Command Reference for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR2

Published: October 16, 2009
Revised: January 4, 2011, OL-20781-01

This section lists new and revised commands for the Cisco PDSN software. All other commands used with this feature are documented in the Cisco IOS Release 12.4 command reference publications.

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

- show cdma pdsn accounting session flow user, page 235
- **show cdma pdsn accounting user, page 236** New
- show cdma pdsn ahdlc, page 240
- show cdma pdsn cac, page 241
- show cdma pdsn cluster controller, page 242
- show cdma pdsn cluster controller configuration, page 243
- **show cdma pdsn cluster controller member, page 244** Modified
- show cdma pdsn cluster controller session, page 246
- show cdma pdsn cluster controller statistics, page 247
- **show cdma pdsn cluster member, page 249** Modified
- **show cdma pdsn flow, page 251** Modified
- show cdma pdsn flow service, page 254
- **show cdma pdsn pcf, page 255** Modified
- show cdma pdsn qos local profile, page 258
- show cdma pdsn redundancy, page 259
- show cdma pdsn redundancy statistics, page 261
- show cdma pdsn resource, page 262
- **show cdma pdsn session, page 263** Modified
- **show cdma pdsn statistics, page 267** Modified
- **show cdma pdsn statistics prepaid, page 277** New
- show cdma pdsn statistics prepaid, page 277
- show ip mobile cdma ipsec, page 278
- show ip mobile cdma ipsec profile, page 279
- show ip mobile proxy, page 280
- show ip mobile secure, page 282
- show ip mobile traffic, page 284
- show ip mobile violation, page 285
- **show ip mobile visitor, page 287** Modified
- show ipc sctp statistics, page 290
- **show policy-map apn realm, page 291** New
- **show redundancy history, page 292** New
- show redundancy inter-device, page 298
- **show redundancy states, page 299** New
- **show sami standby, page 300** New
- **show standby, page 301** New
- show tech-support cdma pdsn, page 302
- snmp-server enable traps cdma, page 310
- snmp-server enable traps ipmobile, page 311

- subscriber redundancy rate, page 312
- tft-allowed (service flows qos subscriber profile sub-mode), page 313
- **vpdn debug show-conditions, page 314** New
- **Osler Commands, page 315** New
- **show subscriber, page 316** New
- **monitor subscriber, page 334** New
- **show subscriber session, page 343** New
- **bulk statistics collection, page 346** New
- **RCAL Functionality, page 350** New

access list

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use encryption access lists to control which packets on an interface are encrypted/decrypted, and which are transmitted as plain text (not encrypted).

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

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

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

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

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

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

Examples

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

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

bandwidth (service flows qos subscriber profile sub-mode)

To configure the maximum aggregate bandwidth value, use the **bandwidth** command in the service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

bandwidth *number*

no bandwidth *number*

Syntax Description

number	The maximum aggregate bandwidth value. The valid range is 8000-2000000000.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode.

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

There are no usage guidelines.

Examples

The following example shows how to enable a maximum aggregate bandwidth value of 9000:

```
Router#(config-qos-profile)# bandwidth ?
  <8000-2000000000>  Value

Router#(config-qos-profile)# bandwidth 9000 ?
  <cr>
```

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 in global configuration mode. To reset the number of AHDLC channel resources to the default, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

In the PDSN 4.0 image, the maximum number of usable channel is increased to 75000.

In the PDSN 5.0 image, the maximum number of usable channel is increased to 105000 per processor.

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.
12.4(15)xx	The maximum number of usable channels was increased to 75000 in the PDSN 4.0 Release.
12.4(22)XR	The maximum number of usable channels was increased to 105000 in the PDSN 5.0 Release.

Usage Guidelines

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

The command also fails when the engine has any active channels.

Examples

The following example shows how to limit the number of service channels provided by the AHDLC engine to 1000:

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

Related Commands

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

cdma pdsn a10 ahdlc prefragment

To enable the packet fragmentation using the PPP method, use the CLI command **cdma pdsn a10 ahdlc prefragment** in global configuration mode. To disable PPP fragmentation, use the **no** form of this command.

cdma pdsn a10 ahdlc prefragment

no cdma pdsn a10 ahdlc prefragment

Syntax Description

There are no keywords or variables for this command.

Defaults

The default behavior is that packet fragmentation is done in PPP method using the AHDLC frames.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(14)YX	This command was introduced.

Usage Guidelines

If you use the **no** form of this command, the packets are fragmented at the IP layer. In other words, the fragmentation occurs only at IP/GRE/AHDLC (PPP/IP) layer and not at the AHDLC layer.

Examples

The following example shows how to enable the PDSN so that the packet fragmentation is done using PPP method:

```
Router (config)# cdma pdsn a10 ahdlc prefragment
```

cdma pdsn a10 ahdlc init-accm zero

When PPP negotiation starts, ACCM is always assumed to be 0x20 initially. With this, asynchronous control character map (ACCM) is negotiated and used. To ensure that the ACCM is always assumed to be zero, use the **no** form of the command in global configuration mode.

cdma pdsn a10 ahdlc init-accm zero

no cdma pdsn a10 ahdlc init-accm zero

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR1	This command was introduced.

Usage Guidelines

If all the mobiles use only ACCM zero in deployment, use the CLI command **no cdma pdsn a10 ahdlc init-accm zero**.

Examples

The following example shows how to enable the PDSN so that the packet fragmentation is done using the PPP layer with ACCM is 0x20 initially:

```
Router (config)# cdma pdsn a10 ahdlc init-accm zero
```

cdma pdsn a10 ahdlc trailer

To enable the PDSN so that AHDLC frames are expected to contain trailer byte, use the **cdma pdsn a10 ahdlc trailer** command 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 ahdlc trailer

no cdma pdsn a10 ahdlc trailer

Syntax Description

There are no keywords or variables 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.

Usage Guidelines

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

Examples

The following example shows how to disable the PDSN so that AHDLC processing does not expect the AHDLC trailer:

```
Router (config)# no cdma pdsn a10 ahdlc 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 PDSN waits for the LCP echo response from 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. 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.

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 starts only after the traffic channel is assigned, (in other 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*

Syntax Description

1-120	Sets the timeout interval before the session is torn down.

Defaults

This CLI is not enabled, therefore, the PDSN initiates PPP negotiation immediately after a Registration Reply is sent to the initial Registration.Request.

When enabled, the default timeout interval is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)ZB4a	This command was introduced.

Usage Guidelines

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.

When this command is enabled, the PPP negotiation with the MN starts 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 is torn down when timeout occurs.By default, this timeout interval is 10 seconds, or can be configured through the CLI.

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.

For example, with a default of 10 seconds, if the timer expires at t1 and a new call comes at t2(t2 >t1), the next run of the timer is at t1+10. It is likely that the uptime for the call is not more than 10 seconds since t2 > t1. So the call is checked at the next run (t1+10+10). Thus, the variation is between 1 and 10.

Examples

The following example shows how to enable the **cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout** command:

```
Router# cdma pdsn a10 init-ppp-after-airlink-start airlink-start-timeout 20
```

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

There are no keywords or variables for this command.

Defaults

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

Command Modes

Global configuration

Command History

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

Examples

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

```
Router# cdma pdsn a10 gre sequencing
```

Related Commands

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

cdma pdsn a10 max-lifetime

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

cdma pdsn a10 max-lifetime *seconds*

no cdma pdsn a10 max-lifetime

Syntax Description

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

Defaults

1800 seconds.

Command Modes

Global configuration

Command History

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

Examples

The following example shows how A10 interface can be maintained for 1440 seconds:

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

Related Commands

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

cdma pdsn a10 police downstream

To enable policing of downstream data traffic for the session, use the **cdma pdsn a10 police downstream** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn a10 police downstream

no cdma pdsn a10 police downstream

Syntax Description

There are no keywords or variable for this command.

Defaults

The default value is that policing is not applied for downstream packets.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn a10 police downstream** command:

```
Router(config)# cdma pdsn a10 police downstream
```

cdma pdsn a11 default-service-option *so-value*

To configure PDSN to send the F5 attribute as default configured value in the accounting records, use the **cdma pdsn a11 default-service-option** *so-value* command in the global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn a11 default-service-option *so-value*

no cdma pdsn a11 default-service-option

The command is used to configure the default Service Option (SO) value for the accounting records, when PDSN receives the F5 SO value as zero or when it did not receive the airlink start and the received service option for A10 is also zero.

Syntax Description

so-value	Indicates the service option value that must be configured as default value. The default value ranges from 1 to 65535.

Defaults

The default value is zero.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn a11 default-service-option** command:

```
Router(config)# cdma pdsn a11 default-service-option ?
<1-65535>  Default Service Option

Router(config)# cdma pdsn a11 default-service-option 59
```

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

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

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

No default values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Disabling this behavior avoids traffic channel allocation for cleaning up ppp sessions at the mobile.

Examples

The following example shows how to enable the **cdma pdsn all dormant ppp-idle-timeout send-termreq** command:

```
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 are 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. Use the **no** form of the command to disable this feature.

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
group-number	Specifies the classified match criteria.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to enable 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 the 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
group-number	Specifies the classified match criteria.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF2	This command was introduced.

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. Basically, 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 setup to deliver these LCP echo requests to the MN. The other option is to use SDBs to deliver the LCP echo requests without setting up a data channel.

Examples

The following example shows how to enable 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. Use the **no** form of the command to disable this feature.

cdma pdsn a11 mandate presence airlink-setup

no cdma pdsn a11 mandate presence airlink-setup

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)ZB1	This command was introduced.

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

The following example shows how to enable the **cdma pdsn all mandate presence airlink-setup** command:

```
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. Use the **no** form of the command to disable this feature.

cdma pdsn a11 receive de-reg send-termreq

no cdma pdsn a11 receive de-reg send-termreq

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF	This command was introduced.

Examples

The following example shows how to enable 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. Use the **no** form of the command to disable this feature.

cdma pdsn a11 reject airlink-start active

no cdma pdsn a11 reject airlink-start active

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YR	This command was introduced.

Examples

The following example shows how to enable 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. Use the **no** form of the command to disable this feature.

cdma pdsn a11 reject airlink-stop dormant

no cdma pdsn a11 reject airlink-stop dormant

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn a11 reject airlink-stop dormant** command:

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

cdma pdsn a11 send reply post ixp-update

To enable the PDSN to send the A11 RRP after receiving the acknowledgement from IXP for the PCF IP/GRE key add message sent, use the **cdma pdsn a11 send reply post ixp-update** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn a11 send reply post ixp-update

no cdma pdsn a11 send reply post ixp-update

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR1	This command was introduced.

Usage Guidelines

This command enables PDSN to send the A11 RRP only after receiving the acknowledgement from IXP. This command must be configured if the MN cannot perform PPP retries.

Examples

The following example shows how to enable the **cdma pdsn a11 send reply post ixp-update** command:

```
san-pdsn(config)# cdma pdsn a11 ?
  airlink-setup           Configure CDMA PDSN a11 Airlink Setup parameters
  default-service-option  Configure CDMA PDSN a11 default SO value
  dormant                 Configure CDMA PDSN a11 dormancy parameters
  mandate                 Configure mandatory parameters in A11 RRQ
  receive                 Configure CDMA PDSN a11 receive parameters
  reject                  reject
  send                    Configure options to send A11 messages
  session-update          Enable A11 Session Update feature

san-pdsn(config)# cdma pdsn a11
*Mar  1 00:01:17.015: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1.1.1.19 port 514
started - reconnection
san-pdsn(config)# cdma pdsn a11 send
san-pdsn(config)# cdma pdsn a11 send ?
  reply  Configure options for send a11 registration reply

san-pdsn(config)# cdma pdsn a11 send rep
san-pdsn(config)# cdma pdsn a11 send reply ?
  post  Configure options for send a11 registration reply

san-pdsn(config)# cdma pdsn a11 send reply po
san-pdsn(config)# cdma pdsn a11 send reply post ?
  ixp-update  Configure to send A11 RRP after updating IXP
```

```
san-pdsn(config)# cdma pdsn a11 send reply post i
san-pdsn(config)# cdma pdsn a11 send reply post ixp-update ?
  <cr>

san-pdsn(config)# cdma pdsn a11 send reply post ixp-update
san-pdsn(config)# end
```

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 RNPDIT (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
always-on	Sends an A11 session update for the Always On attribute that is downloaded from the AAA during the authentication phase.
rn-pdit	Sends an A11 session update for the RN-PDIT attribute that is downloaded from the AAA during the authentication phase.
1-10	Sets the timeout value for re-transmission of the A11 session update message to the PCF. The default timeout value is 3 seconds.
0-9	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.

Examples

The following example shows how to enable 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 a11 session-update qos

To enable sending a Subscriber QoS profile through an A11 session-update and A11 RRP, use the **cdma pdsn a11 session-update qos** command in global configuration mode. Use the **no** form of the command disable this feature. The existing timeout and retransmit a11 session-update configurations also apply to this command.

cdma pdsn a11 session-update qos

no cdma pdsn a11 session-update qos

Syntax Description

There are no keywords or variables for this command.

Defaults

The default value is that subscriber QoS is not sent in session update.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn a11 session-update qos** command:

```
Router(config)# cdma pdsn a11 session-update qos
```

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

There are no keywords or variables for this command.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set the local time in Korea:

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

Related Commands

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

cdma pdsn accounting main-flow

To configure PDSN to stop sending the accounting records for the ipflows, use the **cdma pdsn accounting main-flow** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn accounting main-flow

no cdma pdsn accounting main-flow

When you enable this command, accounting records for ipflows are not sent. Also, any traffic that is accounted in the ipflows is ignored and not added in the traffic details of the main-flow.

Note

- If you did not enable **cdma pdsn accounting main-flow** or **cdma pdsn accounting main-flow include ipflows**, then per-ipflow based accounting is performed, which means accounting records are sent per-ipflow.
- If you configure **cdma pdsn accounting main-flow include ipflows** first and later configure **cdma pdsn accounting main-flow**, the former configuration is removed.

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn accounting main-flow** command:

```
PDSN_ACT(config)# cdma pdsn accounting main-flow
```

cdma pdsn accounting main-flow include ipflows

To configure PDSN to stop sending the accounting records for the ipflows, use the **cdma pdsn accounting main-flow include ipflows** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn accounting main-flow include ipflows

no cdma pdsn accounting main-flow

When you enable this command, accounting records for ipflows are not sent. Also, any traffic that is accounted in the ipflows is added in the traffic details of the main-flow when you send the accounting records for the main-flow.

Note

- If you did not enable **cdma pdsn accounting main-flow** or **cdma pdsn accounting main-flow include ipflows**, then per-ipflow based accounting is performed, which means accounting records are sent per-ipflow.
- If you configure **cdma pdsn accounting main-flow** first and later configure **cdma pdsn accounting main-flow include ipflows**, the former configuration is removed.

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn accounting main-flow include ipflows** command:

```
PDSN_ACT(config)# cdma pdsn accounting main-flow include ipflows
```

cdma pdsn accounting prepaid

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

cdma pdsn accounting prepaid [volume | duration]

no cdma pdsn accounting prepaid [volume | duration]

Syntax Description

Command	Description
volume	Specifies that quota metering on the PDSN is volume-based.
duration	Specifies that quota metering on the PDSN is duration-based.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XW	This command was introduced.

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 the on PDSN for Prepaid service. Use the **cdma pdsn radius disconnect** command to enable the radius disconnect (POD) feature.

Examples

The following example shows 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. Use the **no** form of the command to disable this feature.

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

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

Syntax Description

Command	Description
volume	Specifies the threshold value to be applied to volume-based accounting. The values are 10-100, and they specify the Volume Threshold percentage.
duration	Specifies the threshold value to be applied 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. **Note** The threshold values returned in the Access Accept message, for the user, overrides this value.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows 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 remote address compliance 835b

To enable support for IS 835B compliant RAA table index downloaded from AAA, use the **cdma pdsn accounting remote address compliance 835b** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn accounting remote address compliance 835b

no cdma pdsn accounting remote address compliance 835b

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

When you enable this command RAA table index of IS 835B standard compliant is accepted during access accept. Other forms of the RAA table index are rejected. When you disable the configuration, RAA table index of both IS 835B, IS 835C, and IS 835D formats are accepted.

Examples

The following examples shows how to enable the **cdma pdsn accounting remote address compliance 835b** command:

```
PDSN_STDBY# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PDSN_STDBY(config)# cdma pdsn accounting ?
  local-timezone  Enable local timezone values for accounting
  main-flow       Accounting on Main Flow
  prepaid         Prepaid related configurations
  remote          Configure Remote Accounting
  send            Accounting option
  time-of-day     Generate accounting record at specified time

PDSN_STDBY(config)# cdma pdsn accounting remote ?
  address  Configure Remote Address Account

PDSN_STDBY(config)# cdma pdsn accounting remote address ?
  compliance  Remote address accounting standard compliance
  table       Configure Remote Address Accounting Table

PDSN_STDBY(config)# cdma pdsn accounting remote address compliance ?
  835b  Remote address accounting standard compliance 835b

PDSN_STDBY(config)# cdma pdsn accounting remote address compliance 835b ?
```

```
  <cr>
PDSN_STDBY(config)# cdma pdsn accounting remote address compliance 835b
PDSN_STDBY(config)# no cdma pdsn accounting remote address compliance 835b
PDSN_STDBY(config)#
```

cdma pdsn accounting remote address table

To enable remote address-based accounting, use the **cdma pdsn accounting remote address table** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn accounting remote address table

no cdma pdsn accounting remote address table

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

You must use the **index** *number* in the config-RAA sub-mode to configure an index for the remote address table. You can add the list of remote addresses that are to be tracked in the index.

The **cdma pdsn accounting remote address table** command enables the remote address-based accounting. It also enables the RAA sub-mode (config-RAA) to configure the index for remote accounting.

Examples

The following examples shows how to enable the **cdma pdsn accounting remote address table** command:

```
PDSN-ACT(config)# cdma pdsn accounting ?
  local-timezone  Enable local timezone values for accounting
  main-flow       Accounting on Main Flow
  remote          Configure remote accounting
  send            Accounting option
  time-of-day     Generate accounting record at specified time

PDSN-ACT(config)# cdma pdsn accounting remote ?
  address  Configure remote address account

PDSN-ACT(config)# cdma pdsn accounting remote address ?
  table  Configure Remote Address Accounting Table

PDSN-ACT(config)# cdma pdsn accounting remote address table

PDSN-ACT(config-raa)#?
  exit   Exit from remote address table
  index  Remote table index
  no     negative values of a command
```

```
PDSN-ACT(config-raa)# index ?
  <1-65535>  Value

PDSN-ACT(config-raa)# index 1
```

Note The **index** *number* command configures an index for the remote address table. You can enter the list of remote addresses that must be tracked in the index.

```
PDSN-ACT(config-raa-table)#?
  description  Description about the remote table index
  exit         Exit from remote address table index
  no           negative values of a command
  remote       Configure remote address

PDSN-ACT(config-raa-table)# description test_1
```

Note The **description** *index_name* command provides a short description about the index.

