



## **Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference**

July 2008

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

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

*Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*  
© 2008 Cisco Systems, Inc. All rights reserved.



# About Cisco IOS and Cisco IOS XE Software Documentation

---

**Last updated: August 6, 2008**

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

## Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

## Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

# Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

## Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
<b>^</b> or <b>Ctrl</b>	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

## Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y   z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

## Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
<b>Bold Courier font</b>	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

## Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



### Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

## Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

## Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

## Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

### New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

### Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

### Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

### Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/all\\_release/all\\_mcl.html](http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html).

### Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

## Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i> <i>Cisco IOS XE AppleTalk Configuration Guide</i> <i>Cisco IOS AppleTalk Command Reference</i>	AppleTalk protocol.
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i> <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging Command Reference</i> <i>Cisco IOS IBM Networking Command Reference</i>	<ul style="list-style-type: none"> <li>Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</li> <li>Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</li> </ul>
<i>Cisco IOS Broadband and DSL Configuration Guide</i> <i>Cisco IOS XE Broadband and DSL Configuration Guide</i> <i>Cisco IOS Broadband and DSL Command Reference</i>	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<i>Cisco IOS Carrier Ethernet Configuration Guide</i> <i>Cisco IOS Carrier Ethernet Command Reference</i>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<i>Cisco IOS DECnet Configuration Guide</i> <i>Cisco IOS XE DECnet Configuration Guide</i> <i>Cisco IOS DECnet Command Reference</i>	DECnet protocol.
<i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS XE Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
<i>Cisco IOS Flexible NetFlow Configuration Guide</i> <i>Cisco IOS Flexible NetFlow Command Reference</i>	Flexible NetFlow.



**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Service Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Service Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: <a href="http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html">http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html</a>
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

**Table 1** Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS Multiprotocol Label Switching Command Reference</i>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<i>Cisco IOS Multi-Topology Routing Configuration Guide</i> <i>Cisco IOS Multi-Topology Routing Command Reference</i>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<i>Cisco IOS NetFlow Configuration Guide</i> <i>Cisco IOS XE NetFlow Configuration Guide</i> <i>Cisco IOS NetFlow Command Reference</i>	Network traffic data analysis, aggregation caches, export features.
<i>Cisco IOS Network Management Configuration Guide</i> <i>Cisco IOS XE Network Management Configuration Guide</i> <i>Cisco IOS Network Management Command Reference</i>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<i>Cisco IOS Novell IPX Configuration Guide</i> <i>Cisco IOS XE Novell IPX Configuration Guide</i> <i>Cisco IOS Novell IPX Command Reference</i>	Novell Internetwork Packet Exchange (IPX) protocol.
<i>Cisco IOS Optimized Edge Routing Configuration Guide</i> <i>Cisco IOS Optimized Edge Routing Command Reference</i>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<i>Cisco IOS Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<i>Cisco IOS Security Configuration Guide</i> <i>Cisco IOS XE Security Configuration Guide</i> <i>Cisco IOS Security Command Reference</i>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

**Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)**

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	<p>Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).</p> <p><b>Note</b> For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.</p>
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

**Table 2** Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of <b>debug</b> commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

## Additional Resources and Documentation Feedback

*What's New in Cisco Product Documentation* is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

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

© 2007–2008 Cisco Systems, Inc. All rights reserved.



# Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

---

**Last updated: August 6, 2008**

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

## Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

### Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

## Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

## Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.



**Table 1**     *CLI Command Modes*

<b>Command Mode</b>	<b>Access Method</b>	<b>Prompt</b>	<b>Exit Method</b>	<b>Mode Usage</b>
User EXEC	Log in.	Router>	Issue the <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>• Issue <b>show</b> and <b>debug</b> commands.</li> <li>• Copy images to the device.</li> <li>• Reload the device.</li> <li>• Manage device configuration files.</li> <li>• Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router(config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router(config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router(config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the <b>reload</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	rommon # >  The # symbol represents the line number and increments at each prompt.	Issue the <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	Router(diag) #	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



**Note**

A keyboard alternative to the **end** command is Ctrl-Z.

## Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

**Table 2** CLI Interactive Help Commands

Command	Purpose
<b>help</b>	Provides a brief description of the help feature in any command mode.
<b>?</b>	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

### **help**

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

### **?**

```
Router# ?
```

Exec commands:

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

### **partial command?**

```
Router(config)# zo?
```

```
zone zone-pair
```

### **partial command<Tab>**

```
Router(config)# we<Tab> webvpn
```

### **command ?**

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

### **command keyword ?**

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

## Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

**Table 3**     *CLI Syntax Conventions*

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>
Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

```

## Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

**Note**

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_tech\\_note09186a00801746e6.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml).

## Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



**Note** The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

## Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

## Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

**Table 4** Default Command Aliases

Command Alias	Original Command
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_book.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html).

## Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

## Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

[http://www.cisco.com/en/US/docs/ios/debug/command/reference/db\\_book.html](http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html).



### Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

## Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.



To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

## Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

**Table 5** Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

## Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM.

## Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:  
[http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf\\_cli-basics.html](http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html)
- or
- “Using Cisco IOS XE Software” chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:  
[http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using\\_cli.html](http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html)
- Cisco Product Support Resources  
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)  
<http://www.cisco.com/en/US/support/index.html>
- *White Paper: Cisco IOS Reference Guide*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_white\\_paper09186a008018305e.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml)
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)  
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software  
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

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

© 2007–2008 Cisco Systems, Inc. All rights reserved.





# Packet Data Serving Node Commands

---

# access-list

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

**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

<i>access-list-number</i>	Integer that identifies the access list. If the <i>type-code</i> and <i>wild-mask</i> arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the <i>address</i> and <i>mask</i> arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
<b>permit</b>	Permits the frame.
<b>deny</b>	Denies the frame.
<i>type-code</i>	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 Subnetwork Access Protocol (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.)
<i>wild-mask</i>	16-bit hexadecimal number whose ones bits correspond to bits in the <i>type-code</i> argument. The <i>wild-mask</i> argument indicates which bits in the <i>type-code</i> 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.)
<i>address</i>	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. This field is used for filtering by vendor code.
<i>mask</i>	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. The ones bits in <i>mask</i> are the bits to be ignored in <i>address</i> . This field is used for filtering by vendor code. For source address filtering, the mask always should have the high-order bit set. This is because the IEEE 802 standard uses this bit to indicate whether a Routing Information Field (RIF) is present, not as part of the source address.

## Defaults

No access list is configured.

## Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines**

For a list of type codes, refer to the “Ethernet Type Codes” appendix of this book.

**Examples**

In the following example, the access list permits only Novell frames (LSAP 0xE0E0) and filters out all other frame types. This set of access lists would be applied to an interface via the **source-bridge input-lsap list** or **source-bridge input-lsap list** command (described later in this chapter).

```
access-list 201 permit 0xE0E0 0x0101
access-list 201 deny 0x0000 0xFFFF
```

Combine the DSAP/LSAP fields into one number to do LSAP filtering; for example, 0xE0E0—not 0xE0. Note that the deny condition specified in the preceding example is not required; access lists have an implicit deny as the last statement. Adding this statement can serve as a useful reminder, however.

The following access list filters out only SNAP type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x6007) and lets all other types pass. This set of access lists would be applied to an interface using the **source-bridge input-type-list** or **source-bridge output-type-list** command (described later in this chapter).

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
```

**Note**

Use the last item of an access list to specify a default action; for example, to permit everything else or to deny everything else. If nothing else in the access list matches, the default action is to deny access; that is, filter out all other type codes.

Type code access lists will negatively affect system performance by greater than 30 percent. Therefore, we recommend that you keep the lists as short as possible and use wildcard bit masks whenever possible.

**Related Commands**

Command	Description
<b>access-expression</b>	Defines an access expression.
<b>source-bridge input-address-list</b>	Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the router interface based on the source MAC address.
<b>source-bridge input-lsap-list</b>	Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats.
<b>source-bridge input-type-list</b>	Filters SNAP-encapsulated packets on input.
<b>source-bridge output-address-list</b>	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the router interface based on the destination MAC address.
<b>source-bridge output-lsap-list</b>	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.
<b>source-bridge output-type-list</b>	Filters SNAP-encapsulated frames by type code on output.

# cdma pdsn a10 ahdlc engine

To limit the number of Asynchronous High-Level Data Link Control (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

<i>slot</i>	Slot number of the AHDLC.
<i>usable-channels</i>	Maximum number of channels that can be opened in the AHDLC engine.
<i>usable-channels</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>debug cdma pdsn a10 ahdlc</b>	Displays debug messages for the AHDLC engine.
<b>show cdma pdsn a10 ahdlc</b>	Displays information about the AHDLC engine.
<b>show cdma pdsn resource</b>	Displays AHDLC resource information.



# cdma pdsn a10 ahdhc trailer

To enable the PDSN so that AHDLC frames are expected to contain trailer byte, use the **cdma pdsn a10 ahdhc trailer** command to in global configuration mode. To disable the PDSN so that AHDLC processing does not expect the AHDLC trailer (0x7e), use the **no** form of this command.

**cdma pdsn a10 ahdhc trailer**

**no cdma pdsn a10 ahdhc trailer**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

The default behavior is that trailer byte 0x7e is expected in the AHDLC frames.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

When the **no** version of the command is configured, each AHDLC frame is considered a full AHDLC fragment, and the PDSN will start processing the packet.

## Examples

The following example disables the PDSN so that AHDLC processing does not expect the AHDLC trailer:

```
Router(config)# no cdma pdsn a10 ahdhc trailer
```

# cdma pdsn a10 always-on keepalive

To alter the default always-on service parameters, use the **cdma pdsn a10always-on keepalive** command in global configuration mode. To return to the default values, use the **no** form of this command.

**cdma pdsn a10 always-on keepalive {interval 1-65535 [attempts 0-255] | attempts 0-255}**

**no cdma pdsn a10 always-on keepalive {interval 1-65535 [attempts 0-255] | attempts 0-255}**

## Syntax Description

interval	The duration in seconds, for which the PDSN waits for the LCP echo response from the peer before sending next LCP echo. The default value is 3seconds.
attempts	The number of times the LCP echo is sent before determining an always-on user is not reachable and tearing down the session after idle timer expiry. The default value is 3. Configuring this value to 0 is similar to ignoring the always-on property for the user.

## Defaults

The Always On feature is enabled by default. The default value for **interval** is 3, and the default value for **attempts** is 3.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates that the PDSN waits 5 seconds for the LCP echo response from the peer before sending the next LCP echo.

```
router#cdma pdsn a10 always-on keepalive interval 5 attempts 3
```

# cdma pdsn a10 gre sequencing

To enable inclusion of Generic Routing Encapsulation (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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>debug cdma pdsn a10 gre</b>	Displays debug messages for A10 GRE interface errors.
<b>show cdma pdsn pcf</b>	Displays information about PCFs that have R-P tunnels to the PDSN.
<b>show cdma pdsn</b>	Displays the current status and configuration of the PDSN gateway.

# cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout

To configure the PDSN so that Point-to-Point Protocol (PPP) negotiation with an MN will start only after the traffic channel is assigned, ( inother words, after a Registration Request with airlink-start is received), use the **cdma pdsn a10 init-ppp-after-airlink-start** command in global configuration mode. Use the **no** form of this command to revert to the default behavior.

**cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout** *1-120*

**no cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout** *1-120*

<b>Syntax Description</b>	1-120 Sets the timeout interval before the session is torn down.	
<b>Defaults</b>	By default, this CLI is not enabled, therefore, the PDSN will initiate PPP negotiation immediately after a Registration Reply is sent to the initial Registration.Request.  When enabled, the default timeout interval is 10 seconds.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)ZB4a	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.
<b>Usage Guidelines</b>	<p>The PDSN initiates PPP negotiation immediately after a Registration Reply is sent to the initial Registration Request, but the calls (for which the PPP negotiation has started before the traffic channel is assigned to MN) have failed.</p> <p>When this command is enabled, the PPP negotiation withthe MN will start only after the traffic channel is assigned—after a Registration Request with airlink-start is received. If the airlink start is not received at all, the session will be torn down when timeout occurs.By default, this timeout interval is 10 seconds, or can be configured through the CLI.</p> <p>The session is not torn down immediately after the timeout, so, in order to minimize the impact on the performance, there is just one timer started to keep track of all the sessions waiting for airlink-start to start PPP.</p> <p>For example, take the default of 10 seconds. If the timer expires at t1 and a new call comes at t2( t2 &gt; t1), the next run of the timer will be at t1+10. It is likely that the uptime for the call is not more than 10 seconds since t2 &gt; t1. So the call will be checked at the next next run (t1+10+10). That is , the variation is between 1 and 10.</p>	
<b>Examples</b>	<p>The following example illustrates the <b>cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout</b> command:</p> <pre>router# cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout 20</pre>	

# 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**

<b>Syntax Description</b>	seconds	Maximum A10 registration lifetime accepted by Cisco PDSN. The range is 1 to 65535 seconds. The default is 1800 seconds.
---------------------------	---------	---

<b>Defaults</b>	1800 seconds.
-----------------	---------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example specifies that the A10 interface will be maintained for 1440 seconds:
	<pre>cdma pdsn a10 max-lifetime 1440</pre>

<b>Related Commands</b>	Command	Description
	<b>cdma pdsn a10 gre sequencing</b>	Enables GRE sequence number checking on packets received over the A10 interface.
	<b>debug cdma pdsn a10 gre</b>	Displays debug messages for A10.
	<b>show cdma pdsn pcf</b>	Displays information about PCFs that have R-P tunnels to the PDSN.
	<b>show cdma pdsn</b>	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 disable 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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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 a11 dormant sdb-indication gre-flags

To configure the PDSN so that all packets that are set with the specific group-number will be flagged for SDB usage between the PCF and the PDSN, use the **cdma pdsn a11 dormant sdb-indication gre-flags** command in global configuration mode. To disable this feature, use the no form of the command.

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

**no cdma pdsn a11 dormant sdb-indication gre-flags** *group-number*

## Syntax Description

Command	Description
<i>group-number</i>	Specifies the classified match criteria.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

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

## Examples

The following example illustrates the **cdma pdsn a11 dormant sdb-indication gre-flags** command:

```
router# cdma pdsn a11 dormant sdb-indication gre-flags 12
```

# cdma pdsn a11 dormant sdb-indication match-qos-group

To configure the PDSN to use SDBs to deliver PPP control packets for Always-On sessions, where the session is dormant, use the **cdma pdsn a11 dormant sdb-indication match-qos-group** command in global configuration mode. Use the **no** form of this command to disable this feature.

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

**no cdma pdsn a11 dormant sdb-indication match-qos-group** *group-number* **ppp-ctrl-pkts**

## Syntax Description

Command	Description
<i>group-number</i>	Specifies the classified match criteria.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF2	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

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

## Examples

The following example illustrates the **cdma pdsn a11 dormant sdb-indication match-qos-group** command:

```
router(config)# cdma pdsn a11 dormant sdb-indication match-qos-group 14 ppp-ctrl-pkts
```



# cdma pdsn a11 mandate presence airlink-setup

To mandate that the initial RRQ should have Airlink-Setup in Acct CVSE from PCF, use the **cdma pdsn all mandate presence airlink-setup** command in global configuration mode. To disable this feature, use the **no** form of this command.

**cdma pdsn a11 mandate presence airlink-setup**

**no cdma pdsn a11 mandate presence airlink-setup**

**Syntax Description** This command has no keywords or variables.

**Defaults** There are no default values.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(8)ZB1	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**Usage Guidelines** Issuing this command mandates that the initial RRQ should have Airlink-Setup in Acct CVSE from PCF. As a result, if this Airlink setup is not present in the RRQ, the session is not created, and a RRP with error code “86H - Poorly formed request” is returned.

If you do not configure this command, or disable it, then sessions can be opened even with no accounting CVSE being present in the initial RRQ.

**Examples** router# cdma pdsn a11 mandate presence airlink-setup

# cdma pdsn a11 receive de-reg send-termreq

To enable the PDSN to send an LCP TermReq to the Mobile Node when it receives a A11 de-registration message from the PCF, use the **cdma pdsn a11 receive de-reg send-termreq** command in global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn a11 receive de-reg send-termreq**

**no cdma pdsn a11 receive de-reg send-termreq**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example enables the PDSN to send an LCP TermReq to the Mobile Node when it receives a A11 de-registration message from the PCF:

```
router (config)# cdma pdsn a11 receive de-reg send-termreq
```

# cdma pdsn a11 reject airlink-start active

To enable the PDSN to send RRP (with error code “86H-Poorly formed request”) when the RRQ is received with airlink-start in the Acct CVSE from PCF for an active session, use the **cdma pdsn a11 reject airlink-start active** command in global configuration mode. To disable this function, use the **no** form of the command.

