request is received from the PCF by the Cisco PDSN, the PDSN checks its own session list for an existing session, and also checks session lists within its PDSN group. If it determines that a session exists with another PDSN, it redirects the PCF to that PDSN. This redirection helps to avoid dropping the IP address and, thereby, avoids dropping any existing communication.

If the session does not exist with any other PDSN, the receiving PDSN uses a load-balancing mechanism to determine the appropriate PDSN to use for session establishment. With load balancing, the receiving PDSN looks for the least utilized PDSN in the entire cluster. If the number of active PPP links on that PDSN is some factor less than the number of PPP links on the receiving PDSN, the request will be forwarded. The factor for determining whether the PPP link is forwarded is calculated as a percentage (number of active PPP links vs. total number of possible PPP links).

## Load Balancing

For a new packet data session, one PDSN may direct a connection request to another less “loaded” PDSN within the cluster by proposing the address of that PDSN to the PCF. Such redirection of A10 connection requests is performed among lesser loaded PDSNs in a round-robin manner. In PDSN software releases prior to Release 1.1, the load balancing threshold was implemented in terms of a session *count* differential. Starting in Release 1.1, the threshold is configured in terms of a *load factor*—the ratio of number of sessions supported and total session capacity of the PDSN. In future releases, other factors (such as QoS, session throughput considerations, CPU load, memory utilization) might also be considered as parameters used to determine of load factor of a PDSN.

# 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 is started. 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 Clustering Peer-to-Peer and Controller / Member Architecture" section on page 21, 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 1.2 software, refer to the following documents:

- *Release Notes for the Cisco PDSN Feature in Cisco IOS Release 12.2(2)XC*

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 12.2 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 12.1 documentation module *Cisco IOS Dial Services Command Reference*.
- Mobile IP, refer to the Cisco Release 12.2 documentation modules *Cisco IOS IP Command Reference* and *Cisco IOS IP Configuration Guide*.
- Virtual Private Networks, refer to the Cisco IOS Release 12.2 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. Refer to the following document for more information regarding the respective platforms:

- *Release Notes for the Cisco PDSN 1.2 Feature in Cisco IOS Release 12.2(8)BY* 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 configuration. Refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note* for more information.

## 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

#### 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 (Available only on C-6 images)

- 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 IP Sec 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 in Release 1.2
- Configuring PDSN Cluster Member in Release 1.2
- Configuring Peer-to-Peer PDSN Selection

#### Network Management Configuration Tasks (Required for Network Management in Any Scenario)

To configure network management, complete the following task:

- Enabling Network Management

#### Tuning, Verification, and Monitoring Tasks (Optional)

To tune, verify, and monitor PDSN elements, complete the following tasks:

- Configuring PDSN Accounting Events
- 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. |
| `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 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 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. |
| `Router(config)# aaa authorization network 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. |

## Configuring Prepaid in the PDSN Environment

Currently, there are no configuration commands for prepaid. To configure prepaid, ensure that you include "crb-entity-type=1" in the user profile

## 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 12.2 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 via 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`[1] | Enables 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. |

1. 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.

## Configuring IP Sec for the Cisco PDSN

To configure IPSec for the PDSN, use the following commands in global configuration mode:

| Command | Purpose |
|---|---|
| Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**<br><br>**set peer** *ip address of ha*<br>**set transform-set** transform-set-name<br>**match address** *acl name* | Creates a a crypto map entry for one HA in one Crypto-map set.<br>The Crypto Map definition is not complete until:<br>1. ACL associated with it is defined, and<br>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# **access-list** *acl-name* **deny udp host** *HA IP addr* **eq mobile-ip host** *PDSN IP addr* **eq mobile-ip**<br><br>**access-list** *acl-name* **permit ip host** *PDSN IP addr* **host** *HA IP addr*<br><br>**access-list** *acl-name* **deny ip any any** | Defines the access list.<br>The ACL name “acl-name” is same as in the crypto-map configuration |
| Router# **Interface** *Physical-Interface of PI interface*<br><br>**crypto map** *Crypto-Map set* | Applies the Crypto-Map on Pi Interface, as the PDSN sends/receives Mobile IP traffic to/from HA on this interface |
| Router# **ip mobile tunnel crypto map** *crypto-map set name* | Configure Mobile IP to use the configured Crypto-Map set |

## 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 in Release 1.2

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. |
| `Router(config)# cdma pdsn controller hsrp hsrpIpAddress` | Informs the specified controller about the addition of an HSRP group. This command applies to a cluster of clusters. For more information on HSRP grouping and IP priority, refer to the *HSRP Support for MPLS VPNs*, and *Cisco IOS IP and IP Routing Configuration Guide, Release 12.1*. |

## Configuring PDSN Cluster Member in Release 1.2

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.

| 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. |
| `Router(config)# cdma pdsn controller-hsrp ip ip-addr` | Configures the address of the HSRP group of controllers the member is reporting to. |

## Configuring Peer-to-Peer PDSN Selection

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 failure history. |
| `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 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:<br>• An Accounting Stop record when it receives an active stop airlink record (dormant state)<br>• An Accounting Start record when it receives an active start airlink record (active state) |

# 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 selection** [**pdsn** *ip-addr* \| **msid** *octet-stream*] | Clears the PDSN selection tables. |
| Router# **clear cdma pdsn session** {**all** \| **pcf** *ip-addr* \| **msid** *octet-stream*} | Clears the session. |
| Router# **clear cdma pdsn statistics {ppp \| rp}** | 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 hostcounters** [[*ip-address* \| **nai** *string ip_address*] **undo**]] | Clears the mobility counters specific to each mobile station. |
| Router# **clear ip mobile secure** {**host** *lower* [*upper*] \| **nai** *string* \| **empty** \| **all**} [**load**] | Clears and retrieves remote security associations. |
| Router# **clear ip mobile visitor** [*ip-address* \| **nai** *string ip_address*] | Clears visitor information. |
| Router# **show cdma pdsn** | Displays the status and current configuration of the PDSN gateway. |
| Router# **show cdma pdsn accounting** | Display the accouting 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. |

| Command | Purpose |
|---|---|
| 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 (tith counter names) for the session identified by the msid. |
| 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 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 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 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 stat** | Displays the IP addresses of the members that 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 compress detail-ccp** | Displays the compression information for all users. |
| 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. |

| Command | Purpose |
|---|---|
| Router# **show ip mobile binding** | Displays the mobility binding table. |
| 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 host** | Displays mobile station counters and host information. |
| 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 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. |

# Configuration Examples

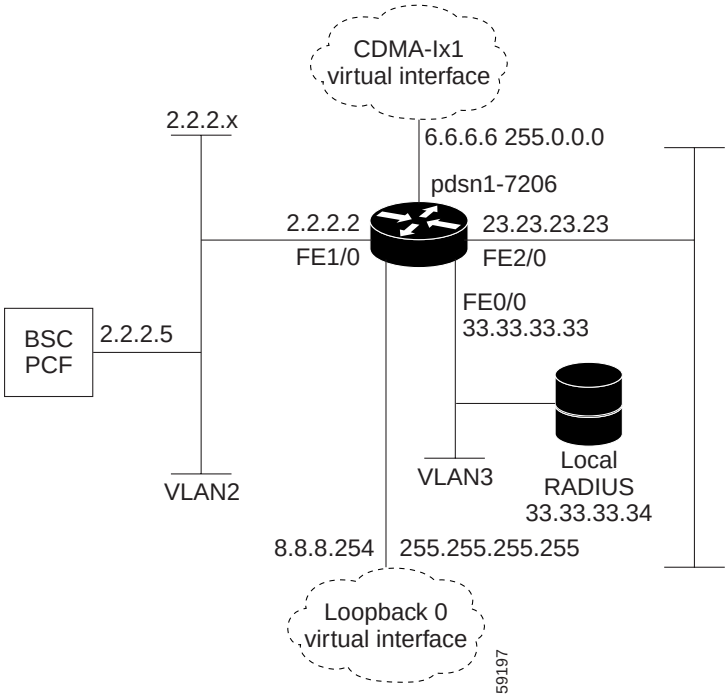
This section provides the following configuration examples:

- Cisco PDSN Configuration for Simple IP, page 41
- Cisco PDSN Configuration for Simple IP with VPDN, page 42
- Cisco PDSN Configuration for Mobile IP, page 43

# Cisco PDSN Configuration for Simple IP

Figure 9 and the information that follows is an example of PDSN architecture for Simple IP and its accompanying configuration.

***Figure 9 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

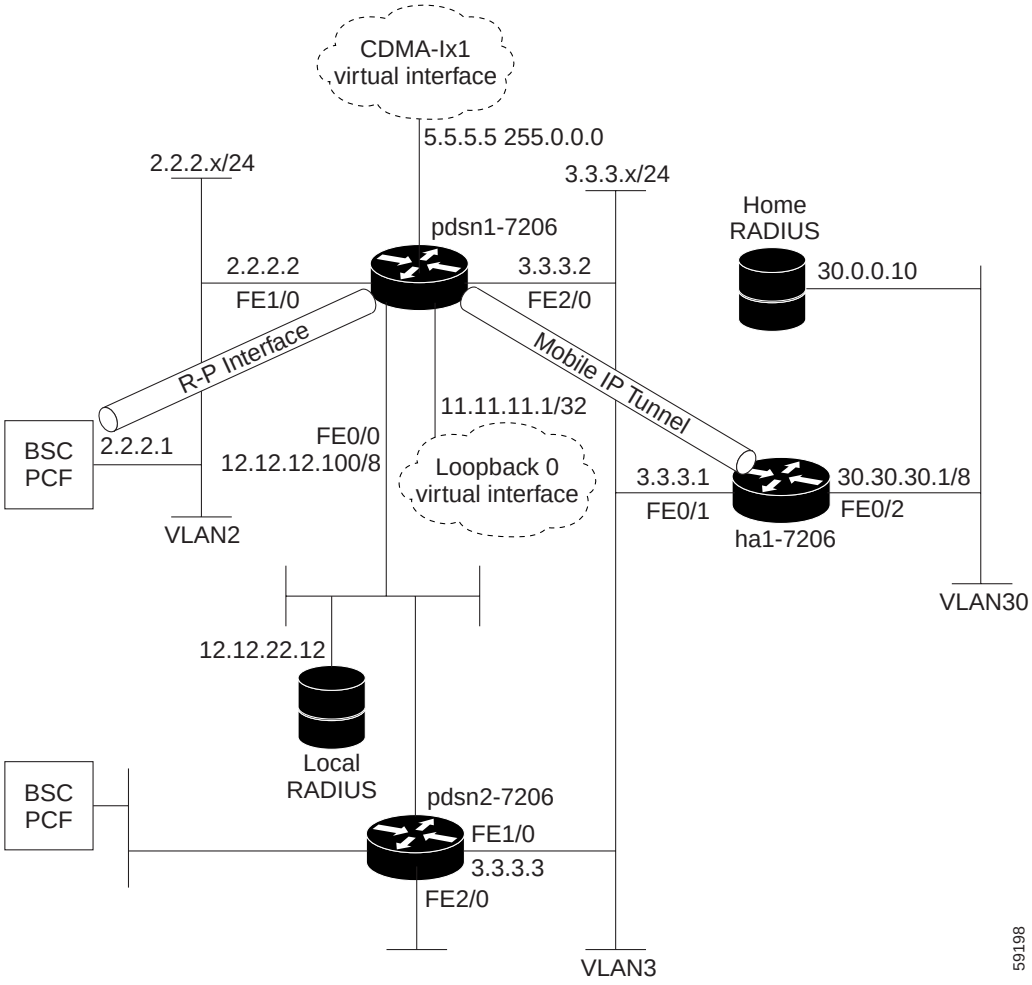
The configuration Simple IP with VPDN is identical to the configuration for Simple IP with two additional lines:

```
vpdn enable
vpdn authen-before-forward
```

# Cisco PDSN Configuration for Mobile IP

Figure 10 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 10 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
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
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
!
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
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
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
!
!
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

S76#
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

S96>
Press RETURN to get started!
```

```
S96>
S96>
S96>
S96>en
S96#sh run
S96#sh 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 S96
!
!
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

S96#

Verify active controller and standby controller
S76#sh 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"
S76#

S96#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"
S96#

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

S73>

Press RETURN to get started!


S73>
S73>en
S73#sh run
S73#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 S73
!
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
 ip mobile foreign-service challenge forward-mfce
 ip mobile foreign-service reverse-tunnel
 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
!
!
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

S73#

Show commands on Controllers
S76#sh cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.401
no R-P signaling proxy
timeout to seek member = 10 seconds
window to seek member is 3 timeouts in a row if no reply (afterwards the member
is declared offline)
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
```

```
  group: 6509-cluster
S76#

S76#sh cdma pdsn cluster controller member load
 Secs until   Seq seeks         Member
(past) seek    no reply      IPv4 Addr      State   Load
-----------------------------------------------------------
          3       0         10.10.95.1      ready      0
          2       0         10.10.93.1      ready      0
          8       0         10.10.92.1      ready      0
          6       0         10.10.94.1      ready      0
          5       0         10.10.72.1      ready      0
          3       0         10.10.74.1      ready      0
          9       0         10.10.75.1      ready      1
          9       0         10.10.73.1      ready      3
-----------------------------------------------------------
                    Controller IPv4 Addr    10.121.68.98

S76#

S76#sh cdma pdsn cluster controller member 10.10.73.1
PDSN cluster member 10.10.73.1 state      ready
 registered with PDSN controller 10.121.68.98
 reported load 7 percent, will be sought in 9 seconds
 member statistics collected in the controller:
        14 CVSEs seek reply received
         9 CVSEs seek received
         0 state changed to admin prohibited
         0 state changed to ready
         0 seek A11-RegReq sent in a row, no reply
     21171 A10 up A11-RegReq received
     23387 A10 end A11-RegReq received

S76#

S76#sh cdma pdsn cluster controller statistics
         0 times did not get a buffer for a packet
         0 times couldn't allocate memory
       836 A11-RegReply received
         0 A11-RegReply discarded, authenticaton problem
         0 A11-RegReply discarded, identification problem
         0 A11-RegReply discarded, unrecognized extension
     68818 A11-RegRequest received
         0 A11-RegRequest discarded, authenticaton problem
      1714 A11-RegRequest discarded, identification problem
         0 A11-RegRequest discarded, unrecognized application type
         0 A11-RegRequest discarded, unrecognized extension
         0 A11-RegRequest with unrecognized type of data
         0 A11-RegRequest not sent, interface cdma-Ix not configed
       836 CVSEs seek reply received
       775 CVSEs seek received
         0 CVSEs state ready received
         0 CVSEs state admin prohibited received
         0 msgs received neither A11-RegReq nor A11-RegReply
     31898 A10 up A11-RegReq received
     34434 A10 end A11-RegReq received
         8 PDSN cluster members

redundancy:
    error: mismatch id 5 authen fail 0
           ignore due to no redundancy 0
    Update rcvd 0 sent 68437 orig sent 67600 fail 221
    UpdateAck rcvd 68411 sent 0
    DownloadReq rcvd 6 sent 0 orig sent 0 fail 0
```

```
    DownloadReply rcvd 0 sent 13 orig sent 13 fail 0 drop 0
    DownloadAck rcvd 13 sent 0 drop 0
S76#

S76#sh cdma pdsn cluster controller session ?
  count   Count of session records
  imsi    Session record for International Mobile Subscriber Identity
  oldest  Oldest session record

S76#sh cdma pdsn cluster controller session ol
S76#sh cdma pdsn cluster controller session oldest ?
  more  The oldest and a few more session records to show
  |     Output modifiers
  <cr>

S76#sh cdma pdsn cluster controller session oldest
           IMSI   Member IPv4 Addr   Age [days]   Anchor changes
----------------------------------------------------------------
62000015434         10.10.73.1
----------------------------------------------------------------

S76#sh cdma pdsn cluster controller session imsi 62000015434
           IMSI   Member IPv4 Addr   Age [days]   Anchor changes
----------------------------------------------------------------
62000015434         10.10.73.1
----------------------------------------------------------------

S76#


Show commands on member:

S73#sh cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.401
IP address of controller is 10.121.68.98
no prohibit administratively
timeout to resend status or seek controller = 10 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
this PDSN cluster member is configured

S73#

S73#sh cdma pdsn cluster member statistics
         0 times did not get a buffer for a packet
         0 times couldn't allocate memory
     48804 A11-RegReply received
         0 A11-RegReply discarded, authenticaton problem
         0 A11-RegReply discarded, identification problem
         0 A11-RegReply discarded, unrecognized extension
        15 A11-RegRequest received
         0 A11-RegRequest discarded, authenticaton problem
         0 A11-RegRequest discarded, identification problem
         0 A11-RegRequest discarded, unrecognized application type
         0 A11-RegRequest discarded, unrecognized extension
         0 A11-RegRequest with unrecognized type of data
         0 A11-RegRequest not sent, interface cdma-Ix not configed
        15 seek A11-RegReq received
         9 CVSEs seek reply received
         0 CVSEs state reply received
         0 msgs received neither A11-RegReq nor A11-RegReply
     24412 A10 up A11-RegReply received
     24405 A10 end A11-RegReply received
         0 CVSEs seek in sequence without a msg from controller
         0 CVSEs state in sequence without a reply from controller
```

```
           controller alive

S73#


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
```

# PDSN Accounting

The following RADIUS attributes are contained in the UDR sent by PDSN.

***Table 2 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 |
| 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 |

*Table 2 In Accounting Start Record*

| Attribute Name | TIA/EIA/IS-835-B | Type/Subtype |
|---|---|---|
| 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 |

*Table 3 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 |
| 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 |

*Table 3 In Accounting Stop Record (continued)*

| Attribute Name | TIA/EIA/IS-835-B | Type/Subtype |
|---|---|---|
| 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 |
| 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-Reason-Ind | F13 | 26/24 |
| CDMA-Session-Continue | C3 | 26/48 |
| CDMA-ESN | A2 | 26/52 |

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 4 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 |
| 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 |

*Table 4 In Interim-accounting Record (continued)*

| Attribute Name | TIA/EIA/IS-835-B | Type/Subtype |
|---|---|---|
| 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 |
| CDMA-NumSDB-Output | G13 | 26/34 |

# 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 ]
    cisco-avpair = lcp:cdma-user-class=1
```

## 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

cisco-avpair = lcp:cdma-user-class=1

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

  cisco-avpair = lcp:cdma-user-class=1
- (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”

# Command Reference

This section lists new and revised commands pertaining to the PDSN software. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **access list**
- **cdma pdsn a10 ahdlc engine**
- **cdma pdsn a10 gre sequencing**
- **cdma pdsn a10 max-lifetime**
- **cdma pdsn a11 dormant ppp-idle-timeout send-termreq**
- **cdma pdsn accounting local-timezone**
- **cdma pdsn accounting send start-stop**
- **cdma pdsn accounting time-of-day**
- **cdma pdsn age-idle-users**
- **cdma pdsn cluster controller**
- **cdma pdsn cluster member**
- **cdma pdsn compliance iosv4.1 session-reference**
- **cdma pdsn compliance is835a esn-optional**
- **cdma pdsn ingress-address-filtering**
- **cdma pdsn maximum pcf**
- **cdma pdsn maximum sessions**
- **cdma pdsn mobile-advertisement-burst**
- **cdma pdsn msid-authentication**
- **cdma pdsn retransmit a11-update**
- **cdma pdsn secure cluster**
- **cdma pdsn secure pcf**
- **cdma pdsn selection interface**
- **cdma pdsn selection keepalive**
- **cdma pdsn selection load-balancing**
- **cdma pdsn selection session-table-size**
- **cdma pdsn send-agent-adv**
- **cdma pdsn timeout a11-update**
- **cdma pdsn timeout mobile-ip-registration**
- **cdma pdsn virtual-template**
- **clear cdma pdsn cluster controller session records age**
- **clear cdma pdsn selection**
- **clear cdma pdsn session**
- **clear cdma pdsn statistics**
- **clear ip mobile binding**

- clear ip mobile host-counters
- clear ip mobile secure
- clear ip mobile visitor
- crypto map (global IPSec)
- ip mobile authentication ignore-spi
- ip mobile bindupdate
- ip mobile foreign-agent
- ip mobile foreign-service
- 
- ip mobile host
- 
- ip mobile pdsn ipsec profile
- ip mobile proxy-host
- ip mobile secure
- ip mobile tunnel
- ppp authentication
- service cdma pdsn
- show cdma pdsn
- show cdma pdsn accounting
- show cdma pdsn accounting detail
- show cdma pdsn accounting session
- show cdma pdsn accounting session detail
- show cdma pdsn accounting session flow
- show cdma pdsn accounting session flow user
- show cdma pdsn ahdlc
- show cdma pdsn cluster controller
- show cdma pdsn cluster controller configuration
- show cdma pdsn cluster controller member
- show cdma pdsn cluster controller session
- show cdma pdsn cluster controller statistics
- show cdma pdsn cluster member
- show cdma pdsn flow
- show cdma pdsn pcf
- show cdma pdsn resource
- show cdma pdsn selection
- show cdma pdsn session
- show cdma pdsn statistics
- show ip mobile binding

- **show ip mobile host**
- **show ip mobile proxy**
- **show ip mobile secure**
- **show ip mobile traffic**
- **show ip mobile violation**
- **show ip mobile visitor**
- **show tech-support cdma pdsn**
- **show tech-support cdma pdsn**
- **snmp-server enable traps cdma**
- **snmp-server enable traps ipmobile**

# access list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** global configuration command. Use the **no** form of this command to remove the single specified entry from the access list.