```
PDSN-ACT(config-raa-table)# remote ?
  address  Configure destination address

PDSN-ACT(config-raa-table)# remote address ?
  A.B.C.D  IP address

PDSN-ACT(config-raa-table)# remote address 1.2.3.4 ?
  A.B.C.D  IP address mask

PDSN-ACT(config-raa-table)# remote address 1.2.3.4 255.255.255.255
PDSN-ACT(config-raa-table)# exit
PDSN-ACT(config-raa)# exit
PDSN-ACT(config)# exit
PDSN-ACT#
PDSN-ACT#sh run | sec remote address
cdma pdsn accounting remote address table
  index 1
    description test_1
    remote address 1.2.3.4 255.255.255.255
PDSN-ACT#

PDSN-ACT(config)# cdma pdsn accounting remote address table index match
```

Note The **cdma pdsn accounting remote address table index match** command forces the condition that the session can be opened only if all the indexes downloaded from the AAA server during access-accept matches with the table configured in PDSN. If there are mismatches, the session is dropped.

cdma pdsn accounting send cdma-ip-tech

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History

Release	Modification
12.1XC	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn accounting send cdma-ip-tech** command:

```
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 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 the command to disable this feature.

cdma pdsn accounting send ipv6-flows *number*

no cdma pdsn accounting send ipv6-flows *number*

Syntax Description

Command	Description
number	Number of flows. The default value is 1, denoting 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.

Usage Guidelines

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

Examples

The following example shows how to enable 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 the command.

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

When this feature is enabled, the PDSN sends:

- 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 shows how to start sending PDSN accounting events:

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

Related Commands

Command	Description
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 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.

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. Use the **no** form of the command to disable this feature.

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

no cdma pdsn accounting time-of-day

Syntax Description

hh:mm:ss	Hour:minutes:seconds.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set an accounting trigger for 13:30:20:

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

Related Commands

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

cdma pdsn accounting vpdn address

To send the accounting records for VPDN calls with the IP address assigned to the mobile by Layer 2 Network Server (LNS), use the **cdma pdsn accounting vpdn address** command. Use the **no** form of the command to disable this feature.

cdma pdsn accounting vpdn address [include re-negotiation]

no cdma pdsn accounting vpdn address

Syntax Description

include re-negotiation	(Optional) When this option is configured for a flow, all the packets from the LNS to the mobile are snooped for IPCP configuration acknowledgement packets. The flow's mobile node IP address is overwritten.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Usage Guidelines

If the IP address changes during PPP renegotiation with the LNS, **Acct-stop** [*old ip*] or **Acct-start** [*new ip*] will be triggered. If the same IP address is assigned during the PPP renegotiation with the LNS, **Acct-stop** [*old ip*] or **Acct-start** [*new ip*] will not be triggered.

Examples

The following example shows how to enable the VPDN client for IP accounting support:

```
router(config)# cdma pdsn accounting vpdn address
```

cdma pdsn age-idle-users

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

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

no cdma pdsn age-idle-users

Syntax Description

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

Defaults

No idle users are aged out.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set 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} a3
    {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}| f17{acct-reqs} | f18 {acct-reqs} | f19 {acct-reqs}
    | f20 {acct-reqs} | f22 {acct-reqs} | 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} a3
    {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}| f17{acct-reqs} | f18 {acct-reqs} | f19 {acct-reqs}
    | f20 {acct-reqs} | f22 {acct-reqs} | g1 {acct-start} | g2 {acct-start} | g17 | esn-optional |
    is835a}
```

Syntax Description

a1	Attribute Calling Station ID
a2	Attribute ESN, Electronic Serial Number
a3	Attribute MEID, Mobile Equipment Identifier.
c5	Attribute c5, Service Reference ID
auth-req	Sends attribute in an access request during pap/chap.
fa-chap	Sends attribute in FA-CHAP.
mip-rrq	Sends attribute in a Mobile IP RRQ.
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 acct-reqs	Attribute f15, always-on
f16 acct-reqs	Attribute f16, Forward PDCH RC
f17 acct-reqs	Attribute f17, Forward DCCH Mux Option
f18 acct-reqs	Attribute f18, Reverse DCCH Mux Option
f19 acct-reqs	Attribute f19, Forward DCCH RC
f20 acct-reqs	Attribute f20, Reverse DCCH RC
f22 acct-reqs	Attribute f22, Reverse 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 *attribute* in fa-chap
mip-rrq	Send *attribute* in mobile ip RRQ

acct-reqs	Send *attribute* in start/stop/interim records for non always-on users
auth-req	Send *attribute* in access request during pap/chap
acct-start	Send *attribute* 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 **F11** attribute was introduced.
12.4(15)XN	The **f17**, **f18**, **f19**, **f20**, and **f22** attributes were added.

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 shows how to enable the **cdma pdsn attribute send** command:

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

The attribute **a1** is sent in the access request during FA-CHAP.

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

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

Here is sample output for PDSN Release 4.0:

```
cdma pdsn attribute send ?
  a1             Attribute Calling Station ID
  a2             Attribute ESN, Electronic Serial Number
  a3             Attribute MEID, Mobile Equipment Identifier
  c5             Service Reference ID
  esn-optional   Send ESN in Access Req/accounting records only when received
                 from PCF

  f11            IP Technology
  f15            Attribute f15, always-on
  f16            Forward PDCH RC ------------------------|
  f17            Forward DCCH MUX------------------------|
  f18            Reverse DCCH MUX------------------------|-----> new
  f19            Forward DCCH RC------------------------ |
  f20            Reverse DCCH RC ------------------------|
  f22            Reverse PDCH RC------------------------ |
  f5             Attribute Service Option
  g1             Attribute Input Octets
  g17            Last known user activity
  g2             Attribute Output Octets
  is835a         is835a specified attributes (g3 and g8 to g16)
  meid-optional  Send MEID in Access req/accounting records only when received from PCF
```

cdma pdsn attribute send 3gpp2 pmip-indicator auth-req

To send Third Generation Partnership Project 2 (3GPP2) proxy mobile IP (PMIP)-based mobility capability attribute in an access-request message to the AAA server (with value as 1 for PMIP4 support if FA is enabled), use the **cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute send 3gpp2 pmip-indicator auth-req

no cdma pdsn attribute send 3gpp2 pmip-indicator auth-req

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** command:

```
Router (config)# cdma pdsn attribute send 3gpp2 pmip-indicator auth-req
```

cdma pdsn attribute send b1 auth-req

To send the framed IP address in access-request message, use the **cdma pdsn attribute send b1 auth-req** command in global configuration mode. The command can be enabled for the authentication-request option. Use the **no** form of the command to disable this feature.

cdma pdsn attribute send b1 auth-req

no cdma pdsn attribute send b1 auth-req

Syntax Description

Command	Description
auth-req	Sends attribute in an access-request message during PAP/CHAP.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Usage Guidelines

Disable the **radius-server attribute 8 include-in-access-req** command to use the **cdma pdsn attribute send b1 auth-req** command for sending the framed-ip-address attribute. To configure the CLI command **cdma pdsn attribute send b1 auth-req**, the CLI command **ip mobile foreign-agent send-mn-address** must be configured already. Without configuring the **ip mobile foreign-agent send-mn-address** CLi command, you can not configure **cdma pdsn attribute send b1 auth-req**.

Similarly, if both the CLI commands, **ip mobile foreign-agent send-mn-address** and **cdma pdsn attribute send b1 auth-req** are enabled, then to disable the CLI command **ip mobile foreign-agent send-mn-address**, first disable the **cdma pdsn attribute send b1 auth-req** CLI command.

Examples

The following example shows how to enable the **cdma pdsn attribute send b1 auth-req** command:

```
Router (config)# cdma pdsn attribute send b1 auth-req
```

cdma pdsn attribute send d3 {auth-req | fa-chap | online-req}

To send the packet control function (PCF) IP address in an access-request message, use the **cdma pdsn attribute send d3 {auth-req | fa-chap | online-req}** command in global configuration mode. You can enable this command for three options: to send an authentication-request (auth-req), to send the d3 attribute in an access-request message during a MIP call (fa-chap) and to send the d3 attribute in prepaid online access-request message (online-req). Use the **no** form of the command to disable this feature.

cdma pdsn attribute send d3 {auth-req | fa-chap | online-req}

no cdma pdsn attribute send d3 {auth-req | fa-chap | online-req}

Syntax Description

Command	Description
auth-req	Sends attribute in an access-request message during PAP/CHAP.
fa-chap	Sends d3 attribute in a access-request message during a MIP call.
online-req	Sends d4 attribute in a prepaid online access-request message.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send d3** command to use the **auth-req** option, or **fa-chap** option, or **online-req** option:

```
Router (config)# cdma pdsn attribute send d3 auth-req
```

or

```
Router (config)# cdma pdsn attribute send d3 fa-chap
```

or

```
Router (config)# cdma pdsn attribute send d3 online-req
```

cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}

To send the base station identification (BSID) in an access-request message use the **cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}** command in global configuration mode. You can enable this command for three options: to send authentication-request (auth-req), to send the d4 attribute in an access-request message during MIP call (fa-chap), and to send the d4 attribute in a prepaid online access-request message (online-req). Use the **no** form of the command to disable this feature.

cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}

no cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}

Syntax Description

Command	Description
auth-req	Sends attribute in an access-request message during PAP/CHAP.
fa-chap	Sends d4 attribute in an access-request message during a MIP call.
online-req	Sends d4 attribute in a prepaid online access-request message.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send d4** command to use the **auth-req** option, or **fa-chap** option, or **online-req** option:

```
Router (config)# cdma pdsn attribute send d4 auth-req
```

or

```
Router (config)# cdma pdsn attribute send d4 fa-chap
```

or

```
Router (config)# cdma pdsn attribute send d4 online-req
```

cdma pdsn attribute send e1 {auth-req | fa-chap | online-req}

To send the user zone in an access-request message, use the **cdma pdsn attribute send e1 {auth-req | fa-chap | online-req}** command in global configuration mode. You can enable this command for three options: to send authentication-request (auth-req), d4 attribute in access-request message during MIP call (fa-chap) and, d4 attribute in prepaid online access-request message (online-req). Use the **no** form of the command to disable this feature.

cdma pdsn attribute send e1 {auth-req | fa-chap | online-req}

no cdma pdsn attribute send e1 {auth-req | fa-chap | online-req}

Syntax Description

Command	Description
auth-req	Sends attribute in an access-request message during PAP/CHAP.
fa-chap	Sends d4 attribute in access-request message during MIP call.
online-req	Sends d4 attribute in prepaid online access-request message.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send e1** command to use the **auth-req** option, or **fa-chap** option, or **online-req** option:

```
Router (config)# cdma pdsn attribute send e1 auth-req
```

or

```
Router (config)# cdma pdsn attribute send e1 fa-chap
```

or

```
Router (config)# cdma pdsn attribute send e1 online-req
```

cdma pdsn attribute send gre_cvse mip_rrq

Cisco PDSN sends the Generic Routing Encapsulation (GRE) of Critical Vendor-Specific Extension (CVSE) in all Mobile IP (MIP) Registration Requests (RRQ) to all Home Agents (HA). This forwarding happens if Cisco PDSN has received a MIP RRQ with the GRE bit set. If GRE CVSE negotiation happens between the FA and HA, the FA must include the GRE CVSE in the revocation message.

To configure Cisco PDSN to send GRE CVSE in all MIP RRQs to all HAs, use the **cdma pdsn attribute send gre_cvse mip_rrq** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute send gre_cvse mip_rrq

no cdma pdsn attribute send gre_cvse mip_rrq

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.
12.4(22)XR1	The condition for FA to include the GRE CVSE in the revocation message is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send gre_cvse mip_rrq** command:

```
Router (config)# cdma pdsn attribute send gre_cvse mip_rrq
```

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. Use the **no** form of the command to disable this feature.

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.

Usage Guidelines

If the MN is not equipped to send the MEID, MEID is excluded from the RRQ. In such circumstances, a blank string is 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 accounting requests and access requests, in FA-CHAP requests and MOIP- requests, only if it is included in the RRQ.

Examples

The following example shows how to enable the **cdma pdsn attribute send meid-optional** command:

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

cdma pdsn attribute send nas-port include-in-authen-req

To send the NAS port in an access-request message, use the **cdma pdsn attribute send nas-port include-in-authen-req** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute send nas-port include-in-authen-req

no cdma pdsn attribute send nas-port include-in-authen-req

Syntax Description

There are no arguments of keywords for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute send nas-port include-in-authen-req** command:

```
Router (config)# cdma pdsn attribute send nas-port include-in-authen-req
```

cdma pdsn attribute vendor

To configure the PDSN to parse the served MDN attribute sent in the China Telecom VSA, and send the attributes in accounting messages, use the **cdma pdsn attribute vendor** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor [**20492**]

no cdma pdsn attribute vendor [**20492]**

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XR2	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor** command:

```
Router (config)# cdma pdsn attribute vendor?
20492 cnctc
```

cdma pdsn attribute vendor 20942

To configure PDSN to parse the charging type that has been downloaded, use the **cdma pdsn attribute vendor 20942** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor 20942

no cdma pdsn attribute vendor 20942

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor 20942** command:

```
Router (config)# cdma pdsn attribute vendor 20942
```

cdma pdsn attribute vendor 20942 send a1 mip_rrq

To configure PDSN to send the calling station ID attribute in the Mobile IP (MIP) Registration Request (RRQ) as CNCTC Normal Vendor Specific Extension (NVSE), use the **cdma pdsn attribute vendor 20942 send a1 mip_rrq** command in Global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor 20942 send a1 mip_rrq

no cdma pdsn attribute vendor 20942 send a1 mip_rrq

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor 20942 send a1 mip_rrq** command:

```
Router (config)# cdma pdsn attribute vendor 20942 send a1 mip_rrq
```

cdma pdsn attribute vendor 20942 send c2 mip_rrq

To configure PDSN to send the correlation ID attribute in the Mobile IP (MIP) Registration Request (RRQ) as CNCTC NVSE, use the **cdma pdsn attribute vendor 20942 send c2 mip_rrq** command in Global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor 20942 send c2 mip_rrq

no cdma pdsn attribute vendor 20942 send c2 mip_rrq

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor 20942 send c2 mip_rrq** command:

```
Router (config)# cdma pdsn attribute vendor 20942 send c2 mip_rrq
```

cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs

To configure PDSN to send the PDSN source IP address in the accounting records, use the **cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs** command in Global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs

no cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs** command:

```
Router (config)# cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs
```

cdma pdsn attribute vendor 20942 send pmip_capability access_request

To configure PDSN to send the Proxy-Mobile IP (PMIP) functionality to the RADIUS server use the **cdma pdsn attribute vendor 20942 send pmip_capability access_request** command in Global configuration mode. The RADIUS server in turn sends the PMIP indicator in the Access-Accept message. PDSN provides the PMIP functionality to the mobile user if it receives the PMIP indicator value as 1. Use the **no** form of the command to disable this feature.

cdma pdsn attribute vendor 20942 send pmip_capability access_request

no cdma pdsn attribute vendor 20942 send pmip_capability access_request

Syntax Description

20492	The attribute number for the China Telecom VSA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn attribute vendor 20942 send pmip_capability access_request** command:

```
Router (config)# cdma pdsn attribute vendor 20942 send pmip_capability access_request
```

cdma pdsn attribute vendor 20942 accept -ct-mhae

To configure PDSN to parse attributes 57 and 58 of the 3gpp2 PMIP MHAE SA:

- Download the attributes from AAA.
- Use the following command in the global configuration mode:

  cdma pdsn attribute vendor 20942 accept-ct-mhae

Use the **no** form of this command to disable parse for attributes 57 and 58:

no cdma pdsn attribute vendor 20942 accept-ct-mhae

Syntax Description

accept-ct-mhae	When you run this command PDSN parses attributes 57 and 58 of the 3gpp2 PMIP MHAE SA.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR 2	This command was introduced.

Examples

The following is an example for enabling the command **accept-ct-mhae**:

```
Router (config)# cdma pdsn attribute vendor 20942 accept-ct-mhae
```

cdma pdsn cac maximum

To enable the Call Admission Control feature, and to control the CAC bandwidth parameter and CAC CPU parameters, use the **cdma pdsn cac maximum** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn cac maximum [**bandwidth** | **cpu**]

no cdma pdsn cac maximum [**bandwidth** | **cpu**]

Syntax Description

bandwidth	Configures the maximum bandwidth.
cpu	Configures the CPU threshold parameters.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Usage Guidelines

The Call Admission Control feature is only enabled if the CAC CLI for CPU and Bandwidth is configured.

Examples

The following example shows how to enable the **cdma pdsn cac maximum bandwidth** command:

```
cdma pdsn cac ?
  maximum          Configure Maximum values for CAC Parameters

cdma pdsn cac maximum ?
  bandwidth        Configure Maximum Bandwidth
  cpu-threshold    Configure CPU Threshold parameters

cdma pdsn cac maximum bandwidth ?
  <8000-2000000000>  Value
```

The following example shows how to enable the **cdma pdsn cac maximum cpu** command:

```
cdma pdsn cac ?
  maximum          Configure Maximum values for CAC Parameters

cdma pdsn cac maximum ?
        bandwidth  Configure CDMA PDSN cac maximum bandwidth
        cpu        Configure CDMA PDSN cac CPU

cdma pdsn cac cpu ?
  <30-90>         Value
```

cdma pdsn cluster controller

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

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

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

Syntax Description

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

Defaults

The timeout default value is 10 seconds and the default value for option window is 2.

Command Modes

Global configuration

Command History

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

Examples

The following example shows how to enable the cdma cluster controller:

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

cdma pdsn cluster controller member

To enable the periodic process to flush the dangling session records on the controller, enable the cluster controller to use CAC parameters to distribute the load, and enable the member selection policy, use the **cdma pdsn cluster controller member** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn cluster controller member {**periodic-update** | **reva-support** | **selection-policy**}

no cdma pdsn cluster controller member {**periodic-update** | **reva-support** | **selection-policy**}

Syntax Description

periodic-update	Enables receiveing periodic session information from members.
reva-support	Configures member reva-support.
selection-policy	Configures member selection-policy.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)ZB1	This command was introduced.
12.4(15)XN	This **reva-support** keyword was introduced.

Examples

The following example shows how to enable the **cdma pdsn cluster controller member reva-support** command:

```
Router(config)# cdma pdsn cluster controller member ?
        periodic-update   Receive periodic session info from members
        reva-support      Member reva-support
        selection-policy  Member selection policy
```

cdma pdsn cluster controller pcf group

To perform PCF redirection in a cluster controller, the PCF and PDSN groups must be configured. Use the **cdma pdsn cluster controller pcf group** command in global configuration mode to configure a list of PCF IP addresses under a group. Use the **no** form of the command to remove the configured PCF group.

cdma pdsn cluster controller pcf group *Group Number*

no cdma pdsn cluster controller pcf group *Group Number*

Syntax Description

Group Number	Indicates the PCF group number.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

Using the command, you can configure a single or a list of PCF IP addresses under one group. You cannot configure overlapping PCF IP addresses within same or different groups.

Examples

The following example shows how to configure a PCF group in a cluster controller:

```
PDSN(config)# cdma pdsn cluster controller ?
  interface           Name of the interface to use to cluster with members
  member              Configure member parameters
  pcf                 PCF Group
  pdsn                PDSN Group
  queueing            Request queueing for controller
  redirect            PDSN Redirection
  rp-signaling-proxy  Proxy R-P signaling to PDSN cluster members
  session-high        Configure cluster controller high session water mark
  session-low         Configure cluster controller low session water mark
  standby             Enable hotstandby support
  timeout             Time without msg from a member until controller seeks
                      this member
  window              Sequential seek msgs sent to member before it is presumed
                      offline

PDSN(config)# cdma pdsn cluster controller pcf ?
  group  PCF Group

PDSN(config)# cdma pdsn cluster controller pcf group ?
  <1-100>  PCF Group number
```

```
PDSN(config)# cdma pdsn cluster controller pcf group 1
PDSN(config-pcf-group)# ?
  description  Group description
  exit         Exit from PCF group mode
  no           negate values of a  command
  pcf          PCF Addresses

PDSN(config-pcf-group)# description ?
  WORD  PCF group description

PDSN(config-pcf-group)# descri
PDSN(config-pcf-group)# description PCF_G1
PDSN(config-pcf-group)#
PDSN(config-pcf-group)# pcf ?
  A.B.C.D  Start IP Address

PDSN(config-pcf-group)# pcf 2.2.2.2 ?
  A.B.C.D  End IP address
  <cr>
PDSN(config-pcf-group)# pcf 2.2.2.2 3.3.3.3
PDSN(config-pcf-group)# end
PDSN#
PDSN# sh run | section pcf group
cdma pdsn cluster controller pcf group 1
  description PCF_G1
  pcf 2.2.2.2 3.3.3.3
PDSN#
```

cdma pdsn cluster controller pdsn group

To perform PCF redirection in a cluster controller, the PCF and PDSN groups must be configured. Use the **cdma pdsn cluster controller pdsn group** command in global configuration mode to configure a list of PDSN IP addresses under a group. Use the **no** form of the command to remove the configured PDSN group.

cdma pdsn cluster controller pdsn group *Group Number*

no cdma pdsn cluster controller pdsn group *Group Number*

Syntax Description

Group Number	Indicates the PDSN group number.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

Use the command to configure a single or a list of PDSN IP addresses under one group. You cannot configure overlapping PDSN IP addresses within same or different groups. Configure one primary PDSN IP address under one PDSN group, and use it whenever you have to select one PDSN from the given PDSN group.

Examples

The following example shows how to configure PDSN group in a cluster controller:

```
PDSN(config)# cdma pdsn cluster controller ?
  interface           Name of the interface to use to cluster with members
  member              Configure member parameters
  pcf                 PCF Group
  pdsn                PDSN Group
  queueing            Request queueing for controller
  redirect            PDSN Redirection
  rp-signaling-proxy  Proxy R-P signaling to PDSN cluster members
  session-high        Configure cluster controller high session water mark
  session-low         Configure cluster controller low session water mark
  standby             Enable hotstandby support
  timeout             Time without msg from a member until controller seeks
                      this member
  window              Sequential seek msgs sent to member before it is presumed
                      offline

PDSN(config)# cdma pdsn cluster controller pdsn ?
  group  PDSN Group

PDSN(config)# cdma pdsn cluster controller pdsn group ?
```

```
  <1-100>  PDSN Group number
PDSN(config)# cdma pdsn cluster controller pdsn group 2
PDSN(config-pdsn-group)#
PDSN(config-pdsn-group)# ?
  description  Group description
  exit         Exit from PDSN group mode
  no           negate values of a  command
  pdsn         PDSN Members in the group
  primary      Primary member of the group

PDSN(config-pdsn-group)# desc
PDSN(config-pdsn-group)# description ?
  WORD  PDSN group description

PDSN(config-pdsn-group)# description PDSN_G2
PDSN(config-pdsn-group)#
PDSN(config-pdsn-group)# pdsn ?
  A.B.C.D  Start IP Address

PDSN(config-pdsn-group)# pdsn 10.10.10.10 ?
  A.B.C.D  End IP address
  <cr>

PDSN(config-pdsn-group)# pdsn 10.10.10.10 20.20.20.1
PDSN(config-pdsn-group)#
PDSN(config-pdsn-group)# primary ?
  A.B.C.D  Primary member IP

PDSN(config-pdsn-group)# primary 30.30.30.30
PDSN(config-pdsn-group)#
PDSN(config-pdsn-group)# exit
PDSN(config)# exit
PDSN#
PDSN# sh ru
*Jul  8 11:02:25.330: %SYS-5-CONFIG_I: Configured from console by console
PDSN# sh run
PDSN# sh running-config | section pdsn group
cdma pdsn cluster controller pdsn group 2
  description PDSN_G2
  pdsn 10.10.10.10 20.20.20.1
  primary 30.30.30.30
PDSN#
```

cdma pdsn cluster controller redirect

To perform IMSI or PCF redirection in a cluster controller, use the **cdma pdsn cluster controller redirect** command in global configuration mode to configure a list of PDSN IP addresses under a group. Use the **no** form of the command to remove the redirection configuration in the controller.

cdma pdsn cluster controller redirect

no cdma pdsn cluster controller redirect

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

Use the command to configure IMSI or PCF redirection in a cluster controller.

Examples

The following examples show how to configure IMSI redirection in a cluster controller:

```
PDSN(config)# cdma pdsn cluster controller ?
  interface           Name of the interface to use to cluster with members
  member              Configure member parameters
  pcf                 PCF Group
  pdsn                PDSN Group
  queueing            Request queueing for controller
  redirect            PDSN Redirection
  rp-signaling-proxy  Proxy R-P signaling to PDSN cluster members
  session-high        Configure cluster controller high session water mark
  session-low         Configure cluster controller low session water mark
  standby             Enable hotstandby support
  timeout             Time without msg from a member until controller seeks
                      this member
  window              Sequential seek msgs sent to member before it is presumed
                      offline

PDSN(config)# cdma pdsn cluster controller redirect
PDSN(config-redirect)#?
  exit  Exit from PCF group mode
  imsi  IMSI redirection
  no    negate values of a  command
  pcf   PCF redirection

PDSN(config-redirect)# imsi ?
  WORD  Start IMSI number
```

```
PDSN(config-redirect)# imsi 123456789012345 ?
  WORD  End IMSI number
  pdsn  PDSN Group

PDSN(config-redirect)# imsi 123456789012345 123456789013400 ?
  pdsn  PDSN Group

PDSN(config-redirect)# imsi 123456789012345 123456789013400 pdsn ?
  <1-100>  PDSN Group number
[Note] PDSN group must be configured before configuring the IMSI redirection.

PDSN(config-redirect)# imsi 123456789012345 123456789013400 pdsn 2 ?
  force  Configure Force option
  <cr>
```

Note When you configure the **force** option of this command, the primary IP address configured under the PDSN group is used by default for IMSI redirection. It ignores the other PDSN IP addresses configured under the PDSN group. To configure the **force** option of this command, you have to configure the **primary** IP address under the PDSN group.

```
PDSN(config-redirect)# imsi 123456789012345 123456789013400 pdsn 2
PDSN(config-redirect)# end
PDSN#
PDSN# sh run | section redirect
cdma pdsn cluster controller redirect
  imsi 123456789012345 123456789013400 pdsn 2
PDSN#
```

Example for PCF redirection configuration:

```
PDSN(config)# cdma pdsn cluster controller ?
  interface           Name of the interface to use to cluster with members
  member              Configure member parameters
  pcf                 PCF Group
  pdsn                PDSN Group
  queueing            Request queueing for controller
  redirect            PDSN Redirection
  rp-signaling-proxy  Proxy R-P signaling to PDSN cluster members
  session-high        Configure cluster controller high session water mark
  session-low         Configure cluster controller low session water mark
  standby             Enable hotstandby support
  timeout             Time without msg from a member until controller seeks
                      this member
  window              Sequential seek msgs sent to member before it is presumed
                      offline

PDSN(config)# cdma pdsn cluster controller red
PDSN(config)# cdma pdsn cluster controller redirect
PDSN(config-redirect)#
PDSN(config-redirect)# ?
  exit  Exit from PCF group mode
  imsi  IMSI redirection
  no    negate values of a  command
  pcf   PCF redirection

PDSN(config-redirect)# pcf ?
  <1-100>  PCF Group number

PDSN(config-redirect)# pcf 1 ?
  pdsn  PDSN Group
```

Note You need to configure the PCF group before you configure the PCF redirection.

```
PDSN(config-redirect)# pcf 1 pdsn ?
  <1-100>  PDSN Group number
```

Note You need to configure the PDSN group before you configure the IMSI redirection.

```
PDSN(config-redirect)# pcf 1 pdsn 2 ?
  force  Configure Force option
  <cr>
```

Note When you configure the **force** option of this command, the primary IP address configured under the PDSN group is used by default for IMSI redirection. It ignores the other PDSN IP addresses configured under the PDSN group. To configure the **force** option of this command, you have to configure the **primary** IP address under the PDSN group.

```
PDSN(config-redirect)# pcf 1 pdsn 2 force
PDSN(config-redirect)# end
PDSN#
PDSN# sh run
PDSN# sh run | section redirect
cdma pdsn cluster controller redirect
  pcf 1 pdsn 2 force
PDSN#
```

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. Use the **no** form of the command to disable this feature.

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

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

Syntax Description

1-1000000	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.

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 shows how to enable 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. Use the **no** form of the command to disable this feature.

cdma pdsn cluster controller session-low *1-999999*

no cdma pdsn cluster controller session-low *1-999999*

Syntax Description

1-999999	The threshold of the maximum number of sessions the controller can handle.

Defaults

The range is 0-999999. The configured value should be less than the upper threshold value. The default value is 190000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)ZB1	This command was introduced.

Usage Guidelines

You should take into account the number of members in the cluster when you configure the low threshold.

Examples

The following example shows how to enable the **cdma pdsn cluster controller session-low** command:

```
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
```

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* | **prohibit** *type* | **timeout** *seconds* [**window** *number*] | **window** *number*]

Syntax Description

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

Defaults

The default timeout value for the cluster member is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.4(22)XR	Support for **queueing** is removed in this release.

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 shows how to enable 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. Use the **no** form of the command to disable this feature.

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 msecs.

Defaults

The default value is 1000 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

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

```
Router# cdma pdsn cluster member periodic-update 1000
```

cdma pdsn cluster member prohibit administratively

To separate a member PDSN out of the cluster use the **cdma pdsn cluster member prohibit administratively** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn cluster member prohibit administratively

no cdma pdsn cluster member prohibit administratively

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

Note By default the same HSRP interface is used for both the active and standby controller seek message exchanges, and active and standby record synchronization. If you choose to not use the HSRP address, and instead use a loopback address, issue this command.

The status of the member is updated to the controller in a subsequent periodic keepalive reply message the member sends to the controller. When the controller receives the message, it does not select this member for any of the new incoming calls. The member PDSNs that are prohibited administratively can be displayed on the controller using the **show cluster controller member prohibited administratively** command.

Examples

The following example shows how to enable the use of the **cdma pdsn cluster member prohibit administratively** command.

```
Router# cdma pdsn cluster member prohibit administratively
```

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 feature.

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

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

Syntax Description

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

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF1	This command was introduced.
12.3(11)YF2	The **sdb** keyword was introduced.

Examples

The following example shows how to enable one instance of the **cdma pdsn compliance** command:

```
Router# cdma pdsn compliance is835a
```

cdma pdsn compliance hrpd ipflow-discriminator

To configure PDSN to send the IP Flow Discriminator of 3 bytes without reserved bytes in the A10s, use the **cdma pdsn compliance hrpd ipflow-discriminator** command in the global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn compliance hrpd ipflow-discriminator

no cdma pdsn compliance hrpd ipflow-discriminator

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn compliance hrpd ipflow-discriminator** command:

```
PDSN(config)# cdma pdsn compliance hrpd ipflow-discriminator
```

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. Use the **no** form of the command to disable this feature.

cdma pdsn compliance iosv4.1 session-reference

no cdma pdsn compliance iosv4.1 session-reference

Syntax Description

There are no keywords or variables for this command.

Defaults

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

Command Modes

Global configuration.

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn dos

To enable dos, use the **cdma pdsn dos** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn dos

no cdma pdsn dos

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn dos** command:

```
Router(config)# cdma pdsn dos
```

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 feature.

Syntax Description

There are no keywords or variables for this command.

Defaults

The default value is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.

Usage Guidelines

When the debug conditions match, every line of the debug message is prefixed 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 CLIs being configured, the username/IMSI is not displayed in the debugs. However, if the CLIs are configured without configuring conditional debugging, the username/IMSI appears along with the debugs.

Examples

The following example shows how to enable 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

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

Defaults

No default values.

Command Modes

Global configuration

Command History

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

Examples

The following example shows how to specify 1000 as the maximum number of entries that can be recorded in the SNMP session table:

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

Related Commands

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

cdma pdsn imsi-min-equivalence

To support inter technology handoff of 1xRTT from Evolved Data Optimized (EVDO) or to EVDO, use the **cdma pdsn imsi-min-equivalence** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn imsi-min-equivalence

no cdma pdsn imsi-min-equivalence

Configure the **cdma pdsn imsi-min-equivalence** command in a fresh server with no sessions.

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable **cdma pdsn imsi-min-equivalence** command:

```
Router(config)# cdma pdsn imsi-min-equivalence
```

Show output when the mobile subscriber id (msid) number is lesser than 11 digits:

```
PDSN-ACT# show cdma pdsn session msid 45678987655
Mobile Station ID IMSI 112345678987655
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:02:33,  registration lifetime 20000 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime 19846 sec
  Always-On not enabled for the user
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 13, receive 0
  Using interface Virtual-Access3, status OPN
  Using AHDLC engine on slot 0, channel ID 2
  Service Option 1xRTT Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs
  Qos subscriber profile
```

Show output when the mobile subscriber id (msid) number is lesser than 10 digits:

```
PDSN-ACT# show cdma pdsn session msid 5678987655
```

```
Mobile Station ID IMSI 112345678987655
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:02:48, registration lifetime 20000 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime 19831 sec
  Always-On not enabled for the user
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 13, receive 0
  Using interface Virtual-Access3, status OPN
  Using AHDLC engine on slot 0, channel ID 2
  Service Option 1xRTT Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs
  Qos subscriber profile
```

cdma pdsn ingress-address-filtering

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

cdma pdsn ingress-address-filtering

no cdma pdsn ingress-address-filtering

Syntax Description

There are no keywords or variables for this command.

Defaults

Ingress address filtering is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable ingress address filtering:

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

Related Commands

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

cdma pdsn 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 feature.

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.

Usage Guidelines

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

```
%CDMA_PDSN-3-PDSNIPV6NOTENABLED: PDSN IPv6 feature has not been enabled.
```

Examples

The following example shows 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. Use the **no** form of the command to disable this feature.

cdma pdsn maximum pcf *maxpcf*

no cdma pdsn maximum pcf

Syntax Description

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

Defaults

No default values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to specify 200 as the maximum PCFs that can be sent:

```
cdma pdsn maximum pcf 200
```

Related Commands

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

cdma pdsn maximum sessions

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

cdma pdsn maximum sessions *maxsessions*

no cdma pdsn maximum sessions

Syntax Description

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

Defaults

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

The PDSN 4.0 Release supports 25000 sessions.

The PDSN 5.0 Release supports 175000 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.
12.4(15)xx	The maximum number of mobile sessions was raised to 25000.
12.4(22)XR	The maximum number of mobile sessions was raised to 175000.

Usage Guidelines

If PDSN runs out of resources before the configured number is reached, the PDSN rejects 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 shows how to set the maximum number of mobile sessions to 100:

```
cdma pdsn maximum sessions 100
```

Related Commands

Command	Description
show cdma pdsn session	Displays PDSN session information.

cdma pdsn mobile-advertisement-burst

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

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

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

Syntax Description

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

Defaults

The default number of agent advertisements to send is 5.

The default interval between advertisements is 200 milliseconds.

Command Modes

Interface or Global configuration.

Command History

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

Usage Guidelines

You must specify at least one of the optional parameters. Otherwise, the command has no effect. When virtual-access interfaces are created from the virtual template, default values are 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 shows how to configure PDSN FA advertisement:

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

Related Commands

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

cdma pdsn msid-authentication

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

cdma pdsn msid-authentication [**close-session-on-failure**] [**imsi** *number*] [**irm** *number*] [**min** *number*] [**profile-password** *password*]

no cdma pdsn msid-authentication

Syntax Description

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

Defaults

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

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

Command Modes

Global Configuration.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(2)XC	The **profile-password** keyword was added.
12.2(8)ZB1	The **close-session-on-failure** keyword was added

Usage Guidelines

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

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

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

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

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

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

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

Examples

The following example shows how to enable MSID-based authentication and access:

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

Related Commands

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

cdma pdsn multiple service-flows

To enable the Multiple flow support feature, use the **cdma pdsn multiple service-flows** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn multiple service-flows [**maximum** *number*]

no cdma pdsn multiple service-flows [**maximum** *number*]

Syntax Description

Command	Description
maximum *number*	Defines the maximum number of auxiliary A10s that can be created between the PDSN and the PCF. The default number of auxiliary A10s allowed is 7.

Defaults

The default number of auxiliary A10s allowed is 7. Main A10 also should be included here.

Command Modes

Global configuration mode.

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Usage Guidelines

Configure the **cdma pdsn multiple service-flows** command on the controller PDSN (no need for maximum number of connections).

Examples

The following example shows how to enable the **cdma pdsn multiple service-flows** command:

```
Router# cdma pdsn multiple service-flows ?
        maximum  Maximum limit
        qos      Configure qos parameters
        <cr>


Router# cdma pdsn multiple service-flows
Router# cdma pdsn multiple service-flows maximum 8
```

cdma pdsn multiple service-flows qos remark-dscp

To configure the DSCP remark value used for marking data packets, use the **cdma pdsn multiple service-flows qos remark-dscp** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn multiple service-flows qos remark-dscp *value*

no cdma pdsn multiple service-flows qos remark-dscp *value*

Syntax Description

Command	Description
value	Used for marking when the data packets from the mobile towards the internet is determined to have the DSCP not within the allowed dscp value for that mobile

Command Default

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Usage Guidelines

This command configures the DSCP remark value used for marking when the data packets from the mobile towards the internet are determined to have a DSCP value that is not within the allowed DSCP values for that mobile. Here are the values:

```
Router# cdma pdsn multiple service-flows qos remark-dscp ?
          AF11     AF11
          AF12     AF12
          AF13     AF13
          AF21     AF21
          AF22     AF22
          AF23     AF23
          AF31     AF31
          AF32     AF32
          AF33     AF33
          AF41     AF41
          AF42     AF42
          AF43     AF43
          Default  Selector Class 0
          EF       EF
          class1   Selector Class 1
          class2   Selector Class 2
          class3   Selector Class 3
          class4   Selector Class 4
          class5   Selector Class 5
          class6   Selector Class 6
          class7   Selector Class 7
```

Examples

The following example shows how to enable the **cdma pdsn multiple service-flows qos remark-dscp** command:

```
Router# cdma pdsn multiple service-flows qos remark-dscp AF11
```

cdma pdsn multiple service-flows qos remark-maxclass

To map the Differentiated Services Code Point (DSCP) value of the unauthorized packet (upstream) to a DSCP value on per-user basis, use the **cdma pdsn multiple service-flows qos remark-maxclass** command in global configuration mode. Use the **no** form of the command to disable this feature.

This command enables PDSN to map the DSCP value of the packet to the max-class value that is either downloaded from AAA or configured locally.

cdma pdsn multiple service-flows qos remark-maxclass

no cdma pdsn multiple service-flows qos remark-maxclass

Syntax Description

There are no keywords or arguments for this command.

Command Default

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn multiple service-flows qos remark-maxclass** command:

```
Router(config)# cdm pds multiple service-flows qos remark-maxclass
```

cdma pdsn multiple service-flows qos subscriber profile

To configure the local subscriber QoS profile, use the **cdma pdsn multiple service-flows qos subscriber profile** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn multiple service-flows qos subscriber profile

no cdma pdsn multiple service-flows qos subscriber profile

Syntax Description

There are no keywords or arguments for this command.

Command Default

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Usage Guidelines

This profile is used for a MN when the subscriber QoS profile is not downloaded from AAA.

Examples

The following example shows how to enable the **cdma pdsn multiple service-flows qos subscriber profile** command:

```
Router(config)# cdma pdsn multiple service-flows qos subscriber profile
        Router(config-qos-profile)#
        Eg:
        cdma pdsn multiple service-flows qos subscriber profile
```

cdma pdsn pcf

To enable sending of vendor specific attributes in subscriber QoS profile based on the PCF, use the **cdma pdsn pcf ip-address** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn pcf *PCF IP address ending IP address* **vendor-id** *NVSE Vendor id*

no cdma pdsn pcf *PCF IP address ending IP Address* **vendor-id** *NVSE Vendor id*

Syntax Description

PCF IP address	Single or starting PCF IP address
ending PCF IP address	Ending PCF IP address.
NVSE Vendor Id	Radius vendor ID of PCF.

Defaults

The default value is that the home area attribute is not sent to the PCF.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XN	This command was introduced.

Examples

The following example shows how to enable the cdma pdsn pcf command to configure vendor-id for a set of PCFs:

```
Router (config)# cdma pdsn pcf 10.1.1.1 10.1.1.50 vendor-id 3729
```

cdma pdsn qos policy flow-only

To enable flow-based policy, use the **cdma pdsn qos policy flow-only** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn qos policy flow-only

no cdma pdsn qos policy flow-only

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn qos policy flow-only** command:

```
Router(config)# cdma pdsn qos policy flow-only
```

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

The PDSN does 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.

Usage Guidelines

By default the PDSN does 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 is sent in Disconnect Request. Additionally, the overhead to maintain tables relating 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 **nai** keyword should be configured.

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

Examples

The following example shows how to enable the **cdma pdsn radius disconnect** command:

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

cdma pdsn redirect imsi

To perform IMSI redirection on a standalone PDSN, use the **cdma pdsn redirect imsi** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn redirect imsi *IMSI ending IMSI* **member** *Member-IP*

no cdma pdsn redirect imsi *IMSI*

Syntax Description

IMSI	Indicates the single or starting IMSI value.
Ending IMSI	Indicates the ending IMSI value.
Member-IP	Indicates the redirected PDSN IP address.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

You can configure the command for a single or a range of IMSI values. If both the values in the range are equal, then the command takes only the single IMSI value. If you enable the **cdma pdsn imsi-min-equivalence** command, only lower10 digits of the configured IMSI values are used effectively for the IMSI redirection.

Examples

The following example shows how to configure IMSI redirection for a Standalone PDSN for a range of IMSIs:

```
Router(config)# cdma pdsn redirect ?
imsi - IMSI Redirection
pcf - PCF Redirection

Router(config)# cdma pdsn redirect imsi ?
Single or Start IMSI - 15 digit IMSI address

Router(config)# cdma pdsn redirect imsi 123456789012345 ?
Ending IMSI - 15 digit IMSI address

Router(config)# cdma pdsn redirect imsi 123456789012345 123456789012400 ?
member - PDSN member

Router(config)# cdma pdsn redirect imsi 123456789012345 123456789012400 member ?
PDSN IP address - IP address of PDSN where A11 need to be redirected

Router(config)# cdma pdsn redirect imsi 123456789012345 123456789012400 member 2.1.1.1
```

cdma pdsn redirect pcf

To perform PCF redirection on a standalone PDSN, use the **cdma pdsn redirect pcf** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn redirect pcf *PCF IP Address ending PCF Address* **member** *Member-IP*

no cdma pdsn redirect pcf *PCF IP Address*

Syntax Description

PCF IP Address	Indicates the single or starting PCF IP address.
Ending PCF IP Address	Indicates the ending PCF IP address.
Member-IP	Indicates the redirected PDSN IP address.

Defaults

No default keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

You can configure the command for a single or a range of PCF IP addresses. If both the values in the range are equal, then the command takes only the single PCF IP address.

Examples

The following example shows how to configure PCF redirection for a Standalone PDSN for a range of IMSIs:

```
Router(config)# cdma pdsn redirect ?
imsi - MSID Redirection
pcf - PCF Redirection

Router(config)# cdma pdsn redirect pcf ?
PCF IP address - Single or Start of the range of PCF IP address

Router(config)# cdma pdsn redirect pcf 11.11.11.11 ?
PCF IP address - Last PCF address in the range

Router(config)# cdma pdsn redirect pcf 11.11.11.11 11.11.11.200 ?
member - PDSN member

Router(config)# cdma pdsn redirect pcf 11.11.11.11 11.11.11.200 member ?
PDSN IP address - IP address of PDSN where A11 need to be redirected

Router(config)# cdma pdsn redirect pcf 11.11.11.11 11.11.11.200 member 2.1.1.1
```

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 feature.

cdma pdsn redundancy

no cdma pdsn redundancy

Syntax Description

There are no arguments or keywords for this command.

Defaults

The PDSN redundancy is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.

Examples

The following example shows how to enable 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. Use the **no** form of the command to disable this feature.

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

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.

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 shows how to enable 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. Use the **no** form of the command to disable this feature.

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

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.

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 are not synced.

Examples

The following example shows how to enable 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

Syntax Description

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

Defaults

5 retransmissions.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set 9 as the maximum number of times for A11 Registration Update messages to be retransmitted:

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

Related Commands

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

cdma pdsn secure cluster

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

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

no cdma pdsn secure cluster

Syntax Description

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

Defaults

No default values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn secure pcf

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. Use the **no** form of the command to disable this feature.

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

no cdma pdsn secure pcf

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

The following example shows how to configure a global default replay time of 60 seconds for all PCFs and all SPIs:

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

The following example shows how to configure 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 shows how to configure 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
cdma pdsn secure cluster	Configures one common security association for all PDSNs in a cluster.
ip mobile secure	Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host.

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. Use the **no** form of the command to disable this feature.

cdma pdsn selection interface *interface_name*

no cdma pdsn selection interface

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to set FastEthernet0/1 interface for sending and receiving PDSN selection messages:

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

Related Commands

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

cdma pdsn selection keepalive

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

cdma pdsn selection keepalive *value*

no cdma pdsn selection keepalive

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Examples

The following example shows how to configure a keepalive value of 200 seconds:

```
cdma pdsn selection keepalive 200
```

Related Commands

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

cdma pdsn selection load-balancing

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

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

no cdma pdsn selection load-balancing

Syntax Description

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

Defaults

The threshold value is 100 sessions.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to configure load-balancing with an advertisement interval of 2 minutes and a threshold of 50 sessions:

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

Related Commands

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

cdma pdsn selection session-table-size

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

cdma pdsn selection session-table-size *size*

no cdma pdsn selection session-table-size

Syntax Description

size	Session table size. Possible values are 2000 through 100000.

Defaults

PDSN selection is disabled.

The default session table size is undefined.

Command Modes

Global Configuration

Command History

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

Examples

The following example shows how to set the size of the distributed session database to 5000 sessions:

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

Related Commands

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

cdma pdsn send-agent-adv

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

cdma pdsn send-agent-adv

no cdma pdsn send-agent-adv

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

This command is used with multiple flows.

Examples

The following example shows how to enable agent advertisements to be sent:

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

Related Commands

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

cdma pdsn sm add mobile route

Host routes for mobiles are added to the TCOPs except in the case of single IP mobiles, where, the ARP request for the mobile IP address lands on the PCOP.

To configure the PCOP to respond to the ARP requests, use **cdma pdsn sm add mobile route** command in configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn sm add mobile route

no cdma pdsn sm add mobile route

The command installs the host route for the mobile on the PCOP when the flow comes up and deletes the host route whenever the flow goes down. The command is needed only in cases where routes are not added to the Supervisor of the mobiles which connects through Simple IP calls.

Syntax Description

There are no keywords or variables for this command.

Defaults

This command is not configured.

Command Modes

Configuration Mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn sm add mobile route** command:

```
Router(config)# cdma pdsn sm add mobile route

PDSN-1# sh run | i mobile
router mobile
ip mobile foreign-agent care-of GigabitEthernet0/0.513
ip mobile secure home-agent 6.6.6.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.6.6.10 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge timeout 10 window 10
ip mobile foreign-service reverse-tunnel
ip mobile router
cdma pdsn sm add mobile route
```

cdma pdsn tft persistent-check

To check, before installing TFT, the 3GPP2 attribute Type 89 (cdma-num-persistence) downloaded from AAA, configure the **cdma pdsn tft persistent-check** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn tft persistent-check

no cdma pdsn tft persistent-check

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command Modes

Global Configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn ft persistent-check** command:

```
Router(config)# cdma pdsn tft persistent-check
```

cdma pdsn tft reject include error extension

To include the error extension in the reject message whenever a TFT is rejected, use the **cdma pdsn tft reject include error extension** command in global configuration mode. Use the **no** form of the command to disable this feature.

cdma pdsn tft reject include error extension

no cdma pdsn tft reject include error extension

Syntax Description

There are no keywords or arguments for this command.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4xx	This command was introduced.

Examples

The following example shows how to enable the **cdma pdsn tft reject include error extension** command:

```
cdma pdsn tft ?
  reject     Configure CDMA PDSN TFT reject

cdma pdsn tft reject ?
  include    Configure CDMA PDSN TFT reject include

cdma pdsn tft reject include ?
  error      Configure CDMA PDSN TFT reject include error

cdma pdsn tft reject include error ?
  extension  Configure CDMA PDSN TFT reject include error extension

cdma pdsn tft reject include error extension ?
```

cdma pdsn timeout

To configure a variety of 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**]

Syntax Description

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

Defaults

a11-session-update default value is 1 second.

Command Modes

Global Configuration

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.3(14)YF	The **close-rp** keyword was added.

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 can be modified using this command.

Examples

The following example shows how to set the timeout value for A11 Registration Update message to 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
```

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

cdma pdsn timeout mobile-ip-registration

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

cdma pdsn timeout mobile-ip-registration *timeout*

no cdma pdsn timeout mobile-ip-registration

Syntax Description

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

Defaults

5 seconds.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set the timeout value for Mobile IP registration to 15 seconds:

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

Related Commands

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

cdma pdsn virtual-template

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

cdma pdsn virtual-template *virtualtemplate_num*

no cdma pdsn virtual-template *virtualtemplate_num*

Syntax Description

virtualtemplate_num	Virtual template number. Possible values are 1 through 25.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear cdma pdsn cluster controller session record age

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

clear cdma pdsn cluster controller session record age *days*

Syntax Description

days	The number of days of the record age.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable the **clear cdma pdsn cluster controller session record age** command:

```
Router# clear cdma pdsn cluster controller session record 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

queuing	Clears statistics associated with controller queuing feature.
redundancy	Clears statistics associated with controller redundancy interface.

Defaults

No default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to enable 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 member statistics [queuing | statistics]

Syntax Description

queuing	Clears statistics associated with member queuing feature.

Defaults

No default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to enable 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

No default values.

Command Modes

EXEC mode

Command History

Release	Modification
12.3(14)YX	This command was introduced.

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 [rate** *value* | **send [a11-update** | **termreq]** *value*]} | **dormant** | **pcf** *ip_addr* | **msid** *number*}

Syntax Description

all	Keyword to clear all sessions on a given PDSN.
rate	Rate for clearing calls
send	Packets to send while clearing calls.
a11-update	Send A11 update to PCF to clear session.
termreq	Send LCP TERMREQ to Mobile to clear session.
value	Clear rate in approximate calls per second. The range is *1- 200*
dormant	Clear CDMA PDSN dormant session.
pcf *ip_addr*	IP address of the PCF sessions that are to be cleared.
msid *number*	Identification of the MSID to be cleared.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.3(11)YF1	The **rate**, **send**, **a11-update**, **dormant** and **termreq** variables were added.

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 clears the session for a given MSID.

Examples

The following example shows how to clear session MSID 0000000002:

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

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.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable the **clear cdma pdsn statistics rp** command before and after the counters are reset.

Before counters are reset

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

Note Non-zero values of counters.

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

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

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

After the counters are reset

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

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

Note The counter values are zeroes.

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

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

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

Related Commands

Command	Description
show cdma pdsn statistics	Displays PDSN statistics.

clear ip mobile

To clear various IP Mobile information, use the **clear ip mobile** EXEC command.

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

Syntax Description

proxy	Clears the Proxy mobile node.
router	Clears mobile router information
traffic	Clears IP Mobility counters.
visitor	Clears visitor information.
ip-address	(Optional) IP address. If not specified, visitor information is removed for all addresses.
nai *string*	(Optional) Network access identifier of the mobile node.

Command Modes

EXEC

Command History

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

Usage Guidelines

The foreign agent creates a visitor entry for each accepted visitor. The visitor entry allows the mobile node to receive packets while in a visited network. Associated with the visitor entry is the ARP entry for the visitor. It is not needed to clear the entry because it expires after lifetime is reached or when the mobile node gets unregistered.

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

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

Examples

The following example shows how to use counters for debugging:

```
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 8, Deregister 0 requests
    Register 7, Deregister 0 replied
    Accepted 6, No simultaneous bindings 0
    Denied 1, Ignored 1
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 1, Bad request form 0
```

```
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 0, Bad request form 0
```

Related Commands

Command	Description
show ip mobile traffic	Displays protocol counters.

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***]**

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

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

Syntax Description

map name	The name you assign to the crypto map set
seq-num	The number you assign to the crypto map entry.
ipsec-manual	Indicates that IKE is not used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	Indicates that IKE is used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands is made available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map is cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.

Defaults

No crypto maps exist.

Peer discovery is not enabled.

Command Modes

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

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	Support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** keyword and *aaalist* argument were added.

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 (using 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 security associations 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 is 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 is 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 is 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.

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

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (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 Layer 2 Transport Protocol (L2TP) Security feature. The relevant Security Associations (SA) of the crypto map profile are 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 is used to establish the security associations:

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

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

```
Router# crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 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 shows how to configure an IPSec crypto map set that includes a reference to a dynamic crypto map set.

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

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

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

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

The following example shows how to configure Tunnel Endpoint Discovery on a Cisco router:

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

The following example shows how to configure a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

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

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. Use the **no** form of the command to disable this feature.

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

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

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
interface-id	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
11.3T	This command was introduced.

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 has its own security association database.
- The IP address of the local interface is 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 is established and shared for traffic through both interfaces.
- The IP address of the specified interface is 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 shows how to assign crypto map set "mymap" to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic is evaluated against 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 is established. This same security association is then applied to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec uses on both interfaces is the IP address of interface loopback0.

```
interface S0

 crypto map mymap


interface S1

 crypto map mymap


crypto map mymap local-address loopback0
```

debug cdma pdsn a10 ahdlc

To display debug messages for AHDLC, use the **debug cdma pdsn a10 ahdlc** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn a10 ahdlc [**errors** | **events**]

no debug cdma pdsn a10 ahdlc [**errors** | **events**]

Syntax Description

errors	(Optional) Displays details of AHDLC packets in error.
events	(Optional) Displays AHDLC events.

Defaults

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

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.2(8)BY	Keywords were made optional.

Examples

The following example shows how to enable the **debug cdma pdsn a10 ahdlc** command:

```
Router# debug cdma pdsn a10 ahdlc errors
ahdlc error packet display debugging is on
Router# debug cdma pdsn a10 ahdlc events
ahdlc events display debugging is on
Router#
*Jan  1 00:18:30:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:18:30:*****OPEN AHDLC*****
*Jan  1 00:18:30: ahdlc_mgr_channel_create
*Jan  1 00:18:30: ahdlc_mgr_allocate_available_channel:
*Jan  1 00:18:30:ahdlc:tell h/w open channel 9 from engine 0
```

debug cdma pdsn a10 gre

To display debug messages for A10 GRE interface errors, events, and packets, use the **debug cdma pdsn a10 gre** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn a10 gre [**errors** | **events** | **packets**] [**tunnel-key** *key*]

no debug cdma pdsn a10 gre [**errors** | **events** | **packets**]

Syntax Description

errors	(Optional) Displays A10 GRE errors.
events	(Optional) Displays A10 GRE events.
packets	(Optional) Displays transmitted or received A10 GRE packets.
tunnel-key *key*	(Optional) Specifies the GRE key.

Defaults

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

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The tunnel-key parameter was added and the existing keywords were made optional.

Examples

The following example shows how to enable the **debug cdma pdsn a10 gre events tunnel-key** command:

```
Router# debug cdma pdsn a10 gre events tunnel-key 1

Router# show debug
CDMA:
  CDMA PDSN A10 GRE events debugging is on for tunnel key 1

PDSN#
*Mar  1 04:00:57.847:CDMA-GRE:CDMA-Ix1 (GRE/CDMA) created with src 5.0.0.2 dst 0.0.0.0
*Mar  1 04:00:57.847:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:00:59.863:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:00:59.863:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:01.879:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:01.879:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:03.899:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
*Mar  1 04:01:03.899:CDMA-GRE:(in) found session 5.0.0.2-4.0.0.1-1
```

debug cdma pdsn a10 ppp

To display debug messages for A10 PPP interface errors, events, and packets, use the **debug cdma pdsn a10 gre** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn a10 ppp [**errors** | **events** | **packets**]

no debug cdma pdsn a10 ppp [**errors** | **events** | **packets**]

Syntax Description

errors	(Optional) Displays A10 PPP errors.
events	(Optional) Displays A10 PPP events.
packets	(Optional) Displays transmitted or received A10 PPP packets.