**cdma pdsn a11 reject airlink-start active**

**no cdma pdsn a11 reject airlink-start active**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default values.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(11)YR	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Examples** The following example illustrates the **cdma pdsn a11 reject airlink-start active** command:

```
Router(config)# cdma pdsn a11 reject airlink-start active
```

# cdma pdsn a11 reject airlink-stop dormant

To enable the PDSN to send RRP (with error code “86H-Poorly formed request”) when the RRQ is received with airlink-stop in the Acct CVSE from PCF for a dormant session, use the **cdma pdsn a11 reject airlink-stop dormant** command in global configuration mode. To disable this function, use the **no** form of the command.

**cdma pdsn a11 reject airlink-stop dormant**

**no cdma pdsn a11 reject airlink-stop dormant**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	No default values.
-----------------	--------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(11)YR	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

<b>Examples</b>	The following example illustrates the <b>cdma pdsn a11 reject airlink-stop dormant</b> command:
-----------------	---

```
Router(config)# cdma pdsn a11 reject airlink-stop dormant
```

# cdma pdsn a11 session-update

To enable the A11 Session update feature on the PDSN, and to send an A11 session update for either the Always On, or RNPDT (or both) attributes that are downloaded from the AAA during the authentication phase, use the **cdma pdsn a11 session-update** command in global configuration. Use the **no** form of the command to disable this feature.

**cdma pdsn a11 session-update** {[always-on] 1-10 [rn-pdit] 0-9}

**no cdma pdsn a11 session-update** {[always-on] [rn-pdit] 1-10}

Syntax Description	Command	Description
	<b>always-on</b>	Sends an A11 session update for the Always On attribute that is downloaded from the AAA during the authentication phase.
	<b>rn-pdit</b>	Sends an A11 session update for the RN-PDIT attribute that is downloaded from the AAA during the authentication phase.
	<i>1-10</i>	Sets the timeout value for re-transmission of the A11 session update message to the PCF. The default timeout value is 3 seconds.
	<i>0-9</i>	Sets the retransmit limit for the A11 session update if A11 session update Ack is not received from the PCF. Default re-transmission value is 3.

**Defaults** The default timeout value is 3 seconds. The default retransmit number is 3.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(11)YF	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Examples** The following example enables both the **always-on** and **rn-pdit** attributes:

```
Router(config)#cdma pdsn a11 session-update ?
  always-on  Send Always-on indicator in A11 Session-Update
  rn-pdit    Send RN-PDIT in A11 Session-Update
```

# 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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>clock timezone</b>	Specifies the hours and minutes (optional) difference between the local time zone and UTC.
<b>cdma pdsn accounting send start-stop</b>	Causes the PDSN to send: <ul style="list-style-type: none"> <li>An Accounting Stop record when it receives an active stop airlink record (dormant state)</li> <li>An Accounting Start record when it receives an active start airlink record (active state)</li> </ul>

# cdma pdsn accounting prepaid

To enable the Prepaid billing feature on PDSN, use the **cdma pdsn accounting prepaid** command in global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn accounting prepaid [volume | duration]**

**no cdma pdsn accounting prepaid [volume | duration]**

## Syntax Description

Command	Description
<b>volume</b>	Specifies that quota metering on the PDSN will be volume-based.
<b>duration</b>	Specifies that quota metering on the PDSN will be duration-based.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

Prepaid quota metering on the PDSN can be configured as volume-based only by enabling the **volume** keyword, or duration-based only by enabling the **duration** keyword. If no option is provided, both volume-based and duration-based metering are enabled on the PDSN, but only one can be effective at a time for one prepaid flow.



### Note

The Radius Disconnect feature should be enabled on PDSN for Prepaid service. Use the **cdma pdsn radius disconnect** command to enable the radius disconnect (POD) feature.

## Examples

The following example illustrates how to enable volume-based billing on the PDSN using the **cdma pdsn accounting prepaid** command:

```
router# cdma pdsn accounting prepaid volume
```


# cdma pdsn accounting prepaid threshold

To set the box-level threshold for all volume-based or duration-based prepaid flows on the PDSN, use the **cdma pdsn accounting prepaid threshold** command in global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn accounting prepaid threshold** [volume | duration] *value*

**no cdma pdsn accounting prepaid threshold** [volume | duration] *value*

## Syntax Description

Command	Description
volume	Specifies that the threshold value will apply to volume-based accounting. The values are 10-100, and they specify the Volume Threshold percentage
duration	Specifies that the threshold value will apply to duration-based accounting. The values are 10-100, and they specify the Duration Threshold percentage
value	Indicates the percentage of allocated quota that is the threshold value for the quota.  Different threshold values can be set for volume-based and duration-based Prepaid service.
 <b>Note</b>	The threshold values returned in the Access Accept message for the user will override this value.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates how to set the threshold for volume-based billing on the PDSN using the **cdma pdsn accounting prepaid threshold** command:

```
router# cdma pdsn accounting prepaid volume 80
router# cdma pdsn accounting prepaid duration 75
```



# 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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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 ipv6-flows

To control the number of flows and UDR records used for IPv4/IPv6 simultaneous sessions, use the **cdma pdsn accounting send ipv6-flows** command in global configuration mode. Use the **no** form of this command to disable this function.

**cdma pdsn accounting send ipv6-flows** *number*

**no cdma pdsn accounting send ipv6-flows** *number*

## Syntax Description

Command	Description
<i>number</i>	Number of flows. The default value is 1, denoting a shared flow. The range of values is 1-2.

## Defaults

The default value of flows is 1, denoting a shared flow.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)XY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

The session will default to 1 flow for a simultaneous IPv4/IPv6 session, but 2 flows can be configured for a simultaneous session.

## Examples

The following example illustrates the **cdma pdsn accounting send ipv6-flows** command:

```
router(config)# cdma pdsn accounting send ipv6-flows 2
```

# 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.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**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**

<b>Syntax Description</b>	<i>hh:mm:ss</i> Hour:minutes:seconds.	
<b>Defaults</b>	No default behavior or values.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(5)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.
<b>Usage Guidelines</b>	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.	
<b>Examples</b>	<p>The following example sets an accounting trigger for 13:30:20:</p> <pre>cdma pdsn accounting time-of-day 13:30:30</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clock set</b>	Sets the system clock.
	<b>debug cdma pdsn accounting time-of-day</b>	Displays debug information for the command.
	<b>show clock</b>	Displays the system clock.
	<b>cdma pdsn accounting send start-stop</b>	Causes the PDSN to send: <ul style="list-style-type: none"> <li>An Accounting Stop record when it receives an active stop airlink record (dormant state)</li> <li>An Accounting Start record when it receives an active start airlink record (active state)</li> </ul>

# 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**

<b>Syntax Description</b>	<i>minimum-age value</i>	(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.
---------------------------	--------------------------	---

<b>Defaults</b>	By default, no idle users are aged out.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	The following example sets a minimum age out value of 5 seconds:  cdma pdsn age-idle-users minimum-age 5
-----------------	--

# cdma pdsn attribute send

To configure the attributes to be sent in an access-request or accounting request, use the **cdma pdsn attribute send** command in global configuration mode. To disable this feature and return to the default settings, use the **no** form of this command.

```
cdma pdsn attribute send {a1 {fa-chap | mip-rrq} | a2 {auth-req | fa-chap | mip-rrq} c5
{acct-reqs} | f11 {auth-req | fa-chap} | f15 {acct-reqs} | f16 {acct-reqs} | f5 {auth-req |
fa-chap} | g1 {acct-start} | g2 {acct-start} | g17 | esn-optional | is835a}
```

```
no cdma pdsn attribute send {a1 {fa-chap | mip-rrq} | a2 {auth-req | fa-chap | mip-rrq} c5
{acct-reqs} | f11 {auth-req | fa-chap} | f15 {acct-reqs} | f16 {acct-reqs} | f5 {auth-req |
fa-chap} | g1 {acct-start} | g2 {acct-start} | g17 | esn-optional | is835a}
```

## Syntax Description

a1	Attribute Calling Station ID
a2	Attribute ESN, Electronic Serial Number
c5	Attribute c5, Service Reference ID
f11 auth-req	Auth-req Send f11 (IP Technology) in access request during pap/chap
f11 fa-chap	fa-chap Send f11 (IP Technology) in FA-CHAP
f15	Attribute f15, always-on
f16	Attribute f16, Forward PDCH RC
f5 auth-req	auth-req Send f5 (Service Option) in access request during pap/chap
f5 fa-chap	fa-chap Send f5 (Service Option) in FA-CHAP
g1	Attribute Input Octets
g2	Attribute Output Octets
g17	Attribute for last-user-activity in accounting stop and interim accounting records.
esn-optional	Send ESN in accounting records only when sent by PCF.
is835a	acct-start Send attributes in accounting start as per is835a.
fa-chap	Send <i>attribute</i> in fa-chap
mip-rrq	Send <i>attribute</i> in mobile ip RRQ
acct-reqs	Send <i>attribute</i> in start/stop/interim records for non always-on users
auth-req	Send <i>attribute</i> in access request during pap/chap
acct-start	Send <i>attribute</i> in accounting start

## Defaults

No default values

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.3(14)YX	The <b>F11</b> attributes were introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

Use this command to enable the optional attributes to be sent in access and accounting requests.

When attributes which have multiple options (for example, **a1**, which can be sent in **fa-chap** as well as **mip-rrq**), the configuration can be done in the following way as well,

```
cdma pdsn attribute send a1 fa-chap mip-rrq,
```

similarly

```
cdma pdsn attribute send a1 auth-req mip-rrq fa-chap
```

## Examples

The following example enables the **cdma pdsn attribute send** command:

```
cdma pdsn attribute send a1 fa-chap
```

The attribute **a1** will be sent in the access request during FA-CHAP

```
cdma pdsn attribute send a1 auth-req
```

The attribute **a2** will be sent in the access request during PPP PAP/CHAP

# cdma pdsn attribute send a3

To include the MEID in Access Request, FA-CHAP, Mobile IP RRQs, use the **cdma pdsn attribute send a3** command in the global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn attribute send a3 {auth-req | fa-chap | mip-rrq}**

**no cdma pdsn attribute send a3 {auth-req | fa-chap | mip-rrq}**

## Syntax Description

auth-req	Send a3(MEID) in access request during pap/chap.
fa-chap	Send a3(MEID) in FA-CHAP.
mip-rrq	Send a3(MEID) in MobileIP RRQ.

## Defaults

No default values

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX1	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates how to include the MEID in FA-CHAP:

```
router#cdma pdsn attribute send a3 fa-chap
```



# cdma pdsn attribute send meid-optional

To include the MEID in the Accounting Requests and access requests, in FA-CHAP requests and MOIP-requests, use the **cdma pdsn attribute send meid-optional** command in global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn attribute send meid-optional**

**no cdma pdsn attribute send meid-optional**

## Syntax Description

There are no arguments of keywords for this command.

## Defaults

No default values

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX1	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

If the MN is not equipped to send the MEID, it will not be included in the RRQ. In such circumstances, a blank string will be included in the Accounting Requests, and the access requests, FA-CHAP and MOIP-rrqs.

If the **cdma pdsn attribute send meid-optional** command is configured, the MEID is included in the Accounting Requests and access requests, in FA-CHAP requests and MOIP- requests, only if it is included in the RRQ.

## Examples

The following example illustrates the **cdma pdsn attribute send meid-optional** command:

```
router#cdma pdsn attribute send meid-optional
```

# 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

<b>interface</b>	Interface name on which the cluster controller has IP connectivity to the cluster members.
<i>timeout</i>	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.
<i>window number</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## Examples

The following example enables the cdma cluster controller:

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

## cdma pdsn cluster controller closed-rp

To configure the VPDN group to be used to establish the L2TP tunnels between the controller and members for the Closed-RP Controller-Member clustering, use the **cdma pdsn cluster controller closed-rp** command in global configuration mode on the PDSN cluster controller. To remove this configuration, use the **no** form of the command.

**cdma pdsn cluster controller closed-rp** *vpdn-group*

**no cdma pdsn cluster controller closed-rp** *vpdn-group*

<b>Syntax Description</b>	vpdn-group	VPDN group to be used for establishment of the controller-member VPDN tunnels.
---------------------------	------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)YX	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

<b>Usage Guidelines</b>	The VPDN group to be used for controller-member L2TP tunnels must be present in the running configuration before this command is configured.
-------------------------	--

<b>Examples</b>	The following example illustrates the <b>cdma pdsn cluster controller closed-rp</b> command: <b>cdma pdsn cluster controller closed-rp</b> <i>vpdn-group</i>
-----------------	---

# cdma pdsn cluster controller member periodic-update

To enable the periodic process to flush the dangling Session Records on the controller, use the **cdma pdsn cluster controller member periodic-update** command in Global configuration mode. Use the **no** form of the command to disable this process.

**cdma pdsn cluster controller member periodic-update**

**no cdma pdsn cluster controller member periodic-update**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)ZB1	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates how to enable the **cdma pdsn cluster controller member periodic-update** command:

```
router(config)# cdma pdsn cluster controller member periodic-update
```

# cdma pdsn cluster controller session-high

To generate an alarm when the controller reaches the upper threshold of the maximum number of sessions it can handle, use the **cdma pdsn cluster member session-high** command. To disable this feature, use the **no** form of this command.

**cdma pdsn cluster controller session-high 1-1000000**

**no cdma pdsn cluster controller session-high 1-1000000**

## Syntax Description

<b>1-1000000</b>	The threshold of the maximum number of sessions the controller can handle.
------------------	--

## Defaults

The range is 1-1000000. The configured value should be more than the lower threshold value. The default value is 200000.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)ZB1	This command was introduced.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## Usage Guidelines

You should take into account the number of members in the cluster when you configure the high threshold. For example, if there are only 2 members in the cluster, the high threshold should be less than 40000.

## Examples

The following example illustrates the **cdma pdsn cluster controller session-high** command:

```
Received SNMPv1 Trap:
Community: public
Enterprise: cCdmaPdsnMIBNotifPrefix
Agent-addr: 9.15.72.15
Enterprise Specific trap.
Enterprise Specific trap: 8
Time Ticks: 9333960
cCdmaServiceAffectedLevel.0 = major(3)
cCdmaClusterSessHighThreshold.0 = 50
```

# cdma pdsn cluster controller session-low

To generate an alarm when the controller reaches the lower threshold of the sessions (hint to NOC that the system is being under utilized), use the **cdma pdsn cluster member session-low** command. To disable this feature, use the **no** form of this command.