**access-list** *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

**no access-list** *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

## Syntax Description

| | |
|---|---|
| *access-list-number* | Integer that identifies the access list. If the type-code wild-mask arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the address and mask arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code. |
| **permit** | Permits the frame. |
| **deny** | Denies the frame. |
| *type-code* | 16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a SNAP type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.) |
| *wild-mask* | 16-bit hexadecimal number whose ones bits correspond to bits in the type-code argument. The wild-mask indicates which bits in the type-code argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.) |
| *address* | 48-bit Token Ring address written in dotted triplet form. This field is used for filtering by vendor code. |
| *mask* | 48-bit Token Ring address written in dotted triplet form. The ones bits in mask are the bits to be ignored in address. This field is used for filtering by vendor code. |

## Defaults

No numbered encryption access lists are defined, and therefore no traffic will be encrypted/decrypted. After being defined, all encryption access lists contain an implicit “deny” (“do not encrypt/decrypt”) statement at the end of the list..

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |

## Usage Guidelines

Use encryption access lists to control which packets on an interface are encrypted/decrypted, and which are transmitted as plain text (unencrypted).

When a packet is examined for an encryption access list match, encryption access list statements are checked in the order that the statements were created. After a packet matches the conditions in a statement, no more statements will be checked. This means that you need to carefully consider the order in which you enter the statements.

To use the encryption access list, you must first specify the access list in a crypto map and then apply the crypto map to an interface, using the crypto map (CET global configuration) and crypto map (CET interface configuration) commands.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match the TCP source port, the type of service value, or the packet's precedence.

**Note** After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list command lines from a specific access list.

**Caution** When creating encryption access lists, we do not recommend using the any keyword to specify source or destination addresses. Using the any keyword with a permit statement could cause extreme problems if a packet enters your router and is destined for a router that is not configured for encryption. This would cause your router to attempt to set up an encryption session with a nonencrypting router. If you incorrectly use the any keyword with a deny statement, you might inadvertently prevent all packets from being encrypted, which could present a security risk.

**Note** If you view your router's access lists by using a command such as show ip access-list, all extended IP access lists will be shown in the command output. This includes extended IP access lists that are used for traffic filtering purposes as well as those that are used for encryption. The show command output does not differentiate between the two uses of the extended access lists.

## Examples

The following example creates a numbered encryption access list that specifies a class C subnet for the source and a class C subnet for the destination of IP packets. When the router uses this encryption access list, all TCP traffic that is exchanged between the source and destination subnets will be encrypted.

```
access-list 101 permit tcp 172.21.3.0 0.0.0.255 172.22.2.0 0.0.0.255
```

# cdma pdsn a10 ahdlc engine

To limit the number of AHDLC channel resources provided by the AHDLC engine, use the **cdma pdsn a10 ahdlc engine** command to in global configuration mode. To reset the number of AHDLC channel resources to the default, use the **no** form of this command.

**cdma pdsn a10 ahdlc engine** *slot* **usable-channels** *usable-channels*

**no cdma pdsn a10 ahdlc engine** *slot* **usable-channels**

## Syntax Description

| | |
|---|---|
| *slot* | Slot number of the AHDLC. |
| **usable-channels** *usable-channels* | Maximum number of channels that can be opened in the AHDLC engine. Valid values range between 0 and 8000 or 20000. Specifying 0 disables the engine. |

## Defaults

The default number of usable channels equals the maximum channels supported by the engine; the c-5 images supports 8000 sessions, and all c-6 image support 20000 sessions.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |
| 12.2(8)BY | The maximum number of usable channels was increased to 20000. |

## Usage Guidelines

If the value of *usable-channels* is greater than default maximum channels provided by the engine, the command will fail.

If the engine has any active channels, the command will fail.

## Examples

The following example limits the number of service channels provided by the AHDLC engine to 1000:

```
cdma pdsn a10 ahdlc engine 0 usable-channels 1000
```

## Related Commands

| Command | Description |
|---|---|
| **debug cdma pdsn a10 ahdlc** | Displays debug messages for the AHDLC engine. |
| **show cdma pdsn a10 ahdlc** | Displays information about the AHDLC engine. |
| **show cdma pdsn resource** | Displays AHDLC resource information. |

# cdma pdsn a10 gre sequencing

To enable inclusion of GRE sequence numbers in the packets sent over the A10 interface, use the **cdma pdsn gre sequencing** command in global configuration mode. To disable the inclusion of GRE sequence number in the packets sent over the A10 interface, use the **no** form of this command.

**cdma pdsn a10 gre sequencing**

**no cdma pdsn a10 gre sequencing**

## Syntax Description

This command has no arguments or keywords.

## Defaults

GRE sequence numbers are included in the packets sent over the A10 interface.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example instructs Cisco PDSN to include per-session GRE sequence numbers in the packets sent over the A10 interface:

```
cdma pdsn a10 gre sequencing
```

## Related Commands

| Command | Description |
|---|---|
| **debug cdma pdsn a10 gre** | Displays debug messages for A10 GRE interface errors. |
| **show cdma pdsn pcf** | Displays information about PCFs that have R-P tunnels to the PDSN. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn a10 max-lifetime

To specify the maximum A10 registration lifetime accepted, use the **cdma pdsn a10 max-lifetime** command in global configuration mode. To return to the default length of time, use the **no** form of this command.

**cdma pdsn a10 max-lifetime** *seconds*

**no cdma pdsn a10 max-lifetime**

## Syntax Description

| | |
|---|---|
| seconds | Maximum A10 registration lifetime accepted by Cisco PDSN. The range is 1 to 65535 seconds. The default is 1800 seconds. |

## Defaults

1800 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example specifies that the A10 interface will be maintained for 1440 seconds:

```
cdma pdsn a10 max-lifetime 1440
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn a10 gre sequencing** | Enables GRE sequence number checking on packets received over the A10 interface. |
| **debug cdma pdsn a10 gre** | Displays debug messages for A10. |
| **show cdma pdsn pcf** | Displays information about PCFs that have R-P tunnels to the PDSN. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn a11 dormant ppp-idle-timeout send-termreq

To specify that for dormant sessions, on ppp idle timeout, ppp termreq will be sent, use the **cdma pdsn all dormant ppp-idle-timeout send-termreq** command in global configuration mode. To disble this feature, use the **no** form of this command.

**cdma pdsn all dormant ppp-idle-timeout send-termreq**

**no cdma pdsn all dormant ppp-idle-timeout send-termreq**

## Syntax Description

There are no keywords or variable for this command.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)ZB | This command was introduced. |

## Usage Guidelines

Disabling this behaviour will avoid traffic channel allocation for cleaning up ppp sessions at the mobile.

## Examples

```
router# cdma pdsn a11 dormant ppp-idle-timeout send-termreq
```

# cdma pdsn accounting local-timezone

To specify the local time stamp for PDSN accounting events, use the **cdma pdsn accounting local-timezone** command in global configuration mode. To return to the default Universal Time (UTC), use the **no** form of this command.

**cdma pdsn accounting local-timezone**

**no cdma pdsn accounting local-timezone**

## Syntax Description

This command has no arguments or keywords.

## Defaults

UTC time, a standard based on GMT, is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)XS | This command was introduced. |

## Usage Guidelines

You must use the *clock timezone hours-offset* [*minutes-offset*] global configuration command to reflect the difference between local time and UTC time.

## Examples

The following example sets the local time in Korea:

```
clock timezone KOREA 9
cdma pdsn accounting local-timezone
```

## Related Commands

| Command | Description |
|---|---|
| **clock timezone** | Specifies the hours and minutes (optional) difference between the local time zone and UTC. |
| **cdma pdsn accounting send start-stop** | Causes the PDSN to send:<br>• An Accounting Stop record when it receives an active stop airlink record (dormant state)<br>• An Accounting Start record when it receives an active start airlink record (active state) |

# cdma pdsn accounting send cdma-ip-tech

To configure specific values for the F11 attribute for proxy Mobile IP and VPDN services, use the **cdma pdsn accounting send cdma-ip-tech** command in global configuration mode. To deconfigure those values, use the **no** form of this command.

**cdma pdsn accounting send cdma-ip-tech** [**proxy-mobile-ip** | **vpdn**]

**no cdma pdsn accounting send cdma-ip-tech** [**proxy-mobile-ip** | **vpdn**]

## Syntax Description

| Command | Description |
|---|---|
| **proxy-mobile-ip** | Sets the IP-Tech proxy-mobile-ip number. Values are 3-65535. |
| **vpdn** | Sets the IP-Tech vpdn number. Values are 3-65535. |

## Defaults

No default behavior or values.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| 12.1XC | This command was introduced. |

## Examples

```
pdsn(config)#cdma pdsn accounting send cdma-ip-tech proxy-mobile-ip 3
pdsn(config)#cdma pdsn accounting send cdma-ip-tech vpdn 4
```

# cdma pdsn accounting send start-stop

To cause the PDSN to send accounting records when the call transitions between active and dormant states, use the **cdma pdsn accounting send start-stop** command in global configuration mode. To stop sending accounting records, use the **no** form of this command.

**cdma pdsn accounting send {start-stop | cdma-ip-tech}**

**no cdma pdsn accounting send {start-stop | cdma-ip-tech}**

## Syntax Description

| Command | Description |
|---|---|
| **start-stop** | Informs the PDSN when to begin sending accounting records and when to stop sending them. |
| **cdma-ip-tech** | Accounting records are generated with special IP-Tech number. |

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

When this feature is enabled, the PDSN will 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).

## Examples

The following example starts sending PDSN accounting events:

```
cdma pdsn accounting send start-stop
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn accounting local-timezone** | Specifies the timestamp for PDSN accounting events. |
| **cdma pdsn accounting time-of-day** | Sets the accounting information for a specific time of day. |
| **aaa accounting network pdsn start-stop group radius** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. |

# cdma pdsn accounting time-of-day

To set the accounting information for specified times during the day, use the **cdma pdsn accounting time-of-day** command in global configuration mode. To disable the specification, use the **no** form of this command.

**cdma pdsn accounting time-of-day** *hh:mm:ss*

**no cdma pdsn accounting time-of-day**

## Syntax Description

| | |
|---|---|
| *hh:mm:ss* | Hour:minutes:seconds. |

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)XS | This command was introduced. |

## Usage Guidelines

This command is used to facilitate billing when a user is charged different prices based upon the time of the day. Up to ten different accounting triggers can be configured.

## Examples

The following example sets an accounting trigger for 13:30:20:

```
cdma pdsn accounting time-of-day 13:30:30
```

## Related Commands

| Command | Description |
|---|---|
| **clock set** | Sets the system clock. |
| **debug cdma pdsn accounting time-of-day** | Displays debug information for the command. |
| **show clock** | Displays the system clock. |
| **cdma pdsn accounting send start-stop** | Causes the PDSN to send:<br>• An Accounting Stop record when it receives an active stop airlink record (dormant state)<br>• An Accounting Start record when it receives an active start airlink record (active state) |

# cdma pdsn age-idle-users

To configure the aging of idle users, use the **cdma pdsn age-idle-users** command. To stop aging out idle users, use the **no** form of this command.

**cdma pdsn age-idle-users [minimum-age** *value*]

**no cdma pdsn age-idle-users**

## Syntax Description

| | |
|---|---|
| **minimum-age** *value* | (Optional) The minimum number of seconds a user should be idle before they are a candidate for being aged out. Possible values are 1 through 65535. |

## Defaults

By default, no idle users are aged out.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

If no value is specified, the user that has been idle the longest will be aged out. If an age is specified and the user that has been idle the longest has not been idle for the specified value, then no users are aged out.

## Examples

The following example sets a minimum age out value of 5 seconds:

```
cdma pdsn age-idle-users minimum-age 5
```

# cdma pdsn cluster controller

To configure the PDSN to operate as a cluster controller, and to configure various parameters on the cluster controller, use the **cdma pdsn cluster controller** command. To disable certain cluster controller parameters, use the **no** form of this command.

**cdma pdsn cluster controller [ interface** *interface-name* | **timeout** *seconds* [**window** *number*] | **window** *number* ]

**no cdma pdsn cluster controller [ interface** *interface-name* | **timeout** *seconds* [**window** *number*] | **window** *number* ]

## Syntax Description

| | |
|---|---|
| **interface** | Interface name on which the cluster controller has IP connectivity to the cluster members. |
| **timeout** | The time the cluster controller waits to seek a member when there is no reply from that cluster member. The range is between 10 and 300 seconds, and the default value is 300 seconds. |
| **window** *number* | The number of sequential seek messages sent to a cluster member before it is presumed offline. |

## Defaults

The timeout default value is 300 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Examples

The following example enables the cdma cluster controller:

```
cdma pdsn cluster controller interface FastEthernet1/0
```

# cdma pdsn cluster member

To configure the PDSN to operate as a cluster member, and to configure various parameters on the cluster member, use the **cdma pdsn cluster member** command. To disable certain cluster controller parameters, use the **no** form of this command.

**cdma pdsn cluster member [ controller** *ipaddr* | **interface** *interface-name* | **prohibit** *type* | **timeout** *seconds* [**window** *number*] | **window** *number* ]

**no cdma pdsn cluster member [ controller** *ipadd* | **interface** *interface-name* | **timeout** *seconds* [**window** *number*] | **window** *number* ]

## Syntax Description

| | |
|---|---|
| **controller** *ipaddr* | The controller that a specific member is connected to, identified by the controller's IP address. |
| **interface** | Interface name on which the cluster controller has IP connectivity to the cluster members. |
| **prohibit** | The type of traffic that the member is allowed to handle, or is prohibited from handling. Administratively prohibits member from accepting new data sessions within the cluster framework. |
| **timeout** | The time the cluster controller waits to seek a member when there is no reply from that cluster member. The range is between 10 and 600 seconds, and the default value is 300 seconds. |
| **window** *number* | The number of sequential seek messages sent to a cluster member before it is presumed offline. |

## Defaults

The default timeout value for the cluster member is 300 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

The **prohibit** field enables a member to administratively rid itself of its load without service interruption. When enabled, the member is no longer given any new data sessions by the controller.

## Examples

The following example enables a cdma pdsn cluster member:

```
cdma pdsn cluster member interface FastEthernet1/0
```

# cdma pdsn compliance iosv4.1 session-reference

3GPP2 IOS version 4.2 mandates that the Session Reference ID in the A11 Registration Request is always set to 1. To configure the PDSN to interoperate with a PCF that is not compliant with 3GPP2 IOS version 4.2, use the **cdma pdsn compliance iosv4.1 session-reference** command inGlobal configuration mode. To disable this configuration, use the **no** form of this command.

**cdma pdsn compliance iosv4.1 session-reference**

**no cdma pdsn compliance iosv4.1 session-reference**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Session Reference ID set to 1 in the A11 registration Request is on by default.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY1 | This command was introduced. |

## Examples

The following command instructs the PDSN to skip any checks done on the session reference id of incoming Registration Requests to ensure that they are set to 1.

```
router # cdma pdsn compliance iosv4.1 session-reference
```

## Related Commands

| Command | Description |
|---|---|
| **debug cdma pdsn a11** | Displays debug messages for A11 interface errors, events, and packets. |

# cdma pdsn compliance is835a esn-optional

To send an ESN value in accounting packets to the RADIUS server only if it has received an ESN value (A2) in the A11 RRQ from PCF, use the **cdma pdsn compliance is835 esn-optional** command in global configuration mode. To disable the specification, use the **no** form of this command.

**cdma pdsn compliance is835 esn-optional**

**no cdma pdsn compliance is835 esn-optional**

## Syntax Description

There are no keywords or arguments for this command.

## Defaults

The default behavior is to send the ESN attribute in all accounting records..

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)ZB4 | This command was introduced. |

## Usage Guidelines

If no A2 is received in the RRQ, the PDSN will not send the ESN attribute in the accounting record. This behavior is in accordance to IS835A.

If this command is not confogired, the PDSN will send the ESN value regardless whether the A2 attribute value is received from PCF or not. This is in accordance to IS835B.

# cdma pdsn failure-history

To configure CDMA PDSN SNMP session failure history size, use the **cdma pdsn failure-history** command in global configuration mode. To return to the default length of time, use the **no** form of this command.

**cdma pdsn failure-history** *entries*

**no cdma pdsn failure-history**

## Syntax Description

| | |
|---|---|
| *entries* | Maximum number of entries that can be recorded in the SNMP session failure table. Possible values are 0 through 2000. |

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example specifies that 1000 is the maximum number of entries that can be recorded in the SNMP session table:

```
cdma pdsn failure-history 1000
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server enable traps cdma** | Specifies the community access string to permit access to the SNMP protocol. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn ingress-address-filtering

To enable ingress address filtering, use the **cdma pdsn ingress-address-filtering** command in global configuration mode. To disable ingress address filtering, use the **no** form of this command.

**cdma pdsn ingress-address-filtering**

**no cdma pdsn ingress-address-filtering**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Ingress address filtering is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

When this command is configured, the PDSN checks the source IP address of every packet received on the PPP link from the mobile station. If the address is not associated with the PPP link to the mobile station and is not an MIP RRQ or Agent Solicitation, then the PDSN discards the packet and sends a request to reestablish the PPP link.

## Examples

The following example enables ingress address filtering:

```
cdma pdsn ingress-address-filtering
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |
| **show cdma pdsn session** | Displays the session information on the PDSN. |

# cdma pdsn maximum pcf

To set the maximum number of PCFs that can connect to a PDSN, use the **cdma pdsn maximum pcf** command in global configuration mode. To disable a configured limit, use the **no** form of this command.

**cdma pdsn maximum pcf** *maxpcf*

**no cdma pdsn maximum pcf**

## Syntax Description

| | |
|---|---|
| *maxpcf* | Maximum number of PCFs that can communicate with a PDSN. Possible values are 1 through 2000. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

If no maximum number of PCFs is configured, the only limitation is the amount of memory.

You can configure the maximum PCFs to be less than the existing PCFs. As a result, when you issue the **show cdma pdsn** command, you may see more existing PCFs than the configured maximum. It is the responsibility of the user to bring down the existing PCFs to match the configured maximum.

## Examples

The following example specifies that 200 PCFs can be sent:

```
cdma pdsn maximum pcf 200
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn maximum sessions

To set the maximum number of mobile sessions allowed on a PDSN, use the **cdma pdsn maximum sessions** command in global configuration mode. To disable a configured limit, use the **no** form of this command.

**cdma pdsn maximum sessions** *maxsessions*

**no cdma pdsn maximum sessions**

## Syntax Description

| | |
|---|---|
| *maxsessions* | Maximum number of mobile sessions allowed on a PDSN. Possible values depend on which image you are using. |

## Defaults

The c-5 images support 8000 sessions, and the c-6 images support 20000 sessions.

## Command Modes

Global Configuration.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | The maximum number of mobile sessions was raised to 20000. |

## Usage Guidelines

If PDSN runs out of resources before the configured number is reached, then PDSN will reject the creation of further sessions.

You can configure the maximum sessions to be less than the existing sessions. As a result, when you issue the **show cdma pdsn** command, you may see more existing sessions than the configured maximum. It is the responsibility of the user to bring down the existing sessions to match the configured maximum.

## Examples

The following example sets the maximum number of mobile sessions to 100:

```
cdma pdsn maximum sessions 100
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn session** | Displays PDSN session information. |

# cdma pdsn mobile-advertisement-burst

To configure the number and interval of Agent Advertisements that a PDSN FA can send, use the **cdma pdsn mobile-advertisement-burst** command in interface configuration mode. To reset the configuration to the defaults, use the **no** form of this command.

**cdma pdsn mobile-advertisement-burst** {**number** *value* | **interval** *msec*}

**no cdma pdsn mobile-advertisement-burst** {**number** | **interval**}

## Syntax Description

| | |
|---|---|
| **number** *value* | The number of agent advertisements. Possible values are 1 through 10. The default is 5. |
| **interval** *msec* | Specifies the interval, in milliseconds, between advertisements. Possible values are 50 through 500. The default is 200 milliseconds. |

## Defaults

The default number of agent advertisements to send is 5.

The default interval between advertisements is 200 milliseconds.

## Command Modes

Interface Configuration.

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

You must specify at least one of the optional parameters. Otherwise, the command has no effect. When virtual-access interfaces are created from the virtual template, default values will be used for any parameters not already configured on the virtual template.

This command should be configured on virtual templates only, and only when PDSN service is configured.

## Examples

The following example configures PDSN FA advertisement:

```
cdma pdsn mobile-advertisement-burst number 10 interval 500
```

## Related Commands

| Command | Description |
|---|---|
| **ip mobile foreign-service challenge** | Configures the challenge timeout value and the number of valid recently-sent challenge values. |
| **ip mobile foreign-service challenge forward-mfce** | Enables the FA to forward MFCE and mobile station-AAA to the HA. |

# cdma pdsn msid-authentication

To enable MSID-based authentication and access, use the **cdma pdsn msid-authentication** command in global configuration mode. To disable MSID-based authentication and access, use the **no** form of this command.

**cdma pdsn msid-authentication** [**imsi** *number*] [**irm** *number*] [**min** *number*] [**profile-password** *password*]

**no cdma pdsn msid-authentication**

## Syntax Description

| | |
|---|---|
| **imsi** *number* | (Optional) The number digits from the International Mobile Station Identifier (IMSI) that are to be used as the User-Name in the Access-Request for MSID authentication. Possible values are 1 to 15. The default is 5. |
| **irm** *number* | (Optional) International Roaming Mobile Identification Number and the identifier used to retrieve the network profile from the RADIUS server. Possible values are 1 through 10. The default is 4. |
| **min** *number* | (Optional) Mobile Identification Number and the identifier used to retrieve the network profile from the RADIUS server. Possible values are 1 through 10. The default is 6. |
| **profile-password** *password* | (Optional) The AAA server access password for MSID-based authentication. The default is “cisco”. |

## Defaults

MSID authentication is disabled. When enabled, the default values are as follows:

- imsi: 5
- irm: 4
- min: 6
- profile-password: cisco

## Command Modes

Global Configuration.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(2)XC | The **profile-password** keyword was added. |

## Usage Guidelines

MSID authentication provides Simple IP service for mobile stations that do not negotiate CHAP or PAP. Cisco PDSN retrieves a network profile based on the MSID from the RADIUS server. The network profile should include the internet realm of the home network that owns the MSID. Cisco PDSN constructs the NAI from the MSID and the realm. The constructed NAI is used in generated accounting records. If the PDSN is unable to obtain the realm, then it denies service to the mobile station.