Defaults

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

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	Keywords were made optional.

Examples

The following example shows how to enable the **debug cdma pdsn a10 ppp** command:

```
Router# debug cdma pdsn a10 ppp errors
CDMA PDSN A10 errors debugging is on

Router# debug cdma pdsn a10 ppp events
CDMA PDSN A10 events debugging is on

Router# debug cdma pdsn a10 ppp packets
CDMA PDSN A10 packet debugging is on

Router# show debug
*Jan  1 00:13:09:CDMA-PPP:create_va tunnel=CDMA-Ix1 virtual-template
template=Virtual-Template2 ip_enabled=1
*Jan  1 00:13:09:CDMA-PPP:create_va va=Virtual-Access1
*Jan  1 00:13:09:CDMA-PPP:clone va=Virtual-Access1 subif_state=1 hwidb->state=0
*Jan  1 00:13:09:          linestate=1 ppp_lineup=0
*Jan  1 00:13:09:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:13:09:CDMA-PPP:clone va=Virtual-Access1 subif_state=1 hwidb->state=4
*Jan  1 00:13:09:          linestate=0 ppp_lineup=0
*Jan  1 00:13:09:*****OPEN AHDLC*****
```

debug cdma pdsn a11

To display debug messages for A11 interface errors, events, and packets, use the **debug cdma pdsn a11** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn a11 [**errors** | **events** | **packets**] [*mnid*]

no debug cdma pdsn a11 [**errors** | **events** | **packets**]

Syntax Description

errors	(Optional) Displays A11 protocol errors.
events	(Optional) Displays A11 events.
packets	(Optional) Displays transmitted or received packets.
mnid	(Optional) Specifies the mobile station's ID.

Defaults

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

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The MNID parameter was added and the existing keywords were made optional.

Examples

The following example shows how to enable the **debug cdma pdsn a11**commands:

```
Router# debug cdma pdsn a11 errors
CDMA PDSN A11 errors debugging is on
Router# show debug
1d21h:CDMA-RP:(in) rp_msgs, code=1, status=0
1d21h:CDMA-RP:(enqueue req) type=1 homeagent=5.0.0.2 coaddr=4.0.0.1
1d21h:                   id=0xBEF750F0-0xBA53E0F lifetime=65535
1d21h:CDMA-RP:len=8, 00-00-00-00-00-00-00-F1 convert to 00000000000001
(14 digits), type=IMSI
1d21h:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
1d21h:               lifetime=65535 id=BEF750F0-BA53E0F
imsi=00000000000001
1d21h:CDMA-RP:(req) rp_req_create, 5.0.0.2-4.0.0.1-1 imsi=00000000000001
1d21h:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=65535
1d21h:CDMA-RP:(out) setup_rp_out_msg, ha=5.0.0.2 coa=4.0.0.1 key=1
1d21h:%LINK-3-UPDOWN:Interface Virtual-Access2000, changed state to up
1d21h:CDMA-RP:ipmobile_visitor add/delete=1, mn=8.0.2.132, ha=7.0.0.2
1d21h:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access2000,
changed state to up


Router# debug cdma pdsn a11 packets events

Router# show debug
CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001
  CDMA PDSN A11 events debugging is on for mnid 000000000000001
```

```
Router#
*Mar  1 03:15:32.507:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:32.511:CDMA-RP:extension type=32, len=20
*Mar  1 03:15:32.511:         00 00 01 00 EE 1F FC 43 0A 7D F9 36 29 C2 BA 28
*Mar  1 03:15:32.511:         5A 64 D5 9C
*Mar  1 03:15:32.511:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:15:32.511:               lifetime=1800 id=AF3BFE55-69A109D IMSI=000000000000001
*Mar  1 03:15:32.511:CDMA-RP:(req) rp_req_create, ha=5.0.0.2, coa=4.0.0.1, key=1
IMSI=000000000000001
*Mar  1 03:15:32.511:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=1800
*Mar  1 03:15:32.511:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1
*Mar  1 03:15:38.555:CDMA-RP:simple ip visitor added, mn=9.2.0.1, ha=0.0.0.0

Router#
*Mar  1 03:15:54.755:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:15:54.755:CDMA-RP:extension type=38, len=0
*Mar  1 03:15:54.755:CDMA-RP:extension type=32, len=20
*Mar  1 03:15:54.755:         00 00 01 00 EA 9C C6 4C BA B9 F9 B6 DD C4 19 76
*Mar  1 03:15:54.755:         51 5A 56 45
*Mar  1 03:15:54.755:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:15:54.755:               lifetime=0 id=AF3BFE6B-4616E475 IMSI=000000000000001
*Mar  1 03:15:54.755:CDMA-RP:(req) rp_req_lifetime_zero 5.0.0.2-4.0.0.1-1
*Mar  1 03:15:54.755:               IMSI=000000000000001
*Mar  1 03:15:54.755:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=0
*Mar  1 03:15:54.755:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1


Router# debug cdma pdsn a11 event mnid 000000000000001

Router# show debug
CDMA:
  CDMA PDSN A11 events debugging is on for mnid 000000000000001

Router#
*Mar  1 03:09:34.339:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:09:34.339:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:09:34.339:               lifetime=1800 id=AF3BFCEE-DC9FC751
IMSI=000000000000001
*Mar  1 03:09:34.339:CDMA-RP:(req) rp_req_create, ha=5.0.0.2, coa=4.0.0.1, key=1
IMSI=000000000000001
*Mar  1 03:09:34.339:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=1800
*Mar  1 03:09:34.339:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1

*Mar  1 03:09:40.379:CDMA-RP:simple ip visitor added, mn=9.2.0.1, ha=0.0.0.0
Router#

close the session
Router#
*Mar  1 03:10:00.575:CDMA-RP:len=8, 01-00-00-00-00-00-00-10 convert to 000000000000001 (15
digits), type=IMSI
*Mar  1 03:10:00.575:CDMA-RP:(req) process_rp_req, homeagent=5.0.0.2 coaddr=4.0.0.1
*Mar  1 03:10:00.575:               lifetime=0 id=AF3BFD09-18040319 IMSI=000000000000001
*Mar  1 03:10:00.575:CDMA-RP:(req) rp_req_lifetime_zero 5.0.0.2-4.0.0.1-1
*Mar  1 03:10:00.575:               IMSI=000000000000001
*Mar  1 03:10:00.575:CDMA-RP:(out) rp_reply session=5.0.0.2-4.0.0.1-1, lifetime=0
*Mar  1 03:10:00.575:CDMA-RP:(out) Setup RP out message, ha=5.0.0.2 coa=4.0.0.1 key=1
```

```
Router# debug cdma pdsn a11 packet mnid 000000000000001

Router# show debug
CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001

Router#
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:37.803:CDMA-RP:extension type=32, len=20
*Mar  1 03:13:37.803:         00 00 01 00 A8 5B 30 0D 4E 2B 83 FE 18 C6 9D C2
*Mar  1 03:13:37.803:         15 BF 5B 57

*Mar  1 03:13:51.575:CDMA-RP:extension type=38, len=0
*Mar  1 03:13:51.575:CDMA-RP:extension type=32, len=20
*Mar  1 03:13:51.575:         00 00 01 00 58 77 E5 59 67 B5 62 15 17 52 83 6D
*Mar  1 03:13:51.579:         DC 0A B0 5B
```

debug cdma pdsn accounting

To display debug messages for accounting events, use the **debug cdma pdsn accounting** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn accounting

no debug cdma pdsn accounting

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.4xx	Enhanced to display the IP flow accounting details.

Examples

The following example shows how to enable the **debug cdma pdsn accounting** command:

```
Router# debug cdma pdsn accounting
CDMA PDSN accounting debugging is on
Router#
*Jan  1 00:15:32:CDMA/ACCT:null vaccess in session_start
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[44] len:[3] 01   Processing Y1
*Jan  1 00:15:32:CDMA/ACCT:    Setup airlink record received
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[41] len:[6] 00 00 00 02 CDMA/ACCT:
Processing Y2
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[42] len:[3] 12 CDMA/ACCT: Processing Y3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1F] len:[17] 30 30 30 30 30 30 30 30
30 30 30 30 30 30 32      Processing A1
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[9] len:[6] 04 04 04 05   Processing D3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[14]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[10] len:[8] 00 00 04 04 04 05
Processing D4
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[44] len:[3] 02   Processing Y1
*Jan  1 00:15:32:CDMA/ACCT:    Start airlink record received
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[41] len:[6] 00 00 00 02 CDMA/ACCT:
Processing Y2
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[42] len:[3] 13 CDMA/ACCT: Processing Y3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[10]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[11] len:[4] 00 02   Processing E1
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[10]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[12] len:[4] 00 F1   Processing F1
```

debug cdma pdsn accounting flow

To display debug messages for accounting flow, use the **debug cdma pdsn accounting flow** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn accounting flow

no debug cdma pdsn accounting flow

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command History

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

Examples

The following example shows how to enable the **debug cdma pdsn accounting flow** command:

```
Router# debug cdma pdsn acc flow
CDMA PDSN flow based accounting debugging is on
pdsn-6500#
01:59:40:CDMA-SM:cdma_pdsn_flow_acct_upstream sess id 1 flow type 0 bytes 100 addr
20.20.20.1
01:59:40:CDMA-SM:cdma_pdsn_flow_acct_downstream sess id 1 flow type 0 bytes 100 addr
20.20.20.1
```

debug cdma pdsn accounting raa

To display debug messages for remote address accounting errors and events, use the **debug cdma pdsn accounting raa events** and **debug cdma pdsn accounting raa errors** commands in privileged EXEC mode respectively. To disable debug messages, use the **no** form of the commands.

debug cdma pdsn accounting raa events

debug cdma pdsn accounting raa errors

no debug cdma pdsn accounting raa events

no debug cdma pdsn accounting raa errors

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **debug cdma pdsn accounting raa events** command:

```
PDSN# debug cdma pdsn accounting raa ?
  errors  CDMA PDSN RAA errors
  events  CDMA PDSN RAA events

PDSN# debug cdma pdsn accounting raa errors ?
  <cr>

PDSN# debug cdma pdsn accounting raa errors
CDMA PDSN Remote Address based accounting errors debugging is on
PDSN#

PDSN#
*Jul 10 07:18:24.131: Parse Subtype 1, Table Index 1
*Jul 10 07:18:24.131: Parse Subtype 1, Table Index 2
*Jul 10 07:18:24.131: Parse Subtype 2, Qualifier 2
PDSN#
```

The following example shows how to enable the **debug cdma pdsn accounting raa errors** command**:**

```
PDSN# debug cdma pdsn accounting raa ?
  errors  CDMA PDSN RAA errors
  events  CDMA PDSN RAA events

PDSN# debug cdma pdsn accounting raa events ?
  <cr>
```

```
PDSN# debug cdma pdsn accounting raa events
CDMA PDSN Remote Address based accounting events debugging is on
PDSN#

PDSN#
*Jul 10 07:20:47.907: Error in downloaded index: not a valid length value
*Jul 10 07:20:47.907: Error Parse Subtype 3
PDSN#
```

debug cdma pdsn accounting time-of-day

To display the timer value, use the **debug cdma pdsn accounting time-of-day** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn accounting time-of-day

no debug cdma pdsn accounting time-of-day

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command History

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

Examples

The following example shows how to enable the **debug cdma pdsn accounting time-of-day** command:

```
Router# debug cdma pdsn accounting time-of-day
CDMA PDSN accounting time-of-day debugging is on

Feb 15 19:13:23.634:CDMA-TOD:Current timer expiring in 22 seconds
Feb 15 19:13:24.194:%SYS-5-CONFIG_I:Configured from console by console
Router#
Feb 15 19:13:45.635:CDMA-TOD:Timer expired...Rearming timer
Feb 15 19:13:45.635:CDMA-TOD:Gathering session info
Feb 15 19:13:45.635:CDMA-TOD:Found 0 sessions
```

debug cdma pdsn cac

To display debug messages for **cac** (call admission control), use the **debug cdma pdsn cac** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command. These debugs display the **cac** related information updates between processors.

debug cdma pdsn cac

no debug cdma pdsn cac

Syntax Description

There are no keywords or variables for this command.

Defaults

All types of debug information are enabled if you enter the command without optional keywords.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **debug cdma pdsn cac** command:

```
PDSN_ACT# debug cdma pdsn cac
CDMA PDSN CAC debugging is on
PDSN_ACT#
PDSN_ACT# show debugging
CDMA:
  CDMA PDSN CAC debugging is on
PDSN_ACT#
SAMI 12/4: Jul 10 08:19:31.832:  CDMA-CAC:CPU Metric is 16 (usage 0) (max cpu:30 wt:16)
SAMI 12/4: Jul 10 08:19:31.832:  CDMA-CAC:Memory is local: 16 iomem: 25
SAMI 12/4: Jul 10 08:19:31.832:  CDMA-CAC:Memory Metric is 16
SAMI 12/4: Jul 10 08:19:31.832:  CDMA-CAC:Diff Cons is 35000
SAMI 12/4: Jul 10 08:19:31.832:  CDMA-CAC:Weight 1
SAMI 12/5: .Jul 10 08:19:36.134:  CDMA-CAC:CPU Metric is 16 (usage 0) (max cpu:30 wt:16)
SAMI 12/5: .Jul 10 08:19:36.134:  CDMA-CAC:Memory is local: 16 iomem: 25
SAMI 12/5: .Jul 10 08:19:36.134:  CDMA-CAC:Memory Metric is 16
SAMI 12/5: .Jul 10 08:19:36.134:  CDMA-CAC:Diff Cons is 35000
SAMI 12/5: .Jul 10 08:19:36.134:  CDMA-CAC:Weight 1
SAMI 12/6: Jul 10 08:19:43.578:  CDMA-CAC:CPU Metric is 16 (usage 0) (max cpu:30 wt:16)
SAMI 12/6: Jul 10 08:19:43.578:  CDMA-CAC:Memory is local: 16 iomem: 25
SAMI 12/6: Jul 10 08:19:43.578:  CDMA-CAC:Memory Metric is 16
SAMI 12/6: Jul 10 08:19:43.578:  CDMA-CAC:Diff Cons is 35000
SAMI 12/6: Jul 10 08:19:43.578:  CDMA-CAC:Weight 1
SAMI 12/7: Jul 10 08:19:50.778:  CDMA-CAC:CPU Metric is 16 (usage 0) (max cpu:30 wt:16)
SAMI 12/7: Jul 10 08:19:50.778:  CDMA-CAC:Memory is local: 16 iomem: 25
SAMI 12/7: Jul 10 08:19:50.778:  CDMA-CAC:Memory Metric is 16
SAMI 12/7: Jul 10 08:19:50.778:  CDMA-CAC:Diff Cons is 35000
SAMI 12/7: Jul 10 08:19:50.778:  CDMA-CAC:Weight 1
SAMI 12/8: Jul 10 08:19:58.128:  CDMA-CAC:CPU Metric is 16 (usage 0) (max cpu:30 wt:16)
SAMI 12/8: Jul 10 08:19:58.128:  CDMA-CAC:Memory is local: 16 iomem: 25
SAMI 12/8: Jul 10 08:19:58.128:  CDMA-CAC:Memory Metric is 16
SAMI 12/8: Jul 10 08:19:58.128:  CDMA-CAC:Diff Cons is 35000
SAMI 12/8: Jul 10 08:19:58.128:  CDMA-CAC:Weight 1
```

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 debug messages, use the **no** form of this command.

debug cdma pdsn cluster {**message** [**error** | **events** | **packets**] **redundancy** [**error** | **events** | **packets**]}

no debug cdma pdsn cluster {**message** [**error** | **events** | **packets**] **redundancy** [**error** | **events** | **packets**]}

Syntax Description

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

Defaults

No default behavior or values.

Command History

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

Usage Guidelines

This debug is **only** allowed on PDSN c6-mz images, and helps to monitor cluster information.

Examples

The following example shows how to enable 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.

Usage Guidelines

The following example shows how to enable 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 debug messages, use the **no** form of this command.

debug cdma pdsn prepaid

no debug cdma pdsn prepaid

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

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

Usage Guidelines

The following example shows how to enable the **debug cdma pdsn prepaid** command:

```
Router# debug cdma pdsn prepaid

*Jan 13 17:46:56: CDMA-PREPAID: Volume Threshold 1000 bytes reached for Quota Id 1,
current quota usage 1000 bytes
*Jan 13 17:46:56: CDMA-PREPAID: Preparing to send on-line Access Request
*Jan 13 17:46:56: CDMA-PREPAID: Update Reason: Threshold Reached
*Jan 13 17:46:56: CDMA-PREPAID: Added Username: mwtr_sip_user
*Jan 13 17:46:56: CDMA-PREPAID: Added Message Authenticator attribute
*Jan 13 17:46:56: CDMA-PREPAID: Added CLID: 00000000000002
*Jan 13 17:46:56: CDMA-PREPAID: Added Service Option: 245
*Jan 13 17:46:56: CDMA-PREPAID: Added Correlation ID: 0000001E
*Jan 13 17:46:56: CDMA-PREPAID: Adding PrepaidAccountingQuota(PPAQ):
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_QUOTA_ID_SUBTYPE[1]: value=1
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_SUBTYPE[2]: value=1000
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_OVERFLOW_SUBTYPE[3]: value=0
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_THRESHOLD_OVERFLOW_SUBTYPE[5]: value=0
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_UPDATE_REASON_SUBTYPE[8]: value=3
------------------------------------------------------------------------------------------

*Jan 13 17:46:56: CDMA-PREPAID: Received prepaid response: status 2
*Jan 13 17:46:56: CDMA-PREPAID: AAA authorised params being processed in on-line Access
Accept
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: addr
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: Framed-Protocol
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: service-type
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: routing
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-prepaid-accounting-capability
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-sess-term-capability
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-prepaid-accounting-quota
*Jan 13 17:46:56: CDMA/PREPAID/AAA: AAA_AT_CDMA_PREPAID_ACCOUNTING_QUOTA
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_QUOTA_ID_SUBTYPE[1]: value=1
```

```
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_SUBTYPE[2]: value=4000
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_THRESHOLD_SUBTYPE[4]: value=3000
*Jan 13 17:46:56: CDMA-PREPAID: Volume Quota received: 4000 bytes with threshold 3000
bytes
*Jan 13 17:46:56: CDMA-PREPAID: Access Accept received and retrieved attributes
successfully
```

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 [errors | events]

no debug cdma pdsn qos [errors | events]

Syntax Description

errors	Displays the QoS errors.
events	Displays the QoS events.

Defaults

No default values.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

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. To disable debug messages, use the **no** form of this command.

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

No default values.

Command Modes

EXEC mode

Command History

Release	Modification
12.3(11)YF	This command was introduced.