**cdma pdsn cluster controller session-low 1-1000000**

**no cdma pdsn cluster controller session-low 1-1000000**

<b>Syntax Description</b>	<b>1-1000000</b>	The threshold of the maximum number of sessions the controller can handle.
<b>Defaults</b>	The range is 0-999999. The configured value should be less than the upper threshold value. The default value is 190000.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)ZB1	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.
<b>Usage Guidelines</b>	You should take into account the number of members in the cluster when you configure the low threshold.	
<b>Examples</b>	<p>The following example illustrates the <b>cdma pdsn cluster controller session-low</b> command:</p> <pre> Received SNMPv1 Trap: Community: public Enterprise: cCdmaPdsnMIBNotifPrefix Agent-addr: 9.15.72.15 Enterprise Specific trap. Enterprise Specific trap: 9 Time Ticks: 9330691 cCdmaServiceAffectedLevel.0 = major(3) cCdmaClusterSessLowThreshold.0 = 10 </pre>	

# 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 ipaddr | interface interface-name | timeout seconds [window number] | window number ]
```

## Syntax Description

<b>controller</b> <i>ipaddr</i>	The controller that a specific member is connected to, identified by the controller's IP address.
<b>interface</b>	Interface name on which the cluster controller has IP connectivity to the cluster members.
<b>prohibit</b>	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.
<b>timeout</b>	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.
<b>window</b> <i>number</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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 cluster member periodic-update

To enable sending only bulk-update on a member PDSN, use the **cdma pdsn cluster member periodic-update** command in Global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn cluster member periodic-update** *time*

**no cdma pdsn cluster member periodic-update** *time*

Syntax Description	time	The time between when the member sends periodic bulk-updates. The time can be between 300 to 3000 msec.
--------------------	------	---

Defaults	The default value is 1000 ms.
----------	-------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples	<p>The following example illustrates the <b>cdma pdsn cluster member periodic-update</b> command:</p> <pre>router(config)# cdma pdsn cluster member periodic-update 1000</pre>
----------	--



# cdma pdsn compliance

To configure PDSN behavior to comply with various standards, use the **cdma pdsn compliance** command in global configuration mode. Use the **no** form of the command to disable this function.

**cdma pdsn compliance** [iosv4.1] [sdb] [is835a] [is835c]

**no cdma pdsn compliance** [iosv4.1] [sdb] [is835a] [is835c]

## Syntax Description

<b>iosv4.1</b>	Configures compliance to 3GPP2-IOS v4.1 features.
<b>sdb</b>	Configures PDSNs to process SDB record sent from PCF as per IOS4.1 Standard.
<b>is835a</b>	Configures IS835A-compliant behavior.
<b>is835c</b>	Configures IS835C-compliant behavior.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF1	This command was introduced.
12.3(11)YF2	The <b>sdb</b> keyword was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates one instance of the **cdma pdsn compliance** command:

```
router(config)# cdma pdsn compliance is835a
```

# 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 in Global 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
	<b>debug cdma pdsn a11</b>	Displays debug messages for A11 interface errors, events, and packets.

# cdma pdsn debug show-conditions

To configure the PDSN to print the username/IMSI along with the debugs even without configuring conditional debugging, use the **cdma pdsn debug show-conditions** command in global configuration mode. Use the **no** form of the command to disable this function.

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default value is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(14)YX	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Usage Guidelines** When the debug conditions match, every line of the debug message is pre-pended with either the username or the IMSI (not both), depending on the condition set.

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

**Examples** The following example enables username and IMSI printing in the debugs:

```
router(config)#cdma pdsn debug show-condition
```

# 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

<i>entries</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>snmp-server enable traps cdma</b>	Specifies the community access string to permit access to the SNMP protocol.
<b>show cdma pdsn</b>	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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
	<b>show cdma pdsn</b>	Displays the current status and configuration of the PDSN gateway.
	<b>show cdma pdsn session</b>	Displays the session information on the PDSN.

# cdma pdsn ipv6

To enable the PDSN IPv6 functionality, use the **cdma pdsn ipv6** command in global configuration mode. Use the **no** form of the command to disable this function.

**cdma pdsn ipv6** {**ra-count** *1-5* [**ra-interval** *1-1800*]}

**no cdma pdsn ipv6** {**ra-count** *1-5* [**ra-interval** *1-1800*]}

## Syntax Description

ra-count	Route Advertisement count determines how many Routing Advertisements (RAs) to send out to the MN.
1-5	Number of IIPV6 route advertisements sent: the default value is 1.
ra-interval	Route Advertisement interval determines how often Routing Advertisements (RAs) are sent to the MN.
1-1800	The interval between IPv6 RAs sent (the unit of measure is in seconds, and the default value is 5).

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)XY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

If the **cdma pdsn ipv6** command is not entered, and a PDSN session is brought up with IPv6, the session will be terminated and the following message displayed:

%CDMA\_PDSN-3-PDSNIPV6NOTENABLED: PDSN IPv6 feature has not been enabled.

## Examples

The following example illustrates how to control the number and interval Routing Advertisements sent to the MN when an IPv6CP session comes up:

```
router(config)# cdma pdsn ipv6 ra-count 2 ra-interval 3
```

# 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

<i>maxpcf</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>show cdma pdsn</b>	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

<i>maxsessions</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>show cdma pdsn session</b>	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

<i>number value</i>	The number of agent advertisements. Possible values are 1 through 10. The default is 5.
<i>interval msec</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>ip mobile foreign-service challenge</b>	Configures the challenge timeout value and the number of valid recently-sent challenge values.
<b>ip mobile foreign-service challenge forward-mfce</b>	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** [close-session-on-failure][*imsi number*] [*irm number*] [*min number*] [profile-password password]

**no cdma pdsn msid-authentication**

## Syntax Description

<b>close-session-on-failure</b>	Closes the session if authorization fails.
<b>imsi</b> <i>number</i>	(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.
<b>irm</b> <i>number</i>	(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.
<b>min</b> <i>number</i>	(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.
<b>profile-password</b> 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 <b>profile-password</b> keyword was added.
12.2(8)ZB1	The <b>close-session-on-failure</b> keyword was added
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

### 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
<b>show cdma pdsn</b>	Displays the current status and configuration of the PDSN gateway.

# cdma pdsn pcf default closed-rp

To enable the Closed-RP interface feature on the PDSN, use the **cdma pdsn pcf default closed-rp** command in global configuration mode. Use the **no** form of the command to disable the Closed-RP interface feature.

**cdma pdsn pcf default closed-rp**

**no cdma pdsn pcf default closed-rp**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

The default setting is that Closed-RP is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

## Usage Guidelines

When the **cdma pdsn pcf default closed-rp** command is configured, the Closed-RP interface feature is enabled on the PDSN. All the PCF's connecting to the PDSN will be considered as Closed-RP PCF's. When this command is configured the 3GPP2 (Open) RP interface will be disabled on the PCF.

## Examples

The following example illustrates the **cdma pdsn pcf default closed-rp** command:

```
Router (config)# cdma pdsn pcf default closed-rp
```

# cdma pdsn radius disconnect

To enable support for Radius Disconnect on the Cisco PDSN, use the **cdma pdsn radius disconnect** command in global configuration. Use the **no** form of the command to disable this feature.

**cdma pdsn radius disconnect [nai]**

**no cdma pdsn radius disconnect [nai]**

## Syntax Description

nai	(Optional) Indicates whether to enable processing of Disconnect Request received with only the NAI attribute.
-----	---

## Defaults

By default the PDSN will not process a Disconnect Request received with only the **nai** attribute.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

By default the PDSN will not process a Disconnect Request received with only NAI attribute. In a Service provider environment all simple IP sessions can be opened with the same user-name (and in case of Resource Management for sessions); therefore, a session identification attribute will be sent in a Disconnect Request. Additionally, the overhead to maintain tables relating to sessions and NAI can be avoided in such cases.

But if the PDSN can receive a Disconnect Request with only an NAI attribute in a particular environment, then the **nai** keyword should be configured.

This configuration will set the Session Termination Capability VSA value to 1. The presence of other feature configurations (like MIP Revocation) can alter this value.

## Examples

The following example illustrates the **cdma pdsn radius disconnect** command:

```
Router(config)#cdma pdsn radius disconnect nai
```

# cdma pdsn redundancy

To enable the active PDSN to synchronize the session and flow related data to its standby peer, use the **cdma pdsn redundancy** command in global configuration mode. Use the **no** form of the command to disable this function.

**cdma pdsn redundancy**

**no cdma pdsn redundancy**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

The default setting is that PDSN redundancy is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

The following example illustrates the **cdma pdsn redundancy** command:

```
router(config)# cdma pdsn redundancy
```

# cdma pdsn redundancy accounting send vsa swact

To send the Cisco VSA (cdma-rfswact) in first interim/stop record after switchover, use the **cdma pdsn redundancy accounting send vsa swact** command in global configuration mode. To disable this feature, use the no form of the command.

**cdma pdsn redundancy accounting send vsa swact**

**no cdma pdsn redundancy accounting send vsa swact**

## Syntax Description

There are no keywords or arguments for this command.

## Defaults

By default, this command is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3.(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

After a switchover takes place, the first interim or stop accounting record (as appropriate) includes a VSA (cdma-rfswact) indicating that a switchover has occurred. The inclusion of this VSA is controllable through this CLI.

If periodic syncing is enabled, you cannot configure the **cdma pdsn redundancy accounting send vsa swact** command, and vice-versa, as the two approaches are mutually exclusive.



### Note

Neither the **cdma pdsn redundancy accounting send vsa swact** command, or periodic syncing can be configured if the **cdma pdsn redundancy** command is not configured.

## Examples

The following example illustrates the **cdma pdsn redundancy accounting send vsa swact** command:

```
Router(config)# cdma pdsn redundancy accounting send vsa swact
```

# cdma pdsn redundancy accounting update-periodic

To enable the active PDSN to periodically synchronize accounting counters, and to synch accounting information between the active and standby in Session Redundancy environment, use the **cdma pdsn redundancy accounting update-periodic** command in global configuration mode. To disable this feature, use the **no** form of the command.

**cdma pdsn redundancy accounting [update-periodic]**

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

## Syntax Description

update-periodic	Syncs the G1/G2 and Packets In/Out with interim AAA updates, and closes the session if authorization fails.
-----------------	---

## Defaults

By default, this command is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

When configured, the byte and packet counts for each flow are synced from the active to the standby unit (only if they undergo a change) at the configured periodic accounting interval (using **aaa accounting update periodic xxx**). If periodic accounting is not configured, the byte and packet counts will not be synced.

## Examples

The following example illustrates the **cdma pdsn redundancy accounting update-periodic** command:

```
Router(config)# cdma pdsn redundancy accounting update-periodic
```



# 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**

<b>Syntax Description</b>	<i>number</i>	Maximum number of times an A11 Registration Update message is retransmitted. Possible values are 0 through 9. The default is 5 retransmissions.
---------------------------	---------------	---

<b>Defaults</b>	5 retransmissions.
-----------------	--------------------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	The following example specifies that A11 Registration Update messages will be retransmitted a maximum of 9 times:  cdma pdsn retransmit a11-update 9
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cdma pdsn timeout a11-update</b>	Specifies A11 Registration Update message timeout.
	<b>debug cdma pdsn a11</b>	Displays debug messages for A11 interface errors, events, and packets.
	<b>show cdma pdsn</b>	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

<b>default</b>	Specifies this is the default security configuration.
<b>spi value</b>	Security parameter index (SPI) used for authenticating packets. Possible values are 0x100 through 0xffffffff.
<b>inbound value outbound value</b>	Inbound and outbound SPI.
<b>key {hex   ascii} string</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>ip mobile secure</b>	Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host.
<b>cdma pdsn secure pcf</b>	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

<b>Syntax Description</b>	<i>lower</i> [ <i>upper</i> ]	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.
	<b>spi</b> <i>value</i>	Security parameter index (SPI) used for authenticating packets. Possible values are 0x100 through 0xffffffff.
	<b>inbound</b> <i>value</i> <b>outbound</b> <i>value</i>	Inbound and outbound SPI.
	<b>key</b> { <b>hex</b>   <b>ascii</b> } <i>string</i>	String of ascii or hexadecimal values. No spaces are allowed.
	<i>local-timezone</i>	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.2(8)BY1	The <b>local-timezone</b> keyword was added.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
<b>ip mobile secure</b>	Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host.
<b>cdma pdsn secure cluster</b>	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

<i>interface_name</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>cdma pdsn selection keepalive</b>	Specifies the keepalive time.

Command	Description
<b>cdma pdsn selection load-balancing</b>	Enables the load-balancing function of the intelligent PDSN selection feature.
<b>cdma pdsn selection session-table-size</b>	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**

<b>Syntax Description</b>	<i>value</i>	The keepalive value, in seconds. Possible values are 5 through 60.
---------------------------	--------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example configures a keepalive value of 200 seconds:  cdma pdsn selection keepalive 200
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cdma pdsn selection load-balancing</b>	Enables the load-balancing function of the intelligent PDSN selection feature.
	<b>cdma pdsn selection session-table-size</b>	Defines the size of the selection session database.
	<b>show cdma pdsn selection</b>	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**

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

**Defaults** The threshold value is 100 sessions.

**Command Modes** Global Configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cdma pdsn selection session-table-size</b>	Defines the size of the selection session database.
	<b>show cdma pdsn session</b>	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**

<b>Syntax Description</b>	<i>size</i>	Session table size. Possible values are 2000 through 100000.
---------------------------	-------------	--

<b>Defaults</b>	PDSN selection is disabled. The default session table size is undefined.
-----------------	---

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example sets the size of the distributed session database to 5000 sessions:  cdma pdsn selection session-table-size 5000
-----------------	--

<b>Related Commands</b>	Command	Description
	<b>cdma pdsn selection load-balancing</b>	Enables the load-balancing function of PDSN selection.
	<b>show cdma pdsn session</b>	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**

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

---

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

---

---

<b>Usage Guidelines</b>	This command is used with multiple flows.
-------------------------	---

---

<b>Examples</b>	The following example enables agent advertisements to be sent:  cdma pdsn send-agent-adv
-----------------	--

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show cdma pdsn	Displays the current status and configuration of the PDSN gateway.

---

# cdma pdsn timeout

To configure a variety of different message timeouts, use the **cdma pdsn timeout** command in global configuration mode. To disable any of these message timeouts, use the **no** form of this command.

**cdma pdsn timeout** [**a11-session-update** | **a11-update** *seconds* | {**airlink-start** [**close-rp** | **initiate-ppp**]} **mobile-ip-registration**]

**no** [**a11-session-update** | **a11-update** *seconds* | {**airlink-start** [**close-rp** | **initiate-ppp**]} **mobile-ip-registration**]

<b>Syntax Description</b>	<b>a11-session-update</b>	Configures an a11 session update message timeout. The timeout value is in seconds, with a range between 1-120.
	<b>a11-update</b> <i>seconds</i>	Configures an a11 update message timeout. <i>seconds</i> is the maximum A11 Registration Update message timeout value, in seconds. Possible values are 0 through 5. The default is 1 second.
	<b>airlink-start</b>	Configures an airlink-start timeout
	<b>close-rp</b>	Close the RP session if airlink start timeout occurs.
	<b>initiate-ppp</b>	Initiates a PPP negotiation if an airlink start timeout occurs.
	<b>mobile-ip-registration</b>	Configures a Mobile IP registration timeout.

**Defaults** **a11-session-update** default value is 1 second.

**Command Modes** Global Configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(14)YF	Closed RP option was added.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

**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:

```
PDSN(config)#cdma pdsn timeout airlink-start 5 ?
```

```
close-rp      Close RP session if airlink start timeout occurs
initiate-ppp  Initiate PPP negotiation if airlink start timeout occurs
```

**cdma pdsn timeout**

```
PDSN(config)#cdma pdsn timeout airlink-start 5 ini
PDSN(config)#cdma pdsn timeout airlink-start 5 initiate-ppp ?
<cr>
PDSN(config)#cdma pdsn timeout airlink-start 5 clo
PDSN(config)#cdma pdsn timeout airlink-start 5 close-rp ?
```

**Related Commands**

Command	Description
<b>cdma pdsn retransmit a11-update</b>	Specifies the maximum number of times an A11 Registration Update message will be retransmitted.
<b>debug cdma pdsn a11</b>	Displays debug messages for A11 interface errors, events, and packets.
<b>show cdma pdsn</b>	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**

<b>Syntax Description</b>	<i>timeout</i>	Time, in seconds. Possible values are 1 through 60. The default is 5 seconds.
---------------------------	----------------	---

<b>Defaults</b>	5 seconds.
-----------------	------------

<b>Command Modes</b>	Global Configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	The following example sets the timeout value for Mobile IP registration to 15 seconds:  cdma pdsn mobile-ip-timeout 15
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip mobile interface</b>	Displays information about interfaces that are providing FA service or are home links for mobile stations.
	<b>show cdma pdsn</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>interface virtual-template</b>	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*

<b>Syntax Description</b>	<b>days</b>	The number of days of the record age.
---------------------------	-------------	---------------------------------------

<b>Defaults</b>	No default keywords or arguments.
-----------------	-----------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)BY	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example shows output from the <b>clear cdma pdsn cluster controller session</b> <i>records age</i> command:
-----------------	---

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

# clear cdma pdsn cluster controller statistics

To clear controller statistics, use the **clear cdma pdsn cluster controller statistics** command in privileged EXEC mode.

**clear cdma pdsn cluster controller statistics [queuing | redundancy]**

## Syntax Description

<b>queuing</b>	Clears statistics associated with controller queuing feature.
<b>redundancy</b>	Clears statistics associated with controller redundancy interface.

## Defaults

There are no default values for this command.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

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

```
router# clear cdma pdsn cluster controller statistics queuing
```



# clear cdma pdsn cluster member statistics

To clear member statistics, use the **clear cdma pdsn cluster member statistics** command in privileged EXEC mode.

**clear cdma pdsn cluster controller statistics [queuing | redundancy]**

## Syntax Description

<b>queuing</b>	Clear s statistics associated with controller queuing feature.
----------------	--

## Defaults

There are no default values for this command.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

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

```
router# clear cdma pdsn cluster member statistics queuing
```

# clear cdma pdsn redundancy statistics

To clear the data counters associated with the PDSN session redundancy to their initial values, use the **clear cdma pdsn redundancy statistics** command in privileged EXEC mode.

**clear cdma pdsn redundancy statistics**

---

**Syntax Description** There are no keywords or arguments for this command.

---

**Defaults** There are no default values for this command.

---

**Command Modes** EXEC mode

---

Command History	Release	Modification
	12.3(14)YX	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

---

---

**Examples** The following example illustrates the **clear cdma pdsn redundancy statistics** command”