The identifier used to retrieve the network profile from the RADIUS server depends on the format of the MSID, which can be one of the following:

- International Mobile Station Identity (IMSI)
- Mobile Identification Number (MIN)
- International Roaming MIN (IRM)

If the mobile station uses IMSI, the default identifier that PDSN uses to retrieve network profile is of the form IMSI-nnnnn where nnnnn is the first five digits of the IMSI. The number of digits from the IMSI to be used can be configured using the command **cdma pdsn msid-authentication imsi**.

If the mobile station uses MIN, the default identifier that PDSN uses to retrieve network profile is of the form MIN-nnnnnn where nnnnnn is the first six digits of the MIN. The number of digits from the MIN to be used can be configured using the command **cdma pdsn msid-authentication min**.

If the mobile station uses IRM, the default identifier that PDSN uses to retrieve network profile is of the form IRM-nnnn where nnnn is the first four digits of the IRM. The number of digits from the IRM to be used can be configured using the command **cdma pdsn msid-authentication irm**.

The realm should be defined in the network profile on the RADIUS user with the Cisco AVPair attribute **cdma:cdma-realm**.

## Examples

The following example enables MSID-based authentication and access:

```
cdma pdsn msid-authentication profile-password test1
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn retransmit a11-update

To specify the maximum number of times an A11 Registration Update message is retransmitted, use the **cdma pdsn retransmit a11-update** command in global configuration mode. To return to the default of 5 retransmissions, use the **no** form of this command.

**cdma pdsn retransmit a11-update** *number*

**no cdma pdsn retransmit a11-update**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of times an A11 Registration Update message is retransmitted. Possible values are 0 through 9. The default is 5 retransmissions. |

## Defaults

5 retransmissions.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

PDSN may initiate the release of an A10 connection by sending an A11 Registration Update message to the PCF. In this case, the PCF is expected to send an A11 Registration Acknowledge message followed by an A11 Registration Request with Lifetime set to 0. If PDSN does not receive an A11 Registration Acknowledge or an A11 Registration Request with Lifetime set to 0, or if it receives an A11 Registration Acknowledge message with an update denied status, PDSN retransmits the A11 Registration Update. The number of retransmissions is 5 by default and is configurable using this command.

## Examples

The following example specifies that A11 Registration Update messages will be retransmitted a maximum of 9 times:

```
cdma pdsn retransmit a11-update 9
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn timeout a11-update** | Specifies A11 Registration Update message timeout. |
| **debug cdma pdsn a11** | Displays debug messages for A11 interface errors, events, and packets. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn secure cluster

To configure one common security association for all PDSNs in a cluster, use the **cdma pdsn secure cluster** command. To remove this configuration, use the **no** form of the command.

**cdma pdsn secure cluster default spi** {*value* | **inbound** *value* **outbound** *value*} **key** {**hex** | **ascii**} *string*

**no cdma pdsn secure cluster**

## Syntax Description

| | |
|---|---|
| **default** | Specifies this is the default security configuration. |
| **spi** *value* | Security parameter index (SPI) used for authenticating packets. Possible values are 0x100 through 0xffffffff. |
| **inbound** *value* **outbound** *value* | Inbound and outbound SPI. |
| **key** {**hex** \| **ascii**} *string* | String of ascii or hexadecimal values. No spaces are allowed. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout, and IP address.

## Examples

The following example shows a security association for a cluster of PDSNs:

```
cdma pdsn secure cluster spi 100 key hex 12345678123456781234567812345678
```

## Related Commands

| Command | Description |
|---|---|
| **ip mobile secure** | Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host. |
| **cdma pdsn secure pcf** | Configures the security association for one or more PCFs or the default security association for all PCFs. |

# cdma pdsn secure pcf

To configure the security association for one or more PCFs or the default security association for all PCFs, use the **cdma pdsn secure pcf** command. To remove this configuration, use the **no** form of the command.

**cdma pdsn secure pcf** {*lower* [*upper*] | **default**} **spi** {*value* | **inbound** *value* **outbound** *value*} **key** {**hex** | **ascii**} *string* [**local-timezone**]

**no cdma pdsn secure pcf**

## Syntax Description

| | |
|---|---|
| *lower* [*upper*] | Range of mobile host or mobile node group IP addresses. The upper end of the range is optional. |
| **default** | Specifies this is the default security configuration. |
| **spi** *value* | Security parameter index (SPI) used for authenticating packets. Possible values are 0x100 through 0xffffffff. |
| **inbound** *value* **outbound** *value* | Inbound and outbound SPI. |
| **key** {**hex** \| **ascii**} *string* | String of ascii or hexadecimal values. No spaces are allowed. |
| **local-timezone** | Adds local timezone support for R-P messages. If this keyword is enabled, the timestamp sent in the R-P messages will contain the timestamp of the local timezone.. |

## Defaults

There are no default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |
| 12.2(8)BY1 | The **local-timezone** keyword was added. |

## Usage Guidelines

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout, and IP address.

You can configure several explicit and default secure PCF entries. (An explicit entry being one in which the IP address of a PCF is specified.) When the PDSN receives an A11 message from a PCF, it attempts to match the message to a secure PCF entry as follows:

- The PDSN first checks the explicit entries and attempts to find a match based on the SPI value and the key.
- If a match is found, the message is accepted. If no match is found, the PDSN checks the default entries (again attempting to match the SPI and the key).

- If a match is found, the message is accepted. If no match is found, the message is discarded and an error message is generated.

When the PDSN receives a request from a PCF, it performs an identity check. As part of this check, the PDSN compares the timestamp of the request to its own local time and determines whether the difference is within a specified range. This range is determined by the *replay time window*. If the difference between the timestamp and the local time is not within this range, a request rejection message is sent back to the PCF along with the value of PDSN's local time.

## Examples

The following example shows PCF 20.0.0.1, which has a key that is generated by the MD5 hash of the string:

```
cdma pdsn secure pcf 20.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

The following example configures a global default replay time of 60 seconds for all PCFs and all SPIs:

```
cdma pdsn secure pcf default replay 60
```

The following example configures a default replay time of 30 seconds for a specific SPI applicable to all PCFs:

```
cdma pdsn secure pcf default spi 100 key ascii cisco replay 30
```

The following example configures a replay time of 45 seconds for a specific PCF/SPI combination:

```
cdma pdsn secure pcf 192.168.105.4 spi 200 key ascii cisco replay 45
```

## Related Commands

| Command | Description |
|---|---|
| **ip mobile secure** | Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host. |
| **cdma pdsn secure cluste**r | Configures one common security association for all PDSNs in a cluster. |

# cdma pdsn selection interface

To configure the interface used to send and receive PDSN selection messages, use the **cdma pdsn selection interface** command in global configuration mode. To remove the configuration, use the **no** form of the command.

**cdma pdsn selection interface** *interface_name*

**no cdma pdsn selection interface**

## Syntax Description

| | |
|---|---|
| *interface_name* | Name (type and number) of the interface that is connected to the LAN to be used to exchange PDSN selection messages with the other PDSNs in the cluster. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

Each PDSN in a cluster maintains information about the mobile stations connected to the other PDSNs in the cluster. All PDSNs in the cluster exchange this information using periodic multicast messages. For this reason, all PDSNs in the cluster should be connected to a shared LAN.

This command identifies the interface on the PDSN that is connected to the LAN used for sending and receiving PDSN selection messages.

The Intelligent PDSN Selection feature will not work if you do not configure this interface on each PDSN in the cluster.

## Examples

The following example specifies that the FastEthernet0/1 interface should be used for sending and receiving PDSN selection messages:

```
cdma pdsn selection interface FastEthernet0/1
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn selection keepalive** | Specifies the keepalive time. |
| **cdma pdsn selection load-balancing** | Enables the load-balancing function of the intelligent PDSN selection feature. |
| **cdma pdsn selection session-table-size** | Defines the size of the selection session database. |

# cdma pdsn selection keepalive

To configure the intelligent PDSN selection keepalive feature, use the **cdma pdsn selection keepalive** command in global configuration mode. To disable the feature, use the **no** form of this command.

**cdma pdsn selection keepalive** *value*

**no cdma pdsn selection keepalive**

## Syntax Description

| | |
|---|---|
| *value* | The keepalive value, in seconds. Possible values are 5 through 60. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example configures a keepalive value of 200 seconds:

```
cdma pdsn selection keepalive 200
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn selection load-balancing** | Enables the load-balancing function of the intelligent PDSN selection feature. |
| **cdma pdsn selection session-table-size** | Defines the size of the selection session database. |
| **show cdma pdsn selection** | Displays the PDSN selection session table. |

# cdma pdsn selection load-balancing

To enable the load-balancing function of the intelligent PDSN selection feature, use the **cdma pdsn selection load-balancing** command in global configuration mode. To disable the load-balancing function, use the **no** form of this command.

**cdma pdsn selection load-balancing [threshold** *val* **[alternate]]**

**no cdma pdsn selection load-balancing**

## Syntax Description

| | |
|---|---|
| **threshold** *val* | (Optional) The maximum number of sessions that can be load-balanced. Possible values are 1 through 20000. The default session threshold is 100. |
| **alternate** | (Optional) The Alternate option alternately suggests two other PDSNs with the least load. |

## Defaults

The threshold value is 100 sessions.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | The maximum number of sessions that can be load-balanced was raised to 20000. |

## Usage Guidelines

You must enable PDSN selection session-table-size first. If sessions in a PDSN go beyond the threshold, PDSN selection will redirect the PCF to the PDSN that has less of a load.

## Examples

The following example configures load-balancing with an advertisement interval of 2 minutes and a threshold of 50 sessions:

```
cdma pdsn selection load-balancing advertisement 2 threshold 50
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn selection session-table-size** | Defines the size of the selection session database. |
| **show cdma pdsn session** | Displays PDSN session information. |

# cdma pdsn selection session-table-size

In PDSN selection, a group of PDSNs maintains a distributed session database. To define the size of the database, use the **cdma pdsn selection session-table-size** command in global configuration mode. To disable PDSN selection, use the **no** form of this command.

**cdma pdsn selection session-table-size** *size*

**no cdma pdsn selection session-table-size**

## Syntax Description

| | |
|---|---|
| *size* | Session table size. Possible values are 2000 through 100000. |

## Defaults

PDSN selection is disabled.

The default session table size is undefined.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example sets the size of the distributed session database to 5000 sessions:

```
cdma pdsn selection session-table-size 5000
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn selection load-balancing** | Enables the load-balancing function of PDSN selection. |
| **show cdma pdsn session** | Displays PDSN session information. |

# cdma pdsn send-agent-adv

To enable agent advertisements to be sent over a newly formed PPP session with an unknown user class that negotiates IPCP address options, use the **cdma pdsn send-agent-adv** command in global configuration mode. To disable the sending of agent advertisements, use the **no** form of this command.

**cdma pdsn send-agent-adv**

**no cdma pdsn send-agent-adv**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

This command is used with multiple flows.

## Examples

The following example enables agent advertisements to be sent:

```
cdma pdsn send-agent-adv
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn timeout a11-update

To specify a A11 Registration Update message timeout, use the **cdma pdsn timeout a11-update** command in global configuration mode. To return to the default of 1 second, use the **no** form of this command.

**cdma pdsn timeout a11-update** *seconds*

**no cdma pdsn timeout a11-update**

## Syntax Description

| | |
|---|---|
| *seconds* | Maximum A11 Registration Update message timeout value, in seconds. Possible values are 0 through 5. The default is 1 second. |

## Defaults

1 second.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

PDSN may initiate the release of an A10 connection by sending an A11 Registration Update message to the PCF. In this case, the PCF is expected to send an A11 Registration Acknowledge message followed by an A11 Registration Request with Lifetime set to 0. If PDSN does not receive an A11 Registration Acknowledge or an A11 Registration Request with Lifetime set to 0, PDSN times out and retransmits the A11 Registration Update. The default timeout is 1 second and is configurable using this command.

## Examples

The following example specifies an A11 Registration Update message timeout value of 5 seconds:

```
cdma pdsn timeout a11-update 5
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn retransmit a11-update** | Specifies the maximum number of times an A11 Registration Update message will be retransmitted. |
| **debug cdma pdsn a11** | Displays debug messages for A11 interface errors, events, and packets. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn timeout mobile-ip-registration

To set the timeout value before which Mobile IP registration should occur for a user skipping the PPP authentication, use the **cdma pdsn timeout mobile-ip-registration** command in global configuration mode. To return to the default 5-second timeout, use the **no** version of the command.

**cdma pdsn timeout mobile-ip-registration** *timeout*

**no cdma pdsn timeout mobile-ip-registration**

## Syntax Description

| | |
|---|---|
| *timeout* | Time, in seconds. Possible values are 1 through 60. The default is 5 seconds. |

## Defaults

5 seconds.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

A CDMA data user using Mobile IP will skip authentication and authorization during PPP and perform those tasks through Mobile IP registration. In order to secure the network, the traffic is filtered. The only packets allowed through the filter are the Mobile IP registration messages. As an additional protection, if the Mobile IP registration does not happen within a defined time, the PPP link is terminated.

## Examples

The following example sets the timeout value for Mobile IP registration to 15 seconds:

```
cdma pdsn mobile-ip-timeout 15
```

## Related Commands

| Command | Description |
|---|---|
| **show ip mobile interface** | Displays information about interfaces that are providing FA service or are home links for mobile stations. |
| **show cdma pdsn** | Displays the current status and configuration of the PDSN gateway. |

# cdma pdsn virtual-template

To associate a virtual template with PPP over GRE, use the **cdma pdsn virtual-template** command in global configuration mode. To remove the association, use the **no** form of this command.

**cdma pdsn virtual-template** *virtualtemplate_num*

**no cdma pdsn virtual-template** *virtualtemplate_num*

## Syntax Description

| | |
|---|---|
| *virtualtemplate_num* | Virtual template number. Possible values are 1 through 25. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

PPP links are dynamically created. Each link requires an interface. The characteristics of each link are cloned from a virtual template. Because there can be multiple virtual templates defined in a single PDSN, this command is used to identify the virtual template that is used for cloning virtual accesses for PPP over GRE.

## Examples

The following example associate virtual template 2 with PPP over GRE:

```
cdma pdsn virtual-template 2
```

## Related Commands

| Command | Description |
|---|---|
| **interface virtual-template** | Creates a virtual template interface. |

# clear cdma pdsn cluster controller session records age

To clear session records of a specified age, use the **clear cdma pdsn cluster controller session records age** command in privileged EXEC mode.

**clear cdma pdsn cluster controller session records age** *days*

## Syntax Description

| | |
|---|---|
| *days* | The number of days of the record age. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **clear cdma pdsn cluster controller session records age** command:

```
Router# clear cdma pdsn cluster controller session records age 1
```

# clear cdma pdsn selection

To clear PDSN selection tables, use the **clear cdma pdsn selection** command in privileged EXEC mode.

**clear cdma pdsn selection** [**pdsn** *ip-addr* | **msid** *number*]

## Syntax Description

| | |
|---|---|
| **pdsn** *ip-addr* | (Optional) IP address of the PDSN selection session table to be cleared. |
| **msid** *number* | (Optional) Identification of the MSID to be cleared. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example clears the pdsn selection session table for PDSN 5.5.5.5:

```
clear cdma pdsn selection pdsn 5.5.5.5
```

## Related Commands

| Command | Description |
|---|---|
| **cdma pdsn selection session-table-size** | Enables the PDSN selection feature and defines the size of the session table. |

# clear cdma pdsn session

To clear one or more user sessions on the PDSN, use the **clear cdma pdsn session** command in privileged EXEC mode.

**clear cdma pdsn session** {**all** | **pcf** *ip_addr* | **msid** *number*}

## Syntax Description

| | |
|---|---|
| **all** | Keyword to clear all sessions on a given PDSN. |
| **pcf** *ip_addr* | IP address of the PCF sessions that are to be cleared. |
| **msid** *number* | Identification of the MSID to be cleared. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

This command terminates one or more user sessions. When this command is issued, the PDSN initiates the session release by sending an A11Registration Update message to the PCF.

The keyword **all** clears all sessions on a given PDSN. The keyword **pcf** with an IP address clears all the sessions coming from a given PCF. The keyword **msid** with a number will clear the session for a given MSID.

## Examples

The following example clears session MSID 0000000002:

```
clear cdma pdsn session msid 0000000002
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn session** | Displays PDSN session information. |

# clear cdma pdsn statistics

To clear the RAN-to-PDSN interface (RP) or PPP statistics on the PDSN, use the **clear cdma pdsn statistics** command in privileged EXEC mode.

**clear cdma pdsn statistics**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Usage Guidelines

Previous releases used the **show cdma pdsn statistics** command to show PPP and RP statistic summaries from the time the system was restarted. The **clear cdma pdsn statistics** command allows the user to reset the counters as desired, and to view the history since the counters were last reset.

## Examples

The following example illustrates the **clear cdma pdsn statistics rp** command before and after the counters are reset.

### Before counters are reset

```
Router#show cdma pdsn statistics rp
RP Interface:
  Reg Request rcvd 5, accepted 5, denied 0, discarded 0
```

**Note** Non-zero values of counters.

```
  Initial Reg Request accepted 4, denied 0
  Re-registration requests accepted 0, denied 0
  De-registration accepted 1, denied 0
  Registration Request Errors:
    Unspecified 0, Administratively prohibited 0
    Resource unavailable 0, Authentication failed 0
    Identification mismatch 0, Poorly formed requests 0
    Unknown PDSN 0, Reverse tunnel mandatory 0
    Reverse tunnel unavailable 0, Bad CVSE 0

  Update sent 1, accepted 1, denied 0, not acked 0
  Initial Update sent 1, retransmissions 0
  Acknowledge received 1, discarded 0
  Update reason lifetime expiry 0, PPP termination 1, other 0
  Registration Update Errors:
```

```
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0

  Service Option:
    asyncDataRate2 (12) success 4, failure 0
```

**After the counters are reset**

```
Router#clear cdma pdsn statistics rp
==> RESETTING COUNTERS

Router#show cdma pdsn statistics rp
RP Interface:
  Reg Request rcvd 0, accepted 0, denied 0, discarded 0
```

**Note** The counter values are zeroes.

```
  Initial Reg Request accepted 0, denied 0
  Re-registration requests accepted 0, denied 0
  De-registration accepted 0, denied 0
  Registration Request Errors:
    Unspecified 0, Administratively prohibited 0
    Resource unavailable 0, Authentication failed 0
    Identification mismatch 0, Poorly formed requests 0
    Unknown PDSN 0, Reverse tunnel mandatory 0
    Reverse tunnel unavailable 0, Bad CVSE 0

  Update sent 0, accepted 0, denied 0, not acked 0
  Initial Update sent 0, retransmissions 0
  Acknowledge received 0, discarded 0
  Update reason lifetime expiry 0, PPP termination 0, other 0
  Registration Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0

  Service Option:
    asyncDataRate2 (12) success 4, failure 0
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn statistics** | Displays PDSN statistics. |

# clear ip mobile binding

To remove mobility bindings, use the **clear ip mobile binding** EXEC command.

**clear ip mobile binding** {**all** [**load** *standby-group-name*] | *ip-address* | **nai** *string ip_address*}

## Syntax Description

| | |
|---|---|
| **all** | Clears all mobility bindings. |
| **load** *standby-group-name* | (Optional) Downloads mobility bindings for a standby group after clear. |
| *ip-address* | IP address of a mobile node. |
| **nai** *string* | Network access identifier of the mobile node. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.1(3)T | The following keywords and argument were added:<br>• **all**<br>• **load**<br>• *standby-group-name* |
| 12.2(2)XC | The **nai** keyword and associated variables were added. |

## Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. The mobility binding allows the mobile node to exchange packets with the correspondent node. Associated with the mobility binding is the tunnel to the visited network and a host route to forward packets destined for the mobile node. There should be no need to clear the binding because it expires after lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed, the number of users on the tunnel is decremented and the host route is removed from the routing table. The mobile node is not notified.

Use this command with care, because it may terminate any sessions used by the mobile node. After using this command, the visitor will need to reregister to continue roaming.

## Examples

The following example administratively stops mobile node 10.0.0.1 from roaming:

```
Router# clear ip mobile binding 10.0.0.1

Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

## Related Commands

| Command | Description |
|---|---|
| **show ip mobile binding** | Displays the mobility binding table. |

# clear ip mobile host-counters

To clear the mobility counters specific to each mobile station, use the **clear ip mobile host-counters** EXEC command.

**clear ip mobile host-counters** [[*ip-address* | **nai** *string ip_address*] **undo**]]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) IP address of a mobile node. |
| **nai** *string* | (Optional) Network access identifier of the mobile node. |
| **undo** | (Optional) Restores the previously cleared counters. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword and associated variables were added. |

## Usage Guidelines

This command clears the counters that are displayed when you use the **show ip mobile host** command. The **undo** keyword restores the counters (this is useful for debugging).