Examples

The following example shows how to enable 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

To debug the PDSN-SR redundancy aspect of errors, use the **debug cdma pdsn redundancy errors** command. To disable debug messages, use the **no** form of this command.

debug cdma pdsn redundancy {**errors** | **events** | **packets** | **attributes**}

no debug cdma pdsn redundancy {**errors** | **events** | **packets** | **attributes**}

Syntax Description

errors	Displays the PDSN redundancy errors.
events	Displays the PDSN redundancy events.
packets	Displays all transmitted or received redundancy packets.
attributes	Displays CDMA PDSN Redundancy attributes.

There are no keywords or arguments for this command.

Defaults

No default values.

Command Modes

EXEC mode

Command History

Release	Modification
12.3(8)XW	This command was introduced.
12.4xx	Enhanced to print TFT and other new parameters like subscriber qos profile, IP flow, and auxiliary A10 synced to standby.

Examples

The following example shows how to enable the **debug cdma pdsn redundancy attributes** command:

```
SAMI 12/3: Jun 24 10:23:17.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to up
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[0] name[Key] length[4] 00000001
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[1] name[Flags] length[4] 00800000
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[2] name[PCF SPI] length[4] 00000101
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[3] name[Tunnel Src Addr] length[4]
21212101
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[4] name[Tunnel Dest. Addr] length[4]
02020204
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[5] name[Src Addr] length[4] 02020204
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[6] name[PCF Addr] length[4] 02020204
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[7] name[MN ID Type] length[2] 0000
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[8] name[MN ID Len] length[1] 0B
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[9] name[MSID] length[8]
09884708942AAAAA
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[10] name[GRE Protocol Type]
length[4] 00008881
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[24] name[Main A10 SR ID] length[1]
01
```

```
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[25] name[Main A10 Service Option]
length[2] 003B
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[11] name[Source Port] length[2] 02BB
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[12] name[Lifetime] length[2] FFFF
SAMI 12/3: Jun 24 10:23:21.303: CDMASR-ACT: Attr type[13] name[Elapsed Time] length[4]
00001288
SAMI 12/3: Jun 24 10:30:47.719: CDMA-CCM: [ACT] SHDB 0x96000001 Sync collection for:
CDMA_SR_EVENT_TFT_CREATE    (event_handle = 0x8A000001)
SAMI 12/3: Jun 24 10:30:47.719: CDMA-CCM: [ACT] SHDB 0x96000001 Sync collection for:
CDMA_SR_EVENT_IPFLOW_ACCT_SEND_START (event_handle = 0x45000001)
```

debug cdma pdsn resource-manager

To display debug messages that help you monitor the resource-manager information, use the **debug cdma pdsn resource-manager** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn resource-manager [error | events]

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

Syntax Description

errors	Displays pdsn resource manager errors.
events	Displays pdsn resource manager events.

Defaults

No default behavior or values.

Command History

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

Examples

The following example shows how to enable the **debug cdma pdsn resource-manager** command:

```
Router# debug cdma pdsn resource-manager ?
    errors  CDMA PDSN resource manager errors
    events  CDMA PDSN resource manager events
```

debug cdma pdsn rsvp

To display details of the RSVP packets received, use the **debug cdma pdsn rsvp** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn rsvp {**events** | **errors**}

no debug cdma pdsn rsvp {**events** | **errors**}

Syntax Description

errors	Displays PDSN RSVP errors.
events	Displays PDSN RSVP events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.4xx	This command was introduced.

Examples

The following example shows how to enable the **debug cdma pdsn rsvp** command:

```
*Jun 19 11:56:38.943: CDMA-RSVP: Received Resv message from 4.4.4.1
*Jun 19 11:56:38.943: CDMA-RSVP: Start Parsing Received Resv Message from 4.4.4.1
*Jun 19 11:56:38.943: CDMA-RSVP: Resv type=2, len=112
*Jun 19 11:56:38.943:     10 02 52 06 FF 00 00 70 00 0C 01 01 04 04 04 01
*Jun 19 11:56:38.943:     11 00 0D 7F 00 08 05 01 00 00 00 01 00 08 0F 01
*Jun 19 11:56:38.943:     04 04 04 01 00 44 E7 01 00 00 00 27 00 1E 00 00
*Jun 19 11:56:38.943:     04 04 04 01 08 01 01 02 01 01 00 07 00 05 50 06
*Jun 19 11:56:38.943:     1F 02 02 00 07 00 05 50 06 1F 00 1E 00 00 04 04
*Jun 19 11:56:38.943:     04 01 48 01 01 02 01 01 00 07 00 05 50 06 1F 03
*Jun 19 11:56:38.943:     02 00 07 00 05 50 06 1F 00 08 08 01 00 00 00 11
*Jun 19 11:56:38.943: CDMA-RSVP: Parsing Done Successfully,Sending 3GPP2 object to PDSN
*Jun 19 11:56:38.943: CDMA-RSVP: Building Objects for ResvError message
*Jun 19 11:56:38.943: CDMA-RSVP: Resv type=4, len=52
*Jun 19 11:56:38.943:     10 04 C3 C6 FF 00 00 34 00 0C 01 01 04 04 04 01
*Jun 19 11:56:38.943:     11 00 0D 7F 00 04 06 01 00 14 E7 01 00 00 00 27
*Jun 19 11:56:38.943:     00 0C 00 01 04 04 04 01 08 00 00 01 00 08 08 01
*Jun 19 11:56:38.943:     00 00 00 11
*Jun 19 11:56:38.943: CDMA-RSVP: Sending ResvError message from PDSN 1.1.1.1 to Mn 4.4.4.1
```

debug cdma pdsn selection

To display debug messages for the intelligent PDSN selection feature, use the **debug cdma pdsn selection** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

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

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

Syntax Description

errors	Displays pdsn selection errors.
events	Displays pdsn selection events.
packets	Displays transmitted or received packets.

Defaults

No default behavior or values.

Command History

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

Examples

The following example shows how to enable the **debug cdma pdsn selection** command with the keyword **events** specified:

```
Router# debug cdma pdsn selection events
CDMA PDSN selection events debugging is on
Router#
00:27:46: CDMA-PSL: Message(IN) pdsn 51.4.2.40 interface 70.4.2.40
00:27:46:                Keepalive 10
00:27:46:                Count 0
00:27:46:                Capacity 16000
00:27:46:                Weight 0
00:27:46:                Hostname 11 7206-PDSN-2
00:27:46: CDMA-PSL: Reset keepalive, pdsn 51.4.2.40 current 10 new 10
00:27:46: CDMA-PSL: Message processed, pdsn 51.4.2.40 tsize 0 pendings 0
00:27:47: CDMA-PSL: Send KEEPALIVE, len 32
00:27:47: CDMA-PSL: Message(OUT) dest 224.0.0.11
00:27:47:                Keepalive 10
00:27:47:                Count 1
00:27:47:                Capacity 16000
00:27:47:                Weight 0
00:27:47:                Hostname 11 7206-PDSN-1
00:27:47: CDMA-PSL: RRQ sent, s=70.4.1.40 (FastEthernet0/1), d=224.0.0.11
```

debug cdma pdsn service-selection

To display debug messages for service selection, use the **debug cdma pdsn service-selection** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn service-selection

no debug cdma pdsn service-selection

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command History

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

Examples

The following example shows how to enable the **debug cdma pdsn service-selection** command:

```
Router# debug cdma pdsn service-selection
CDMA PDSN service provisioning debugging is on
Router#
1d02h:%LINK-3-UPDOWN:Interface Virtual-Access3, changed state to up
1d02h:Vi3 CDMA-SP:user_class=1, ms_ipaddr_req=1, apply_acl=0
1d02h:Vi3 CDMA-SP:Adding simple ip flow, user=bsip, mn=6.0.0.2,
1d02h:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access3,
changed state to up
```

debug cdma pdsn session

To display debug messages for Session Manager errors, events, and packets, use the **debug cdma pdsn session-manager** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

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

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

Syntax Description

errors	(Optional) Displays session protocol errors.
events	(Optional) Displays session events.

Defaults

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

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	Keywords were made optional.
12.4xx	Enhanced to display the Auxiliary A10 and IP flow parsing and installation details.

Examples

The following example shows how to enable 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 cdma pdsn sm

To display debug messages for sm (**cdma singleip session manager**) errors, events, and packets, use the **debug cdma pdsn sm** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command. These debugs display the sm interaction related information.

debug cdma pdsn sm [errors | events | packets]

no debug cdma pdsn sm [errors | events | packets]

Syntax Description

errors	(Optional) Displays session manager errors.
events	(Optional) Displays session manager events.
packets	(Optional) Displays transmitted or received packets related to session manager.

Defaults

All types of debug information are enabled if you enter the command without optional keywords.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **debug cdma pdsn sm** command:

```
PDSN_ACT# debug cdma pdsn sm events
CDMA PDSN SM events debugging is on

PDSN_ACT# show debugging
CDMA:
  CDMA PDSN SM events debugging is on
PDSN_ACT#
SAMI 12/3: Jul 10 07:59:29.260:  CDMA-PDSN-SM: Msg rcvd from PPC-5, size 12
SAMI 12/3: Jul 10 07:59:29.260:  CDMA-PDSN-SM: Data received from PPC-5
SAMI 12/3: Jul 10 07:59:29.260:  CDMA-PDSN-SM: Tunnel information added successfully
SAMI 12/3: Jul 10 07:59:29.260:  CDMA-PDSN-SM: Tunnel create acknowledge sent to PPC-5
SAMI 12/5: Jul 10 07:59:29.267:  CDMA-PDSN-SM: Fwd Msg Type Dequeued SM FWD CONTROL PLANE
MSG request_id 0
SAMI 12/5: Jul 10 07:59:29.267:  CDMA-PDSN-SM: Fwd Msg: Received len 418 IP Length 408
SAMI 12/5: Jul 10 07:59:29.267:  CDMA-PDSN-SM: Enqueing to IP
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Tunnel create timer is started
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Tunnel create information is updated to
PPC-3
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Msg rcvd from PPC-3, size 12
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Msg rcvd from PPC-3,2.2.2.5, key=1,
imsi=09884708943    , imph_dst=30 handle=B000011
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Sent to PPC Msg Type : SM TCOP IMSI
CREATE,Length : 45
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Data received from PPC-3
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Tunnel create timer is stopped
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Tunnel info updated in PPC-3 and ack
received successfully
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: Msg type Dequeued : SM SESSION IMSI CREATE
ACK
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: IMSI create timer stopped
SAMI 12/5: Jul 10 07:59:29.271:  CDMA-PDSN-SM: IXP PCFIP GRE Add Success handle B000011
SAMI 12/5: Jul 10 07:59:29.279:  CDMA-PDSN-SM: Send to PPC Msg Type : SM SESSION CCB
CREATE,Length : 87
SAMI 12/5: Jul 10 07:59:29.279:  CDMA-PDSN-SM: Sent mnip add to IXP mnip=20.0.0.2,
imph_dst= 30, vrf=0 handle=2F000008
SAMI 12/5: Jul 10 07:59:29.283:  CDMA-PDSN-SM: IXP MNIP Add Success for handle 2F000008
SAMI 12/5: Jul 10 07:59:29.283:  CDMA-PDSN-SM: Msg type Dequeued : SM SESSION CCB CREATE
ACK
SAMI 12/5: Jul 10 07:59:29.283:  CDMA-PDSN-SM: FLOW create timer stopped

PDSN_ACT# debug cdma pdsn sm packets
CDMA PDSN SM packets debugging is on

PDSN_ACT# show debugging
CDMA:
  CDMA PDSN SM packets debugging is on
PDSN_ACT#
4FFEEA50:                            00000000              ....
4FFEEA60: 0700000C 0000000C 02                  .........
B0330DA0:       00 00000101 A2000000 00450001     ....."....E..
B0330DB0: 9871EB00 00FF1102 41020202 05212121  .qk.....A....!!!
B0330DC0: 0102BB02 BB01843E EB010A1C 20000000  ..;.;..>k... ...
B0330DD0: 00212121 01020202 05CE0174 8EC18917  .!!!.....N.t.A..
B0330DE0: 67271388 81000000 33000000 01000606  g'......3.......
B0330DF0: 01894807 98392600 00570000 159F0101  ..H..9&..W......
B0330E00: 1A0C0000 159F2806 00000001 1A0C0000  ......(.........
B0330E10: 159F2906 00000033 1A0C0000 159F2A06  ..)....3......*.
B0330E20: 00000000 1F0D3039 38383437 30383939  ......0988470899
B0330E30: 331A0C00 00159F09 06020202 051A1400  3...............
B0330E40: 00159F0A 0E303030 30303030 30303030  .....00000000000
B0330E50: 30260000 BA000015 9F01011A 0C000015  0&..:...........
B0330E60: 9F280600 0000021A 0C000015 9F290600  .(...........)..
B0330E70: 0000331A 0C000015 9F2A0600 0000011A  ..3......*......
B0330E80: 0C000015 9F0B0600 0000001A 0C000015  ................
B0330E90: 9F0C0600 0000F11A 0C000015 9F0D0600  ......q.........
B0330EA0: 0000F21A 0C000015 9F0E0600 0000F31A  ..r...........s.
B0330EB0: 0C000015 9F0F0600 0000F41A 0C000015  ..........t.....
B0330EC0: 9F100600 00003B1A 0C000015 9F110600  ......;.........
B0330ED0: 0000F61A 0C000015 9F120600 0000F71A  ..v...........w.
B0330EE0: 0C000015 9F130600 0000F81A 0C000015  ..........x.....
B0330EF0: 9F140600 0000F91A 0C000015 9F150600  ......y.........
B0330F00: 0000FA1A 0C000015 9F320600 00000026  ..z......2.....&
B0330F10: 00001000 00159F04 01000000 00000002  ................
B0330F20: 02020586 0A000000 00159F09 01003B20  ..............;
B0330F30: 14000001 01A3576F D97F59C7 70951B39  .....#WoY.YGp..9
B0330F40: 400BB5C9 0ECE                        @.5I.N
52211FF0:                   00 00000257 00001207         ....W....
52212000: 002D0601 89480798 39AAAA00 00000000  .-...H..9**.....
52212010: 00000000 00000000 00000000 00000000  ................
52212020: 00000000 00                          .....
5085A6F0:          00000000 0300000C 0002000C      ............
5085A700: 02                                   .
5817ABC0:                        0000 00030157            .....W
5817ABD0: 00001200                             ....
52212830:                   00 0000081C 00000807         .........
52212840: 00570601 89480798 39AAAA00 00000000  .W...H..9**.....
52212850: 00000000 1400000B 00000000 00000000  ................
52212860: 00000000 15000F61 72616A65 73686B75  .......arajeshku
52212870: 6D617211 00100003 73697000 056B7269  mar.....sip..kri
```

```
52212880: 73680112 000B0000 00000000 753000    sh..........u0.
5817ADC0:                       0000 0009011C           ......
5817ADD0: 00000800                             ....
PDSN_ACT#

PDSN_ACT# debug cdma pdsn sm errors
CDMA PDSN SM errors debugging is on

PDSN_ACT# show debugging
CDMA:
  CDMA PDSN SM errors debugging is on
PDSN_ACT#
SAMI 12/4: Jul 10 08:08:31.603:  CDMA-PDSN-SM: Abnormal condition for SM SESSION IMSI
DELETE ACK with request id 3A000017
SAMI 12/4: Jul 10 08:08:31.603:  CDMA-PDSN-SM: Abnormal condition for SM SESSION IMSI
DELETE ACK with request id C8000018
```

debug cdma pdsn tft

To display information details about TFT parsing, use the command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn tft {**errors** | **events**}

no debug cdma pdsn tft {**errors** | **events**}

Syntax Description

errors	Displays PDSN tft errors.
events	Displays PDSN tft events.

Defaults

No default behavior or values.

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

The TFT debug is prefixed with IP address:Tft opcode:direction

Tft opcode ranges from 1 to 5, and direction is forward (0), or reverse (1).

For example, 4.4.4.1:1:1 represents mobile node IP address as 4.4.4.1, Opcode as 1 (Create Tft), and dierction as 1 (Reverse).

Examples

The following example shows how to enable the **debug cdma pdsn tft** command:

```
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Tft IE 1 P 1 NS 1 PF count 2
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Flow id 1 Prec 1
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Component: Single Source Port 1567
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Flow id 2 Prec 2
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Component: Single Source Port 1567
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Deleting all Pf's in TFT
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Pf 1 added to Tft EC 0
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Pf 2 added to Tft EC 0
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:0: Parsing success for Tft Ie 1
*Jun 19 11:56:38.943: CDMA-TFT:              TFT not successfully synced to standby
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Tft IE 2 P 1 NS 1 PF count 2
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Flow id 1 Prec 1
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Component: Single Source Port 1567
*Jun 19 11:56:38.943: CDMA-TFT:              Error: IPFlow 3 [Reverse] not found for Flow
Attach
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Error: IPFlow Attach to Flow Failed
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Parsing Failure

PDSN1_ACT#
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Tft Error IE 2 Reason: Pf Add Failure
*Jun 19 11:56:38.943: CDMA-TFT: 4.4.4.1:1:1: Error Response Sent
```

debug condition calling

To enable conditional debug feature for clustering, use the **debug condition calling** command in privileged EXEC mode. Use the **no** form of the command to disable this feature.

debug condition calling *msid*

no debug condition calling *msid*

Syntax Description

msid	(Optional) Displays MSID information.

Defaults

When all the conditions are removed, the debugging information appears without any filtering mechanism.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to enable conditional debugging for the clustering feature:

```
Router# debug condition calling
```

debug condition username

To filter the output of the **debug ip mobile** command, use the **debug condition username** command to set the conditions. Use the **no** form of the command to disable this feature.

debug condition username *username*

no debug condition username *username*

Syntax Description

username	Displays the username associated with the **debug ip mobile** command.

Defaults

When all the conditions are removed, the debugging information appears without any filtering mechanism.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to filter conditional debugging for the **debug ip mobile** command:

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

debug ip mobile

Use the **debug ip mobile** command in privileged EXEC mode to display debugging information about the Mobile IP subsystem. To disbale debug messages, use the **no** form of this command.

debug ip mobile [**advertise** | **local-area** | **proxy** | **redundancy** | **router**]

no debug ip mobile [**advertise** | **local-area** | **proxy** | **redundancy** | **router**]

Syntax Description

advertise	(Optional) Displays advertisement information.
local-area	(Optional) Displays local-area mobility information.
proxy	(Optional) Displays proxy mobile node activities.
redundancy	(Optional) Displays mobile redundancy activities.
router	(Optional) Displays mobile router activities.

Defaults

No default values.

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(8)XW	The **local-area**, **proxy**, **redundancy**, and **router** keywords were added.

Examples

The following example shows how to enable the **debug ip mobile advertise** command.