```
router#clear cdma pdsn redundancy statistics
```

# clear cdma pdsn selection

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

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

<b>Syntax Description</b>	<i>psdn ip-addr</i>	(Optional) IP address of the PDSN selection session table to be cleared.
	<i>msid number</i>	(Optional) Identification of the MSID to be cleared.

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example clears the pdsn selection session table for PDSN 5.5.5.5:
	<pre>clear cdma pdsn selection pdsn 5.5.5.5</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cdma pdsn selection session-table-size</b>	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

<b>all</b>	Keyword to clear all sessions on a given PDSN.
<b>pcf</b> <i>ip_addr</i>	IP address of the PCF sessions that are to be cleared.
<b>msid</b> <i>number</i>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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
<b>show cdma pdsn session</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

### 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
```

## ■ clear cdma pdsn statistics

```

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
<b>show cdma pdsn statistics</b>	Displays PDSN statistics.

# clear ip mobile visitor

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

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


<b>Syntax Description</b>	<i>ip-address</i>	(Optional) IP address. If not specified, visitor information will be removed for all addresses.
	<b>nai</b> <i>string</i>	(Optional) Network access identifier (NAI) of the mobile node.
	<b>session-id</b> <i>string</i>	(Optional) Session identifier. The string value must be fewer than 25 characters in length.
	<i>ip-address</i>	(Optional) IP address associated with the NAI.

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.
	12.2(2)XC	The <b>nai</b> keyword and associated variables were added.
	12.2(13)T	The <b>nai</b> keyword and associated variables were integrated into Cisco IOS Release 12.2(13)T.
	12.3(4)T	The <b>session-id</b> keyword was added.

<b>Usage Guidelines</b>	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 Address Resolution Protocol (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.
	If the <b>nai</b> <i>string</i> <b>session-id</b> <i>string</i> option is specified, only the visitor entry with that session identifier is cleared. If the <b>session-id</b> keyword is not specified, all visitor entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the <b>session-id</b> <i>string</i> value by using the <b>show ip mobile visitor</b> command.
	Use this command with care because it may terminate any sessions used by the mobile node. After you use this command, the visitor will need to reregister to continue roaming.

<b>Examples</b>	The following example administratively stops visitor 172.21.58.16 from visiting:
	Router# <b>clear ip mobile visitor 172.21.58.16</b>

 clear ip mobile visitor**Related Commands**

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



# crypto map (global IPsec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, 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**]  
[**profile** *profile-name*]

**crypto map** *map-name* [**client-accounting-list** *aaalist*]

**crypto map** *map-name seq-num* [**gdoi**]

**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

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>seq-num</i>	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the “Usage Guidelines” section.
<b>ipsec-manual</b>	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
<b>ipsec-isakmp</b>	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
<b>dynamic</b>	(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.
<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
<b>discover</b>	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
<b>profile</b>	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
<i>profile-name</i>	(Optional) Name of the crypto profile being created.
<b>client-accounting-list</b>	(Optional) Designates a client accounting list.
<i>aaalist</i>	(Optional) List name.
<b>gdoi</b>	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

**Command Default** No crypto maps exist.  
Peer discovery is not enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	11.3T	The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <b>ipsec-manual</b></li> <li>• <b>ipsec-isakmp</b></li> <li>• <b>dynamic</b></li> <li>• <i>dynamic-map-name</i></li> </ul>
	12.0(5)T	The <b>discover</b> keyword was added to support Tunnel Endpoint Discovery (TED).
	12.2(4)T	The <b>profile</b> <i>profile-name</i> keyword and argument combination was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
	12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
	12.2(15)T	The <b>client-accounting-list</b> <i>aaalist</i> keyword and argument combination was added.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
	12.4(6)T	The <b>gdoi</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB without support for the <b>gdoi</b> keyword.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After 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, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; 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.

#### Crypto Map Functions

Crypto maps provide two functions: filtering and 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 define the following:

- What traffic should be protected
- To which IPsec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and SAs should be used or managed (or what the keys are, if IKE is not used)

### Multiple Crypto Map 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* argument but the same *map-name* argument. 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 differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

### Sequence Numbers

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, consider 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 serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement 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 SAs 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.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to 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.

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving it the highest *seq-num* value 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** (global IPsec) command using the **dynamic** keyword.

### TED

TED is an enhancement to the IPsec feature. Defining a dynamic crypto map allows you to dynamically determine an IPsec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPsec peer for secure IPsec communications.

Dynamic TED helps to simplify IPsec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPsec transforms that are required.

**Note**

TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPsec. Thus, TED does not improve the scalability of IPsec (in terms of performance or the number of peers or tunnels).

**Crypto Map Profiles**

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the L2TP Security feature. The relevant SAs in the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

**Note**

The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

**Examples**

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

```
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 SAs are manually established:

```
crypto transform-set someaset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someaset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 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 SAs 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 SA 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 SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (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 any access list 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.

```
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 TED on a Cisco router:

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

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPsec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example configures a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
 set group diffint
```

## Related Commands

Command	Description
<b>crypto dynamic-map</b>	Creates a dynamic crypto map entry and enters crypto map configuration command mode.
<b>crypto isakmp profile</b>	Audits IPsec user sessions.
<b>crypto map (interface IPsec)</b>	Applies a previously defined crypto map set to an interface.
<b>crypto map local-address</b>	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
<b>match address (IPsec)</b>	Specifies an extended access list for a crypto map entry.
<b>set peer (IPsec)</b>	Specifies an IPsec peer in a crypto map entry.
<b>set pfs</b>	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
<b>set session-key</b>	Specifies the IPsec session keys within a crypto map entry.
<b>set transform-set</b>	Specifies which transform sets can be used with the crypto map entry.
<b>show crypto map (IPsec)</b>	Displays the crypto map configuration.

# crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPSec traffic, use the **crypto map local-address** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

**crypto map** *map-name* **local-address** *interface-id*

**no crypto map** *map-name* **local-address**

## Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>interface-id</i>	The identifying interface that should be used by the router to identify itself to remote peers.  If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Usage Guidelines

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you are using the second interface as redundant to the first interface, it could be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

This command allows a peer to establish a single security association (and use a single local IP address) that is shared by the two redundant interfaces.

If applying the same crypto map set to more than one interface, the default behavior is as follows:

- Each interface will have its own security association database.
- The IP address of the local interface will be used as the local address for IPSec traffic originating from/destined to that interface.

However, if you use a local-address for that crypto map set, it has multiple effects:

- Only one IPSec security association database will be established and shared for traffic through both interfaces.
- The IP address of the specified interface will be used as the local address for IPSec (and IKE) traffic originating from or destined to that interface.

One suggestion is to use a loopback interface as the referenced local address interface, because the loopback interface never goes down.

## Examples

The following example assigns crypto map set “mymap” to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic will be evaluated against the all the crypto maps in the “mymap” set. When traffic through either interface matches an access list in one of the “mymap” crypto maps, a security association will be established. This same security association will then apply to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec will use on both interfaces will be the IP address of interface loopback0.

```
interface S0
  crypto map mymap

interface S1
  crypto map mymap

crypto map mymap local-address loopback0
```

## Related Commands

Command	Description
<b>crypto map (interface IPSec)</b>	Applies a previously defined crypto map set to an interface.

# debug cdma pdsn a10 gre

To display debug messages for A10 Generic Routing Encapsulation (GRE) interface errors, events, and packets, use the **debug cdma pdsn a10 gre** command in privileged EXEC mode. To disable debugging output, 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

<b>errors</b>	(Optional) Displays A10 GRE errors.
<b>events</b>	(Optional) Displays A10 GRE events.
<b>packets</b>	(Optional) Displays transmitted or received A10 GRE packets.
<b>tunnel-key</b> <i>key</i>	(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 Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The <b>tunnel-key</b> keyword was added and the existing keywords were made optional.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## 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 Point-to-Point protocol (PPP) interface errors, events, and packets, use the **debug cdma pdsn a10 ppp** command in privileged EXEC mode. To disable debugging output, 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

<b>errors</b>	(Optional) Displays A10 PPP errors.
<b>events</b>	(Optional) Displays A10 PPP events.
<b>packets</b>	(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 Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	Keywords were made optional.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## 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 debugging output, 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

<b>errors</b>	(Optional) Displays A11 protocol errors.
<b>events</b>	(Optional) Displays A11 events.
<b>packets</b>	(Optional) Displays transmitted or received packets.
<i>mnid</i>	(Optional) Specifies the ID of the mobile station.

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The <i>mnid</i> argument was added and the existing keywords were made optional.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## 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 000000000000001
(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=0000000000000001
1d21h:CDMA-RP:(req) rp_req_create, 5.0.0.2-4.0.0.1-1 imsi=0000000000000001
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 0000000000000001

CDMA PDSN A11 events debugging is on for mnid 0000000000000001

Router#

```
*Mar 1 03:15:32.507:CDMA-RP:len=8, 01-00-00-00-00-00-10 convert to 0000000000000001 (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=0000000000000001
*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=0000000000000001
*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, 01-00-00-00-00-00-10 convert to 0000000000000001 (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=0000000000000001
*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=0000000000000001
*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 0000000000000001**

Router# **show debug**

CDMA:

CDMA PDSN A11 events debugging is on for mnid 0000000000000001

Router#

```
*Mar 1 03:09:34.339:CDMA-RP:len=8, 01-00-00-00-00-00-10 convert to 0000000000000001 (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=AF3BFCCE-DC9FC751
IMSI=0000000000000001
*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=0000000000000001
*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#

## ■ debug cdma pdsn a11

```
*Mar 1 03:10:00.575:CDMA-RP:len=8, 01-00-00-00-00-00-10 convert to 0000000000000001 (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=0000000000000001
*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=0000000000000001
*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 0000000000000001**

Router# **show debug**

CDMA:

CDMA PDSN A11 packet debugging is on for mnid 0000000000000001

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. To disable debugging output, use the **no** form of this command.

**debug cdma pdsn accounting**

**no cdma pdsn accounting**

**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 introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**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 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]
```

**debug cdma pdsn accounting**

```
*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. To disable debugging output, use the **no** form of this command.

**debug cdma pdsn accounting flow**

**no debug cdma pdsn accounting flow**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following is sample output from the <b>debug cdma pdsn accounting flow</b> command:
-----------------	---

```
Router# debug cdma pdsn accounting 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 debugging output, use the **no** form of this command.

**debug cdma pdsn accounting time-of-day**

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

---

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

---

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

---

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

---

---

<b>Examples</b>	The following is sample output from the <b>debug cdma pdsn accounting time-of-day</b> 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, and packets received, use the **debug cdma pdsn cluster** command in privileged EXEC mode. To disable debugging output, 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

<b>message</b>	Displays cluster messages for errors, events and packets received.
<b>redundancy</b>	Displays redundancy information for errors, events, and sent or received packets.
<b>error</b>	Displays either cluster or redundancy error messages.
<b>events</b>	Displays either all cluster or all redundancy events.
<b>packets</b>	Displays all transmitted or received cluster or redundancy packets.

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This debug is *only* allowed on PDSN c6-mz images, and helps to monitor prepaid 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 ipv6

To display IPV6 error or event messages, use the **debug cdma pdsn IPV6** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn ipv6**

**no debug cdma pdsn ipv6**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

No default behavior or values.

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

The following example illustrates the **debug cdma pdsn ipv6** command:

```
Router# debug cdma pdsn ipv6
```

# debug cdma pdsn prepaid

To display debug messages about prepaid flow, use the **debug cdma pdsn prepaid** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cdma pdsn prepaid**

**no debug cdma pdsn prepaid**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(8)BY	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**Usage Guidelines** This debug is *only* allowed on PDSN c6-mz images, and helps to monitor 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 qos

To display debug messages about quality of service features, use the **debug cdma pdsn qos** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

**debug cdma pdsn qos**

**no debug cdma pdsn qos**

---

## Syntax Description

There are no arguments or keywords for this command.

---

## Defaults

There are no default values for this command.

---

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

---

## Examples

There are currently no sample outputs for this command.

# debug cdma pdsn radius disconnect nai

To display debug messages about RADIUS disconnect functions, use the **debug cdma pdsn radius disconnect nai** command in Privileged EXEC mode. Use the **no** form of the command to disable debug messages.

**debug cdma pdsn radius disconnect nai**

**no debug cdma pdsn radius disconnect nai**

## Syntax Description

There are no keywords or arguments for this command.

## Defaults

There are no default values for this command.

## Command Modes

EXEC mode

## Command History

Release	Modification
12.3(11)YF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

## Examples

Here is sample output for the **debug cdma pdsn radius disconnect nai** command:

```
Jan 5 12:17:59.671: CDMA-POD: POD request received
Jan 5 12:17:59.671: CDMA-POD: NAI in POD request : mwtr-mip-sa2sp1-user1@ispxyz.com
Jan 5 12:17:59.671: CDMA-POD: IMSI in POD request : 00000000000201
Jan 5 12:17:59.671: CDMA-POD: Delete flow for NAI: mwtr-mip-sa2sp1-user1@ispxyz.com
Jan 5 12:17:59.671: CDMA-POD: Delete flow for NAI: mwtr-mip-sa2sp1-user1@ispxyz.com
```

# debug cdma pdsn redundancy attributes

To debug the PDSN session redundancy attributes, use the **debug cdma pdsn redundancy attributes** command.

**debug cdma pdsn redundancy attributes**

---

**Syntax Description**      There are no keywords or arguments for this command.

---

**Defaults**                      There are no default values for this command.

---

**Command Modes**            EXEC mode

---

Command History	Release	Modification
	12.3(14)YX	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

---

# debug cdma pdsn redundancy errors

To debug the PDSN-SR redundancy aspect of errors, use the **debug cdma pdsn redundancy errors** command.

**debug cdma pdsn redundancy errors**

## Syntax Description

There are no keywords or arguments for this command.

## Defaults

There are no default values for this command.

## Command Modes

EXEC mode

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

# debug cdma pdsn redundancy events

To debug events for PDSN session redundancy, use the **debug cdma pdsn redundancy events** command.

## debug cdma pdsn redundancy events

---

**Syntax Description**      There are no keywords or arguments for this command.

---

**Defaults**                There are no default values for this command.

---

**Command Modes**        EXEC mode

---

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

---



# debug cdma pdsn redundancy packets

To debug and collect any data pertaining to PDSN-SR, use the **debug cdma pdsn redundancy packets** command.

**debug cdma pdsn redundancy packets**

**Syntax Description** There are no keywords or arguments for this command.

**Defaults** There are no default values for this command.

**Command Modes** EXEC mode

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

# 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 debugging output, use the **no** form of this command.

**debug cdma pdsn resource-manager [error | events]**

**no debug cdma pdsn resource-manager [error | events]**

## Syntax Description

<b>errors</b>	Displays Packet Data Service node (PDSN) resource manager errors.
<b>events</b>	Displays PDSN resource manager events.

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Examples

The following is sample output from the **debug cdma pds 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 Packet Data Serving Node (PDSN) selection feature, use the **debug cdma pdsn selection** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cdma pdsn selection {errors | events | packets}**

**no debug cdma pdsn selection {errors | events | packets}**

## Syntax Description

<b>errors</b>	Displays PDSN selection errors.
<b>events</b>	Displays PDSN selection events.
<b>packets</b>	Displays transmitted or received packets.

## Defaults

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## 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 debugging output, 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 Modes** Privileged EXEC

---

Command History	Release	Modification
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

---



---

**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** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug cdma pdsn session [errors | events ]**

**no debug cdma pdsn session [errors | events ]**

## Syntax Description

<b>errors</b>	(Optional) Displays session protocol errors.
<b>events</b>	(Optional) Displays session events.

## Defaults

If the command is entered without any optional keywords, all of the types of debug information are enabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	Keywords were made optional.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## 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 condition

To filter debugging output for certain **debug** commands on the basis of specified conditions, use the **debug condition** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

**debug condition** {**called** *dial-string* | **caller** *dial-string* | **calling** *tid/imsi string* | **domain** *domain-name* | **ip** *ip-address* | **mac-address** *hexadecimal-MAC-address* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-id** *session-number* | **username** *username* | **vcid** *vc-id*}

**no debug condition** {*condition-id* | **all**}

Syntax Description		
<b>called</b> <i>dial-string</i>		Filters output on the basis of the called party number.
<b>caller</b> <i>dial-string</i>		Filters output on the basis of the calling party number.
<b>calling</b> <i>tid/imsi string</i>		Filters debug messages for general packet radio service (GPRS) tunneling protocol (GTP) processing on the gateway GPRS support node (GGSN) based on the tunnel identifier (TID) or international mobile system identifier (IMSI) in a Packet Data Protocol (PDP) Context Create Request message.
<b>domain</b> <i>domain-name</i>		Filters output on the basis of the specified domain.
<b>ip</b> <i>ip-address</i>		Filters output on the basis of the specified IP address.
<b>mac-address</b> <i>hexadecimal-MAC-address</i>		Filters messages on the specified MAC address.
<b>portbundle ip</b> <i>IP-address</i>		Filters output on the basis of the port-bundle host key (PBHK) that uniquely identifies the session.
<b>bundle</b> <i>bundle-number</i>		Specifies the port bundle.
<b>session-id</b> <i>session-number</i>		Filters output on the specified Intelligent Service Architecture (ISA) session identifier.
<b>username</b> <i>username</i>		Filters output on the basis of the specified username.
<b>vcid</b> <i>vc-id</i>		Filters output on the basis of the specified VC ID.
<i>condition-id</i>		Removes the condition indicated.
<b>all</b>		Removes all debugging conditions, and conditions specified by the <b>debug condition interface</b> command. Use this keyword to disable conditional debugging and reenable debugging for all interfaces.

**Defaults** All debugging messages for enabled protocol-specific **debug** commands are generated.

**Command Modes** Privileged EXEC

## Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. This command was updated with the <b>void</b> and <b>ip</b> keywords to support the debugging of Any Transport over MPLS (AToM) messages.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)XB	This command was introduced on the GGSN.
12.3(8)T	The <b>calling</b> keyword and <i>tid/imsi string</i> argument were added.
12.2(28)SB	The ability to filter output on the following conditions was added: domain, MAC address, PBHK, and ISA session ID.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

Use the **debug condition** command to restrict the debug output for some commands. If any **debug condition** commands are enabled, output is generated only for interfaces associated with the specified keyword. In addition, this command enables debugging output for conditional debugging events. Messages are displayed as different interfaces meet specific conditions.

If multiple **debug condition** commands are enabled, output is displayed if at least one condition matches. All the conditions do not need to match.

The **no** form of this command removes the debug condition specified by the condition identifier. The condition identifier is displayed after you use a **debug condition** command or in the output of the **show debug condition** command. If the last condition is removed, debugging output resumes for all interfaces. You will be asked for confirmation before removing the last condition or all conditions.

Not all debugging output is affected by the **debug condition** command. Some commands generate output whenever they are enabled, regardless of whether they meet any conditions.

The following components are supported for Intelligent Service Architecture (ISA) distributed conditional debugging:

- Authentication, authorization, and accounting (AAA) and RADIUS
- ATM components
- Feature Manager
- Policy Manager
- PPP
- PPP over Ethernet (PPPoE)
- Session Manager
- Virtual Private Dialup Network (VPDN)

Ensure that you enable TID/IMSI-based conditional debugging by entering **debug condition calling** before configuring **debug gprs gtp** and **debug gprs charging**. In addition, ensure that you disable the **debug gprs gtp** and **debug gprs charging** commands using the **no debug all** command before disabling conditional debugging using the **no debug condition** command. This will prevent a flood of debugging messages when you disable conditional debugging.

## Examples

### Example 1

In the following example, the router displays debugging messages only for interfaces that use a username of “user1”. The condition identifier displayed after the command is entered identifies this particular condition.