## Examples

The following example shows how the counters can be used for debugging:

```
Router# show ip mobile host

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0

    .
Router# clear ip mobile host-counters
Router# show ip mobile host-counters

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip mobile host** | Displays mobile station counters and information. |

# clear ip mobile secure

To clear and retrieve remote security associations, use the **clear ip mobile secure** EXEC command.

**clear ip mobile secure** {**host** *lower* [*upper*] | **nai** *string* | **empty** | **all**} [**load**]

## Syntax Description

| | |
|---|---|
| **host** | Mobile node host. |
| *lower* | IP address of mobile node. Can be used alone, or as lower end of a range of addresses. |
| *upper* | (Optional) Upper end of range of IP addresses. |
| **nai** *string* | Network access identifier of the mobile node. |
| **empty** | Load in only mobile nodes without security associations. Must be used with the **load** keyword. |
| **all** | Clears all mobile nodes. |
| **load** | (Optional) Reload the security association from the AAA server after security association has been cleared. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword and associated variables were added. |

## Usage Guidelines

Security associations are required for registration authentication. They can be stored on an AAA server. During registration, they may be stored locally after retrieval from the AAA server. The security association on the router may become stale or out of date when the security association on the AAA server changes.

This command clears security associations that have been downloaded from the AAA server.

**Note** Security associations that are manually configured on the router or not stored on the router after retrieval from the AAA server are not applicable.

## Examples

In the following example, the AAA server has the security association for user 10.0.0.1 after registration:

```
Router# show ip mobile secure host 10.0.0.1

Security Associations (algorithm,mode,replay protection,key):
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

The security association of the AAA server changes as follows:

```
Router# clear ip mobile secure host 10.0.0.1 load

Router# show ip mobile secure host 10.0.0.1

10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

## Related Commands

| Command | Description |
|---|---|
| **ip mobile secure** | Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent. |

# clear ip mobile visitor

To remove visitor information, use the **clear ip mobile visitor** EXEC command.

**clear ip mobile visitor** [*ip-address* | **nai** *string ip_address*]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) IP address. If not specified, visitor information will be removed for all addresses. |
| **nai** *string* | (Optional) Network access identifier of the mobile node. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword and associated variables were added. |

## Usage Guidelines

The foreign agent creates a visitor entry for each accepted visitor. The visitor entry allows the mobile node to receive packets while in a visited network. Associated with the visitor entry is the ARP entry for the visitor. There should be no need to clear the entry because it expires after lifetime is reached or when the mobile node deregisters.

When a visitor entry is removed, the number of users on the tunnel is decremented and the ARP entry is removed from the ARP cache. The visitor is not notified.

Use this command with care because it may terminate any sessions used by the mobile node. After using this command, the visitor will need to reregister to continue roaming.

## Examples

The following example administratively stops visitor 10.0.0.1 from visiting:

```
Router# clear ip mobile visitor 10.0.0.1
```

## Related Commands

| Command | Description |
|---|---|
| **show ip mobile visitor** | Displays the table containing the visitor list of the foreign agent. |

# crypto map (global IPSec)

To create or modify a crypto map entry and enter the crypto map configuration mode, use the **crypto map** global configuration command. To delete a crypto map entry or set, use the no form of this command.

**crypto map** *map-name seq-num* **ipsec-manual**

**crypto map** *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*] [**discover**]

**no crypto map** *map-name* [*seq-num*]

**Note** Issue the crypto map map-name seq-num command without a keyword to modify an existing crypto map entry.

## Syntax Description

| | |
|---|---|
| *map name* | The name you assign to the crypto map set |
| *seq-num* | The number you assign to the crypto map entry. |
| **ipsec-manual** | Indicates that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. |
| **ipsec-isakmp** | Indicates that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. |
| **dynamic** | (Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available. |
| *dynamic-map-name* | (Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template. |
| **discover** | (Optional) Enables peer discovery. By default, peer discovery is not enabled. |

## Defaults

No crypto maps exist.

Peer discovery is not enabled.

## Command Modes

Global configuration. Using this command puts you into crypto map configuration mode, unless you use the dynamic keyword.

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 11.3T | The following keywords and arguments were added:<br>• **ipsec-manual**<br>• **ipsec-isakmp**<br>• **dynamic**<br>• *dynamic-map-name* |
| 12.0(5)T | The **discover** keyword was added to support Tunnel Endpoint Discovery (TED). |

## Usage Guidelines

Use this command to create a new crypto map entry or to modify an existing crypto map entry.

Once a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, once a map entry has been created as ipsec-isakmp, you cannot change it to ipsec-manual or cisco; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

### What Crypto Maps Are For

Crypto maps provide two functions: filtering/classifying traffic to be protected, and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps link together definitions of the following:

- What traffic should be protected
- Which IPSec peer(s) the protected traffic can be forwarded to—these are the peers with which a security association can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used/managed (or what the keys are, if IKE is not used)

### Multiple Crypto Maps Entries with the Same map-name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries each with a different seq-num but the same map-name. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic, and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish this you would create two crypto maps, each with the same map-name, but each with a different seq-num.

### The seq-num Argument

The number you assign to the seq-num argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower seq-num is evaluated before a map entry with a higher seq-num; that is, the map entry with the lower number has a higher priority.

For example, imagine there is a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named mymap is applied to interface Serial 0. When traffic passes through the Serial 0 interface, the traffic is evaluated first for mymap 10. If the traffic matches a **permit** entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec security associations when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a **permit** entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

#### Dynamic Crypto Maps

Refer to the "Usage Guidelines" section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

You should make crypto map entries which reference dynamic map sets the lowest priority map entries, so that inbound security association negotiations requests will try to match the static maps first. Only after the request does not match any of the static maps do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest seq-num of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the crypto map (IPSec global configuration) command using the dynamic keyword.

#### Tunnel Endpoint Discovery

Tunnel Endpoint Discovery is an enhancement to the IP Security Protocol (IPSec) feature. Defining a dynamic crypto map allows you to be able to dynamically determine an IPSec peer; however, only the receiving router has this ability. With Tunnel Endpoint Discovery, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic Tunnel Endpoint Discovery allows IPSec to scale to large networks by reducing multiple encryptions, reducing the setup time, and allowing for simple configurations on participating peer routers. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

## Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the security associations:

```
Router# crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the security associations are manually established:

```
Router# crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 9876543210987654987654321098765 4
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows security associations to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound security association negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow “permitted” by the access list 103, IPSec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match a permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
Router# crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures Tunnel Endpoint Discovery on a Cisco router:

```
Router# crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

# interface cdma-Ix

To define the virtual interface for the R-P tunnels, use the **interface cdma-Ix** command in global configuration mode. To disable the interface, use the **no** form of this command.

**interface cdma-Ix1**

**no interface cdma-Ix1**

## Syntax Description

| | |
|---|---|
| **Ix1** | Interface number 1. Only one interface definition per PDSN is allowed. |

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

The only interface level command allowed on the virtual interface is the IP address configuration.

## Examples

The following example defines the virtual interface for the R-P tunnel and configures the IP address:

```
interface cdma-Ix1
 ip address 1.1.1.1 255.255.0.0
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics about the network interfaces. |

# ip mobile authentication ignore-spi

To enable MNs and Foreign Agents to use the SPI while calculating the authenticator value for Mobile-Home Auth or Foreign-Home authorization, use the **ip mobile authentication ignore-spi** global configuration command.

**ip mobile authentication ignore-spi**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default values.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example illustrates the **ip mobile authentication ignore-spi** command:

```
Router# ip mobile authentication ignore-spi
```

# ip mobile bindupdate

During an inter-PDSN handoff, to enable an HA to send a binding update message to an old FA to release the unused PPP session the FA is holding, use the **ip mobile bindupdate** global configuration command. To disable this configuration, use the **no** form of the command.

**ip mobile bindupdate** [**acknowledge** | **maximum** *secs* | **minimum** *secs* | **retry** *value*]

**no ip mobile bindupdate** [**acknowledge** | **maximum** *secs* | **minimum** *secs* | **retry** *value* ]

## Syntax Description

| | |
|---|---|
| **acknowledge** | (Optional) Old FA will send an acknowledge message to the HA in response to the binding update message. |
| **maximum** *secs* | (Optional) If acknowledge message is not received then maximum time HA has to wait before retransmitting the message (allowed 1-10 secs) |
| **minimum** *secs* | (Optional) If acknowledge message is not received then minimum time HA has to wait before retransmitting the message (allowed 1-10 secs) |
| **retry** *value* | (Optional) If acknowledge message is not received then number of times HA has to send the binding update message (allowed 1-4 times) |

## Defaults

No default values.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example illustrates the **ip mobile bindupdate** command:

```
Router# ip mobile bindupdate
```

# ip mobile foreign-agent

To enable foreign agent service, use the **ip mobile foreign-agent** global configuration command. To disable this service, use the **no** form of this command.

**ip mobile foreign-agent** [**care-of** *interface* | **reg-wait** *seconds* | **local-timezone**]

**no ip mobile foreign-agent** [**care-of** *interface* | **reg-wait** *seconds* | **local-timezone**]

## Syntax Description

| | |
|---|---|
| **care-of** *interface* | (Optional) IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured. |
| **reg-wait** *seconds* | (Optional) Pending registration expires after the specified number of seconds if no reply is received. Range is from 5 to 600. Default is 15. |
| **local-timezone** | (Optional) Adjusts the UTC time based on the local time zone configured and uses the adjusted time for proxy mobile IP registration. |

## Defaults

Disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **local-timezone** keyword was added. |

## Usage Guidelines

This command enables foreign agent service when at least one care-of address is configured. When no care-of address exists, foreign agent service is disabled.

The foreign agent is responsible for relaying the registration request to the home agent, setting up tunnel to the home agent, and forwarding packets to the mobile node. The show commands used to display relevant information are shown in parentheses in the following paragraph.

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on interface or no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated (**show ip mobile secure visitor** command). The registration bitflag is handled as described in Table 5 (**show ip mobile interface** command). The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending** command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in Table 6). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command). (Violation reasons are listed in Table 16.)

When a registration reply comes in, the home agent is authenticated (**show ip mobile secure home-agent** command) if a security association exists for the home agent (IP source address or home agent address in reply). The reply is relayed to the mobile node.

When registration is accepted, the foreign agent creates or updates the visitor table, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the mobile node via the interface (of the incoming request) is added to the routing table (show ip route mobile command), and an ARP entry is added to avoid sending ARP requests for the visiting mobile node. Visitor binding is removed (along with its associated host route, tunnel, and ARP entry) when the registration lifetime expires or deregistration is accepted.

When registration is denied, the foreign agent will remove the request from the pending registration table. The table and timers of the visitor will be unaffected.

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent will deencapsulates the packet and forwards it out its interface to the visiting mobile node, without sending ARP requests.

The care-of address must be advertised by the foreign agent. This is used by the mobile node to register with the home agent. The foreign agent and home agent use this address as the source and destination point of tunnel, respectively. The foreign agent is not enabled until at least one care-of address is available. The foreign agent will advertise on interfaces configured with the **ip mobile foreign-service** command.

Only care-of addresses with interfaces that are up are considered available.

***Table 5 Foreign Agent Registration Bitflags***

| Bit Set | Registration Request |
|---|---|
| S | No operation. Not applicable to foreign agent. |
| B | No operation. Not applicable to foreign agent. |
| D | Make sure source IP address belongs to the network of the interface. |
| M | Deny request. Minimum IP encapsulation is not supported. |
| G | No operation. GRE encapsulation is supported. |
| V | Deny request. Van Jacobson Header compression is not supported. |
| T | Deny request. Reverse tunnel is not supported. |
| reserved | Deny request. Reserved bit must not be set. |

***Table 6 Foreign Agent Reply Codes***

| Code | Reason |
|---|---|
| 64 | Reason unspecified. |
| 65 | Administratively prohibited. |
| 66 | Insufficient resource. |
| 67 | Mobile node failed authentication. |
| 68 | Home agent failed authentication. |
| 69 | Requested lifetime is too long. |
| 70 | Poorly formed request. |
| 71 | Poorly formed reply. |

*Table 6 Foreign Agent Reply Codes (continued)*

| Code | Reason |
|---|---|
| 72 | Requested encapsulation is unavailable. |
| 73 | Requested Van Jacobson Header compression is unavailable. |
| 74 | Reverse tunnel unsupported. |
| 80-95 | ICMP Unreachable message code 0 to 15. |

## Examples

The following example enables foreign agent service on interface Ethernet1, advertising 1.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 1.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

## Related Commands

| Command | Description |
|---|---|
| **ip mobile home-agent** | Enables home agent service on the router |
| **ip mobile foreign-service** | Enables foreign agent service on an interface if care-of addresses are configured. |
| **show ip mobile globals** | Displays global information for mobile agents. |
| **show ip mobile interface** | Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes. |
| **show ip mobile secure** | Displays mobility security associations for mobile host, mobile visitor, foreign agent, or home agent. |
| **show ip mobile violation** | Displays information about security violations. |
| **show ip mobile visitor** | Displays the table containing the visitor list of the foreign agent. |

# ip mobile foreign-service

To enable foreign agent service on an interface if care-of addresses are configured, use the **ip mobile foreign-service** interface configuration command. To disable this service, use the **no** form of this command.

**ip mobile foreign-service** [**home-access** *acl*] [**limit** *number*] [**registration-required**] [**challenge** {**timeout** *value* | **window** *num* | **forward-mfce}**] [**reverse-tunnel** [**mandatory**]]

**no ip mobile foreign-service** [**home-access** *acl*] [**limit** *number*] [**registration-required**] [**challenge** {**timeout** *value* | **window** *num* | **forward-mfce}**] [**reverse-tunnel** [**mandatory**]]

## Syntax Description

| | |
|---|---|
| **home-access** *acl* | (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** *number* | (Optional) Number of visitors allowed on interface. The Busy (B) bit will be advertised when the number of registered visitors reach this limit. Range is from 1 to 1000. Default is no limit. |
| **registration-required** | (Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. |
| **challenge** | (Optional) Configures configure the FA challenge parameters. |
| **timeout** *value* | Challenge timeout in seconds. Possible values are 1 through 10. |
| **window** *num* | Maximum number of valid challenge values to maintain. Possible values are 1 through 10. The default is 2. |
| **forward-mfce** | Enables the FA to forward MFCE and mobile station-AAA to the HA. |
| **reverse-tunnel** [**mandatory**] | (Optional) Enables reverse tunneling on the FA. |

## Defaults

Disabled. Default is no limit to the number of visitors allowed on an interface. The default number of challenge values is 2.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.1(3)XS | The **challenge** keyword and associated parameters were added. |
| 12.2(2)XC | The **reverse-tunnel** keyword was added. |

## Usage Guidelines

This command enables foreign agent service on the interface. The foreign agent (F) bit will be set in the agent advertisement, which is appended to the IRDP router advertisement whenever the foreign agent or home agent service is enabled on the interface.

**Note** The Registration-required bit only tells the visiting mobile node to register even if the visiting mobile node is using a colocated care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from the interface of this foreign agent.

Table 7 lists the advertised bitflags.

***Table 7 Foreign Agent Advertisement Bitflags***

| Bit Set | Service Advertisement |
|---|---|
| R | Set if the **registration-required** parameter is enabled. |
| B | Set if the number of visitors reached the **limit** parameter. |
| H | Set if the interface is the home link to the mobile host (group). |
| F | Set if foreign-agent service is enabled. |
| M | Never set. |
| G | Always set. |
| V | Never set. |
| reserved | Never set. |

## Examples

The following example enables foreign agent service for up to 100 visitors:

```
interface Ethernet 0
 ip mobile foreign-service limit 100 registration-required
```

## Related Commands

| Command | Description |
|---|---|
| **show ip mobile interface** | Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes. |
| **cdma pdsn mobile-advertisement -burst** | Configures FA advertisements. |

# ip mobile host

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics about the network interfaces. |

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command. For PDSN, use this command to configure the static IP address or address pool for multiple flows with the same NAI.

**ip mobile host** {*lower* [*upper*] | **nai** *string* {**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*} | **address {***addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]} {**interface** *name* | **virtual-network** *network_address mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

**no ip mobile host** {*lower* [*upper*] | **nai** *string* {**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*} | **address {***addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]} {**interface** *name* | **virtual-network** *network_address mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

## Syntax Description

| | |
|---|---|
| *lower* [*upper*] | One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional. |
| **nai** *string* | Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (realm). |
| **static-address** | Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm. |
| *addr1, addr2, ...* | (Optional) One or more IP addresses to be assigned using the **static-address** keyword. |
| **local-pool** *name* | Name of the local pool of addresses to use for assigning a static IP address to this NAI. |
| **address** | Indicates that a dynamic IP address is to be assigned to the flows on this NAI. |
| *addr* | IP address to be assigned using the **address** keyword. |
| **pool** | Indicates that pool of addresses is to be used in assigning a dynamic IP address. |
| **local** *name* | The name of the local pool to use in assigning addresses. |
| **dhcp-proxy-client** | Indicates that the pool should come from a DHCP client. |
| **dhcp-server** *addr* | IP address of the DHCP server. |
| **interface** *name* | Mobile node that belongs to the specified interface. When used with DHCP, this specifies the address pool from which the DHCP server should select the address. |
| **virtual-network** *network_address mask* | Indicates that the mobile station resides in the specified virtual network, which was created using the **ip mobile virtual-network** command. |
| **aaa** | (Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server. |
| **load-sa** | (Optional) Stores security associations in memory after retrieval. |

| | |
|---|---|
| **care-of-access** *acl* | (Optional) Access list. This can be a string or number from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses. |
| **lifetime** *number* | (Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. Possible values are 3 through 65535. |

## Defaults

No host is configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword and associated parameters were added. |

## Usage Guidelines

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from an AAA server. When using an AAA server, the router will attempt to download all security associations when the command is entered. If no security associations are retrieved, retrieval will be attempted when a registration request arrives or the **clear ip mobile secure** command is entered.

All hosts must have security associations for registration authentication. Mobile nodes can have more than one security association. The memory consumption calculations shown in Table 8 are based on the assumption of one security association per mobile node.

The **nai** keyword allows you to specify a particular mobile station or range of mobile stations. The mobile station can request a static IP address (**static-address** keyword), which is configured using the *addr1* variable (for a specific address) or the **local-pool** keyword (for an IP address from an address pool). Or, the mobile station can request a dynamic address (**address** keyword), which is configured using the *addr* variable (for a specific address) or the **pool** keyword (for an IP address from a pool or DHCP server). If this command is use with the PDSN proxy Mobile IP feature and a realm is specified in the **ip mobile proxy-host nai** command, then only a pool of addresses can be specified in this command.

The address pool can be defined by a local pool or using a DHCP proxy client. For DHCP, the **interface** *name* specifies the address pool from which the DHCP server selects and **dhcp-server** specifies DHCP server address.

Security associations can be stored using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in
- On the AAA server, retrieve and store security association

Each method has advantages and disadvantages, which are described in Table 8.

***Table 8 Methods for Storing Security Associations***

| Storage Method | Advantage | Disadvantage |
|---|---|---|
| On the router | • Security association is in router memory, resulting in fast lookup.<br>• For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router). | • NVRAM of router is limited, cannot store many security associations. Each security association configuration takes about 80 bytes. For 125 KB NVRAM, you can store about 1500 security associations on a home agent. |
| On the AAA server, retrieve security association each time registration comes in | • Central administration and storage of security association on AAA server.<br>• If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration.<br>• Router memory (DRAM) is conserved. Router will only need memory to load in a security association, and then release the memory when done. Router can support unlimited number of mobile nodes. | • Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance.<br>• Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response.<br>• Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode). |
| On the AAA server, retrieve and store security association | • AAA acts as an offload configuration server, security associations are loaded into router DRAM, which is more abundant (for example, 16 MB, 32 MB, 64 MB) when the first registration comes in. Each security association takes only about 50 bytes of DRAM, so 10,000 mobile nodes will use up 0.5 MB.<br>• If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router.<br>• Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory. | • If keys change on the AAA server after the mobile node registered, then you need to use **clear ip mobile secure** command to clear and load in new security association from AAA, otherwise the security association of the router is stale. |

## Examples

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and store its security associations on the AAA server:

```
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 aaa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile stations in the cisco.com domain.

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 9.0.0.0
255.0.0.0 aaa lifetime 65535
```

The following example configures a local pool of static addresses to be used in assigning IP addresses to mobile stations in the cisco.com domain.

```
ip mobile host nai @cisco.com static-address local-pool mobilenodes
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization ipmobile** | Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS. |
| **ip mobile secure** | Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent. |
| **show ip mobile host** | Displays mobile station counters and information. |
| **ip mobile proxy-host** | Configures the proxy Mobile IP attributes of the PDSN. |

# ip mobile proxy-host

To locally configure the proxy Mobile IP attributes of the PDSN, use the **ip mobile proxy-host** global configuration command. To remove the configuration, use the **no** form of this command.

**ip mobile proxy-host nai** *username@realm* [**flags** *rrq-flags*] [**home-agent** *homeagent*] [**home-addr** *home_address*] [**lifetime** *value*] [**local-timezone**]

**no ip mobile proxy-host nai** *username@realm* [**flags** *rrq-flags*] [**home-agent** *homeagent*] [**home-addr** *home_address*] [**lifetime** *value*] [**local-timezone**]

## Syntax Description

| | |
|---|---|
| **nai** *username@realm* | Network access identifier. |
| **flags** *rrq-flags* | (Optional) Registration request flags. |
| **home-agent** *homeagent* | (Optional) IP address of the home agent. |
| **home-addr** *home_address* | (Optional) Home IP address of the mobile station. |
| **lifetime** *value* | (Optional) Global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Possible values are 3 through 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value. |
| **local-timezone** | (Optional) Adjusts the UTC time based on the local time zone configured and uses the adjusted time for proxy mobile IP registration. |

## Defaults

No security association is specified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

All proxy Mobile IP attributes can be retrieved from the AAA server. You can use this command to configure the attributes locally.

If only a realm is specified, the home address cannot be specified.

## Examples

The following example shows the **ip mobile proxy-host** command:

```
ip mobile proxy-host nai MoIPProxy1@cisco.com flags 40 ha 3.3.3.1 lifetime 6000
```

**Related Commands**

| Command | Description |
|---|---|
| **ip mobile host** | Configures the mobile host or mobile node group. |
| **ntp server** | Allows the system clock to be synchronized by a time server. |
| **ip mobile secure** | Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host. |
| **show ip mobile proxy** | Displays information about the proxy host configuration. |

# ip mobile secure

To specify the mobility security associations for the mobile host, visitor, home agent, foreign agent, and proxy host, use the **ip mobile secure** global configuration command. To remove the mobility security associations, use the **no** form of this command.