Table 1 describes significant fields shown in the display.

```
Router# debug ip mobile advertise

MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8)
```

Table 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, lower case letters represent bits that are not set.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.

debug ip mobile cdma ipsec

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

debug ip mobile cdma ipsec

no debug ip mobile cdma ipsec

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

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

```
Router# debug ip mobile csma ipsec
```

dscp (service flows qos subscriber profile sub-mode)

To configure the allowed differentiated services markings parameter, use the **dscp** command in the service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

dscp {**allowed-class** {**AF** | **EF** | **O**} | **max-class** *value*| **reverse-marking** *value*}

no {**allowed-class** {**AF** | **EF** | **O**} | **max-class** *value*| **reverse-marking** *value*}

Syntax Description

allowed-class	Allowed DSCP classes which you can mark packets
AF	You can send packets with AF dscp (A bit).
EF	You can send packets with EF dscp (E bit).
O	You mark packets for experiment or local use (O bit).
max-class *value*	Max-class selection marking. Range is 1-63.
reverse-marking *value*	Reverse tunnel marking. Range is 1-63.

Defaults

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **dscp** command:

```
Router#(config-qos-profile)# dscp ?
  allowed-class    allowed dscp's classes with which user can mark
packets
  max-class        User may mark packets with a class selector code
point
  reverse-marking  marking level pdsn apply to reverse tunneled packets

Router#(config-qos-profile)# dscp allowed-class ?
  AF  User can send packets with AF dscp (A bit)
  EF  User can send packets with EF dscp (E bit)
  O  User can mark packets for experiment or local use (O bit)

Router#(config-qos-profile)#dscp allowed-class AF ?
  <cr>
```

Here is an example of the max-class and reverse-marking keywords:

```
Router(config-qos-profile)# dscp max-class ?
  AF11     AF11
  AF12     AF12
  AF13     AF13
  AF21     AF21
  AF22     AF22
  AF23     AF23
  AF31     AF31
  AF32     AF32
  AF33     AF33
  AF41     AF41
  AF42     AF42
  AF43     AF43
  Default  Selector Class 0
  EF       EF
  class1   Selector Class 1
  class2   Selector Class 2
  class3   Selector Class 3
  class4   Selector Class 4
  class5   Selector Class 5
  class6   Selector Class 6
  class7   Selector Class 7

Router(config-qos-profile)#
```

```
Router(config-qos-profile)# dscp reverse-marking ?
  AF11     AF11
  AF12     AF12
  AF13     AF13
  AF21     AF21
  AF22     AF22
  AF23     AF23
  AF31     AF31
  AF32     AF32
  AF33     AF33
  AF41     AF41
  AF42     AF42
  AF43     AF43
  Default  Selector Class 0
  EF       EF
  class1   Selector Class 1
  class2   Selector Class 2
  class3   Selector Class 3
  class4   Selector Class 4
  class5   Selector Class 5
  class6   Selector Class 6
  class7   Selector Class 7

Router(config-qos-profile)#
```

flow-priority (service flows qos subscriber profile sub-mode)

To configure the maximum per flow priority parameter, use the **flow-priority** command in service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

flow-priority *value*

no flow-priority *value*

Syntax Description

value	The maximum aggregate bandwidth value. The valid range is 1-65535.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **flow-priority** command:

```
Router#(config-qos-profile)# flow-priority ?
   <1-65535> Value

Router#(config-qos-profile)# flow-priority 100 ?
```

flow-profile direction (service flows qos subscriber profile sub-mode)

To configure authorized flow profile IDs for each direction, use the **flow-profile direction** command in the service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

flow-profile direction {**forward** | **reverse** | **bi-direction**} **flow-id** *flow-id*

no bandwidth {**forward** | **reverse** | **bi-direction**} **flow-id** *flow-id*

Syntax Description

forward	Configures the authorized flow profile ID in the forward direction.
reverse	Configures the authorized flow profile ID in the reverse direction.
bi-direction	Configures the authorized flow profile ID in both directions.
flow-id	Flow profile ID.
flow-id	flow-id is optional.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode.

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **flow-profile** direction command:

```
Router#(config-qos-profile)# flow-profile ?
  direction  Configure direction for flow of packet


Router#(config-qos-profile)# flow-profile direction ?
  <1-3>  1-Reverse  2-Forward  3-Bi-direction

Router#(config-qos-profile)# flow-profile direction 1 ?
  flow-id  defines qos treatment to apply to a packet flow

Router#(config-qos-profile)# flow-profile direction 1 flow-id ?
  <1-255>  Value
Router#(config-qos-profile)# flow-profile direction 1 flow-id 100 ?
```

interface cdma-Ix

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

interface cdma-Ix1

no interface cdma-Ix1

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to define the virtual interface for the R-P tunnel and configures the IP address:

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

Related Commands

Command	Description
show interfaces	Displays statistics about the network interfaces.

inter-user-priority (service flows qos subscriber profile sub-mode)

To configure inter-user priority parameter, use the **inter-user-priority** command in the service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

inter-user-priority *value*

no inter-user-priority *value*

Syntax Description

value	The inter-user priority value. The valid range is 1- 4294967295.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode.

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **inter-user-priority** command:

```
Router#(config-qos-profile)# inter-user-priority ?
  <1-4294967295>  Value

Router#(config-qos-profile)# inter-user-priority 200 ?
  <cr>
```

ip mobile authentication ignore-spi

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

ip mobile authentication ignore-spi

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration.

Command History

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

Examples

The following example shows how to enable the **ip mobile authentication ignore-spi** command:

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

ip mobile bindupdate

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

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

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

Syntax Description

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

Defaults

No default values.

Command Modes

Global configuration.

Command History

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

Examples

The following example shows how to enable the **ip mobile bindupdate** command:

```
Router# ip mobile bindupdate
```

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

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF3	This command was introduced.

Examples

The following example shows 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

No default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Usage Guidelines

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

Examples

The following example shows 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** global configuration command. Use the **no** form of the command to disable this feature.

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

When a registration request comes in, the foreign agent ignores the request when foreign agent service is not enabled on interface or when no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated (**show ip mobile secure visitor** command). The registration bitflag is handled as described in Table 2 (**show ip mobile interface** command). The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending** command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in Table 3). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command). (Violation reasons are listed in Table 9.)

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

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

When registration is denied, the foreign agent removes the request from the pending registration table. The table and timers of the visitor are unaffected.

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

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

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

Table 2 Foreign Agent Registration Bitflags

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

Table 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.

Table 3 Foreign Agent Reply Codes (continued)

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

Examples

The following example shows how to enable foreign agent service on interface Ethernet1, advertising 1.0.0.1 as the care-of address:

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

Related Commands

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

ip mobile foreign-agent accept stale-challenge-requests

To configure PDSN to accept RRQs with previously used challenges, use the **ip mobile foreign-agent accept stale-challenge-requests** command. Use the **no** form of the command to disable this feature.

ip mobile foreign-agent accept stale-challenge-requests

no ip mobile foreign-agent accept stale-challenge-requests

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable **ip mobile foreign-agent accept stale-challenge-requests** command:

```
Router(config)# ip mobile foreign-agent accept stale-challenge-requests
```

ip mobile foreign-agent extension gre home-agent *address range or a single address*

To configure PDSN to send the Generic Routing Encapsulation (GRE) Critical Vendor Specific Externsion (CVSE) for every HA, use the **ip mobile foreign-agent extension gre home-agent** *address range or a single address* command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile foreign-agent extension gre home-agent *address range or a single address*

no ip mobile foreign-agent extension gre home-agent *address range or a single address*

This command enables PDSN to send the GRE CVSE irrespective of whether the GRE bit is set in the received MIP-RRQ or not.

Syntax Description

There are no keywords or variables for this command.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable **ip mobile foreign-agent extension gre home-agent** *address range or a single address* command:

```
Router(config)# ip mobile foreign-agent extension gre home-agent address range or a single
address
```

ip mobile foreign-agent mn-identifier calling-station-id

To configure PDSN to support a common NAI, use the **ip mobile foreign-agent mn-identifier calling-station-id** command in global configuration mode. Use the **no** form of the command to disable this feature.

Note When configuring this command, ensure that no sessions are active.

ip mobile foreign-agent mn-identifier calling-station-id

no ip mobile foreign-agent mn-identifier calling-station-id

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **ip mobile foreign-agent mn-identifier calling-station-id** command:

```
Router(config)# ip mobile foreign-agent mn-identifier calling-station-id
```

ip mobile foreign-service

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

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

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

Syntax Description

home-access *acl*	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99.
limit *number*	(Optional) Number of visitors allowed on interface. The Busy (B) bit is advertised when the number of registered visitors reach this limit. Range is from 1 to 1000. Default is no limit.
registration-required	(Optional) Solicits registration from the mobile node even if it uses collocated care-of addresses. The Registration-required (R) bit is advertised.
challenge	(Optional) Configures configure the FA challenge parameters.
timeout *value*	Challenge timeout in seconds. Possible values are 1 through 10.
window *num*	Maximum number of valid challenge values to maintain. Possible values are 1 through 10. The default is 2.
forward-mfce	Enables the FA to forward MFCE and mobile station-AAA to the HA.
reverse-tunnel [**mandatory**]	(Optional) Enables reverse tunneling on the FA.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enables foreign agent service on the interface. The foreign agent (F) bit is 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 collocated care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from the interface of this foreign agent.

Table 4 lists the advertised bitflags.

Table 4 Foreign Agent Advertisement Bitflags

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

Examples

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

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

Related Commands

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

ip mobile foreign-service revocation

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

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

Syntax Description

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

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 shows how to enable the **ip mobile foreign-service revocation** command:

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

ip mobile foreign-service revocation exclude-nai

To exclude the MN NAI extension in the registration-revocation message, use the **ip mobile foreign-service revocation exclude-nai** command in the global configuration mode. Use the **no** form of the command to disable this feature.

Syntax Descriptioni

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Description
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **ip mobile foreign-service revocation exclude-nai** command:

```
Router(config)# ip mobile foreign-service revocation exclude-nai
```

ip mobile prefix-length

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

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

There are no keywords or variables for this command.

Defaults

The prefix-length extension is not appended.

Command Modes

Interface configuration

Command History

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

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 shows how to append the prefix-length extension to agent advertisements sent by a foreign agent:

```
ip mobile prefix-length
```

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile proxy-host

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

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

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

Syntax Description

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

Defaults

No security association is specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip mobile proxy-registration lifetime

To locally configure the proxy Mobile IP attributes of the PDSN, use the **ip mobile proxy-registration lifetime** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile proxy-registration lifetime

no ip mobile proxy-registration lifetime

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XR6	This command was introduced.

Usage Guidelines

This command allows an administrator to specify lifetime in registration request, which is sent as part of the Proxy MIP RRQ from FA to HA.

Examples

The following example shows how to enable the proxy-registration lifetime:

```
ip mobile proxy-registration lifetime ?
  <3-65535>  Specify lifetime in registration request
```

ip mobile proxy-registration mn-aaa-auth

To add MN-HAAA authentication to NVSE ip mobile attribute in PMIP RRQ, use the **ip mobile proxy-registration mn-aaa-auth** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile proxy-registration mn-aaa-auth

no ip mobile proxy-registration mn-aaa-auth

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XR6	This command was introduced.

Usage Guidelines

This command allows an administrator to enable the Cisco vendor specific MN-AAA authentication (HA-chap) chap NVSE, which is sent as part of the Proxy MIP RRQ from Foreign Agent (FA) to Home Agent (HA). This command is recommended only if FA operates with CISCO HA.

Examples

The following example shows how to enable the **ip mobile proxy-registration mn-aaa-auth** command:

```
ip mobile proxy-registration mn-aaa-auth
```

ip mobile proxy-registration sequencing

To configure the Proxy Mobile IP sequencing, use the **ip mobile proxy-registration sequencing** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile proxy-registration sequencing

no ip mobile proxy-registration sequencing

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XR6	This command was introduced.

Usage Guidelines

This command allows an administrator to enable the PMIP sequence number CVSE, which is sent as part of the Proxy MIP RRQ from FA to HA. This command is recommended only if FA operates with CISCO HA.

Examples

The following example shows how to enable the PMIP sequence number CVSE to send as part of the PMIP RRQ from FA:

```
ip mobile proxy-registration sequencing
```

ip mobile registration-lifetime

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

ip mobile registration-lifetime seconds

Syntax Description

seconds	Lifetime in seconds. Range is from 3 to 65535 (infinity).

Defaults

36000 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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 are denied.

Examples

The following example shows how to set 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
show ip mobile interface	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** global configuration command. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure {**aaa-download** | **visitor** | **home-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key** {**hex** | **ascii**} *string* [**replay timestamp** [*number*] **algorithm md5 mode prefix-suffix**]

no ip mobile secure {**aaa-download** | **visitor** | **foreign-agent** | **proxy-host**} {*lower-address* [*upper-address*] | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key** {**hex** | **ascii**} *string* [**replay timestamp** [*num*] **algorithm md5 mode prefix-suffix**]

Syntax Description

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

Defaults

No security association is specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ip mobile tunnel

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to assign and specifically names a crypto map:

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

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

ip mobile tunnel ip-ip conserve-ip-id threshold *value*

To configure the threshold of the packet size, use the **ip mobile tunnel ip-ip conserve-ip-id threshold** *value* command in Global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile tunnel ip-ip conserve-ip-id threshold *value*

no ip mobile tunnel ip-ip conserve-ip-id threshold *value*

The new command enables you to set:

- A unique non-zero value for the IP-ID of the packet if the packet size is above the threshold value.
- Zero value for the IP-ID of the packet if the packet size is less than the threshold value.

Syntax Description

There are no keywords or variables for this command.

Defaults

By default or when you do not configure the command, all the packets have a non-zero ip-id.

Command Modes

Global configuration

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **ip mobile tunnel ip-ip conserve-ip-id threshold** *value* command:

```
Router (config)# ip mobile tunnel ip-ip conserve-ip-id threshold value
```

link-flow (service flows qos subscriber profile sub-mode)

To configure the maximum service connection parameter, use the **link-flow** command in the service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

link-flow *number*

no linkflow *number*

Syntax Description

number	The maximum service connection parameter value. The valid range is 1-255.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode.

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **link-flow** command:

```
Router#(config-qos-profile)# link-flow ?
  <1-255>  Value

Router#(config-qos-profile)# link-flow 40 ?
```

ppp accm

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

ppp accm *number*

no ppp accm

Syntax Description

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

Defaults

The default value is 000A0000.

Command Modes

Interface Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to specify that PDSN propose an ACCM of 0x00000000:

```
ppp accm 00000000
```

Related Commands

Command	Description
ppp authentication	Specifies CHAP or PAP authentication.

ppp authentication

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

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

no ppp authentication

Syntax Description

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

Defaults

PPP authentication is not enabled.

Command Modes

Interface Configuration

Command History

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

Usage Guidelines

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

```
ppp authentication chap pap optional
```

Examples

The following example shows how to configure virtual-template interface 4:

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

Related Commands

Command	Description
ppp accm	Identifies the ACCM table.

service cdma pdsn

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

service cdma pdsn

no service cdma pdsn

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable PDSN service:

```
service cdma pdsn
```

Related Commands

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

set dos

To make a packet eligible for dos, use the **set dos** command under policy-map sub-command mode. Use the **no** form of the command to disable this feature.

set dos

no set dos

Syntax Description

There are no keywords or variables for this command.

Defaults

No default behavior or values.

Command Modes

Policy-map sub-command mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable dos marking under the policy map named policy-pdsn that uses a previously configured class-map named class-pdsn:

```
PDSN_ACTIVE(config)# policy-map policy-pdsn
PDSN_ACTIVE(config-pmap)# class class-pdsn
PDSN_ACTIVE(config-pmap-c)# set dos
PDSN_ACTIVE(config-pmap-c)# exit
PDSN_ACTIVE(config-pmap)# exit
PDSN_ACTIVE(config)# exit
PDSN_ACTIVE#
```

show cdma pdsn

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

Note This command, if executed on PCOP, aggregates data or statistics from each TCOP and displays the data in PCOP.

show cdma pdsn

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(8)XW	QoS and Prepaid output was included in the example.
12.3(8)XW1	Closed-RP output was included in the example.
12.4(15)XR	The output was enhanced to display the following: • The number of sessions that have QoS enabled • If policing is installed and enabled. • If the multiple service flow feature is enabled, or not. • The maximum number of auxiliary A10s allowed. • The Number of sessions active with service flows. • The total number of service flows currently active in the system.
12.4(22)XR	PDSN 5.0 uses Single IP architecture and so the following values are not displayed in the output: • The number of connected PCFs • The number of PCFs 3GPP2-RP The output is enhanced to display the status of dos, status of flow-based policy, and number of RAA-enabled sessions. Enable RAA for the output to display the RAA statistics.
12.4(22)XR1	New example is added for the command when CLID is enabled.

Examples

The following example shows how to enable the **show cdma pdsn** command:

```
PDSN# show cdma pdsn
```

```
PDSN software version 5.0, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  A11 session-update timeout 2 sec, retransmissions 3
  Mobile IP registration timeout 100 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCFs limit not set
  Maximum sessions limit not set (default 175000 maximum)
  SNMP failure history table size 100
  MSID Authentication is enabled
      Network code digits for IMSI 5, MIN 6, IRM 4
      Profile Password is cisco
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is enabled
  Allow CI_ADD option during IPCP Phase  is disabled
  Aging of idle users disabled
  Radius Disconnect Capability enabled
  Multiple Service flows enabled
  Maximum number of service-flows per MN allowed is 6
  Call Admission Control disabled
  Police Downstream enabled
  Data Over Signaling disabled
  Flow based policy disabled

  Number of pcfs connected 1,
  Number of pcfs 3GPP2-RP 1,
  Number of sessions connected 1,
  Number of sessions 3GPP2-RP 1,
  Number of sessions Active 1, Dormant 0,
  Number of sessions using HDLCoGRE 1, using PPPoGRE 0
  Number of sessions using Auxconnections 0, using Policing 0, using DSCP 0
  Number of service flows 0
  Number of RAA flows 0 -------------------|-----> new
  Number of sessions connected to VRF 0,-------------------|-----> new
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 1, VPDN flows 0
```

The following example shows the output for the **show cdma pdsn** command when CLID is enabled:

```
PDSN_SBY# show cdma pdsn
PDSN software version 5.0, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 5 sec
  A10 maximum lifetime allowed 1800 sec
  GRE sequencing is on
  Maximum PCFs limit not set
  Maximum sessions limit not set (default 9950 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
  Allow CI_ADD option during IPCP Phase  is disabled
  Aging of idle users disabled
  Radius Disconnect Capability disabled
  Multiple Service flows enabled
  Maximum number of service-flows per MN allowed is 10
  Call Admission Control disabled
  Police Downstream disabled
  Calling-station-Id as NAI for Mobile IP enabled
  Data Over Signaling disabled
  Flow based policy disabled
```

```
Number of pcfs connected 1,
Number of pcfs 3GPP2-RP 1,
Number of sessions connected 2,
Number of sessions 3GPP2-RP 2,
Number of sessions Active 2, Dormant 0,
Number of sessions using HDLCoGRE 2, using PPPoGRE 0
Number of sessions using Auxconnections 0, using Policing 0, using DSCP 0
Number of service flows 0
Number of flows using flow based qos 0
Number of sessions connected to VRF 0,
  Simple IP flows 0, Mobile IP flows 1,
  Proxy Mobile IP flows 1, VPDN flows 0
```

Note The RAA information appears only if you have enabled RAA.