```
Router# debug condition username user1
```

```
Condition 1 set
```

### Example 2

The following example specifies that the router should display debugging messages only for VC 1000:

```
Router# debug condition vcid 1000
```

```
Condition 1 set
```

```
01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1
```

```
01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1
```

The following example enables other debugging commands. These debugging commands will only display information for VC 1000.

```
Router# debug mpls l2transport vc event
```

```
AToM vc event debugging is on
```

```
Router# debug mpls l2transport vc fsm
```

```
AToM vc fsm debugging is on
```

The following commands shut down the interface on which VC 1000 is established.

```
Router(config)# interface s3/1/0
```

```
Router(config-if)# shut
```

The debugging output shows the change to the interface where VC 1000 is established.

```
01:15:59: AToM MGR [13.13.13.13, 1000]: Event local down, state changed from established to remote ready
```

```
01:15:59: AToM MGR [13.13.13.13, 1000]: Local end down, vc is down
```

```
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing imposition update, vc_handle 6227BCF0, update_action 0, remote_vc_label 18
```

```
01:15:59: AToM SMGR [13.13.13.13, 1000]: Imposition Disabled
```

```
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing disposition update, vc_handle 6227BCF0, update_action 0, local_vc_label 755
```

```
01:16:01:%LINK-5-CHANGED: Interface Serial3/1/0, changed state to administratively down
```

```
01:16:02:%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1/0, changed state to down
```

## Related Commands

Command	Description
<b>debug condition interface</b>	Limits output for some debugging commands based on the interfaces.



# debug ip mobile

To display IP mobility activities, use the **debug ip mobile** command in privileged EXEC mode.

**debug ip mobile** [**advertise** | **host** [*access-list-number*] | **local-area** | **redundancy** | **udp-tunneling**]

## Syntax Description

<b>advertise</b>	(Optional) Advertisement information.
<b>host</b>	(Optional) The mobile node host.
<i>access-list-number</i>	(Optional) The number of an IP access list.
<b>local-area</b>	(Optional) The local area.
<b>redundancy</b>	(Optional) Redundancy activities.
<b>udp-tunneling</b>	(Optional) User Datagram Protocol (UDP) tunneling activities.

## Defaults

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The <b>standby</b> keyword was added.
12.2(8)T	The <b>standby</b> keyword was replaced by the <b>redundancy</b> keyword.
12.2(13)T	This command was enhanced to display information about foreign agent reverse tunnels and the mobile networks attached to the mobile router.
12.3(8)T	The <b>udp-tunneling</b> keyword was added and the command was enhanced to display information about NAT traversal using UDP tunneling.
12.3(7)XJ	This command was enhanced to include the Resource Management capability.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

Use the **debug ip mobile redundancy** command to troubleshoot redundancy problems.

No per-user debugging output is shown for mobile nodes using the network access identifier (NAI) for the **debug ip mobile host** command. Debugging of specific mobile nodes using an IP address is possible through the access list.

## Examples

The following is sample output from the **debug ip mobile** command when foreign agent reverse tunneling is enabled:

```
MobileIP:MN 14.0.0.30 deleted from ReverseTunnelTable of Ethernet2/1(Entries 0)
```

The following is sample output from the **debug ip mobile advertise** command:

```
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 )
FA Challenge value:769C808D
```

[Table 1](#) describes the significant fields shown in the display.

**Table 1** *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; lowercase 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.
FA Challenge value	Foreign Agent challenge value (randomly generated by the foreign agent.)

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 sbdmgyT
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
```

The following is sample output from the **debug ip mobile redundancy** command. In this example, the active home agent receives a registration request from mobile node 20.0.0.2 and sends a binding update to peer home agent 1.0.0.2:

```
MobileIP:MN 20.0.0.2 - sent BindUpd to HA 1.0.0.2 HAA 20.0.0.1
MobileIP:HA standby maint started - cnt 1
MobileIP:MN 20.0.0.2 - sent BindUpd id 3780410816 cnt 0 elapsed 0
adjust -0 to HA 1.0.0.2 in grp 1.0.0.10 HAA 20.0.0.1
```

In this example, the standby home agent receives a binding update for mobile node 20.0.0.2 sent by the active home agent:

```
MobileIP:MN 20.0.0.2 - HA rcv BindUpd from 1.0.0.3 HAA 20.0.0.1
```

The following is sample output from the **debug ip mobile udp-tunneling** command and displays the registration, authentication, and establishment of UDP tunneling of a mobile node (MN) with a foreign agent (FA):

```
Dec 31 12:34:25.707: UDP: rcvd src=10.10.10.10(434),dst=10.30.30.1(434), length=54
Dec 31 12:34:25.707: MobileIP: ParseRegExt type MHAE(32) addr 2000FEEC end 2000FF02
Dec 31 12:34:25.707: MobileIP: ParseRegExt skipping 10 to next
Dec 31 12:34:25.707: MobileIP: FA rcv registration for MN 10.10.10.10 on Ethernet2/2 using
COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options sbdmg-T-identification
C1BC0D4FB01AC0D8
Dec 31 12:34:25.707: MobileIP: Ethernet2/2 glean 10.10.10.10 accepted
Dec 31 12:34:25.707: MobileIP: Registration request byte count = 74
Dec 31 12:34:25.707: MobileIP: FA queued MN 10.10.10.10 in register table
Dec 31 12:34:25.707: MobileIP: Visitor registration timer started for MN 10.10.10.10,
lifetime 120
Dec 31 12:34:25.707: MobileIP: Adding UDP Tunnel req extension
Dec 31 12:34:25.707: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.707: MobileIP: MN 10.10.10.10 FHAE added to HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.707: MobileIP: FA forwarded registration for MN 10.10.10.10 to HA
10.10.10.100
Dec 31 12:34:25.715: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=94
Dec 31 12:34:25.715: MobileIP: ParseRegExt type NVSE(134) addr 20010B28 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MN-config NVSE(14) subtype 1 (MN prefix
length) prefix length (24)
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 12 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MHAE(32) addr 20010B36 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 10 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 20010B4C end 20010B6A
Dec 31 12:34:25.715: Parsing UDP Tunnel Reply Extension - length 6
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type FHAE(34) addr 20010B54 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: FA rcv accept (0) reply for MN 10.10.10.10 on Ethernet2/3
using HA 10.10.10.100 lifetime 65535
Dec 31 12:34:25.719: MobileIP: Authenticating HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.719: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.719: MobileIP: Authenticated HA 10.10.10.100 using SPI 1000 and 16 byte
key
Dec 31 12:34:25.719: MobileIP: HA accepts UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Update visitor table for MN 10.10.10.10
Dec 31 12:34:25.719: MobileIP: Enabling UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.30.30.1 dst
10.10.10.100
Dec 31 12:34:25.719: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.30.30.1:0 -
10.10.10.100:0 with keep-alive 30
Dec 31 12:34:25.719: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:25.719: MobileIP: ARP entry for MN 10.10.10.10 using 10.10.10.10 inserted on
Ethernet2/2
Dec 31 12:34:25.719: MobileIP: FA route add 10.10.10.10 successful. Code = 0
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 added to ReverseTunnelTable of Ethernet2/2
(Entries 1)
Dec 31 12:34:25.719: MobileIP: FA dequeued MN 10.10.10.10 from register table
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 using 10.10.10.10 visiting on Ethernet2/2
Dec 31 12:34:25.719: MobileIP: Reply in for MN 10.10.10.10 using 10.10.10.10, accepted
Dec 31 12:34:25.719: MobileIP: registration reply byte count = 84
Dec 31 12:34:25.719: MobileIP: FA forwarding reply to MN 10.10.10.10 (10.10.10.10 mac
0060.70ca.f021)
Dec 31 12:34:26.095: MobileIP: agent advertisement byte count = 48
Dec 31 12:34:26.095: MobileIP: Agent advertisement sent out Ethernet2/2: type=16, len=10,
seq=55, lifetime=65535, flags=0x1580(rbhFmG-TU),
Dec 31 12:34:26.095: Care-of address: 10.30.30.1
Dec 31 12:34:26.719: MobileIP: swif coming up Tunnel0
```

```
!
Dec 31 12:34:35.719: UDP: sent src=10.30.30.1(434), dst=10.10.10.100(434)
Dec 31 12:34:35.719: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=32d0
```

The following is sample output from the **debug ip mobile udp-tunneling** command and displays the registration, authentication, and establishment of UDP tunneling of a MN with a home agent (HA):

```
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type UDPTUNREQE(144) addr 2001E762 end 2001E780
Dec 31 12:34:26.167: MobileIP: Parsing UDP Tunnel Request Extension - length 6
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type FHAE(34) addr 2001E76A end 2001E780
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: HA 167 rcv registration for MN 10.10.10.10 on Ethernet2/1
    using HomeAddr 10.10.10.10 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options
    sbdmg-T-identification C1BC0D4FB01AC0D8
Dec 31 12:34:26.167: MobileIP: NAT detected SRC:10.10.10.50 COA: 10.30.30.1
Dec 31 12:34:26.167: MobileIP: UDP Tunnel Request accepted 10.10.10.50:434
Dec 31 12:34:26.167: MobileIP: Authenticating FA 10.30.30.1 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated FA 10.30.30.1 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticating MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated MN 10.10.10.10 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Mobility binding for MN 10.10.10.10 created
Dec 31 12:34:26.167: MobileIP: NAT detected for MN 10.10.10.10. Terminating tunnel on
    10.10.10.50
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.10.10.100 dst
    10.10.10.50
Dec 31 12:34:26.167: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.10.10.100:0 -
    10.10.10.50:0 with keep-alive 30
Dec 31 12:34:26.167: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 Insert route for 10.10.10.10/255.255.255.255
    via gateway 10.10.10.50 on Tunnel0
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 is now roaming
Dec 31 12:34:26.171: MobileIP: Gratuitous ARPs sent for MN 10.10.10.10 MAC 0002.fca5.bc39
Dec 31 12:34:26.171: MobileIP: Mask for address is 24
Dec 31 12:34:26.171: MobileIP: HA accepts registration from MN 10.10.10.10
Dec 31 12:34:26.171: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Dec 31 12:34:26.171: MobileIP: Composed mobile network extension length:0
Dec 31 12:34:26.171: MobileIP: Added prefix length vse in reply
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 - HA sent reply to 10.10.10.50
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: ParseRegExt type CVSE(38) addr 2000128C end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HA red. version CVSE(6)
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 8 to next
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HHAE(35) addr 20001298 end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.175: MobileIP: Authenticating HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authenticated HA 10.10.10.3 using SPI 1000 and 16 byte key
Dec 31 12:34:27.167: MobileIP: swif coming up Tunnel0d0
```

# debug ip mobile cdma ipsec

To enable debugging on the IS835 IPsec feature, use the **debug ip mobile cdma ipsec** command in privileged EXEC mode. To disable debugging for this feature, use the **no** form of the command.

**debug ip mobile cdma ipsec**

**no debug ip mobile cdma ipsec**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

---

---

**Examples** The following example illustrates how to issue the **debug ip mobile cdma ipsec** command:

```
router# debug ip mobile csma ipsec
```

# interface cdma-lx

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

**interface cdma-lx1**

**no interface cdma-lx1**

Syntax Description	<i>lx1</i> 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

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: <pre>interface cdma-lx1  ip address 1.1.1.1 255.255.0.0</pre>
----------	--

Related Commands	Command	Description
	<b>show interfaces</b>	Displays statistics about the network interfaces.

# ip mobile authentication ignore-spi

To enable the home agent or foreign agent to accept RFC-2002 based mobile nodes or foreign agents that don't include the security parameter index (SPI) in the authentication extension of the registration message, use the **ip mobile authentication ignore-spi** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile authentication ignore-spi**

**no ip mobile authentication ignore-spi**

**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(8)BY	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**Usage Guidelines**

Cisco IOS software supports the Mobile-Home Authentication Extension (MHAE). All registration messages between a mobile and a home agent include a mandatory authentication extension.

In RFC 2002, the SPI field was not included to calculate the authenticator value in the authentication extension of the registration message. In RFC 3220 and 3344, the SPI field in the authentication extension is used as part of the data over which the authentication algorithm must be computed.

The command turns off authentication and allows an RFC-2002 based mobile node and foreign agent to register with the home agent even though the SPI field is not included in the authentication extension of the registration message. The foreign agent will accept both RFC 2002 and RFC 3220/3344 based visitors and the home agent will accept both RFC 2002 and RFC 3220/3344 based mobile nodes and foreign agents.

**Examples** The following example allows the home agent to accept registration messages without the SPI in the authentication extension:

```
ip mobile authentication ignore-spi
```

# ip mobile bindupdate

To enable a home agent to send a binding update message to a foreign agent, use the **ip mobile bindupdate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile bindupdate** [**acknowledge**] [**maximum seconds**] [**minimum seconds**] [**retry number**]

**no ip mobile bindupdate** [**acknowledge**] [**maximum seconds**] [**minimum seconds**] [**retry number**]

## Syntax Description

<b>acknowledge</b>	(Optional). Indicates that the foreign agent must acknowledge receipt of a binding update message.
<b>maximum seconds</b>	(Optional) Maximum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 10 seconds.
<b>minimum seconds</b>	(Optional) Minimum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 1 second.
<b>retry number</b>	(Optional) Number of times to retry sending the binding update message. Retransmission stops after the maximum number of retries are attempted. The range is from 1 to 4; the default retry is 4.