**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**]

**no ip mobile secure** {**aaa-download** | **visitor** | **foreign-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** [*num*] **algorithm md5 mode prefix-suffix**]

## Syntax Description

| | |
|---|---|
| **aaa-download** | Download SA from AAA every timer interval. |
| **visitor** | Security association of the mobile host on the foreign agent. |
| **home-agent** | Security association of the remote home agent on the foreign agent. |
| **foreign-agent** | Security association of the remote foreign agent on the home agent. |
| **proxy-host** | Security association of the proxy Mobile IP users. |
| *lower-address* | IP address of host, visitor, or mobility agent, or lower range of IP address pool. |
| *upper-address* | (Optional) Upper range of IP address pool. |
| **nai** *string* | Network access identifier. |
| **inbound-spi** *spi-in* | Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff. |
| **outbound-spi** *spi-out* | Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff. |
| **spi** *spi* | Bidirectional SPI. Range is from 0x100 to 0xffffffff. |
| **key ascii** \| **hex** *string* | ASCII or hexadecimal string of values. No spaces are allowed. |
| **replay** | (Optional) Replay protection used on registration packets. |
| **timestamp** | (Optional) Used to validate incoming packets to ensure that they are not being "replayed" by a spoofer using timestamp method. |
| *number* | (Optional) Number of seconds. Registration is valid if received within the specified time. This means the sender and receiver are in time synchronization (NTP can be used). |
| **algorithm** | (Optional) Algorithm used to authenticate messages during registration. |
| **md5** | (Optional) Message Digest 5. |
| **mode** | (Optional) Mode used to authenticate during registration. |
| **prefix-suffix** | (Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest. |

## Defaults

No security association is specified.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **proxy-host** and **nai** keywords were added. |

**Usage Guidelines**

The security association consists of the entity address, SPI, key, replay protection method, authentication algorithm, and mode.

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout, and IP address.

On a home agent, the security association of the mobile host is mandatory for mobile host authentication. If desired, configure a foreign agent security association on your home agent. On a foreign agent, the security association of the visiting mobile host and security association of the home agent are optional. Multiple security associations for each entity can be configured.

If registration fails because the **timestamp** value is out of bounds, the time stamp of the home agent is returned so the mobile node can reregister with the time-stamp value closer to that of the home agent, if desired.

The **nai** keyword is only valid for a host, visitor, and proxy host. To configure security associations for proxy Mobile IP users, use the following form of the command:

**ip mobile secure proxy-host nai** *string* **spi** *spi* **key** {**hex** | **ascii**} *string*

**Note** NTP can be used to synchronize time for all parties.

**Examples**

The following example shows mobile node 20.0.0.1, which has a key that is generated by the MD5 hash of the string:

```
ip mobile secure host 20.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

**Related Commands**

| Command | Description |
|---|---|
| **ip mobile host** | Configures the mobile host or mobile node group. |
| **ntp server** | Allows the system clock to be synchronized by a time server. |
| **show ip mobile secure** | Displays the mobility security associations for mobile host, mobile visitor, foreign agent, or home agent. |
| **ip mobile proxy-host** | Configures the proxy Mobile IP attributes of the PDSN. |

# ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the ip mobile tunnel interface configuration command.

**ip mobile tunnel** {**crypto map** *map-name* | **route-cache** | **path-mtu-discovery** | **nat** {**inside** | **outside**}}

## Syntax Description

| | |
|---|---|
| **crypto map** | Enables encryption/decryption on new tunnels. |
| *map-name* | Specifies the name of the crypto map. |
| **route-cache** | Sets tunnels to default or process switching mode. |
| **path-mtu-discovery** | Specifies when the tunnel MTU should expire if set by Path MTU Discovery. |
| **age-timer** *minutes* | (Optional) Time interval in minutes after which the tunnel reestimates the path MTU. |
| **infinite** | (Optional) Turns off the age timer. |
| **nat** | Applies Network Address Translation (NAT) on the tunnel interface. |
| **inside** | Sets the dynamic tunnel as the inside interface for NAT. |
| **outside** | Sets the dynamic tunnel as the outside interface for NAT. |

## Defaults

Disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | The **proxy-host** and **nai** keywords were added. |

## Usage Guidelines

These commands are only available in ipsec images (K9).

Path MTU discovery is used by end stations to find a packet size that does not need fragmentation between them. Tunnels have to adjust their MTU to the smallest MTU interior to achieve this. This is described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from case where sub-optimum MTU existed at time of discovery. It is reset to the outgoing interface's MTU.

## Examples

The following example assigns and specifically names a crypto map:

```
router (config)#ip mobile tunnel crypto ?
               map  Assign a Crypto Map

router (config)#ip mobile tunnel crypto map ?
               WORD  Crypto Map tag
```

# ppp accm

To configure the Asynchronous Control Character Map (ACCM) to be negotiated with the mobile station, use the **ppp accm** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

**ppp accm** *number*

**no ppp accm**

## Syntax Description

| | |
|---|---|
| *number* | Hexadecimal number identifying the ACCM. Possible values are 0 through FFFFFFFF. The default value is 000A0000. |

## Defaults

The default value is 000A0000.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

The ACCM is a four octet hexadecimal number that indicates the set of control characters to be mapped during transmission of AHDLC frames. During the LCP, each end of the PPP connection informs its peer the ACCM that should be used when transmitting the Asynchronous HDLC (AHDLC) frames. The TIA/EIA/IS-835-B requires that the PDSN propose an ACCM of 0x00000000. To be compliant with TIA/EIA/IS-835-B, “ppp accm 00000000" must be configured on the virtual template interface on Cisco PDSN.

## Examples

The following example specifies that PDSN propose an ACCM of 0x00000000:

```
ppp accm 00000000
```

## Related Commands

| Command | Description |
|---|---|
| **ppp authentication** | Specifies CHAP or PAP authentication. |

# ppp authentication

To enable CHAP, PAP or EAP, and to specify the order in which authentication is selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

**ppp authentication** {*protocol1* [*protocol2...*] *eap*} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] [eap]

**no ppp authentication**

## Syntax Description

| | |
|---|---|
| *protocol1* [*protocol2...*] | CHAP, PAP, Extensible Authentication protocol |
| **if-needed** | (Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces. |
| *list-name* | (Optional) Used with AAA. Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command. |
| **default** | (Optional) Name of the method list is created with the **aaa authentication ppp** command. |
| **callin** | (Optional) Specifies authentication on incoming (received) calls only. |
| **one-time** | (Optional) Accepts the username and password in the username field. |
| **optional** | (Optional) Used with PDSN configuration to allow a mobile station to receive Simple IP service and Mobile IP service without CHAP or PAP. |

## Defaults

PPP authentication is not enabled.

## Command Modes

Interface Configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.1(3)XS | The **optional** keyword was added. |

## Usage Guidelines

To configure Cisco PDSN in compliance with the TIA/EIA/IS-835-B standard, you must configure the PDSN virtual template as follows:

```
ppp authentication chap pap optional
```

## Examples

The following example configures virtual-template interface 4:

```
interface virtual-template 4
 ip unnumbered loopback0
 ppp authentication chap pap optional
```

## Related Commands

| Command | Description |
|---|---|
| **ppp accm** | Identifies the ACCM table. |

# service cdma pdsn

To enable PDSN service, use the **service cdma pdsn** command in global configuration mode. To disable PDSN service, use the **no** form of this command.

**service cdma pdsn**

**no service cdma pdsn**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

This command must be configured to enable CDMA PDSN on the router.

## Examples

The following example enables PDSN service:

```
service cdma pdsn
```

## Related Commands

| Command | Description |
|---|---|
| **show cdma pdsn pcf brief** | Displays a table of all PCFs that have R-P tunnels to the PDSN. |
| **show cdma pdsn session** | Displays PDSN session information. |

# show cdma pdsn

To display the status and current configuration of the PDSN gateway, use the **show cdma pdsn** command in privileged EXEC mode.

**show cdma pdsn**

## Syntax Description

This command has no keywords or arguments.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn** command:

**7200-c5 image:**

```
PRG5-7206-PDSN#show cdma pdsn
PDSN software version 1.2, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 300 sec
  A10 maximum lifetime allowed 1800 sec
  GRE sequencing is on
  Maximum PCFs limit not set
  Maximum sessions limit not set (default 8000 maximum)  <<<<<<< changed
  SNMP failure history table size 10
  MSID Authentication is disabled
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is disabled
  Aging of idle users disabled

  Number of pcfs connected 0
  Number of sessions connected 0,
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 0
```

**7200-c6 image**

```
PRG5-7206-PDSN#sho cdma pdsn
PDSN software version 1.2, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 300 sec
  A10 maximum lifetime allowed 1800 sec
  GRE sequencing is on
```

```
Maximum PCFs limit not set
Maximum sessions limit not set (default 20000 maximum) <<<<< changed
SNMP failure history table size 10
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation  is disabled
Aging of idle users disabled

Number of pcfs connected 0
Number of sessions connected 0,
  Simple IP flows 0, Mobile IP flows 0,
  Proxy Mobile IP flows 0
```

# show cdma pdsn accounting

To display the accouting information for all sessions and the corresponding flows, use the **show cdma pdsn accounting** command in privileged EXEC mode.

**show cdma pdsn accounting**

## Syntax Description

This command has no keywords or arguments.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

The counter names appear in abbreviated format.

## Examples

The following example shows output from the **show cdma pdsn accounting** command:

```
PDSN-6500#sh cdma pdsn accounting
 UDR for session
 session ID: 12
 Mobile Station ID IMSI 123451234512357

    A - A1:123451234512357
    C - ' 'C3:0
    D - D3:4.0.0.11 D4:000000000000
    E - E1:0000
    F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
    G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:655 G15:408 G16:378
    I - I1:0 I4:0
    Y - Y2:12

 UDR for flow
    Mobile Node IP address 15.0.0.3
    B - B1:15.0.0.3 B2:mwts-mip-p1-user121@ispxyz.com
    C - ' 'C2:36
    D - D1:0.0.0.0
    F - F11:02 F12:01 F13:00
    G - G1:0 G2:0 G4:1023906326
    Packets- in:0 out:0

 UDR for flow
    Mobile Node IP address 15.0.0.4

    B - B1:15.0.0.4 B2:mwts-mip-p1-user122@ispxyz.com
    C - ' 'C2:37
```

```
   D - D1:0.0.0.0
   F - F11:02 F12:01 F13:00
   G - G1:0 G2:0 G4:1023906326
   Packets- in:0 out:0

UDR for flow
   Mobile Node IP address 15.0.0.5

   B - B1:15.0.0.5 B2:mwts-mip-p1-user123@ispxyz.com
   C - ' 'C2:38
   D - D1:0.0.0.0
   F - F11:02 F12:01 F13:00
   G - G1:0 G2:0 G4:1023906326
   Packets- in:0 out:0

UDR for session
session ID: 2
Mobile Station ID IMSI 00000000003

   A - A1:00000000003
   C - ' 'C3:0
   D - D3:4.0.0.1 D4:000000000000
   E - E1:0000
   F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
   G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:201 G15:0 G16:0
   I - I1:0 I4:0
   Y - Y2:2

UDR for flow
   Mobile Node IP address 6.0.0.5

   B - B1:6.0.0.5 B2:mwt10-sip-user1
   C - ' 'C2:39
   D - D1:0.0.0.0
   F - F11:01 F12:00 F13:00
   G - G1:0 G2:0 G4:1023906826
   Packets- in:0 out:0

UDR for session
session ID: 3
Mobile Station ID IMSI 00000000004

   A - A1:00000000004
   C - ' 'C3:0
   D - D3:4.0.0.1 D4:000000000000
   E - E1:0000
   F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
   G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:241 G15:0 G16:0
   I - I1:0 I4:0
   Y - Y2:3

UDR for flow
   Mobile Node IP address 6.0.0.14

   B - B1:6.0.0.14 B2:mwt10-sip-user1
   C - ' 'C2:40
   D - D1:0.0.0.0
   F - F11:01 F12:00 F13:00
   G - G1:0 G2:0 G4:1023906826
   Packets- in:0 out:0

PDSN-6500#
```

# show cdma pdsn accounting detail

To display accounting information for all sessions and the corresponding flows, and to display the counter names (along with the abbreviated names), use the **show cdma pdsn accounting detail** command in privileged EXEC mode.

**show cdma pdsn accounting detail**

## Syntax Description

This command has no keywords or arguments.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn accounting detail** command:

```
PDSN-6500#sh cdma pdsn accounting detail
 UDR for session
 session ID: 12
 Mobile Station ID IMSI 123451234512357

   Mobile Station ID (A1) IMSI 123451234512357
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 4.0.0.11 Base Station ID (D4) 000000000000
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 245  Forward Traffic Type (F6) 246
   Reverse Traffix type (F7) 247  Fundamental Frame size (F8) 248
   Forward Fundamental RC (F9) 249  Reverse Fundamntal RC (F10) 250
   DCCH Frame Format (F14) 0
   Bad PPP Frame Count (G3) 0 Active Time (G8) 0
   Number of Active Transitions (G9) 0
   SDB Octet Count Terminating (G10) 0
   SDB Octet Count Originating (G11) 0
   Number of SDBs Terminating (G12) 0
   Number of SDBs Originating G13 0
   Number of HDLC Layer Bytes Received (G14) 655
   In-Bound Mobile IP Signalling Octet Count (G15) 408
   Out-bound Mobile IP Signalling Octet Count (G16) 378
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   R-P Session ID (Y2) 12

 UDR for flow
    Mobile Node IP address 15.0.0.3

    IP Address (B1) 15.0.0.3,  Network Access Identifier (B2)
```

```
mwts-mip-p1-user121@ispxyz.com
    Correlation ID (C2) ' ' 36
    MIP Home Agent  (D1) 0.0.0.0
    IP Technology (F11) 02 Compulsory Tunnel indicator (F12) 01
    Release Indicator (F13) 00
    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:1023906326
    Packets- in:0 out:0

 UDR for session
 session ID: 2
 Mobile Station ID IMSI 00000000003

   Mobile Station ID (A1) IMSI 00000000003
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 4.0.0.1 Base Station ID (D4) 000000000000
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 245  Forward Traffic Type (F6) 246
   Reverse Traffix type (F7) 247  Fundamental Frame size (F8) 248
   Forward Fundamental RC (F9) 249  Reverse Fundamntal RC (F10) 250
   DCCH Frame Format (F14) 0
   Bad PPP Frame Count (G3) 0 Active Time (G8) 0
   Number of Active Transitions (G9) 0
   SDB Octet Count Terminating (G10) 0
   SDB Octet Count Originating (G11) 0
   Number of SDBs Terminating (G12) 0
   Number of SDBs Originating G13 0
   Number of HDLC Layer Bytes Received (G14) 201
   In-Bound Mobile IP Signalling Octet Count (G15) 0
   Out-bound Mobile IP Signalling Octet Count (G16) 0
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   R-P Session ID (Y2) 2

 UDR for flow
    Mobile Node IP address 6.0.0.5

    IP Address (B1) 6.0.0.5,  Network Access Identifier (B2)
mwt10-sip-user1
    Correlation ID (C2) ' ' 39
    MIP Home Agent  (D1) 0.0.0.0
    IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
    Release Indicator (F13) 00
    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:1023906826
    Packets- in:0 out:0

 UDR for session
 session ID: 3
 Mobile Station ID IMSI 00000000004

   Mobile Station ID (A1) IMSI 00000000004
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 4.0.0.1 Base Station ID (D4) 000000000000
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 245  Forward Traffic Type (F6) 246
   Reverse Traffix type (F7) 247  Fundamental Frame size (F8) 248
   Forward Fundamental RC (F9) 249  Reverse Fundamntal RC (F10) 250
   DCCH Frame Format (F14) 0
   Bad PPP Frame Count (G3) 0 Active Time (G8) 0
   Number of Active Transitions (G9) 0
   SDB Octet Count Terminating (G10) 0
```

```
   SDB Octet Count Originating (G11) 0
   Number of SDBs Terminating (G12) 0
   Number of SDBs Originating G13 0
   Number of HDLC Layer Bytes Received (G14) 241
   In-Bound Mobile IP Signalling Octet Count (G15) 0
   Out-bound Mobile IP Signalling Octet Count (G16) 0
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   R-P Session ID (Y2) 3

 UDR for flow
    Mobile Node IP address 6.0.0.14

    IP Address (B1) 6.0.0.14,  Network Access Identifier (B2)
mwt10-sip-user1
    Correlation ID (C2) ' ' 40
    MIP Home Agent  (D1) 0.0.0.0
    IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
    Release Indicator (F13) 00
    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:1023906826
    Packets- in:0 out:0

PDSN-6500#
```

# show cdma pdsn accounting session

To display the accounting information for the session identified by the msid, and the acounting information for the flows tied to the session, use the **show cdma pdsn accounting session** command in privileged EXEC mode.

**show cdma pdsn accounting session** *msid*

**Syntax Description**

| | |
|---|---|
| *msid* | The ID number of the mobile subscriber. |

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

**Usage Guidelines**

The counter names appear in abbreviated format.

**Examples**

The following example shows output from the **show cdma pdsn accounting session** command:

```
PDSN-6500#show cdma pdsn accounting session 00000000004
 UDR for session
 session ID: 3
 Mobile Station ID IMSI 00000000004

    A - A1:00000000004
    C - ' 'C3:0
    D - D3:4.0.0.1 D4:000000000000
    E - E1:0000
    F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
    G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:241 G15:0 G16:0
    I - I1:0 I4:0
    Y - Y2:3

 UDR for flow
    Mobile Node IP address 6.0.0.14

    B - B1:6.0.0.14 B2:mwt10-sip-user1
    C - ' 'C2:40
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:0 G2:0 G4:1023906826
    Packets- in:0 out:0
PDSN-6500#
```

# show cdma pdsn accounting session detail

To display the accounting information (tith counter names) for the session identified by the msid, and the acounting information for the flows tied to the session, use the **show cdma pdsn accounting session detail** command in privileged EXEC mode.

**show cdma pdsn accounting session** *msid* **detail**

## Syntax Description

| | |
|---|---|
| *msid* | The ID number of the mobile subscriber. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

The counter names appear in abbreviated format.

## Examples

The following example shows output from the **show cdma pdsn accounting session** command:

```
PDSN-6500#sh cdma pdsn accounting session 00000000004 detail
 UDR for session
 session ID: 3
 Mobile Station ID IMSI 00000000004

   Mobile Station ID (A1) IMSI 00000000004
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 4.0.0.1 Base Station ID (D4) 000000000000
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 245  Forward Traffic Type (F6) 246
   Reverse Traffix type (F7) 247  Fundamental Frame size (F8) 248
   Forward Fundamental RC (F9) 249  Reverse Fundamntal RC (F10) 250
   DCCH Frame Format (F14) 0
   Bad PPP Frame Count (G3) 0 Active Time (G8) 0
   Number of Active Transitions (G9) 0
   SDB Octet Count Terminating (G10) 0
   SDB Octet Count Originating (G11) 0
   Number of SDBs Terminating (G12) 0
   Number of SDBs Originating G13 0
   Number of HDLC Layer Bytes Received (G14) 241
   In-Bound Mobile IP Signalling Octet Count (G15) 0
   Out-bound Mobile IP Signalling Octet Count (G16) 0
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   R-P Session ID (Y2) 3
```

```
 UDR for flow
    Mobile Node IP address 6.0.0.14

    IP Address (B1) 6.0.0.14,  Network Access Identifier (B2)
mwt10-sip-user1
    Correlation ID (C2) ' ' 40
    MIP Home Agent  (D1) 0.0.0.0
    IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
    Release Indicator (F13) 00
    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:1023906826
    Packets- in:0 out:0

PDSN-6500#
```

# show cdma pdsn accounting session flow

To display the accounting information for a specific flow that is associated with the session identified by the msid, use the **show cdma pdsn accounting session flow** command in privileged EXEC mode.

**show cdma pdsn accounting session** *msid* **flow** { **mn-ip-address** *IP_address* }

## Syntax Description

| | |
|---|---|
| *msid* | The ID number of the mobile subscriber. |
| **mn-ip-address** *ip_address* | Specifies the IP addresses assigned to the mobile numbers in each session. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

The counter names appear in abbreviated format.

## Examples

The following example shows output from the **show cdma pdsn accounting session flow** command:

```
PDSN-6500#show cdma pdsn accounting session 00000000004 flow
mn-ip-address 6.0.0.14
 UDR for flow
    Mobile Node IP address 6.0.0.14

    B - B1:6.0.0.14 B2:mwt10-sip-user1
    C - ' 'C2:40
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:0 G2:0 G4:1023906826
    Packets- in:0 out:0

PDSN-6500#
```

# show cdma pdsn accounting session flow user

To display accounting information for a flow with username that is associated with the session identified by the msid, use the **show cdma pdsn accounting session flow user** command in privileged EXEC mode.

**show cdma pdsn accounting session** *msid* **flow user** *username*

## Syntax Description

| | |
|---|---|
| *username* | The username that is associated with the session identified by the msid. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn accounting session flow user** command:

```
PDSN-6500#show cdma pdsn accounting session 123451234512357 flow user
mwts-mip-p1-user121@ispxyz.com

 UDR for flow
    Mobile Node IP address 15.0.0.3

    B - B1:15.0.0.3 B2:mwts-mip-p1-user121@ispxyz.com
    C - ' 'C2:36
    D - D1:0.0.0.0
    F - F11:02 F12:01 F13:00
    G - G1:0 G2:0 G4:1023906326
    Packets- in:0 out:0