## Defaults

**maximum seconds**: 10 seconds  
**minimum seconds**: 1 second  
**retry number**: 4 retries

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This command enables the home agent to send a binding update message to the previous foreign agent when the mobile node moves to a new care-of address. The binding update message informs the foreign agent that a mobile node has moved and it can reclaim resources associated with that mobile node such as a visitor entry or visitor route.

Typically, resources on the foreign agent are not reclaimed until the mobility binding lifetime expires for that mobile node. By using this command, the foreign agent does not have to wait to reclaim resources used by the mobile node when that mobile node is no longer associated with the foreign agent.

Without this command configured, when a mobile node moves from foreign agent 1 to foreign agent 2 or when the home agent removes the binding, foreign agent 1 does not know that the mobile node has moved and the resources on foreign agent 1 associated with the mobile node will not be cleared until the lifetime expires for the mobile node.



If the **acknowledge** keyword is specified, the home agent periodically retransmits a binding update message until it receives a binding acknowledgement from the foreign agent or until the number of retries is exceeded.

The home agent and foreign agent must share a security association. The binding update message from the home agent and the binding update acknowledgement from the foreign agent must contain a FHAE (Foreign-Home Authentication Extension). If the FHAE is not configured on the home agent with the **ip mobile secure** command, the home agent will not send a binding update message even if the **ip mobile bindupdate** command is configured.

---

### Examples

The following example configures the home agent to wait a maximum of 8 seconds before retransmitting a binding update message to a foreign agent. The foreign agent must send an acknowledgement of this binding update message upon receipt.

```
ip mobile bindupdate acknowledge maximum 8 retry 3
ip mobile secure foreign-agent 10.31.1.1 spi 100 key hex 23456781234567812345678123456781
```

The following example configures the security association on the foreign agent. Without the security association configured on the home agent and the foreign agent, the binding update message would not be sent or processed.

```
ip mobile secure home-agent 172.31.10.1 spi 100 key hex 23456781234567812345678123456781
```

# ip mobile cdma imsi dynamic

To enable the PDSN to delete the first call session for dynamic home address cases (1x-RTT to EVDO handoff where IMSI changes during the handoff), and allow the new session to come up, use the **ip mobile cdma imsi dynamic** command in global configuration mode. Use the **no** form of the command to disable this feature.

**ip mobile cdma imsi dynamic**

**no ip mobile cdma imsi dynamic**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)YF3	This command was introduced.
12.4(11)T	This command was integrated into the Cisco IOS 12.4(11)T release.

## Examples

The following example illustrates how to issue the **ip mobile cdma imsi dynamic** command:

```
router(config)# ip mobile cdma imsi dynamic
```

# ip mobile cdma ipsec

To enable IS835 IPSec security, use the **ip mobile cdma ipsec** command in global configuration mode. Use the **no** form of the command to disable this feature.

**ip mobile cdma ipsec**

**no ip mobile cdma ipsec**

## Syntax Description

There are no arguments or keywords for this command.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into the Cisco IOS 12.4(11)T release.

## Usage Guidelines

This command is only present in crypto images for the 7200, and non-crypto images for the MWAM.

## Examples

The following example illustrates how to enable IS835 IPsec on the PDSN:

```
router# ip mobile cdma ipsec
```

# ip mobile foreign-agent

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

**ip mobile foreign-agent** [*care-of interface* {**interface-only**} [**transmit-only**] | **reg-wait seconds** | **local-timezone** | **reverse-tunnel private-address**]

**no ip mobile foreign-agent** { *care-of interface* [**interface-only**] [**transmit-only**] | **reg-wait** | **local-timezone** | **reverse-tunnel private-address** }

Syntax Description		
<b>care-of interface</b>		IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured. At least one care-of address must be configured for foreign agent service.
<b>interface-only</b>		(Optional) Enables the specified interface to advertise only its own address as the care-of address. Other interfaces configured for foreign agent service will not advertise this care-of address.
<b>transmit-only</b>		(Optional) Informs Mobile IP that the <i>interface</i> is being used on a unidirectional link and will transmit only. This interface will be used as the source interface for this care-of address for any registration request received on another interface. Only serial interfaces can be configured as transmit only.
<b>reg-wait seconds</b>		(Optional) Pending registration expires after <i>the specified number of</i> seconds if no reply is received. Range is from 5 to 600 seconds. Default is 15.
<b>local-timezone</b>		(Optional) Uses the local time zone to generate identification fields.
<b>reverse-tunnel private-address</b>		(Optional) Forces a mobile node with a private address to register with reverse tunneling.

**Defaults** **reg-wait seconds:** 15

**Command Modes** Global configuration

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(13)T	The <b>interface-only</b> , <b>transmit-only</b> , and <b>reverse-tunnel private-address</b> keywords were added.
	12.2(3)XC	The <b>local-timezone</b> keyword was added.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**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 a 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 an interface or when no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated. The registration bitflag is handled as described in Table 2. 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 3). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command).

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 the sending of 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 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 address 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.

The **interface-only** and **transmit-only** keywords are used in an asymmetric link environment, such as satellite communications, where separate uplinks and downlinks exist. The **ip mobile foreign-agent care-of interface interface-only** command enables the specified interface to advertise only its own address as the care-of address. All other care-of addresses are not advertised. Other foreign agent interfaces configured for foreign-service will not advertise interface-only care-of addresses. The **ip mobile foreign-agent care-of interface transmit-only** command informs Mobile IP that the interface acts as an uplink. Registration requests and replies received for this care-of address are treated as transmit-only. This interface will not hear any solicitations. Any care-of address can be configured with the **interface-only** keyword, but only serial interfaces can be configured with the **transmit-only** keyword.

Use the **reverse-tunnel private-address** keywords to force a mobile node with a private address to register with reverse tunnel. Private addresses are IP addresses in the following ranges:

- 10.0.0.0 to 10.255.255.255 (10/8 prefix)
- 172.16.0.0 to 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Table 2 lists mobile node registration request service bitflags.

**Table 2 Mobile Node Registration Request Service 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.
r	Sent as zero; ignored on reception. Do not allocate for any other uses.
V	Reserved.
T	Deny if reverse tunneling is disabled on the foreign agent.
reserved	Deny request. Reserved bit must not be set.

Table 3 lists foreign agent reply codes.

**Table 3 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.
72	Requested encapsulation is unavailable.
74	Reverse tunnel unsupported.
75	Reverse tunnel is mandatory and T bit is not set.
76	Mobile node too distant.
77	Invalid care-of address.
78	Registration timeout.
79	Delivery style not supported.
80	Home network unreachable (ICMP error received).
81	Home agent host unreachable (ICMP error received).
82	Home agent port unreachable (ICMP error received).
88	Home agent unreachable (other ICMP error received).
98	Missing home agent.
99	Missing home agent address.

**Table 3 Foreign Agent Reply Codes (continued)**

Code	Reason
100	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the mobile node to the foreign agent.
101	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the home agent to the foreign agent.
104	Unknown challenge.
105	Missing challenge.
106	Stale challenge.

### Examples

The following example enables foreign agent service on Ethernet interface 1, advertising 10.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

The following example enables foreign agent service on serial interface 4, advertising 10.0.0.2 as the only care-of address. The uplink interface is configured as a transmit-only interface.

```
ip mobile foreign-agent care-of Serial4 interface-only transmit-only
interface Serial4
 ! Uplink interface
 ip address 10.0.0.2 255.255.255.0
 ip irdp
 !
 ip mobile foreign-service
 !
```

### Related Commands

Command	Description
<b>debug ip mobile advertise</b>	Displays advertisement information.
<b>ip mobile foreign-service</b>	Enables foreign agent service on an interface if care-of addresses are configured.
<b>show ip mobile globals</b>	Displays global information for mobile agents.
<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
<b>show ip mobile secure</b>	Displays mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.
<b>show ip mobile violation</b>	Displays information about security violations.
<b>show ip mobile visitor</b>	Displays the table containing the visitor list of the foreign agent.
<b>show ip route mobile</b>	Displays the current state of the routing table for mobile routes.

# ip mobile foreign-service

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

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

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

Syntax Description	
<b>challenge</b>	(Optional) Configures the foreign agent challenge parameters. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>forward-mfce</b>	(Optional) Enables the foreign agent to forward mobile foreign challenge extensions (MFCEs) and mobile node-AAA extensions to the home agent.
<b>timeout</b> <i>value</i>	(Optional) Challenge timeout in seconds. Possible values are from 1 to 10.
<b>window</b> <i>number</i>	(Optional) Maximum number of valid challenge values to maintain. Possible values are from 1 to 10. The default is 2.
<b>home-access</b> <i>access-list</i>	(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. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>limit</b> <i>number</i>	(Optional) Number of visitors allowed on the interface. The Busy (B) bit will be advertised when the number of registered visitors reaches this limit. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>registration-required</b>	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>reverse-tunnel</b> [ <b>mandatory</b> ]	(Optional) Enables reverse tunneling on the foreign agent. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

## Defaults

Foreign agent service is not enabled.

There is no limit to the number of visitors allowed on an interface.

**window** *number*: 2

Foreign agent reverse tunneling is not enabled. When foreign agent reverse tunneling is enabled, it is not mandatory by default.

## Command Modes

Interface and global configuration



## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)XS	The <b>challenge</b> keyword and associated parameters were added.
12.2(2)XC	The <b>reverse-tunnel [mandatory]</b> keywords were added.
12.2(13)T	The <b>challenge</b> keyword and associated parameters and the <b>reverse-tunnel [mandatory]</b> keywords were integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	Global configuration mode was added.

## Usage Guidelines

This command enables foreign agent service on the interface or all interfaces (global configuration). 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.

When you use the **reverse-tunnel** keyword to enable foreign agent reverse tunneling on an interface, the reverse tunneling support (T) bit is set in the agent advertisement.

Cisco Express Forwarding (CEF) switching is currently not supported on a foreign agent when reverse tunneling is enabled. If reverse tunneling is enabled at the foreign agent, disable CEF on the foreign agent, using the **no ip cef** global configuration command. If the foreign agent does not support reverse tunneling, then there is no need to disable CEF at the global configuration level.

Table 4 lists the advertised bitflags.

**Table 4 Foreign Agent Advertisement Bitflags**

Bit Set	Service Advertisement
T	Set if the <b>reverse-tunnel</b> parameter is enabled.
R	Set if the <b>registration-required</b> parameter is enabled.
B	Set if the number of visitors reached the <b>limit</b> 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	Reserved.
reserved	Never set.

## Examples

The following example shows how to enable foreign agent service for up to 100 visitors:

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

The following example shows how to enable foreign agent reverse tunneling:

```
interface ethernet 0
 ip mobile foreign-service reverse-tunnel
```

The following example shows how to configure foreign agent challenge parameters:

```
interface ethernet 0
 ip mobile foreign-service challenge window 2
```

**Related Commands**

Command	Description
<b>ip cef</b>	Enables CEF on the RP card.
<b>ip mobile tunnel</b>	Specifies the settings of tunnels created by Mobile IP.
<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

# ip mobile foreign-service revocation

To enable registration revocation support on the PDSN, use the **ip mobile foreign-service revocation** command in global configuration. To disable this feature, use the **no** form of the command.

**ip mobile foreign-service revocation** [*timeout value*] [*retransmit value*] [*timestamp msec*]

## Syntax Description

<i>timeout value</i>	The time interval in seconds between re-transmission of Registration Revocation Messages. The <i>value</i> is the wait time. The range of values is 1-100, and the default value is 3 seconds.
<i>retransmit value</i>	The maximum number of re-transmissions of MIPv4 Registration Revocation Messages. The <i>value</i> is the number of retries for a transaction. The range of values is 1-100, and the default value is 3.
<i>timestamp msec</i>	Specifies the unit of timestamp field for revocation. The <i>msec</i> is the unit of timestamp value for revocation in milliseconds.

## Defaults

The default value for **timeout** is 3 seconds, and the default value for **retransmit** is 3 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

The Registration Revocation feature requires that all the foreign-service configurations should be done globally, and not under the virtual-template interface.

## Examples

The following example illustrates the **ip mobile foreign-service revocation** command:

```
Router(config)#ip mobile foreign-service revocation timeout 6 retransmit 10
```

# ip mobile prefix-length

To append the prefix-length extension to the advertisement, use the **ip mobile prefix-length** command in interface configuration mode. To restore the default, use the **no** form of this command.

**ip mobile prefix-length**

**no ip mobile prefix-length**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The prefix-length extension is not appended.

**Command Modes** Interface and Global configuration

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.3(11)T	Global configuration mode was added.

**Usage Guidelines** The prefix-length extension is used for movement detection. When a mobile node registered with one foreign agent receives an agent advertisement from another foreign agent, the mobile node uses the prefix-length extension to determine whether the advertisements arrived on the same network. The mobile node needs to register with the second foreign agent if it is on a different network. If the second foreign agent is on the same network, reregistration is not necessary.

**Examples** The following example appends the prefix-length extension to agent advertisements sent by a foreign agent:

```
ip mobile prefix-length
```

Related Commands	Command	Description
	<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

# ip mobile proxy-host

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

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

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

## Syntax Description

<b>nai</b> <i>username@realm</i>	Network access identifier.
<b>flags</b> <i>rrq-flags</i>	(Optional) Registration request flags.
<b>home-agent</b> <i>ip-address</i>	(Optional) IP address of the home agent.
<b>home-addr</b> <i>home-address</i>	(Optional) Home IP address of the mobile node.
<b>lifetime</b> <i>seconds</i>	(Optional) Global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Values are from 3 to 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.
<b>local-timezone</b>	(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.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T for Packet Data Serving Node (PDSN) platforms.

## Usage Guidelines

This command is only available on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

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 configures the Mobile IP proxy host with an IP address of 10.3.3.1 and a lifetime value of 6000 seconds:

```
ip mobile proxy-host nai moipproxy1@cisco.com flags 40 home-agent 10.3.3.1 lifetime 6000
```

---

**Related Commands**

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

# ip mobile registration-lifetime

To set the registration lifetime value advertised, use the **ip mobile registration-lifetime** command in interface or global configuration mode.

**ip mobile registration-lifetime** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Lifetime in seconds. Range is from 3 to 65535 (infinity).
---------------------------	----------------	---

<b>Defaults</b>	36000 seconds
-----------------	---------------

<b>Command Modes</b>	Interface and global configuration
----------------------	------------------------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.3(11)T	Global configuration mode was added.

<b>Usage Guidelines</b>	This command allows an administrator to control the advertised lifetime on the interface. The foreign agent uses this command to control duration of registration. Visitors requesting longer lifetimes will be denied.
-------------------------	---

<b>Examples</b>	The following example sets the registration lifetime to 10 minutes on interface Ethernet 1 and 1 hour on interface Ethernet 2:
-----------------	--

```
interface e1
 ip mobile registration-lifetime 600
interface e2
 ip mobile registration-lifetime 3600
```

Related Commands	Command	Description
	<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

# 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** command in global configuration mode. To remove the mobility security associations, use the **no** form of this command.

```
ip mobile secure {aaa-download | host | visitor | home-agent | foreign-agent | proxy-host}
    {lower-address [upper-address] | nai string} {inbound-spi spi-in outbound-spi spi-out | spi
    spi} key hex string [replay timestamp [number] algorithm {md5 | hmac-md5}
    mode prefix-suffix]
```

```
no ip mobile secure {aaa-download | host | visitor | home-agent | foreign-agent | proxy-host}
    {lower-address [upper-address] | nai string} {inbound-spi spi-in outbound-spi spi-out | spi
    spi} key hex string [replay timestamp [number] algorithm {md5 | hmac-md5}
    mode prefix-suffix]
```

## Syntax Description

<b>aaa-download</b>	Downloads security association from AAA at every timer interval.
<b>host</b>	Security association of the mobile host on the home agent.
<b>visitor</b>	Security association of the mobile host on the foreign agent.
<b>home-agent</b>	Security association of the remote home agent on the foreign agent.
<b>foreign-agent</b>	Security association of the remote foreign agent on the home agent.
<b>proxy-host</b>	Security association of the proxy Mobile IP users. This keyword is only available on Packet Data Serving Node (PDSN) platforms.
<i>lower-address</i>	IP address of a host or lower range of IP address pool.
<i>upper-address</i>	(Optional) Upper range of an IP address pool. If specified, security associations for multiple hosts are configured. The value used in the <i>upper-address</i> argument must be greater than that used in the <i>lower-address</i> argument.
<b>nai string</b>	Network access identifier of the mobile node. The <b>nai string</b> is valid only for a host, visitor, and proxy host.
<b>inbound-spi spi-in</b>	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.
<b>outbound-spi spi-out</b>	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
<b>spi spi</b>	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
<b>key hex string</b>	ASCII string of hexadecimal values. No spaces are allowed.
<b>replay</b>	(Optional) Specifies replay protection used on registration packets.
<b>timestamp</b>	(Optional) Validates incoming packets to ensure that they are not being “replayed” by a spoofer using the timestamp method.
<i>number</i>	(Optional) Number of seconds. Registration is valid if received within the router’s clock +/- 7 seconds. This means the sender and receiver are in time synchronization (NTP can be used).
<b>algorithm</b>	(Optional) Algorithm used to authenticate messages during registration.
<b>md5</b>	(Optional) Message Digest 5.
<b>hmac-md5</b>	(Optional) Hash-based message authentication code (HMAC) message digest 5.



<b>mode</b>	(Optional) Mode used to authenticate during registration.
<b>prefix-suffix</b>	(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	The <i>lower-address</i> and <i>upper-address</i> arguments were added.
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	The <b>hmac-md5</b> keyword was added and this command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The <b>proxy-host</b> keyword was added for PDSN platforms.

### 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.

The HMAC-MD5 authentication algorithm is mandatory for mobile-home authentication (MHAЕ), mobile-foreign authentication (MFAЕ), and foreign-home authentication (FHAЕ)

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 that the mobile node can reregister with the time-stamp value closer to that of the home agent, if desired.

The **nai** keyword is valid only for a host, visitor, and proxy host.

The **proxy-host** keyword is available only on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.



#### Note

NTP is not required for operation but NTP can be used to synchronize time for all parties.

---

**Examples**

The following example shows mobile node 10.0.0.4, which has a key that is generated by the MD5 hash of the string:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

---

**Related Commands**

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

# ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** command in global configuration mode. To disable the setting of tunnels created by Mobile IP, use the **no** form of this command.

**ip mobile tunnel** { **crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag* }

**no ip mobile tunnel** { **crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag* }

## Syntax Description

<b>crypto map</b>	Enables encryption or decryption on new tunnels. This keyword is only available on platforms running specific Packet Data Serving Node (PDSN) code images.
<i>map-name</i>	The name of the crypto map. This argument is available only on platforms running specific PDSN code images.
<b>route-cache</b>	Sets tunnels to fast-switching mode.
<b>cef</b>	Sets tunnels to Cisco Express Forwarding (CEF) switching mode if CEF is enabled on the router.
<b>path-mtu-discovery</b>	Specifies when the tunnel MTU should expire if set by Path MTU Discovery.
<b>age-timer</b> <i>minutes</i>	(Optional) Time interval in minutes after which the tunnel reestimates the path MTU.
<b>infinite</b>	(Optional) Turns off the age timer.
<b>nat</b>	Applies Network Address Translation (NAT) on the tunnel interface.
<b>inside</b>	Sets the dynamic tunnel as the inside interface for NAT.
<b>outside</b>	Sets the dynamic tunnel as the outside interface for NAT.
<b>route-map</b> <i>map-tag</i>	Defines a meaningful name for the route map.

## Defaults

Disabled.  
If enabled, default value for the *minutes* argument is 10 minutes.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	The <b>nat</b> , <b>inside</b> , and <b>outside</b> keywords were added.
12.2T	The <b>cef</b> keyword was added.
12.2(13)T	The <b>route-map</b> keyword and <i>map-tag</i> argument were added.
12.3(4)T	The <b>crpto map</b> keyword and <i>map-name</i> argument were added for PDSN platforms.

---

**Usage Guidelines**

Path MTU Discovery is used by end stations to find a packet size that does not need to be fragmented when being sent between the end stations. Tunnels must adjust their MTU to the smallest MTU interior to achieve this condition, as described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from a case where suboptimum MTU existed at time of discovery. It is reset to the outgoing MTU of the interface.

The **no ip mobile tunnel route-cache** command disables fast switching and CEF switching (if CEF is enabled) on Mobile IP tunnels. The **no ip mobile tunnel route-cache cef** command disables CEF switching only.

CEF switching is currently not supported on a foreign agent when reverse tunneling is enabled. If reverse tunneling is enabled at the foreign agent, disable CEF on the foreign agent using the **no ip cef** global configuration command. If the foreign agent does not support reverse tunneling, there is no need to disable CEF at the global configuration level.

The **crypto map** *map-name* keyword and argument combination are available only on platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

---

**Examples**

The following example sets the discovered tunnel MTU to expire in 10 minutes (600 seconds):

```
ip mobile tunnel path-mtu-discovery age-timer 600
```

---

**Related Commands**

Command	Description
<b>ip cef</b>	Enables CEF on the RP card.
<b>show ip mobile tunnel</b>	Displays active tunnels.

# ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

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

**no ppp authentication**

Syntax Description	
<i>protocol1</i> [ <i>protocol2...</i> ]	At least one of the keywords described in <a href="#">Table 5</a> .
<b>if-needed</b>	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
<i>list-name</i>	(Optional) Used with authentication, authorization, and accounting (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 <b>aaa authentication ppp</b> command.
<b>default</b>	(Optional) Name of the method list created with the <b>aaa authentication ppp</b> command.
<b>callin</b>	(Optional) Authentication on incoming (received) calls only.
<b>one-time</b>	(Optional) The username and password are accepted in the username field.
<b>optional</b>	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

**Defaults** PPP authentication is not enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(1)	The <b>optional</b> keyword was added.
	12.1(3)XS	The <b>optional</b> keyword was added.
	12.2(2)XB5	Support for the <b>eap</b> authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
	12.2(13)T	The <b>eap</b> authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Usage Guidelines

When you enable Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.



### Caution

If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 5 lists the protocols used to negotiate PPP authentication.

**Table 5** *ppp authentication Protocols*

<b>chap</b>	Enables CHAP on a serial interface.
<b>eap</b>	Enables EAP on a serial interface.
<b>ms-chap</b>	Enables MS-CHAP on a serial interface.
<b>pap</b>	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

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
```

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

## Related Commands

Command	Description
<b>aaa authentication ppp</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
<b>aaa new-model</b>	Enables the AAA access control model.
<b>autoselect</b>	Configures a line to start an ARAP, PPP, or SLIP session.
<b>encapsulation</b>	Sets the encapsulation method used by the interface.
<b>ppp accm</b>	Identifies the ACCM table.
<b>username</b>	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.

# 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
	<b>show cdma pdsn pcf brief</b>	Displays a table of all PCFs that have R-P tunnels to the PDSN.
	<b>show cdma pdsn session</b>	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

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

<b>Defaults</b>	No default keywords or arguments.
-----------------	-----------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	The following example shows output from the <b>show cdma pdsn</b> 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
```

**show cdma pdsn**

```
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 accounting 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
```

## ■ show cdma pdsn accounting

```

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-pl-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 000000000003

```

A - A1:000000000003
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 000000000004

```

A - A1:000000000004
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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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
```

# show cdma pdsn accounting detail

```

    IP Address (B1) 15.0.0.3, Network Access Identifier (B2)
mwt5-mip-pl-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 000000000003

    Mobile Station ID (A1) IMSI 000000000003
    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 000000000004

    Mobile Station ID (A1) IMSI 000000000004
    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 accounting 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines	The counter names appear in abbreviated format.
------------------	---

Examples	The following example shows output from the <b>show cdma pdsn accounting session</b> command:
----------	---

```
PDSN-6500#show cdma pdsn accounting session 000000000004
UDR for session
session ID: 3
Mobile Station ID IMSI 000000000004

  A - A1:000000000004
  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 (with counter names) for the session identified by the msid, and the accounting 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**

<b>Syntax Description</b>	msid	The ID number of the mobile subscriber.
---------------------------	------	---

<b>Defaults</b>	No default keywords or arguments.
-----------------	-----------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Usage Guidelines</b>	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
```

**show cdma pdsn accounting session detail**

```
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* }**

<b>Syntax Description</b>	<b>msid</b>	The ID number of the mobile subscriber.
	<b>mn-ip-address <i>ip_address</i></b>	Specifies the IP addresses assigned to the mobile numbers in each session.

**Defaults** No default keywords or arguments.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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-pl-user121@ispxyz.com
```

```
UDR for flow
Mobile Node IP address 15.0.0.3

B - B1:15.0.0.3 B2:mwts-mip-pl-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*]

<b>Syntax Description</b>	<b>slot_number</b>	Slot number of the AHDLC of interest.
	<b>channel</b> [ <i>channel_id</i> ]	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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.2(8)BY	The possible values for channel ID were extended to 20000.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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

<b>configuration</b>	Displays configuration information associated with the cluster controller.
<b>statistics</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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

<b>load</b>	The load reported by every PDSN member in the cluster, sorted from the lowest load value.
<b>time</b>	The seek time of the member, sorted from the past to the future.
<b>ipaddr</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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 ahd1c 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		
<b>count</b>		The number of session records on cluster controller.
<b>age</b>		The number of session records of this age on the cluster controller. Age measured in days.
<b>oldest</b>		The oldest session record on the cluster controller.
<i>more 1-20 records</i>		Displays the configured number (from 1 to 20) of the oldest session records on the cluster controller.
<i>imsi BCDs</i>		Displays the session record with this imsi on the cluster controller.
<i>more 1-20 records</i>		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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

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

```
Router# show cdma pdsn clu contr session imsi 000000000007
```

```

      IMSI      Member IPv4 Addr   Age [days]   Anchor changes
-----
000000000007      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
-----
000000000002      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.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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, authentication problem
  0 A11-RegReply discarded, identification problem
  0 A11-RegReply discarded, unrecognized extension
975 A11-RegRequest received
  0 A11-RegRequest discarded, authentication 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}**

<b>Syntax Description</b>	<b>configuration</b>	Displays configuration information associated with the cluster member.
	<b>statistics</b>	Displays various statistics collected on cluster member signaling messages with the cluster controller.

<b>Defaults</b>	No default keywords or arguments.
-----------------	-----------------------------------

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)BY	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

<b>Examples</b>	<p>The following example shows output from the <b>show cdma pdsn cluster member</b> command:</p> <pre>Router# show cdma pdsn cluster member</pre>
-----------------	---

# 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

<b>mn- ip-address ip_address</b>	Specifies the IP addresses assigned to the mobile numbers in each session.
<b>msid string</b>	Specifies the mobile subscriber id number.
<b>service-type</b>	Specifies the service type.
<b>user string</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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

```

3000000000000025 sim1 Simple 100.4.1.22 ACT
1000000000000123 sim1 Simple 100.4.1.24 ACT
2000000000000071 sim1 Simple 100.4.1.23 ACT
3000000000000026 sim1 Simple 100.4.1.25 ACT
1000000000000124 sim1 Simple 100.4.1.26 ACT
2000000000000072 sim1 Simple 100.4.1.27 ACT
3000000000000027 sim1 Simple 100.4.1.28 ACT
1000000000000125 sim1 Simple 100.4.1.29 ACT
2000000000000073 sim1 Simple 100.4.1.30 ACT
3000000000000028 sim1 Simple 100.4.1.31 ACT
1000000000000126 sim1 Simple 100.4.1.33 ACT
2000000000000074 sim1 Simple 100.4.1.32 ACT
3000000000000029 sim1 Simple 100.4.1.34 ACT
1000000000000127 sim1 Simple 100.4.1.36 ACT
2000000000000075 sim1 Simple 100.4.1.35 ACT
3000000000000030 sim1 Simple 100.4.1.37 ACT
1000000000000128 sim1 Simple 100.4.1.39 ACT
2000000000000076 sim1 Simple 100.4.1.38 ACT
3000000000000101 sim1 Simple 100.4.1.41 ACT
1000000000000199 sim1 Simple 100.4.1.43 ACT
2000000000000147 sim1 Simple 100.4.1.42 ACT
3000000000000102 sim1 Simple 100.4.1.44 ACT
1000000000000200 sim1 Simple 100.4.1.46 ACT
--More--

```

# show cdma pdsn flow service

To display flow-based information for a specified service type in each session, use the **show cdma pdsn flow service** command in privileged EXEC mode.

**show cdma pdsn flow service** { **mobile** | **proxy-mobile** | **simple** | **simple-ipv6** }

## Syntax Description

mobile	Specifies mobile service type.
proxy-mobile	Specifies the proxy-mobile service type.
simple	Specifies the simple service type .
simple-ipv6	Specifies the simple-IPv6 service type.

## Defaults

No default keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(14)YX	<b>simple-ipv6</b> output was introduced.
12.4(11)T	This command was incorporated into Cisco IOS Release 12.4(11)T.

## Examples

The following example shows output from the **show cdma pdsn flow service simple-ipv6** command:

```
Router# show cdma pdsn flow service simple-ipv6
```

```
MSID NAI Type MN IP
```

```
Address St
```

```
000000000000101 mwts-uc1-np-user1 Simple-ipv6
```

```
2001:420:10:0:211:20FF:FE43:61C ACT
```

# 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** }

<b>Syntax Description</b>	<b>brief</b>	Displays information about all PCFs with connected sessions.
	<i>ip_addr</i>	Displays detailed PCF information by IP address.
	<b>secure</b>	Displays the security associations for all PCFs on this PDSN.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.2(2)XC	The parameters of this command were changed.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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 6](#) describes the fields shown in the output of the brief version of the command.

**Table 6** *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)
```

# show cdma pdsn pcf

```
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 7](#) describes the fields shown in the output of the command when an IP address is specified.

**Table 7** *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 8](#) describes the fields shown in the output of the command when the keyword **secure** is specified.

**Table 8** *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 redundancy

To show whether or not the PDSN redundancy feature is enabled or not, use the **show cdma pdsn redundancy** command in Privileged EXEC mode.

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default keywords or arguments.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(14)YX	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Examples** The following example illustrates the output for the **show cdma pdsn redundancy** command:

```
router# show cdma pdsn redundancy

CDMA PDSN Redundancy is enabled
CDMA PDSN Session Redundancy system status
PDSN state = ACTIVE
PDSN-peer state = STANDBY HOT
CDMA PDSN Session Redundancy Statistics
Last clearing of cumulative counters never
Synced to standby Current
since peer up Connected
Sessions 1 2
SIP Flows 0 0
MIP Flows 1 0
PMIP Flows 0 0
```

# show cdma pdsn redundancy statistics

To display a variety of information about the sessions and the associated flows that have been/are synchronized to/from the standby/active, use **show cdma pdsn redundancy statistics** command in privileged EXEC mode.

**show cdma pdsn redundancy statistics**

**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.
	12.3(8)XW	Prepaid output was included in examples.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

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

**Examples** The following output is displayed with the **show cdma pdsn redundancy statistics** command:

```
Router# show cdma pdsn redundancy statistics
Last clearing of cumulative counters never Number of messages sent to standby:

Session Events
Up 10, Down 39, Reregistration 0
Handoff 0, PPP renegotiation 0
Flow Events
Simple IP Up 1, Down 1
Mobile IP Up 7, Down 7
Proxy Mobile IP Up 2, Down 2
Accounting Events
Update 0, Flow Start0, Stop 0
Active to Dormant 0, Dormant to Active 0
```

# 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*]]]

<b>Syntax Description</b>	<b>slot_number</b>	(Optional) Slot number of the AHDLC of interest.
	<b>ahdlc-channel</b> [ <i>channel_id</i> ]	(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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(2)XC	This command was introduced.
	12.2(8)BY	The possible values for channel ID was extended to 20000.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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

<b>summary</b>	Displays a summary of the session table entry.
<b>msid number</b>	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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

## 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**]

<b>Syntax Description</b>	<b>brief</b>	(Optional) Displays a summary of all sessions.
	<b>dormant</b>	(Optional) Displays information about dormant PDSN sessions.
	mn-ip-address <i>address</i>	(Optional) Displays user information for the specified IP address.
	<b>msid number</b>	(Optional) Displays information for the specified MSID.
	<b>user nai</b>	(Optional) Displays information for the specified NAI.
	<b>prepaid</b>	(Optional) Displays information about prepaid flows.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.2(2)XC	The parameters of this command were altered.
	12.2(8)BY	The <b>prepaid</b> variable was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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 ]**

<b>Syntax Description</b>	<b>rp</b>	Displays all RP interface statistics.
	<b>ppp</b>	Displays all PPP interface statistics
	<b>ahdlc 0-6</b>	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/deframing statistics of the engine.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)XS	This command was introduced.
	12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

**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/PCP 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:
All 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
Deframing output 0 bytes, 0 paks
Deframing errors 0, insufficient memory 0,
    queue overflow 0, invalid size 0, CRC errors 0
```

# show cdma pdsn statistics prepaid

To display statistics related to all prepaid enabled flows, use the **show cdma pdsn statistics prepaid** command in Privileged EXEC mode.