PDSN-6500#
```

# show cdma pdsn ahdlc

To display AHDLC engine information, use the **show cdma pdsn ahdlc** command in privileged EXEC mode.

**show cdma pdsn ahdlc** *slot_number* **channel** [*channel_id*]

## Syntax Description

| | |
|---|---|
| *slot_number* | Slot number of the AHDLC of interest. |
| **channel** [*channel_id*] | Channel on the AHDLC. Possible values are 0 through 8000, or 0 to 20000 depending on the image you are using. If no channel is specified, information for all channels is displayed. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |
| 12.2(8)BY | The possible values for channel ID were extended to 20000. |

## Examples

The following example shows output from the **show cdma pdsn ahdlc** command:

```
Router# show cdma pdsn ahdlc 0 channel
 Ch id  State   Framing ACCM            Deframing ACCM  FCS size
 12     OPENED  00000000                 00000000           16
 13     OPENED  00000000                 00000000           16
 14     OPENED  00000000                 00000000           16

Router# show cdma pdsn ahdlc 0 channel 12
 Channel id = 12 State = OPENED Framing ACCM = 00000000
Deframing ACCM = 00000000 FCS size = 16
 Framing input 153 bytes 7 paks
 Framing output 242 bytes 7 paks 0 errors
 Deframing input 181 bytes 9 paks
 Deframing output 121 bytes 5 paks 0 errors
 0 Bad FCS 0 Escaped end
```

# show cdma pdsn cluster controller

To display configuration and statistics for the PDSN cluster controller, use the **show cdma pdsn cluster controller** command in privileged EXEC mode.

**show cdma pdsn cluster controller** {**configuration | statistics** }

## Syntax Description

| | |
|---|---|
| **configuration** | Displays configuration information associated with the cluster controller. |
| **statistics** | Displays various statistics collected on the cluster controller signaling messages with the cluster member, and redundancy message statistics with the redundancy peer. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn cluster controller** command:

```
Router# show cdma pdsn cluster controller
```

# show cdma pdsn cluster controller configuration

To display the IP addresses of the members that registered with a specific controller, use the **show cdma pdsn cluster controller configuration** command in privileged EXEC mode.

**show cdma pdsn cluster controller configuration**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn cluster controller configuration** command:

```
Router# show cdma pdsn cluster controller configuration
sh cdma pdsn cluster controller config
cluster interface FastEthernet0/0
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)
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
  group: sit_cluster1
```

# show cdma pdsn cluster controller member

To display detailed information about a specific cluster controller member, use the **show cdma pdsn cluster controller member** command in privileged EXEC mode.

**show cdma pdsn cluster controller member** { **load** | **time** | *ipaddr*}

## Syntax Description

| | |
|---|---|
| **load** | The load reported by every PDSN member in the cluster, sorted from the lowest load value. |
| **time** | The seek time of the member, sorted from the past to the future. |
| *ipaddr* | Specifies the controller member. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn cluster controller member** command:

```
Router# show cdma pdsn cluster controller member
 Ch id  State   Framing ACCM            Deframing ACCM  FCS size
 12     OPENED  00000000                 00000000           16
 13     OPENED  00000000                 00000000           16
 14     OPENED  00000000                 00000000           16

Router# show cdma pdsn ahdlc 0 channel 12
 Channel id = 12 State = OPENED Framing ACCM = 00000000
Deframing ACCM = 00000000 FCS size = 16
 Framing input 153 bytes 7 paks
 Framing output 242 bytes 7 paks 0 errors
 Deframing input 181 bytes 9 paks
 Deframing output 121 bytes 5 paks 0 errors
 0 Bad FCS 0 Escaped end
```

# show cdma pdsn cluster controller session

To display session count, or count by age, or one or a few oldest session records, or a session records corresponding to the IMSI entered and a few session records that arrived afterwards, use the **show cdma pdsn cluster controller session** command in privileged EXEC mode.

**show cdma pdsn cluster controller session** { **count** [**age** *days*] | **oldest** [**more** *1-20 records*] | **imsi** *BCDs* [**more** *1-20 records*] }

## Syntax Description

| | |
|---|---|
| **count** | The number of session records on cluster controller. |
| **age** | The number of session records of this age on the cluster controller. Age measured in days. |
| **oldest** | The oldest session record on the cluster controller. |
| **more** *1-20 records* | Displays the configured number (from 1 to 20) of the oldest session records on the cluster controller. |
| **imsi** *BCDs* | Displays the session record with this imsi on the cluster controller. |
| **more** *1-20 records* | Displays the configured number (from 1 to 20) of additional session records on the cluster controller. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn cluster controller session** command:

```
Router# show cdma pdsn clu contr session imsi 00000000007

    IMSI   Member IPv4 Addr   Age [days]   Anchor changes
-----------------------------------------------------------------
00000000007          10.0.0.50
-----------------------------------------------------------------

Router# show cdma pdsn clu contr session count
        10 session records

Router# show cdma pdsn clu contr session oldest
    IMSI   Member IPv4 Addr   Age [days]   Anchor changes
-----------------------------------------------------------------
00000000002          10.0.0.50
-----------------------------------------------------------------
```

# show cdma pdsn cluster controller statistics

To display the IP addresses of the members that registered with a specific controller, use the **show cdma pdsn cluster controller statistics** command in privileged EXEC mode.

**show cdma pdsn cluster controller statistics**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn controller statistics** command:

```
Router# show cdma pdsn cluster controller statistics
0 times did not get a buffer for a packet
         0 times couldn't allocate memory
       744 A11-RegReply received
         0 A11-RegReply discarded, authenticaton problem
         0 A11-RegReply discarded, identification problem
         0 A11-RegReply discarded, unrecognized extension
       975 A11-RegRequest received
         0 A11-RegRequest discarded, authenticaton problem
         0 A11-RegRequest discarded, identification problem
         0 A11-RegRequest discarded, unrecognized application type
         0 A11-RegRequest discarded, unrecognized extension
         0 A11-RegRequest with unrecognized type of data
         0 A11-RegRequest not sent, interface cdma-Ix not configed
       744 CVSEs seek reply received
       755 CVSEs seek received
         4 CVSEs state ready received
         4 CVSEs state admin prohibited received
         0 msgs received neither A11-RegReq nor A11-RegReply
       116 A10 up A11-RegReq received
        96 A10 end A11-RegReq received
         2 PDSN cluster members
redundancy:
    error: mismatch id 0 authen fail 0
           ignore due to no redundancy 0
    Update rcvd 0 sent 1481 orig sent 1300 fail 4
    UpdateAck rcvd 1466 sent 0
    DownloadReq rcvd 1 sent 4 orig sent 2 fail 0
    DownloadReply rcvd 4 sent 2 orig sent 2 fail 0 drop 0
    DownloadAck rcvd 2 sent 4 drop 0
mwt13-6500c#
```

# show cdma pdsn cluster member

To display configuration and statistics for the PDSN cluster member, use the **show cdma pdsn cluster member** command in privileged EXEC mode.

**show cdma pdsn cluster member** {**configuration | statistics**}

## Syntax Description

| | |
|---|---|
| **configuration** | Displays configuration information associated with the cluster member. |
| **statistics** | Displays various statistics collected on cluster member signaling messages with the cluster controller. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn cluster member** command:

```
Router# show cdma pdsn cluster member
```

# show cdma pdsn flow

To display flow-based summary of active sessions, and the flows and IP addresses assigned to the mobile numbers in each session, use the **show cdma pdsn flow** command in privileged EXEC mode.

**show cdma pdsn flow {mn-ip-address** *ip_address* | **msid** *string* | **service-type** | **user** *string*}

## Syntax Description

| | |
|---|---|
| **mn- ip-address** *ip_address* | Specifies the IP addresses assigned to the mobile numbers in each session. |
| **msid** *string* | Specifies the mobile subscriber id number. |
| **service-type** | Specifies the service type. |
| **user** *string* | Specifies the user. |

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following example shows output from the **show cdma pdsn flow** command:

```
Router# show cdma pdsn flow

MSID            NAI                                Type         MN IP Address    St
100000000000099 sim1                               Simple       100.4.1.1        ACT
200000000000047 sim1                               Simple       100.4.1.2        ACT
100000000000100 sim1                               Simple       100.4.1.40       ACT
200000000000048 sim1                               Simple       100.4.1.3        ACT
100000000000101 sim1                               Simple       100.4.1.5        ACT
200000000000049 sim1                               Simple       100.4.1.4        ACT
100000000000102 sim1                               Simple       100.4.1.6        ACT
200000000000050 sim1                               Simple       100.4.1.7        ACT
100000000000103 sim1                               Simple       100.4.1.9        ACT
200000000000051 sim1                               Simple       100.4.1.8        ACT
100000000000104 sim1                               Simple       100.4.1.11       ACT
200000000000052 sim1                               Simple       100.4.1.10       ACT
100000000000105 sim1                               Simple       100.4.1.12       ACT
200000000000053 sim1                               Simple       100.4.1.13       ACT
300000000000008 sim1                               Simple       100.4.1.14       ACT
100000000000106 sim1                               Simple       100.4.1.15       ACT
200000000000054 sim1                               Simple       100.4.1.16       ACT
300000000000009 sim1                               Simple       100.4.1.17       ACT
100000000000107 sim1                               Simple       100.4.1.19       ACT
200000000000055 sim1                               Simple       100.4.1.18       ACT
100000000000122 sim1                               Simple       100.4.1.21       ACT
200000000000070 sim1                               Simple       100.4.1.20       ACT
300000000000025 sim1                               Simple       100.4.1.22       ACT
100000000000123 sim1                               Simple       100.4.1.24       ACT
```

```
200000000000071 sim1                    Simple      100.4.1.23      ACT
300000000000026 sim1                    Simple      100.4.1.25      ACT
100000000000124 sim1                    Simple      100.4.1.26      ACT
200000000000072 sim1                    Simple      100.4.1.27      ACT
300000000000027 sim1                    Simple      100.4.1.28      ACT
100000000000125 sim1                    Simple      100.4.1.29      ACT
200000000000073 sim1                    Simple      100.4.1.30      ACT
300000000000028 sim1                    Simple      100.4.1.31      ACT
100000000000126 sim1                    Simple      100.4.1.33      ACT
200000000000074 sim1                    Simple      100.4.1.32      ACT
300000000000029 sim1                    Simple      100.4.1.34      ACT
100000000000127 sim1                    Simple      100.4.1.36      ACT
200000000000075 sim1                    Simple      100.4.1.35      ACT
300000000000030 sim1                    Simple      100.4.1.37      ACT
100000000000128 sim1                    Simple      100.4.1.39      ACT
200000000000076 sim1                    Simple      100.4.1.38      ACT
300000000000101 sim1                    Simple      100.4.1.41      ACT
100000000000199 sim1                    Simple      100.4.1.43      ACT
200000000000147 sim1                    Simple      100.4.1.42      ACT
300000000000102 sim1                    Simple      100.4.1.44      ACT
100000000000200 sim1                    Simple      100.4.1.46      ACT
 --More--
```

# show cdma pdsn pcf

To display information about PCFs that have R-P tunnels to the PDSN, use the **show cdma pdsn pcf** command in privileged EXEC mode.

**show cdma pdsn pcf** {**brief** | *ip_addr* | **secure**}

## Syntax Description

| | |
|---|---|
| **brief** | Displays information about all PCFs with connected sessions. |
| *ip_addr* | Displays detailed PCF information by IP address. |
| **secure** | Displays the security associations for all PCFs on this PDSN. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(2)XC | The parameters of this command were changed. |

## Examples

The following example shows output of the **show cdma pdsn pcf** command with the keyword **brief** specified, with an IP address specified, and with the keyword **secure** specified:

```
router# show cdma pdsn pcf brief
PCF IP Address     Sessions      Pkts In     Pkts Out     Bytes In    Bytes Out
4.0.0.1                   1           14          275           23          936
```

Table 9 describes the fields shown in the output of the brief version of the command.

***Table 9 show cdma pdsn pcf brief Field Descriptions***

| Field | Description |
|---|---|
| PCF IP Address | IP address of the PCF. |
| Sessions | Number of active sessions. |
| Pkts In | Total packets received from a PCF. |
| Pkts Out | Total packets sent to a PCF. |
| Bytes In | Total bytes received from a PCF. |
| Bytes Out | Total bytes sent to a PCF. |

```
router# show cdma pdsn pcf 4.0.0.1
PCF 4.0.0.1 has 1 session
  Received 14 pkts (275 bytes), sent 23 pkts (936 bytes)
```

```
PCF Session ID 1, Mobile Station ID MIN 2000000001
  A10 connection age 00:00:28
  A10 registration lifetime 65535 sec, time since last registration 28 sec
```

Table 10 describes the fields shown in the output of the command when an IP address is specified.

***Table 10 show cdma pdsn pcf Field Descriptions***

| Field | Description |
|---|---|
| PCF (*x.x.x.x*) has *x* session | PCF address and the number of active sessions. |
| received *x* pkts (*x* bytes) | Total packets received from a PCF. |
| sent *x* pkts (*x* bytes) | Total packets sent to a PCF. |
| PCF Session ID *x* | Session ID associated with the PCF. |
| Mobile Station ID MIN *xxxx* | MIN of the mobile station initiating the session. |
| status | Status of the IMSI session. |
| A10 connection age | Amount of time the connection has been active. |
| A10 registration lifetime | Duration for which the A10 registration will be active. |

```
Router# show cdma pdsn pcf secure
Security Associations (algorithm, replay protection, key):
default:
 spi 300, Timestamp +/- 60, key ascii foo
4.0.0.1:
 spi 100, Timestamp +/- 60, key ascii test
 spi 200, Timestamp +/- 60, key ascii foo
4.0.0.2:
 spi 100, Timestamp +/- 0, key ascii test
 spi 400, Timestamp +/- 0, key hex 12345678901234567890123456789012
4.0.0.3:
 spi inbound 100 outbound 200, Timestamp +/- 0, key ascii test
```

Table 11 describes the fields shown in the output of the command when the keyword **secure** is specified.

***Table 11 show cdma pdsn pcf secure Field Descriptions***

| Field | Description |
|---|---|
| default | The default security associations (used for PCFs that do not have an explicitly configured security association). |
| *x.x.x.x* | IP address of the PCF |
| spi *spi_value* | Security Parameter Index, a 4-byte hex index within the security association that selects the specific security parameters to be used. |
| Timestamp +/- *value* | Maximum difference allowed between the timestamp received in the A11 message and the system time on the PDSN for the A11 message to be accepted. |
| key {ascii\|hex} *key* | The shared secret key for the security associations |

# show cdma pdsn resource

To display AHDLC resources allocated in resource manager, use the **show cdma pdsn resource** command in privileged EXEC mode.

**show cdma pdsn resource** [*slot_number* [**ahdlc-channel** [*channel_id*]]]

## Syntax Description

| | |
|---|---|
| *slot_number* | (Optional) Slot number of the AHDLC of interest. |
| **ahdlc-channel** [*channel_id*] | (Optional) Channel on the AHDLC. If no channel is specified, information for all channels is displayed. |

## Defaults

The c6500-c5 image supports 8000 sessions and the c6500-c6 image supports 20000 sessions.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |
| 12.2(8)BY | The possible values for channel ID was extended to 20000. |

## Examples

The following example shows output from the **show cdma pdsn resource** command:

```
Router# show cdma pdsn resource
Resource allocated/available in the resource manager

slot 0:
        AHDLC Engine Type:CDMA HDLC ENGINE
                  Engine is ENABLED
                 total channels:16000, available channels:16000


Router#show cdma pdsn resource 0 ahdlc-channel 0
        AHDLC Channel 0 State CLOSED
```

# show cdma pdsn selection

To display a summary of a session table entry or the entry by MSID, use the **show cdma pdsn selection** command in privileged EXEC mode.

**show cdma pdsn selection** {**summary** | **msid** *octet_stream*}

## Syntax Description

| | |
|---|---|
| **summary** | Displays a summary of the session table entry. |
| **msid** *number* | Keyword to indicate that the PDSN selection table entry for a particular MSID is to be displayed. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example shows output of the **show cdma pdsn selection** command with the **msid** specified:

```
router#show cdma pdsn selection msid 00000000400000
MSID=00000000400000 PDSN=51.4.1.40 (7206-PDSN-1)
```

The following example shows output of the **show cdma pdsn selection** command with **summary** specified:

```
Router#show cdma pdsn selection summary
CDMA PDSN selection summary
    Hostname         PDSN         Session-count     Max-sessions
   *7206-PDSN-1      51.4.1.40        0                 16000
    7206-PDSN-3      51.4.3.40        0                 16000
    7206-PDSN-2      51.4.2.40        0                 16000

    Hostname         Keepalive    Interface         Load-factor
   *7206-PDSN-1         10        70.4.1.40            0.00
    7206-PDSN-3         10        70.4.3.40            0.00
    7206-PDSN-2         10        70.4.2.40            0.00
```

# show cdma pdsn session

To display the session information on the PDSN, use the **show cdma pdsn session** command in privileged EXEC mode.

**show cdma pdsn session** [**brief** | **dormant** | **mn-ip-address** *address* | **msid** *number* | **user** *nai* | **prepaid**]

## Syntax Description

| | |
|---|---|
| **brief** | (Optional) Displays a summary of all sessions. |
| **dormant** | (Optional) Displays information about dormant PDSN sessions. |
| **mn-ip-address** *address* | (Optional) Displays user information for the specified IP address. |
| **msid** *number* | (Optional) Displays information for the specified MSID. |
| **user** *nai* | (Optional) Displays information for the specified NAI. |
| **prepaid** | (Optional) Displays information about prepaid flows. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(2)XC | The parameters of this command were altered. |
| 12.2(8)BY | The **prepaid** variable was introduced. |

## Examples

The following example shows output of the **show cdma pdsn session** command:

```
router# show cdma pdsn session
Mobile Station ID IMSI 111111111111111
  PCF IP Address 2.2.2.100, PCF Session ID 1
  A10 connection time 00:00:09,  registration lifetime 65535 sec
  Number of A11 re-registrations 0, time since last registration 9 sec
  Current Access network ID 0002-0202-64
  Last airlink record received is Active Start, airlink is active
  GRE sequence number transmit 8, receive 10
  Using interface Virtual-Access1, status ACT
  Using AHDLC Engine on slot 1, channel ID 2
  This session has 1 flow

Flow service Proxy-Mobile, NAI mwts-mipp-np-homeaddr@ispxyz.com
  Mobile Node IP address 30.0.0.2
  Home Agent IP address 7.0.0.2
  Packets in 0, bytes in 0
  Packets out 0, bytes out 0
  Prepaid duration 36000 secs, used 6500 secs, cumulative 13000 secs
```

# show cdma pdsn statistics

To display VPDN, PPP, and RP interface statistics for the PDSN, use the **show cdma pdsn selection** command in privileged EXEC mode.

**show cdma pdsn statistics [ rp | ppp | ahdlc** *0-6* **]**

## Syntax Description

| | |
|---|---|
| **rp** | Displays all RP interface statistics. |
| **ppp** | Displays all PPP interface statistics |
| **ahdlc** *0-6* | Displays all AHDLC statistics. where the range <0-6> is engine slot-id and an optional parameter. In the absence of the optional parameter, the statistics for all the engines will get displayed. The output of this command with the new option is the framing/defarming statistics of the engine. |

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example shows output of the **show cdma pdsn statistics** command:

```
router# show cdma pdsn statistics
RP Interface:
    Reg Request rcvd 23, accepted 22, denied 1, discarded 0
    Initial Reg Request accepted 4, denied 0
    Re-registration requests accepted 14, denied 0
    De-registration accepted 4, denied 0
    Error: Unspecified 23, Administratively prohibited 0
      Resource unavailable 4, Authentication failed 4
      Identification mismatch 2, Poorly formed requests 2
      Unknown PDSN 2, Reverse tunnel mandatory 22
      Reverse tunnel unavailable 1, Bad CVSE 0

    Update sent 2, accepted 2, denied 0, not acked 0
    Initial Update sent 2, retransmissions 0
    Acknowledge received 2, discarded 0
    Update reason lifetime expiry 1, PPP termination 0, other 1
    Error: Unspecified 23 Administratively prohibited 0
      Authentication failed 4, Identification mismatch 4
      Poorly formed request 2

PPP:
    Current Connections 0
    Connection requests 4, success 4, failure 0
    Failure reason LCP 0, authentication 0, IPCP 3
    Connection enters stage LCP 4, Auth 4, IPCP 7
```

```
    Renegotiation total 0, by PDSN 0, by Mobile Node 0
    Renegotiation reason LCP/IPCP 0, address mismatch 0, other 0

    CHAP attempt 4, success 4, failure 0
    PAP attempt 0, success 0, failure 0
    MSCHAP attempt 0, success 0, failure 0
    EAP attempt 0, success 0, failure 0
    Release total 4, by PDSN 4, by Mobile Node 0
    Release by ingress address filtering 0
    Release reason: administrative 1, LCP termination 0, idle timeout 0
      L2TP tunnel NOT READY YET
      insufficient resources 0, session timeout 0
      service unavailable 0, other 0

    Connection negotiated compression 0
    Compression Microsoft 0, Stack 0, other 0
    Connections negotiated MRRU 0, IPX 0, IP 4
    Connections negotiated VJ-Compression 0, BAP 0
    PPP bundles 0

VPDN Flows:
  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 5 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCFs limit not set
  Maximum sessions limit not set (default 20000 maximum)
  SNMP failure history table size 100
  MSID Authentication is disabled
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is disabled
  Aging of idle users disabled

  Number of pcfs connected 1
  Number of sessions connected 29,
    Simple IP flows 10, Mobile IP flows 9,
    Proxy Mobile IP flows 0, VPDN flows 10

AHDLC:

PDSN#show cdma pdsn statistics ahdlc
slot 0:
  AHDLC Engine Type: CDMA HDLC SW ENGINE
     Engine is ENABLED
    total channels: 8000, available channels: 8000

  Framing input 0 bytes, 0 paks
  Framing output 0 bytes, 0 paks
  Framing errors 0, insufficient memory 0,
        queue overflow 0, invalid size 0

  Deframing input 0 bytes, 0 paks
  Defaming output 0 bytes, 0 paks
  Deframing errors 0, insufficient memory 0,
        queue overflow 0, invalid size 0, CRC errors 0
```

# show ip mobile binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

**show ip mobile binding** [**home-agent** *address* | **nai** *string* | **summary**]

## Syntax Description

| | |
|---|---|
| **home-agent** *address* | (Optional) IP address of mobile node. |
| **nai** *string* | (Optional) Network access identifier. |
| **summary** | (Optional) Total number of bindings in the table. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.0(2)T | The following keyword and argument were added:<br>• **home-agent**<br>• *address* |
| 12.1(2)T | The **summary** keyword was added. |
| 12.2(2)XC | The **nai** keyword was added. |

## Usage Guidelines

The home agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

## Examples

The following is sample output from the **show ip mobile binding** command:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
20.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Table 12 describes the significant fields shown in the display.

***Table 12 show ip mobile binding Field Descriptions***

| Field | Description |
|---|---|
| Total | Total number of mobility bindings. |
| *IP address* | Home IP address of the mobile node. |

*Table 12 show ip mobile binding Field Descriptions*

| Field | Description |
|---|---|
| Care-of Addr | Care-of address of the mobile node. |
| Src Addr | IP source address of the Registration Request as received by the home agent. Will be either the collocated care-of address of a mobile node or an address of the foreign agent. |
| Lifetime granted | The lifetime granted to the mobile node for this registration. Number of seconds in parentheses. |
| Lifetime remaining | The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the home agent. |
| Flags | Registration flags sent by mobile node. Uppercase characters denote bit set. |
| Identification | Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request, and replay protection. |
| Tunnel | The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field. |
| Routing Options | Routing options list all home agent-accepted services. For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the home agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel). |

# show ip mobile host

To display mobile station counters and information, use the **show ip mobile host** EXEC command.

**show ip mobile host** [*address* | **interface** *interface* | **network** *address* | **nai** *string* | **group** [**nai** *string*] | **summary**]

## Syntax Description

| | |
|---|---|
| *address* | (Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed. |
| **interface** *interface* | (Optional) Displays all mobile nodes whose home network is on this interface. |
| **network** *address* | (Optional) Displays all mobile nodes residing on this network or virtual network. |
| **nai** *string* | (Optional) Network access identifier. |
| **group** | (Optional) Displays all mobile node groups configured using the **ip mobile host** command. |
| **summary** | (Optional) Displays all values in the table. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword was added. |

## Examples

The following is sample output from the **show ip mobile host** command:

```
Router# show ip mobile host

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
```

Table 13 describes the significant fields shown in the display.

*Table 13 show ip mobile host Field Descriptions*

| Field | Description |
|---|---|
| *IP address* | Home IP address of the mobile node. |
| Allowed lifetime | Allowed lifetime of the mobile node. By default, it is set to the global lifetime (**ip mobile home-agent lifetime** command). Setting this lifetime will override global value. |
| Roaming status | When the mobile node is registered, the roaming status is - Registered - ; otherwise, it is - Unregistered -. Use the **show ip mobile binding** command for more information when the user is registered. |
| Home link | Interface or virtual network. |
| Accepted | Total number of service requests for the mobile node accepted by the home agent (Code 0 + Code 1). |
| Last time | The time at which the most recent Registration Request was accepted by the home agent for this mobile node. |
| Overall service time | Overall service time that has accumulated for the mobile node since the home agent last rebooted. |
| Denied | Total number of service requests for the mobile node denied by the home agent (sum of all registrations denied with Code 128 through Code 159). |
| Last time | The time at which the most recent Registration Request was denied by the home agent for this mobile node. |
| Last code | The code indicating the reason why the most recent Registration Request for this mobile node was rejected by the home agent. |
| Total violations | Total number of security violations. |
| Tunnel to mobile station | Number of packets and bytes tunneled to mobile node. |
| Reverse tunnel from mobile station | Number of packets and bytes reverse tunneled from mobile node. |

The following is sample output from the **show ip mobile host group** command for groups configured with the **ip mobile host** command:

```
Router# show ip mobile host group

20.0.0.1 - 20.0.0.20:
    Home link on virtual network 20.0.0.0 /8, Care-of ACL -none-
    Security associations on router, Allowed lifetime 10:00:00 (36000/default)
```

Table 14 describes the significant fields shown in the display.

*Table 14 show ip mobile host group Field Descriptions*

| Field | Description |
|---|---|
| *IP address* | Mobile host IP address or grouping of addresses. |
| Home link | Interface or virtual network. |
| Care-of ACL | Care-of address access list. |

*Table 14 show ip mobile host group Field Descriptions (continued)*

| Field | Description |
|---|---|
| Security association | Router or AAA server. |
| Allowed lifetime | Allowed lifetime for mobile host or group. |

## Related Commands

| Command | Description |
|---|---|
| **show ip mobile binding** | Displays the mobility binding table. |
| **clear ip mobile host-counters** | Clears the mobile station-specific counters. |

# show ip mobile proxy

To display information about a proxy Mobile IP host, use the **show ip mobile proxy** EXEC command.

**show ip mobile proxy** [**host** [**nai** *string*] | **registration** | **traffic**]

## Syntax Description

| | |
|---|---|
| **host** | (Optional) Displays information about the proxy host. |
| **nai** *string* | (Optional) Network access identifier. |
| **registration** | (Optional) Displays proxy registration information. |
| **traffic** | (Optional) Displays proxy traffic information. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Usage Guidelines

None.

## Examples

The following is sample output from the **show ip mobile proxy host** command:

```
Router# show ip mobile proxy host
Proxy Host List:

MoIPProxy1@cisco.com:
    Home Agent Address 3.3.3.1
    Lifetime 6000
    Flags :sBdmgvt
```

# show ip mobile secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, home agent, or proxy Mobile IP host use the **show ip mobile secure** EXEC command.

**show ip mobile secure** {**host** | **visitor** | **foreign-agent** | **home-agent** | **summary**} {*address* | **proxy-host** [**nai** *string*]}

## Syntax Description

| | |
|---|---|
| **host** | Displays security association of the mobile host on the home agent. |
| **visitor** | Displays security association of the mobile visitor on the foreign agent. |
| **foreign-agent** | Displays security association of the remote foreign agents on the home agent. |
| **home-agent** | Displays security association of the remote home agent on the foreign agent. |
| **summary** | Displays all values in the table. |
| *address* | IP address. |
| **proxy-host** | Displays security association of the proxy mobile user. |
| **nai** *string* | (Optional) Network access identifier. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** and **proxy-host** keywords were added. |

## Usage Guidelines

Multiple security associations can exist for each entity.

## Examples

The following is sample output from the **show ip mobile secure** command:

```
Router# show ip mobile secure

Security Associations (algorithm,mode,replay protection,key):
20.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 15 describes the significant fields shown in the display.

*Table 15 show ip mobile secure Field Descriptions*

| Field | Description |
|---|---|
| *IP address* | IP address. |
| In/Out SPI | The SPI is the 4-byte opaque index within the Mobility Security Association that selects the specific security parameters to be used to authenticate the peer. Allows either “SPI” or “In/Out SPI.” The latter specifies an inbound and outbound SPI pair. If an inbound SPI is received, then outbound SPI will be used when a response is sent. |
| MD5 | Message Digest 5 authentication algorithm. |
| Prefix-suffix | Authentication mode. |
| Timestamp | Replay protection method. |
| Key | The shared secret key for the security associations, in hexadecimal format. |

# show ip mobile traffic

To display Foreign Agent protocol counters, use the **show ip mobile traffic** EXEC command.

**show ip mobile traffic**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |

## Usage Guidelines

Counters can be reset to zero (0) using the **clear ip mobile traffic** command, which also allows you to undo the reset.

## Examples

The following is sample output from the **show ip mobile traffic** command:

```
Router# show ip mobile traffic

IP Mobility traffic:
Advertisements:
    Solicitations received 102
    Advertisements sent 13758, response to solicitation 102
Foreign Agent Registrations:
    Register requests rcvd 8580, valid 7243, forwarded 7243, denied 1009, ignored 328
    Register requests valid initial 7242, re-register 0, de-register 1
    Register requests forwarded initial 7242, re-register 0, de-register 1
    Register requests denied initial 1009, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0,  de-register 0
    Register replies rcvd 7242, forwarded 7234, bad 0, ignored 8
    Register replies rcvd initial 7241, re-register 0, de-register 1
    Register replies forwarded initial 7233, re-register 0, de-register 1
    Registration Errors:
      Unspecified 1005, HA unreachable 0
      Administrative prohibited 0, No resource 0
      Bad lifetime 0, Bad request form 0
      Unavailable encapsulation 0, Compression 0
      Unavailable reverse tunnel 0, Reverse tunnel mandatory 0
      Authentication failed MN 4, HA 0
      Received challenge/gen. authentication extension, feature not enabled 0
      Unknown challenge 1001, Missing challenge 0, Stale challenge 4
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
```

# show ip mobile violation

To display information about security violations, use the **show ip mobile violation** EXEC command.

**show ip mobile violation** [*address* | **nai** *string*]

## Syntax Description

| | |
|---|---|
| *address* | (Optional) Displays violations from a specific IP address. |
| **nai** *string* | (Optional) Network access identifier. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword and associated parameters were added. |

## Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the **logging** global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the **show logging** command.

## Examples

The following is sample output from the **show ip mobile violation** command:

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1:
    Violations: 1, Last time: 06/18/97 01:16:47
    SPI: 300, Identification: B751B581.77FD0E40
    Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

Table 16 describes significant fields shown in the display.

***Table 16 show ip mobile violation Field Descriptions***

| Field | Description |
|---|---|
| 20.0.0.1 | IP address of the violator. |
| Violations | Total number of security violations for this peer. |
| Last time | Time of the most recent security violation for this peer. |

*Table 16 show ip mobile violation Field Descriptions (continued)*

| Field | Description |
|---|---|
| SPI | SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the Mobile-Home Authentication Extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero. |
| Identification | Identification used in request or reply of the most recent security violation for this peer. |
| Error Code | Error code in request or reply. |
| Reason | Reason for the most recent security violation for this peer. Possible reasons are:<br>• No mobility security association<br>• Bad authenticator<br>• Bad identifier<br>• Bad SPI<br>• Missing security extension<br>• Other |

# show ip mobile visitor

To display the table containing the visitor list of the foreign agent, use the **show ip mobile visitor** EXEC command.

**show ip mobile visitor** [[**pending**] [*address* | **summary**] | **nai** *string*]

## Syntax Description

| | |
|---|---|
| **pending** | (Optional) Displays the pending registration table. |
| *address* | (Optional) IP address. |
| **summary** | (Optional) Displays all values in the table. |
| **nai** *string* | (Optional) Network access identifier. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(2)XC | The **nai** keyword was added. |

## Usage Guidelines

The foreign agent updates the table containing the visitor list of the foreign agent in response to registration events from mobile nodes.

## Examples

The following is sample output from the **show ip mobile visitor** command:

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
20.0.0.1:
    Interface Ethernet1/2, MAC addr 0060.837b.95ec
    IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
    HA addr 66.0.0.5, Identification B7510E60.64436B38
    Lifetime 08:20:00 (30000) Remaining 08:19:16
    Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
    Routing Options - (T)Reverse-tunnel
```

Table 17 describes the significant fields shown in the display.

***Table 17 show ip mobile visitor Field Descriptions***

| Field | Description |
|---|---|
| Total | 1 |
| *IP address* | Home IP address of a visitor. |
| Interface | Name of the interface. |
| MAC addr | MAC address of the visitor. |
| IP src | Source IP address the Registration Request of a visitor. |

*Table 17 show ip mobile visitor Field Descriptions (continued)*

| Field | Description |
|---|---|
| IP dest | Destination IP address of Registration Request of a visitor. When a foreign agent sends a reply to a visitor, the IP source address is set to this address, unless it is multicast or broadcast, in which case it is set to IP address of the output interface. |
| UDP src port | Source UDP port of Registration Request of the visitor. |
| HA addr | Home agent IP address for that visiting mobile node. |
| Identification | Identification used in that registration by the mobile node. |
| Lifetime | The lifetime granted to the mobile node for this registration. |
| Remaining | The number of seconds remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent. |
| Tunnel | The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field. |
| Routing Options | Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Possible options are:<br>• (S) Mult-binding<br>• (B) Broadcast<br>• (D) Direct-to-mobile station<br>• (M) MinIP<br>• (G) GRE<br>• (V) VJH-compress<br>• (T) Reverse-tunnel |

# show tech-support cdma pdsn

To display PDSN information that is useful to Cisco Customer Engineers for diagnosing problems, use the **show tech-support cdma pdsn** command in privileged EXEC mode.

**show tech support cdma pdsn**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was modified to include PDSN status. |

## Usage Guidelines

This command displays the output of several **show** commands. We recommend that you attach the output of this command whenever you submit a PDSN problem report.

## Examples

The following example shows typical output of the **show tech-support cdma pdsn** command:

```
pdsn-6500#show tech-support cdma pdsn

------------------ show version ------------------

Cisco Internetwork Operating System Software
IOS (tm) 6500 Software (C6500-C5IS-M), Experimental Version 12.2(20020306:074931)
[user-dw91527 104]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 06-Mar-02 22:21 by user
Image text-base:0x600088E0, data-base:0x6169A000

ROM:System Bootstrap, Version 12.0(19990210:195103) [12.0XE 105], DEVELOPMENT SOFTWARE
BOOTLDR:6500 Software (C6500-BOOT-M), Version 12.0(3)T,  RELEASE SOFTWARE (fc1)

mwt10-7206a uptime is 20 minutes
System returned to ROM by reload at 23:17:59 UTC Wed Mar 6 2002
System image file is "tftp://223.255.254.254/user/c6500-c5is-mz.dw91527"

cisco 7206VXR (NPE300) processor (revision D) with 229376K/65536K bytes of memory.
Processor board ID 21302179
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.1

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
```

```
8 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
125K bytes of non-volatile configuration memory.

8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0


------------------ show running-config ------------------


Building configuration...

Current configuration :3015 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
!
hostname mwt10-7206a
!
aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default group radius
aaa authentication ppp VPDN group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network VPDN group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 10
aaa accounting network pdsn start-stop group radius
aaa session-id common
enable secret 5 <removed>
enable password <removed>
!
username abc password 0 <removed>
ip subnet-zero
no ip gratuitous-arps
ip cef
ip cef accounting per-prefix non-recursive prefix-length
!
!
!
ip ftp source-interface Ethernet2/0
no ip domain-lookup
!
vpdn enable
vpdn authen-before-forward
virtual-profile aaa
!
!
!
!
```

```
!
!
!
interface Loopback0
 ip address 6.0.0.1 255.0.0.0
!
interface CDMA-Ix1
 ip address 5.0.0.1 255.0.0.0
 tunnel source 5.0.0.1
 tunnel key 0
 tunnel sequence-datagrams
!
interface FastEthernet1/0
 ip address 4.0.0.101 255.0.0.0
 duplex half
 speed auto
 no cdp enable
!
interface Ethernet2/0
 ip address 7.0.0.1 255.0.0.0
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 150.1.10.4 255.255.0.0
 duplex half
 no cdp enable
!
interface Ethernet2/2
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/4
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/5
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/6
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
```

```
 no cdp enable
!
interface Ethernet2/7
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface ATM4/0
 no ip address
 no ip mroute-cache
 shutdown
 no atm ilmi-keepalive
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip mobile foreign-service challenge
 ip mobile foreign-service reverse-tunnel
 ip mobile registration-lifetime 65535
 no peer default ip address
 ppp authentication chap pap optional
!
router mobile
!
ip local pool ispabc-pool1 9.0.0.1 9.0.0.255
ip classless
ip route 10.0.0.0 255.0.0.0 7.0.0.2
no ip http server
ip pim bidir-enable
ip mobile foreign-agent care-of Ethernet2/0
ip mobile proxy-host nai mwts-mipp-np-user1@ispxyz.com flags 42
!
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
!
!
radius-server host 150.1.0.1 auth-port 1645 acct-port 1646 key <removed>
radius-server retransmit 3
radius-server optional-passwords
radius-server key <removed>
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdlc-engine 5 usable-channels 8000
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn msid-authentication
cdma pdsn selection interface Ethernet2/0
cdma pdsn secure pcf default spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 1000 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
```

```
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password <removed>
!
!
end


------------------ show cdma pdsn ------------------


PDSN software version 1.2, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 300 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCFs limit not set, maximum sessions limit not set
  SNMP failure history table size 100
  MSID Authentication is enabled
      Network code digits for IMSI 5, MIN 6, IRM 4
      Profile Password is cisco
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is disabled
  Aging of idle users disabled

  Number of pcfs connected 1
  Number of sessions connected 1,
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 1


------------------ show ip interface brief ------------------


Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet1/0            4.0.0.101       YES NVRAM  up                    up
Ethernet2/0                7.0.0.1         YES manual up                    up
Ethernet2/1                150.1.10.4      YES NVRAM  up                    up
Ethernet2/2                unassigned      YES NVRAM  administratively down down
Ethernet2/3                unassigned      YES NVRAM  administratively down down
Ethernet2/4                unassigned      YES NVRAM  administratively down down
Ethernet2/5                unassigned      YES NVRAM  administratively down down
Ethernet2/6                unassigned      YES NVRAM  administratively down down
Ethernet2/7                unassigned      YES NVRAM  administratively down down
ATM4/0                     unassigned      YES NVRAM  administratively down down
Loopback0                  6.0.0.1         YES NVRAM  up                    up
CDMA-Ix1                   5.0.0.1         YES NVRAM  up                    up
Virtual-Template1          6.0.0.1         YES unset  down                  down
Virtual-Access1            unassigned      YES unset  up                    up
Mobile0                    unassigned      YES unset  up                    up
Tunnel0                    unassigned      YES unset  up                    up
Tunnel1                    7.0.0.1         YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
Virtual-Access3            unassigned      YES unset  up                    up
```

```
Virtual-Access3.1          6.0.0.1         YES unset  up                    up

------------------ show ip route ------------------


Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    4.0.0.0/8 is directly connected, FastEthernet1/0
C    5.0.0.0/8 is directly connected, CDMA-Ix1
C    6.0.0.0/8 is directly connected, Loopback0
C    7.0.0.0/8 is directly connected, Ethernet2/0
S    10.0.0.0/8 [1/0] via 7.0.0.2
C    150.1.0.0/16 is directly connected, Ethernet2/1
     30.0.0.0/32 is subnetted, 1 subnets
C       30.0.0.1 is directly connected, Virtual-Access3.1

------------------ show cdma pdsn session brief ------------------

MSID            PCF IP Address          PSI      Age  St Flows Interface
11122000050031  4.0.0.1                   1 00:19:57 ACT     1 Virtual-Access3.1


------------------ show cdma pdsn session ------------------


Mobile Station ID IMSI 11122000050031
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:19:57,  registration lifetime 1800 sec
  Number of A11 re-registrations 1, time since last registration 1193 sec
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE sequence number transmit 12, receive 12
  Using interface Virtual-Access3.1, status ACT
  Using AHDLC engine on slot 5, channel ID 0
  This session has 1 flow

  Flow service Proxy-Mobile, NAI mwts-mipp-np-user1@ispxyz.com
    Mobile Node IP address 30.0.0.1
    Home Agent IP address 7.0.0.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0


------------------ show cdma pdsn pcf brief ------------------

PCF IP Address     Sessions      Pkts In     Pkts Out     Bytes In    Bytes Out
4.0.0.1                   1            0           12            0          396


------------------ show cdma pdsn pcf ------------------


PCF 4.0.0.1 has 1 session
  Received 0 pkts (0 bytes), sent 12 pkts (396 bytes)

  PCF Session ID 1, Mobile Station ID IMSI 11122000050031
```

```
    A10 connection age 00:19:58
    A10 registration lifetime 1800 sec, time since last registration 1194 sec



------------------ show cdma pdsn selection summary ------------------


CDMA PDSN selection summary:
    Hostname         PDSN            Session-count  Max-sessions
   *mwt10-7206a      5.0.0.1             1              8000
    mwt10-7206b      12.0.0.1            0              8000

    Hostname         Keepalive    Interface       Load-factor
   *mwt10-7206a          30       7.0.0.1            0.00
    mwt10-7206b          30       7.0.0.2            0.00

------------------ show ip mobile traffic ------------------

IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0 , Dropped 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0, active HA 0
    Bad identification 0, Bad request form 0
    Unavailable encap 0, reverse tunnel 0
    Reverse tunnel mandatory 0
    Binding Updates received 0, sent 0 total 0 fail 0
    Binding Update acks received 0 sent 0
    Binding info requests received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Reverse tunnel mandatory 0
    Replies in 1
    Forwarded 0, Bad 0, Ignored 1
    Authentication failed MN 0, HA 0
    Received challenge/gen. authentication extension, feature not enabled 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Unknown challenge 0, Missing challenge 0, Stale challenge 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0

------------------ show ip mobile globals ------------------

IP Mobility global information:
```

```
Home Agent is not enabled

Foreign Agent

    Pending registrations expire after 15 secs
    Care-of addresses advertised
        Ethernet2/0 (7.0.0.1) - up

0 interfaces providing service
Encapsulations supported:IPIP and GRE
Tunnel fast switching enabled
Tunnel path MTU discovery aged out after 10 min

------------------ show ip mobile interface ------------------

IP Mobility interface information:

------------------ show vpdn tunnel ------------------



------------------ show cdma pdsn resource ------------------


Resource allocated/available in the resource manager

slot 0:
        AHDLC Engine Type:CDMA HDLC SW ENGINE
                 Engine is ENABLED
                total channels:16000, available channels:16000
```

# snmp-server enable traps cdma

To enable network management traps for CDMA, use the **snmp-server enable traps cdma** command in global configuration mode. To disable network management traps for CDMA, use the **no** form of this command.

**snmp-server enable traps cdma**

**no snmp-server enable traps cdma**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Network management traps disabled.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following example enables network management traps for CDMA:

```
snmp-server enable traps cdma
```

# snmp-server enable traps ipmobile

To configure Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the no form of this command.

**snmp-server enable traps ipmobile**

**no snmp-server enable traps ipmobile**

## Syntax Description

This command has no arguments or keywords.

## Defaults

SNMP notifications are disabled by default.

## Command Modes

Global Configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

## Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at

http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

## Examples

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

# Debug Commands

This section documents the **debug** commands specific to the PDSN feature. PDSN uses the Cisco CLI to support conditional debug messages that are based on existing IOS debug conditions. The conditional triggers that are supported for PDSN are **Username** and **Calling Party Number (MSID)**. Refer to the *Cisco IOS Debug Command Reference* for more information regarding conditional debug commands.

- **debug cdma pdsn a10 ahdlc**
- **debug cdma pdsn a10 gre**
- **debug cdma pdsn a10 ppp**
- **debug cdma pdsn a11**
- **debug cdma pdsn accounting**
- **debug cdma pdsn accounting flow**
- **debug cdma pdsn accounting time-of-day**
- **debug cdma pdsn cluster**
- **debug cdma pdsn prepaid**
- **debug cdma pdsn resource-manager**
- **debug cdma pdsn selection**
- **debug cdma pdsn service-selection**
- **debug cdma pdsn session**
- **debug ip mobile advertise**
- **debug ip mobile host**

# debug cdma pdsn a10 ahdlc

To display debug messages for AHDLC, use the **debug cdma pdsn a10 ahdlc** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn a10 ahdlc** [ **errors** | **events** ]

**no debug cdma pdsn a10 ahdlc** [ **errors** | **events** ]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays details of AHDLC packets in error. |
| **events** | (Optional) Displays AHDLC events. |

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |
| 12.2(8)BY | Keywords were made optional. |

## Examples

The following is sample output from the **debug cdma pdsn a10 ahdlc** command:

```
Router# debug cdma pdsn a10 ahdlc errors
ahdlc error packet display debugging is on
Router# debug cdma pdsn a10 ahdlc events
ahdlc events display debugging is on
Router#
*Jan  1 00:18:30:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:18:30:*****OPEN AHDLC*****
*Jan  1 00:18:30: ahdlc_mgr_channel_create
*Jan  1 00:18:30: ahdlc_mgr_allocate_available_channel:
*Jan  1 00:18:30:ahdlc:tell h/w open channel 9 from engine 0
```

# debug cdma pdsn a10 gre

To display debug messages for A10 GRE interface errors, events, and packets, use the **debug cdma pdsn a10 gre** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn a10 gre** [**errors** | **events** | **packets**] [**tunnel-key** *key*]

**no debug cdma pdsn a10 gre** [**errors** | **events** | **packets**]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays A10 GRE errors. |
| **events** | (Optional) Displays A10 GRE events. |
| **packets** | (Optional) Displays transmitted or received A10 GRE packets. |
| **tunnel-key** *key* | (Optional) Specifies the GRE key. |

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | The tunnel-key parameter was added and the existing keywords were made optional. |

## Examples

The following is sample output from the **debug cdma pdsn a10 gre events tunnel-key** command:

```
Router#debug cdma pdsn a10 gre events tunnel-key 1

Router#show debug
CDMA:
  CDMA PDSN A10 GRE events debugging is on for tunnel key 1

PDSN#
*Mar  1 04:00:57.847:CDMA-GRE:CDMA-Ix1 (GRE/CDMA) created with src 5.0.0.2 dst 0.0.0.0
*Mar  1 04:00:57.847:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:00:59.863:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:00:59.863:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:01.879:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:01.879:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:03.899:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:03.899:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
```

# debug cdma pdsn a10 ppp

To display debug messages for A10 PPP interface errors, events, and packets, use the **debug cdma pdsn a10 gre** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn a10 ppp** [**errors** | **events** | **packets**]

**no debug cdma pdsn a10 ppp** [**errors** | **events** | **packets**]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays A10 PPP errors. |
| **events** | (Optional) Displays A10 PPP events. |
| **packets** | (Optional) Displays transmitted or received A10 PPP packets. |

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | Keywords were made optional. |

## Examples

The following is sample output from the **debug cdma pdsn a10 ppp** command:

```
Router# debug cdma pdsn a10 ppp errors
CDMA PDSN A10 errors debugging is on

Router# debug cdma pdsn a10 ppp events
CDMA PDSN A10 events debugging is on

Router# debug cdma pdsn a10 ppp packets
CDMA PDSN A10 packet debugging is on

Router#show debug
*Jan  1 00:13:09:CDMA-PPP:create_va tunnel=CDMA-Ix1 virtual-template
template=Virtual-Template2 ip_enabled=1
*Jan  1 00:13:09:CDMA-PPP:create_va va=Virtual-Access1
*Jan  1 00:13:09:CDMA-PPP:clone va=Virtual-Access1 subif_state=1 hwidb->state=0
*Jan  1 00:13:09:          linestate=1 ppp_lineup=0
*Jan  1 00:13:09:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:13:09:CDMA-PPP:clone va=Virtual-Access1 subif_state=1 hwidb->state=4
*Jan  1 00:13:09:          linestate=0 ppp_lineup=0
*Jan  1 00:13:09:*****OPEN AHDLC*****
```

# debug cdma pdsn a11

To display debug messages for A11 interface errors, events, and packets, use the **debug cdma pdsn a11** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn a11** [**errors** | **events** | **packets ]** [*mnid*]

**no debug cdma pdsn a11** [**errors** | **events** | **packets** ]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays A11 protocol errors. |
| **events** | (Optional) Displays A11 events. |
| **packets** | (Optional) Displays transmitted or received packets. |
| *mnid* | (Optional) Specifies the mobile station's ID. |

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | The MNID parameter was added and the existing keywords were made optional. |

## Examples

The following is sample output from the **debug cdma pdsn a11**commands:

```
Router#debug cdma pdsn a11 errors
CDMA PDSN A11 errors debugging is on
Router#show debug
1d21h:CDMA-RP:(in) rp_msgs, code=1, status=0
1d21h:CDMA-RP:(enqueue req) type=1 homeagent=5.0.0.2 coaddr=4.0.0.1
1d21h:                   id=0xBEF750F0-0xBA53E0F lifetime=65535
1d21h:CDMA-RP:len=8, 00-00-00-00-00-00-00-F1 convert to 00000000000001
(14 digits), type=IMSI
1d21h:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
1d21h:               lifetime=65535 id=BEF750F0-BA53E0F
imsi=00000000000001
1d21h:CDMA-RP:(req) rp_req_create, 5.0.0.2-4.0.0.1-1 imsi=00000000000001
1d21h:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=65535
1d21h:CDMA-RP:(out) setup_rp_out_msg, ha=5.0.0.2 coa=4.0.0.1 key=1
1d21h:%LINK-3-UPDOWN:Interface Virtual-Access2000, changed state to up
1d21h:CDMA-RP:ipmobile_visitor add/delete=1, mn=8.0.2.132, ha=7.0.0.2
1d21h:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access2000,
changed state to up


Router#debug cdma pdsn a11 packets events

Router#show debug
CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001
  CDMA PDSN A11 events debugging is on for mnid 000000000000001
```

```
Router#
*Mar  1 03:15:32.507:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=32, len=20
*Mar  1 03:15:32.511:         00 00 01 00 EE 1F FC 43 0A 7D F9 36 29 C2 BA 28
*Mar  1 03:15:32.511:         5A 64 D5 9C
*Mar  1 03:15:32.511:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:15:32.511:               lifetime=1800 id=AF3BFE55-69A109D IMSI=000000000000001
*Mar  1 03:15:32.511:CDMA-RP:(req) rp_req_create, ha=5.0.0.2, coa=4.0.0.1, key=1
IMSI=000000000000001
*Mar  1 03:15:32.511:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=1800
*Mar  1 03:15:32.511:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1
*Mar  1 03:15:38.555:CDMA-RP:simple ip visitor added, mn=9.2.0.1, ha=0.0.0.0

Router#
*Mar  1 03:15:54.755:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:15:54.755:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:54.755:CDMA-RP:extension type=32, len=20
*Mar  1 03:15:54.755:         00 00 01 00 EA 9C C6 4C BA B9 F9 B6 DD C4 19 76
*Mar  1 03:15:54.755:         51 5A 56 45
*Mar  1 03:15:54.755:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:15:54.755:               lifetime=0 id=AF3BFE6B-4616E475 IMSI=000000000000001
*Mar  1 03:15:54.755:CDMA-RP:(req) rp_req_lifetime_zero 5.0.0.2-4.0.0.1-1
*Mar  1 03:15:54.755:               IMSI=000000000000001
*Mar  1 03:15:54.755:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=0
*Mar  1 03:15:54.755:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1


Router#debug cdma pdsn a11 event mnid 000000000000001

Router#show debug
CDMA:
  CDMA PDSN A11 events debugging is on for mnid 000000000000001

Router#
*Mar  1 03:09:34.339:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:09:34.339:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:09:34.339:               lifetime=1800 id=AF3BFCEE-DC9FC751
IMSI=000000000000001
*Mar  1 03:09:34.339:CDMA-RP:(req) rp_req_create, ha=5.0.0.2, coa=4.0.0.1, key=1
IMSI=000000000000001
*Mar  1 03:09:34.339:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=1800
*Mar  1 03:09:34.339:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1

*Mar  1 03:09:40.379:CDMA-RP:simple ip visitor added, mn=9.2.0.1, ha=0.0.0.0
Router#

close the session
Router#
*Mar  1 03:10:00.575:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:10:00.575:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:10:00.575:               lifetime=0 id=AF3BFD09-18040319 IMSI=000000000000001
*Mar  1 03:10:00.575:CDMA-RP:(req) rp_req_lifetime_zero 5.0.0.2-4.0.0.1-1
*Mar  1 03:10:00.575:               IMSI=000000000000001
*Mar  1 03:10:00.575:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=0
*Mar  1 03:10:00.575:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1
```

```
Router#debug cdma pdsn a11 packet mnid 000000000000001

Router#show debug
CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001

Router#
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=32, len=20
*Mar  1 03:13:37.803:         00 00 01 00 A8 5B 30 0D 4E 2B 83 FE 18 C6 9D C2
*Mar  1 03:13:37.803:         15 BF 5B 57

*Mar  1 03:13:51.575:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:51.575:CDMA-RP:extension type=32, len=20
*Mar  1 03:13:51.575:         00 00 01 00 58 77 E5 59 67 B5 62 15 17 52 83 6D
*Mar  1 03:13:51.579:         DC 0A B0 5B
```

# debug cdma pdsn accounting

To display debug messages for accounting events, use the **debug cdma pdsn accounting** command in privileged EXEC mode.

**debug cdma pdsn accounting**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn accounting** command:

```
Router# debug cdma pdsn accounting
CDMA PDSN accounting debugging is on
Router#
*Jan  1 00:15:32:CDMA/ACCT:null vaccess in session_start
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[44] len:[3] 01   Processing Y1
*Jan  1 00:15:32:CDMA/ACCT:    Setup airlink record received
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[41] len:[6] 00 00 00 02 CDMA/ACCT:
Processing Y2
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[42] len:[3] 12 CDMA/ACCT: Processing Y3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1F] len:[17] 30 30 30 30 30 30 30 30
30 30 30 30 30 30 32      Processing A1
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[9] len:[6] 04 04 04 05   Processing D3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[14]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[10] len:[8] 00 00 04 04 04 05
Processing D4
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[44] len:[3] 02   Processing Y1
*Jan  1 00:15:32:CDMA/ACCT:    Start airlink record received
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[41] len:[6] 00 00 00 02 CDMA/ACCT:
Processing Y2
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[42] len:[3] 13 CDMA/ACCT: Processing Y3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[10]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[11] len:[4] 00 02   Processing E1
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[10]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[12] len:[4] 00 F1   Processing F1
```

# debug cdma pdsn accounting flow

To display debug messages for accounting flow, use the **debug cdma pdsn accounting flow** command in privileged EXEC mode.

**debug cdma pdsn accounting flow**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.2(2)XC | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn accounting flow** command:

```
Router# debug cdma pdsn acc flow
CDMA PDSN flow based accounting debugging is on
pdsn-6500#
01:59:40:CDMA-SM:cdma_pdsn_flow_acct_upstream sess id 1 flow type 0 bytes 100 addr
20.20.20.1
01:59:40:CDMA-SM:cdma_pdsn_flow_acct_downstream sess id 1 flow type 0 bytes 100 addr
20.20.20.1
```

# debug cdma pdsn accounting time-of-day

To display the timer value, use the **debug cdma pdsn accounting time-of-day** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn accounting time-of-day**

**no debug cdma pdsn accounting time-of-day**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn accounting time-of-day** command:

```
Router# debug cdma pdsn accounting time-of-day
CDMA PDSN accounting time-of-day debugging is on

Feb 15 19:13:23.634:CDMA-TOD:Current timer expiring in 22 seconds
Feb 15 19:13:24.194:%SYS-5-CONFIG_I:Configured from console by console
Router#
Feb 15 19:13:45.635:CDMA-TOD:Timer expired...Rearming timer
Feb 15 19:13:45.635:CDMA-TOD:Gathering session info
Feb 15 19:13:45.635:CDMA-TOD:Found 0 sessions
```

# debug cdma pdsn cluster

To display the error messages, event messages s and packets received, use the **debug cdma pdsn cluster** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn cluster** {**message** [**error** | **events** | **packets** ] **redundancy** [ **error** | **events** | **packets** ]}

**no debug cdma pdsn cluster** {**message** [**error** | **events** | **packets** ] **redundancy** [ **error** | **events** | **packets** ]}

## Syntax Description

| | |
|---|---|
| **message** | Displays cluster messages for errors, events and packets received. |
| **redundancy** | Displays redundancy information for errors, events, and sent or received packets. |
| **error** | Displays either cluster or redundancy error messages. |
| **events** | Displays either all cluster or all redundancy events. |
| **packets** | Displays all transmitted or received cluster or redundancy packets. |

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Usage Guidelines

This debug is **only** allowed on c-6 images, and helps monitor the clustering information.

## Examples

The following is sample output from the **debug cdma pdsn cluster** command:

```
Router# debug cdma pdsn cluster ?
  message     Debug PDSN cluster controller messages
  redundancy  Debug PDSN cluster controller redundancy
```

# debug cdma pdsn prepaid

To display debug messages about prepaid flow, use the **debug cdma pdsn prepaid** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn prepaid**

**no debug cdma pdsn prepaid**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Usage Guidelines

This debug is **only** allowed on c6 images and help monitor the prepaid information.

## Examples

The following is sample output from the **debug cdma pdsn prepaid** command:

```
Router# debug cdma pdsn prepaid

*Mar  1 00:09:38.391: CDMA-PREPAID:  Initialized the authorization request
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added username into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added CLID into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added session id for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added correlation id into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added auth reason for prepaid into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added USER_ID for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added service id for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Built prepaid VSAs
*Mar  1 00:09:38.391: CDMA-PREPAID:   Sent the request to AAA
*Mar  1 00:09:38.391: CDMA-PREPAID:   Auth_reason: CRB_RSP_PEND_INITIAL_QUOTA
*Mar  1 00:09:38.395: CDMA-PREPAID:   Received prepaid response: status 2
*Mar  1 00:09:38.395: CDMA-PREPAID:   AAA authorised parms being processed
*Mar  1 00:09:38.395: CDMA-PREPAID:   Attr in Grp Prof: crb-entity-type
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: AAA_AT_CRB_ENTITY_TYPE
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: entity type returns 1
*Mar  1 00:09:38.395: CDMA-PREPAID:   Attr in Grp Prof: crb-duration
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: AAA_AT_CRB_DURATION
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: duration returns 120
*Mar  1 00:09:38.395: CDMA-PREPAID:   Retrieved attributes successfully
*Mar  1 00:09:38.395: CDMA-PREPAID:   Reset duration to 120, mn 9.3.0.1
*Mar  1 00:09:38.395: CDMA-PREPAID: : Started duration timer for 120 sec
```

# debug cdma pdsn resource-manager

To display debug messages that help you monitor the resource-manager information, use the **debug cdma pdsn resource-manager** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn resource-manager**

**no debug cdma pdsn resource-manager**

## Syntax Description

| | |
|---|---|
| **errors** | Displays pdsn resource manager errors. |
| **events** | Displays pdsn resource manager events. |

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.2(8)BY | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn resource-manager** command:

```
Router# debug cdma pdsn resource-manager ?
   errors  CDMA PDSN resource manager errors
   events  CDMA PDSN resource manager events
```

# debug cdma pdsn selection

To display debug messages for the intelligent PDSN selection feature, use the **debug cdma pdsn selection** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn selection** {**errors** | **events** | **packets**}

**no debug cdma pdsn selection** {**errors** | **events** | **packets**}

## Syntax Description

| | |
|---|---|
| **errors** | Displays pdsn selection errors. |
| **events** | Displays pdsn selection events. |
| **packets** | Displays transmitted or received packets. |

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn selection** command with the keyword **events** specified:

```
Router#debug cdma pdsn selection events
CDMA PDSN selection events debugging is on
Router#
00:27:46: CDMA-PSL: Message(IN) pdsn 51.4.2.40 interface 70.4.2.40
00:27:46:                Keepalive 10
00:27:46:                Count 0
00:27:46:                Capacity 16000
00:27:46:                Weight 0
00:27:46:                Hostname 11 7206-PDSN-2
00:27:46: CDMA-PSL: Reset keepalive, pdsn 51.4.2.40 current 10 new 10
00:27:46: CDMA-PSL: Message processed, pdsn 51.4.2.40 tsize 0 pendings 0
00:27:47: CDMA-PSL: Send KEEPALIVE, len 32
00:27:47: CDMA-PSL: Message(OUT) dest 224.0.0.11
00:27:47:                Keepalive 10
00:27:47:                Count 1
00:27:47:                Capacity 16000
00:27:47:                Weight 0
00:27:47:                Hostname 11 7206-PDSN-1
00:27:47: CDMA-PSL: RRQ sent, s=70.4.1.40 (FastEthernet0/1), d=224.0.0.11
```

# debug cdma pdsn service-selection

To display debug messages for service selection, use the **debug cdma pdsn service-selection** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn service-selection**

**no debug cdma pdsn service-selection**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |

## Examples

The following is sample output from the **debug cdma pdsn service-selection** command:

```
Router# debug cdma pdsn service-selection
CDMA PDSN service provisioning debugging is on
Router#
1d02h:%LINK-3-UPDOWN:Interface Virtual-Access3, changed state to up
1d02h:Vi3 CDMA-SP:user_class=1, ms_ipaddr_req=1, apply_acl=0
1d02h:Vi3 CDMA-SP:Adding simple ip flow, user=bsip, mn=6.0.0.2,
1d02h:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access3,
changed state to up
```

# debug cdma pdsn session

To display debug messages for Session Manager errors, events, and packets, use the **debug cdma pdsn session-manager** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn session [errors** | **events** ]

**no debug cdma pdsn session** [**errors** | **events** ]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays session protocol errors. |
| **events** | (Optional) Displays session events. |

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command History

| Release | Modification |
|---|---|
| 12.1(3)XS | This command was introduced. |
| 12.2(8)BY | Keywords were made optional. |

## Examples

The following is sample output from the **debug cdma pdsn session** command:

```
Router# debug cdma pdsn session events
CDMA PDSN session events debugging is on

Router# debug cdma pdsn session errors
CDMA PDSN session errors debugging is on

Router# show debug
CDMA:
  CDMA PDSN session events debugging is on
  CDMA PDSN session errors debugging is on
Router#
*Jan  1 00:22:27:CDMA-SM:create_session 5.5.5.5-4.4.4.5-2
*Jan  1 00:22:27:CDMA-SM:create_tunnel 5.5.5.5-4.4.4.5
*Jan  1 00:22:27:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:22:29:CDMA-SM:create_flow mn=0.0.0.0, ha=8.8.8.8 nai=l2tp2@cisco.com
*Jan  1 00:22:30:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access1, changed
state to up
```

# debug ip mobile advertise

Use the debug ip mobile advertise EXEC command to display advertisement information.

**debug ip mobile advertise**

**no debug ip mobile advertise**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default values.

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |

## Examples

The following is sample output from the **debug ip mobile advertise** command. Table 18 describes significant fields shown in the display.

```
Router# debug ip mobile advertise

MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8 )
```

*Table 18 Debug IP Mobile Advertise Field Descriptions*

| Field | Description |
|---|---|
| type | Type of advertisement. |
| len | Length of extension in bytes. |
| seq | Sequence number of this advertisement. |
| lifetime | Lifetime in seconds. |
| flags | Capital letters represent bits that are set, lower case letters represent unset bits. |
| Care-of address | IP address. |
| Prefix Length ext | Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection. |

# debug ip mobile host

Use the debug ip mobile host EXEC command to display IP mobility events.

**debug ip mobile host** *acl*

**no debug ip mobile host**

**Syntax Description**

| | |
|---|---|
| *acl* | (Optional) Access list. |

**Defaults**

No default values.

**Command History**

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |

**Examples**

The following is sample output from the debug ip mobile host command:

```
Router# debug ip mobile host

MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA
68.0.0.31 HA 66.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6

MobileIP: HA sent reply to MN 20.0.0.6
```

# Glossary

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 DivisionMultiple 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 System 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

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

PDN—Packet Data Network

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—Route Processor

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