**show cdma pdsn statistics prepaid**

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default keywords or arguments.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(8)XW	Prepaid output was included in examples.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Examples** Here is sample output of the **show cdma pdsn statistics prepaid** command:

```
router# show cdma pdsn statistics prepaid
Prepaid-related statistics:
Total prepaid flows opened: 0
Volume-based 0, Duration-based 0
Simple IP 0, VPDN 0, Proxy Mobile IP 0, Mobile IP 0
Total online Access Requests sent 0
Total online Access Response received 0
Accepted 0, Discarded 0, Timeout 0
Online Access Requests sent with Update Reason:
Pre-Initialization 0
Initial Request 0
Threshold Reached 0
Quota Reached 0
Remote Forced Disconnect 0
Client Service Termination 0
Main SI Released 0
SI not established 0
Tariff Switch Update 0
```



# show ip mobile cdma ipsec

To display if IS835 IPSec security is enabled, use the **show ip mobile cdma ipsec** command in EXEC mode.

**show ip mobile cdma ipsec**

<b>Syntax Description</b>	There are no arguments or keywords for this command.
---------------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

<b>Usage Guidelines</b>	This command is only present in crypto images for the 7200, and non-crypto images for the MWAM.
-------------------------	---

<b>Examples</b>	<p>The following example illustrates how to enable the <b>show ip mobile cdma ipsec</b> command:</p> <pre>router# show ip mobile cdma ipsec</pre>
-----------------	---

# show ip mobile cdma ipsec profile

To display the crypto profile configured for IPsec, use the **show ip mobile cdma ipsec profile** command in EXEC mode.

**show ip mobile cdma ipsec profile**

---

**Syntax Description** There are no arguments or keywords for this command.

---

**Command Modes** EXEC

---

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

---

---

**Usage Guidelines** This command is only present in crypto images for the 7200, and non-crypto images for the MWAM.

---

**Examples** The following example illustrates how to enable the **show ip mobile cdma ipsec profile** command:

```
router# show ip mobile cdma ipsec profile
```

# show ip mobile proxy

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

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

## Syntax Description

<b>host</b>	(Optional) Displays information about the proxy host.
<b>nai string</b>	(Optional) Network access identifier.
<b>registration</b>	(Optional) Displays proxy registration information.
<b>traffic</b>	(Optional) Displays proxy traffic information.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T for PDSN platforms.

## Usage Guidelines

This command is available only on Packet Data Serving Node (PDSN) platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

## 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 10.3.3.1
  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** command in privileged EXEC mode.

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

## Syntax Description

<b>host</b>	Displays security association of the mobile host on the home agent.
<b>visitor</b>	Displays security association of the mobile visitor on the foreign agent.
<b>foreign-agent</b>	Displays security association of the remote foreign agents on the home agent.
<b>home-agent</b>	Displays security association of the remote home agent on the foreign agent.
<b>proxy-host</b>	Displays security association of the proxy mobile user. This keyword is only available on Packet Data Serving Node (PDSN) platforms running specific PDSN code images.
<b>summary</b>	Displays number of security associations in table.
<i>ip-address</i>	IP address.
<i>nai string</i>	Network access identifier (NAI).

## Command Modes

EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The <b>proxy-host</b> keyword was added for PDSN platforms.

## Usage Guidelines

Multiple security associations can exist for each entity.

The **proxy-host** keyword is only available on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

## 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):
10.0.0.6
  SPI 300, MD5, Prefix-suffix, Timestamp +/- 7,
  Key 00112233445566778899001122334455
```

[Table 9](#) describes the significant fields shown in the display.

**Table 9** *show ip mobile secure Field Descriptions*

Field	Description
10.0.0.6	IP address. The NAI is displayed if configured.
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. HMAC-MD5 id displayed if configured.
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 protocol counters, use the **show ip mobile traffic** command in privileged EXEC mode.

## show ip mobile traffic

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(13)T	This command was enhanced to display successful registration requests with NAT detect and to display information about foreign agent reverse tunnels and foreign agent challenge and response extensions.
	12.3(14)T	The command output was enhanced to display the count of UDP Port 434 input packets that were dropped by UDP.

**Usage Guidelines** Counters can be reset to zero 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:
UDP:
  Port: 434 (Mobile IP) input drops: 0
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
  Unspecified 0, Unknown HA 0
  Administrative prohibited 0, No resource 0
  Authentication failed MN 0, FA 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 request 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
  Total incoming requests using NAT detect 1
```

## 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
Replies in 0
Forwarded 0, Bad 0, Ignored 0
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 1, Missing challenge 0, Stale challenge 0

```

Table 10 describes the significant fields shown in the display.

**Table 10** *show ip mobile traffic Field Descriptions*

Field	Description
Port: 434 (Mobile IP) input drops	Total number of UDP Port 434 (Mobile IP) packets dropped by UDP processing due to a full input queue. These packets are not processed by the home agent or foreign agent and so are not otherwise counted or displayed by Mobile IP. This count is the same count displayed by using the <b>show ip socket detail</b> command.
Solicitations received	Total number of solicitations received by the mobility agent.
Advertisements sent	Total number of advertisements sent by the mobility agent.
response to solicitation	Total number of advertisements sent by the mobility agent in response to mobile node solicitations.
<b>Home Agent</b>	
Register requests	Total number of registration requests received by the home agent.
Deregister requests	Total number of registration requests received by the home agent with a lifetime of zero (requests to deregister).
Register replied	Total number of registration replies sent by the home agent.
Deregister replied	Total number of registration replies sent by the home agent in response to requests to deregister.
Accepted	Total number of registration requests accepted by the home agent (Code 0).
No simultaneous bindings	Total number of registration requests accepted by the home agent—simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of registration requests denied by the home agent.
Ignored	Total number of registration requests ignored by the home agent.
Unspecified	Total number of registration requests denied by the home agent—reason unspecified (Code 128).
Unknown HA	Total number of registration requests denied by the home agent—unknown home agent address (Code 136).
Administrative prohibited	Total number of registration requests denied by the home agent—administratively prohibited (Code 129).

**Table 10**      *show ip mobile traffic Field Descriptions (continued)*

Field	Description
No resource	Total number of registration requests denied by the home agent—insufficient resources (Code 130).
Authentication failed MN	Total number of registration requests denied by the home agent—mobile node failed authentication (Code 131).
Authentication failed FA	Total number of registration requests denied by the home agent—foreign agent failed authentication (Code 132).
Bad identification	Total number of registration requests denied by the home agent—identification mismatch (Code 133).
Bad request form	Total number of registration requests denied by the home agent—poorly formed request (Code 134).
Unavailable encap	Total number of registration requests denied by the home agent—unavailable encapsulation (Code 139).
Reverse tunnel mandatory	Total number of registration requests denied by the home agent—reverse tunnel is mandatory and the “T” bit is not set (Code 138).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 137).
Binding updates	A Mobile IP standby message sent from the active router to the standby router when a registration request comes into the active router.
Binding update acks	A Mobile IP standby message sent from the standby router to the active router to acknowledge the reception of a binding update.
Binding info request	A Mobile IP standby message sent from a router coming up from reboot/or a down interface. The message is a request to the current active router to send the entire Mobile IP binding table.
Binding info reply	A reply from the active router to the standby router that has part or all of the binding table (depending on size).
Binding info reply acks	An acknowledge message from the standby router to the active router that it has received the binding info reply.
Gratuitous ARP	Total number of gratuitous ARPs sent by the home agent on behalf of mobile nodes.
Proxy ARPs sent	Total number of proxy ARPs sent by the home agent on behalf of mobile nodes.
Total incoming registration requests...	Total number incoming registration requests using NAT detect.
<b>Foreign Agent</b>	
Request in	Total number of registration requests received by the foreign agent.
Forwarded	Total number of registration requests relayed to the home agent by the foreign agent.
Denied	Total number of registration requests denied by the foreign agent.
Ignored	Total number of registration requests ignored by the foreign agent.
Unspecified	Total number of registration requests denied by the foreign agent—reason unspecified (Code 64).



**Table 10** *show ip mobile traffic Field Descriptions (continued)*

Field	Description
HA unreachable	Total number of registration requests denied by the foreign agent—home agent unreachable (Codes 80-95).
Administrative prohibited	Total number of registration requests denied by the foreign agent—administratively prohibited (Code 65).
No resource	Total number of registration requests denied by the home agent—insufficient resources (Code 66).
Bad lifetime	Total number of registration requests denied by the foreign agent—requested lifetime too long (Code 69).
Bad request form	Total number of registration requests denied by the home agent—poorly formed request (Code 70).
Unavailable encapsulation	Total number of registration requests denied by the home agent—unavailable encapsulation (Code 72).
Unavailable compression	Total number of registration requests denied by the foreign agent—requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 74).
Reverse tunnel mandatory	Total number of registration requests denied by the foreign agent—reverse tunnel is mandatory and the “T” bit is not set (Code 75).
Replies in	Total number of well-formed registration replies received by the foreign agent.
Forwarded	Total number of valid registration replies relayed to the mobile node by the foreign agent.
Bad	Total number of registration replies denied by the foreign agent—poorly formed reply (Code 71).
Ignored	Total number of registration replies ignored by the foreign agent.
Authentication failed MN	Total number of registration requests denied by the home agent—mobile node failed authentication (Code 67).
Authentication failed HA	Total number of registration replies denied by the foreign agent—home agent failed authentication (Code 68).
Received challenge/gen. authentication extension, feature not enabled	Total number of registration requests dropped by the foreign agent—received challenge/generalized-authentication extension in registration request but Mobile IP foreign agent challenge/response extension is not enabled.
Unknown challenge	Total number of registration requests denied by the foreign agent—unknown challenge (Code 104).
Missing Challenge	Total number of registration requests denied by the foreign agent—missing challenge (Code 105).
Stale Challenge	Total number of registration requests denied by the foreign agent—stale challenge (Code 106).

# show ip mobile violation

To display information about security violations, use the **show ip mobile violation** command in privileged EXEC mode.

**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 <b>nai</b> keyword and associated parameters were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, which are the violators without security associations. 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 11](#) describes significant fields shown in the display.

**Table 11** *show ip mobile violation* Field Descriptions

Field	Description
<i>IP address</i>	IP address of the violator. The network access identifier (NAI) is displayed if configured.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.

**Table 11** *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 Codes	Reason for the most recent security violation for this peer. Possible reasons are: <ul style="list-style-type: none"> <li>• (1) No mobility security association</li> <li>• (2) Bad authenticator</li> <li>• (3) Bad identifier</li> <li>• (4) Bad SPI</li> <li>• (5) Missing security extension</li> <li>• (6) Other</li> </ul>

# show ip mobile visitor

To display the visitor table that contains information on mobile nodes (MNs) using this foreign agent (FA), use the **show ip mobile visitor** command in privileged EXEC mode.

**show ip mobile visitor** *[[pending] [ip-address | summary] | nai string [session-id string]]*

## Syntax Description

<b>pending</b>	(Optional) Displays the pending registration table.
<i>ip-address</i>	(Optional) IP address of visiting MNs.
<b>summary</b>	(Optional) Displays all values in the table.
<b>nai string</b>	(Optional) Network access identifier (NAI).
<b>session-id string</b>	(Optional) Session identifier. The string value must be fewer than 25 characters.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The <b>session-id</b> keyword was added.
12.3(8)T	The output was enhanced to display UDP tunneling.

## Usage Guidelines

Use this command to find out information on MNs that are registered with their (home agent) HA via this FA. The FA updates the visitor table that contain a list of the MNs using a FA.

A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

## Examples

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

```
Router# show ip mobile visitor
```

```
Mobile Visitor List:
```

```
Total 1
```

```
10.0.0.1:
```

```
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
```

If the mobile node has visited and is associated with a session identifier, then the visitor entry for the mobile node shows the session identifier as shown below:

```
Router# show ip mobile visitor
```

```
Mobile Visitor List:
Total 1
  user01@cisco.com
  Home addr 100.100.100.17
    Interface Ethernet3/3, MAC addr 0004.6d25.b857
    IP src 0.0.0.0, dest 100.100.100.1, UDP src port 434
    HA addr 100.100.100.100, Identification BC189864.B2FE6CC4
    Lifetime 00:33:20 (2000) Remaining 00:33:06
    Tunnel0 src 70.70.70.2, dest 100.100.100.100, reverse-allowed
    Routing Options - (B)Broadcast
    Session identifier PD
```

The following sample output shows that the MN is registering with the HA (at the FA):

```
Router# show ip mobile visitor
```

```
Mobile Visitor List:
Total 1
10.99.100.2:
  Interface FastEthernet3/0, MAC addr 00ff.ff80.002b
  IP src 10.99.100.2, dest 30.5.3.5, UDP src port 434
  HA addr 200.1.1.1, Identification BCE7E391.A09E8720
  Lifetime 01:00:00 (3600) Remaining 00:30:09
  Tunnel1 src 200.1.1.5, dest 200.1.1.1, reverse-allowed
  Routing Options - (T)Reverse Tunneling
```

Table 12 describes the significant fields shown in the display.

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

Field	Description
Total	Number of mobile nodes visiting the foreign agent.
10.0.0.1	Home IP address of a visitor. The NAI is displayed if configured.
Interface	Interface the FA received the MN's registration on.
MAC addr	MAC address of the visitor.
IP src	Source IP address of the registration request of a visitor.
IP dest	Destination IP address of the registration request of a visitor. A MN solicits an advertisement from the FA, and the FA uses the output interface's address (where it received the solicitation) as the source IP address in the advertisement. The MN picks up on this address and sends in a RRQ to it. This tells you which destination address the MN used when it sent in its registration request to the FA (typically the interface address). If it had sent the registration request to a broadcast or multicast address, or advertised address (not knowing the interface address), the FA will reply using the output interface address (typically the interface where it received the RRQ).
UDP src port	UDP src port used by the visiting mobile node in its registration request.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime (in hh:mm:ss) granted to the mobile node for this registration.

**Table 12**      *show ip mobile visitor Field Descriptions (continued)*

Field	Description
Remaining	The time (in hh:mm:ss) 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 options are IPIP, GRE, and UDP. The default is IPIP encapsulation.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Options are: <ul style="list-style-type: none"> <li>• (S) Multi-binding (not supported on home agent)</li> <li>• (B) Broadcast</li> <li>• (D) Direct-to-mobile node</li> <li>• (M) MinIP (not supported on home agent)</li> <li>• (G) GRE</li> <li>• (T) Reverse-tunnel</li> </ul>
Session identifier	Session identifier can be the device name or MAC address.

**Related Commands**

Command	Description
<b>debug ip mobile</b>	Displays IP mobility activities.
<b>ip mobile foreign-agent nat traversal</b>	Enables NAT UDP traversal support for MIP FAs.
<b>ip mobile home-agent nat traversal</b>	Enables NAT UDP traversal support for MIP HAs.
<b>show ip mobile binding</b>	Displays the mobility binding table.
<b>show ip mobile globals</b>	Displays global information about MIP HAs, FAs, and MNs.
<b>show ip mobile tunnel</b>	Displays information about UDP tunneling.

# show ipc sctp

To display ipc sctp statistics, use the **show ipc sctp** command.

## show ipc sctp

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default keywords or arguments.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(8)XW	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Examples** Sample show output for the **show ipc sctp** command:

```
router # show ipc sctp statistics
IPC default Zone:
  IPC association Id: 1
    SCTP Protocol Local: port: 6602 ip: 10.2.86.26
      keepalive 1500
      retransmit-timeout 300 600
      bundling 20
      cumulative-sack 200
      path-retransmit 4
      assoc-retransmit 4
      max-inbound-streams 2
      init-timeout 1000
      init-retransmit 8
      receive-window 24000
    SCTP Protocol Remote: port: 22 ip: 10.2.87.26
router #
```

# 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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

---

## Examples

The following example enables network management traps for CDMA:

```
snmp-server enable traps cdma
```



# snmp-server enable traps ipmobile

To enable 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
12.2(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. This command enables Mobile IP Authentication Failure notifications. This notification is defined in RFC2006-MIB.my as the mipAuthFailure notification type {mipMIBNotifications 1}. This notification, when enabled, is triggered when there is an authentication failure for the Mobile IP entity during validation of the mobile registration request or reply.

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
```

## Related Commands

Command	Description
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.
<b>snmp-server trap-source</b>	Specifies the interface from which an SNMP trap should originate.