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

Note Accounting information varies for each session. Hence, if you run this command on PCOP, it does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

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(14)YX	IPv6 UDR show output was added.

Usage Guidelines

The counter names appear in abbreviated format.

Examples

The following example shows how to enable the **show cdma pdsn accounting** command:

```
PDSN-ACT# show cdma pdsn accounting
 UDR for session -----------------|-----> new
 session ID: 1
 Mobile Station ID IMSI 00123456790

    A - A1:00123456790 A2: A3:
    C - C3:0
    D - D3:4.0.0.1 D4:000000000000
    E - E1:0000
    F - F1:00F1 F2:00F2 F5:003B F6:F6 F7:F7 F8:F8
        F9:F9 F10:FA F14:00 F15:1
        F16:00 F17:00 F18:00
        F19:00 F20:00 F22:00
    G - G3:0 G8:0 G9:1 G10:0 G11:0 G12:0
        G13:0 G14:1294 G15:0 G16:0 G17:0
    I - I1:0 I4:0
    Y - Y2:1

 UDR for flow
```

```
    Mobile Node IP address 3.0.0.5
    B - B1:3.0.0.5 B2:mwtr-sip-user
    C - C1:0039 C2:11 C4:0
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:280 G2:1000 G4:1239692184
        G22:0 G23:0 G24:0 G25:0
    Packets- in:10 out:5
    G5:RAA Table Address 10.10.10.1 Mask 255.255.255.255 -------------------|-----> new

    Bytes In : 1000 Bytes Out : 0
    G5:RAA Table Index 2 Summarized
    Bytes In : 1000 Bytes Out : 0
```

Note If you enable RAA, the G5 container displays the byte count.

When you configure the **cdma pdsn imsi-min-equivalence** command, the following output is displayed for the **show cdma pdsn accounting** command:

```
UDR for session
 session ID: 1
 Mobile Station ID IMSI 112345678987655
    A - A1:5678987655 A2: A3:
    C - C3:0
    D - D3:11.1.1.12 D4:000000000000
    E - E1:0000
    F - F1:0000 F2:0000 F5:003B F6:00 F7:00 F8:00
        F9:00 F10:00 F14:00 F15:0
        F16:00 F17:00 F18:00
        F19:00 F20:00 F22:00
    G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0
        G13:0 G14:176 G15:0 G16:0 G17:0
    I - I1:0 I4:0
    Y - Y2:1

 UDR for flow
    Mobile Node IP address 9.1.1.9
    B - B1:9.1.1.9 B2:g7SIP1@xxx.com
    C - C1:0025 C2:98 C4:0
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:0 G2:0 G4:1243836799
        G22:0 G23:0 G24:0 G25:0
    Packets- in:0 out:0
```

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.
12.4xx	This output has been enhanced to display the HRPD and IP Flow details.

Examples

The following example shows how to enable the **show cdma pdsn accounting detail** command:

```
PDSN-ACT# show cdma pdsn accounting detail

 UDR for session
 session ID: 1
 Mobile Station ID IMSI 987654321098766

   Mobile Station ID (A1) IMSI 987654321098766
   ESN (A2)
   MEID (A3)
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 123412341234 ---------------|-----> new
   HRPD Subnet (D7) SNL 128 --------------------|-----> new
                    SN  00010002000300040000000000000005 ----------------------|-----> new
                    SID 00070008000900100000000000000011 ----------------------|-----> new
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 59   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    Always On (F15) 0
   Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0
   Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0
   Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 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) 659
  In-Bound Mobile IP Signalling Octet Count (G15) 0
  Out-bound Mobile IP Signalling Octet Count (G16) 0
  Last User Activity Time (G17) 0
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 1

UDR for flow
   Mobile Node IP address 9.1.1.5
   IP Address (B1) 9.1.1.5,  Network Access Identifier (B2) g7SIP1@xxx.com
   Account Session ID (C1) 16
   Correlation ID (C2) ' ' 58
   Beginning Session (C4) ' ' 1
   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 G4:1245923648
   Rsvp Signaling Inbound  Count (G22) 0 Outbound Count (G23) 0
   Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
   Packets- in:0 out:0
   Remote Address Accounting ---------------------|-----> new
   IP Address : 10.10.10.1 Mask : 255.255.255.255 --------------------|-----> new
   Bytes In : 1000 Bytes Out: 0 --------------------|-----> new
   Remote Address Accounting Table Index 1, Summarized ----------------|-----> new
   Bytes In : 1000 Bytes Out: 0


UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x04 Direction : Forward
    Account Session ID (C1) 000D Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 4
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :4
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
```

```
 R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
 Session ID : 2 Flow ID : 0x05 Direction : Forward
  Account Session ID (C1) 000E Correlation (C2) 0
  Service Reference ID (C5) 2 Flow ID (C6) 5
  Serving PCF (D3) 11.1.1.12
  HRPD Subnet (D7) SNL 128 --------------------|-----> new
                   SN  00010002000300040000000000000005 --------------------|-----> new
                   SID 00070008000900100000000000000011 --------------------|-----> new
  Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
  Service Option (F5) 59   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    Forward PDCH RC (F16) 0
  Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
  Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
  Reverse PDCH RC (F22) 0    Flow Status (F24) Active

  Data Octet Count Terminating (G1) 0
  Data Octet Count Originating (G2) 0  Event Time G4:0
  Active Time (G8) 0
  Number of Active Transitions (G9) 1
  SDB Octet Count Terminating (G10) 0
  SDB Octet Count Originating (G11) 0
  Number of SDBs Terminating (G12) 0
  Number of SDBs Originating G13 0
  Granted Qos (I5):
   Flow direction :0 Flow ID :5
   Qos Attribute Set ID :1
   Flow Profile ID :0 Traffic Class :1
   Peak Rate :2 Bucket Size :13
   Token Rate :15 Maximum Latency :1
   Max IP Packet Loss Rate :12
   Packet Size :15 Delay Variance Sensitive :1
 IP Quality of Service (I1) 0
 Airlink Quality of Service (I4) 0
 R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
 Session ID : 2 Flow ID : 0x06 Direction : Reverse
  Account Session ID (C1) 000B Correlation (C2) 0
  Service Reference ID (C5) 2 Flow ID (C6) 6
  Serving PCF (D3) 11.1.1.12
  HRPD Subnet (D7) SNL 128 --------------------|-----> new
                   SN  00010002000300040000000000000005 --------------------|-----> new
                   SID 00070008000900100000000000000011 --------------------|-----> new
  Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
  Service Option (F5) 59   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    Forward PDCH RC (F16) 0
  Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
  Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
  Reverse PDCH RC (F22) 0    Flow Status (F24) Active

  Data Octet Count Terminating (G1) 0
  Data Octet Count Originating (G2) 0  Event Time G4:0
  Active Time (G8) 0
  Number of Active Transitions (G9) 1
  SDB Octet Count Terminating (G10) 0
  SDB Octet Count Originating (G11) 0
  Number of SDBs Terminating (G12) 0
  Number of SDBs Originating G13 0
```

```
     Granted Qos (I5):
       Flow direction :1 Flow ID :6
       Qos Attribute Set ID :1
       Flow Profile ID :0 Traffic Class :1
       Peak Rate :2 Bucket Size :13
       Token Rate :15 Maximum Latency :1
       Max IP Packet Loss Rate :12
       Packet Size :15 Delay Variance Sensitive :1
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   R-P Session ID (Y2) 2

 UDR for IPFlow (new: Yes)
   Session ID : 2 Flow ID : 0x07 Direction : Reverse
     Account Session ID (C1) 000C Correlation (C2) 0
     Service Reference ID (C5) 2 Flow ID (C6) 7
     Serving PCF (D3) 11.1.1.12
     HRPD Subnet (D7) SNL 128 --------------------|-----> new
                      SN  00010002000300040000000000000005 --------------------|-----> new
                      SID 00070008000900100000000000000011 --------------------|-----> new
     Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
     Service Option (F5) 59   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    Forward PDCH RC (F16) 0
     Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
     Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
     Reverse PDCH RC (F22) 0    Flow Status (F24) Active

     Data Octet Count Terminating (G1) 0
     Data Octet Count Originating (G2) 0  Event Time G4:0
     Active Time (G8) 0
     Number of Active Transitions (G9) 1
     SDB Octet Count Terminating (G10) 0
     SDB Octet Count Originating (G11) 0
     Number of SDBs Terminating (G12) 0
     Number of SDBs Originating G13 0
     Granted Qos (I5):
       Flow direction :1 Flow ID :7
       Qos Attribute Set ID :1
       Flow Profile ID :0 Traffic Class :1
       Peak Rate :2 Bucket Size :13
       Token Rate :15 Maximum Latency :1
       Max IP Packet Loss Rate :12
       Packet Size :15 Delay Variance Sensitive :1
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
    R-P Session ID (Y2) 2
```

Note If you enable RAA, the Remote Address Accounting statistics are displayed.

When you configure the **cdma pdsn imsi-min-equivalence** command, the following output is displayed for the **show cdma pdsn accounting detail** command:

```
UDR for session
 session ID: 1
 Mobile Station ID IMSI 112345678987656

   Mobile Station ID (A1) IMSI 5678987656
   ESN (A2)
   MEID (A3)
```

```
  Session Continue (C3) ' ' 0
  Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 000000000000
  User Zone (E1) 0000
  Forward Mux Option (F1) 0    Reverse Mux Option (F2) 0
  Service Option (F5) 59   Forward Traffic Type (F6) 0
  Reverse Traffix type (F7) 0    Fundamental Frame size (F8) 0
  Forward Fundamental RC (F9) 0    Reverse Fundamntal RC (F10) 0
  DCCH Frame Format (F14) 0    Always On (F15) 0
  Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0
  Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0
  Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 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) 290
  In-Bound Mobile IP Signalling Octet Count (G15) 0
  Out-bound Mobile IP Signalling Octet Count (G16) 0
  Last User Activity Time (G17) 0
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 1

UDR for flow
   Mobile Node IP address 9.1.1.1
   IP Address (B1) 9.1.1.1,  Network Access Identifier (B2) g7SIP1@xxx.com
   Account Session ID (C1) 2
   Correlation ID (C2) ' ' 18
   Beginning Session (C4) ' ' 0
   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 G4:1243950581
   Rsvp Signaling Inbound  Count (G22) 0 Outbound Count (G23) 0
   Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
   Packets- in:0 out:0
```

show cdma pdsn accounting mn-ip-addr

To display accounting information for sessions, the corresponding flows, and the counter names (along with the abbreviated names) of a specified mn-ip-address, use the **show cdma pdsn accounting mn-ip-addr** command in privileged EXEC mode.

show cdma pdsn accounting mn-ip-addr *mn-ip-address* **detail**

Syntax Description

mn-ip-addr *mn-ip-address*	Specifies the IP addresses assigned to the mobile numbers in each session.
detail	Displays information about existing details.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show cdma pdsn accounting user** command:

```
Router# show cdma pdsn accounting mn-ip-address 6.0.0.14 detail

UDR for session
 session ID: 1
 Mobile Station ID IMSI 987654321098766

   Mobile Station ID (A1) IMSI 987654321098766
   ESN (A2)
   MEID (A3)
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 123412341234 ---------------|-----> new
   HRPD Subnet (D7) SNL 128 --------------------|-----> new
                    SN  00010002000300040000000000000005 ----------------------|-----> new
                    SID 00070008000900100000000000000011 ----------------------|-----> new
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 59   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    Always On (F15) 0
   Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0
   Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0
   Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 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) 659
  In-Bound Mobile IP Signalling Octet Count (G15) 0
  Out-bound Mobile IP Signalling Octet Count (G16) 0
  Last User Activity Time (G17) 0
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 1

UDR for flow
   Mobile Node IP address 9.1.1.5
   IP Address (B1) 9.1.1.5,  Network Access Identifier (B2) g7SIP1@xxx.com
   Account Session ID (C1) 16
   Correlation ID (C2) ' ' 58
   Beginning Session (C4) ' ' 1
   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 G4:1245923648
   Rsvp Signaling Inbound  Count (G22) 0 Outbound Count (G23) 0
   Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
   Packets- in:0 out:0
   Remote Address Accounting ---------------------|-----> new
   IP Address : 10.10.10.1 Mask : 255.255.255.255 --------------------|-----> new
   Bytes In : 1000 Bytes Out: 0 --------------------|-----> new
   Remote Address Accounting Table Index 1, Summarized ----------------|-----> new
   Bytes In : 1000 Bytes Out: 0


UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x04 Direction : Forward
    Account Session ID (C1) 000D Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 4
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :4
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x05 Direction : Forward
    Account Session ID (C1) 000E Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 5
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :5
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x06 Direction : Reverse
    Account Session ID (C1) 000B Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 6
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :6
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x07 Direction : Reverse
    Account Session ID (C1) 000C Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 7
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :7
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2
```

Note If you enable RAA, the Remote Address Accounting statistics are displayed.

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.

Usage Guidelines

The counter names appear in abbreviated format.

Examples

The following example shows how to enable the **show cdma pdsn accounting session** command:

```
Router# show cdma pdsn accounting session sipuser ?
  detail  detailed accounting information by MSID
  flow    flow id for session
  ip-flow IP flow id for session
  |       Output modifiers
  <cr>

show cdma pdsn accounting session sipuser ip-flow ?
  <1-255> IP flow id for session

show cdma pdsn accounting session sipuser ip-flow 5 ?
  direction Direction of the IP flow
  <cr>

show cdma pdsn accounting session sipuser ip-flow 5 direction ?
  forward  Forward IP Flow accounting details
  reverse  Reverse IP Flow accounting details

show cdma pdsn accounting session sipuser ip-flow 5 direction forward ?
  <cr>

show cdma pdsn accounting session sipuser ip-flow 5
UDR for IPFlow (new: Yes)
   Session ID : 0 Flow ID : 0x05 Direction : Forward
   Serving PCF (D3) 80.0.0.20
    C - C1:0010 C2:16
    D - D3:80.0.0.20D7:00000000
    F - F1:0000 F2:0000 F5:0000 F6:00 F7:00 F8:00
        F9:00 F10:00 F14:00 F16:00 F17:00 F18:00
         F19:00 F20:00 F22:00 F24:0000
    G - G1:0 G2:0 G4:0 G8:0
        G9:0 G10:0 G11:0 G12:0 G13:0
    I - I1:0 I4:0
    Y - Y2:0


show cdma pdsn accounting
UDR for session
 session ID: 1
 Mobile Station ID IMSI 123455432112346

    A - A1: A2: A3:
    C - C3:0 C5: C6:
    D - D3:0.0.0.0 D4: D8:
    E - E1:0000
    F - F1:0000 F2:0000 F5:0000 F6:00 F7:00 F8:00
        F9:00 F10:00 F14:00 F15:0
    G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:173 G15:0 G16:162
    I - I1:0 I4:0 I5:
    Y - Y2:0

 UDR for flow
    Mobile Node IP address 32.1.35.204
    B - B1:32.1.35.204 B2:gSIP1@xxx.com
    C - C1:25A5CA3 C2:13158870 C4:0
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:0 G2:0 G4:1173256572 G20: G21: G22: G23: G24: G25:
    Packets- in:0 out:0
```

The following session details are new:

```
UDR for IPFlow (new: Yes)
   Session ID : 0 Flow ID : 0x05 Direction : Forward
   Serving PCF (D3) 80.0.0.20
    C - C1:0010 C2:16
    D - D3:80.0.0.20
    F - F1:0000 F2:0000 F5:0000 F6:00 F7:00 F8:00
        F9:00 F10:00 F14:00 F16:00 F17:00 F18:00
         F19:00 F20:00 F22:00 F24:0000
    G - G1:0 G2:0 G4:0 G8:0
        G9:0 G10:0 G11:0 G12:0 G13:0
    I - I1:0 I4:0
    Y - Y2:0
```

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**

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.
12.4xx	

Usage Guidelines

The counter names appear in abbreviated format.

Examples

The following example shows how to enable the **show cdma pdsn accounting session detail** command:

```
Router# sh cdma pdsn accounting session 00000000004 detail
UDR for session
 session ID: 1
 Mobile Station ID IMSI 987654321098766

   Mobile Station ID (A1) IMSI 987654321098766
   ESN (A2)
   MEID (A3)
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 123412341234 ---------------|-----> new
   HRPD Subnet (D7) SNL 128 --------------------|-----> new
                    SN  00010002000300040000000000000005 ----------------------|-----> new
                    SID 00070008000900100000000000000011 ----------------------|-----> new
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 59   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    Always On (F15) 0
   Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0
   Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0
   Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 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) 659
  In-Bound Mobile IP Signalling Octet Count (G15) 0
  Out-bound Mobile IP Signalling Octet Count (G16) 0
  Last User Activity Time (G17) 0
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 1

UDR for flow
   Mobile Node IP address 9.1.1.5
   IP Address (B1) 9.1.1.5,  Network Access Identifier (B2) g7SIP1@xxx.com
   Account Session ID (C1) 16
   Correlation ID (C2) ' ' 58
   Beginning Session (C4) ' ' 1
   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 G4:1245923648
   Rsvp Signaling Inbound  Count (G22) 0 Outbound Count (G23) 0
   Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
   Packets- in:0 out:0
   Remote Address Accounting ---------------------|-----> new
   IP Address : 10.10.10.1 Mask : 255.255.255.255 --------------------|-----> new
   Bytes In : 1000 Bytes Out: 0 --------------------|-----> new
   Remote Address Accounting Table Index 1, Summarized ----------------|-----> new
   Bytes In : 1000 Bytes Out: 0


UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x04 Direction : Forward
    Account Session ID (C1) 000D Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 4
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :4
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x05 Direction : Forward
    Account Session ID (C1) 000E Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 5
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :5
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x06 Direction : Reverse
    Account Session ID (C1) 000B Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 6
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :6
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x07 Direction : Reverse
    Account Session ID (C1) 000C Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 7
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :7
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2
```

Note If you enable RAA, the Remote Address Accounting statistics are displayed.

Here is show output for the **show cdma pdsn accounting session detail** command in the PDSN 4.0 Release:

```
UDR for session
 session ID: 1
 Mobile Station ID IMSI 123455432112346
```

```
   Mobile Station ID (A1) IMSI
   ESN (A2)
   MEID (A3)
   Session Continue (C3) ' ' 0
   Service Ref ID (C5)
   Flow ID (C6)
   Serving PCF (D3) 0.0.0.0 Base Station ID (D4)
   Carrier-ID (D8)
   User Zone (E1) 0000
   Forward Mux Option (F1) 0    Reverse Mux Option (F2) 0
   Service Option (F5) 0    Forward Traffic Type (F6) 0
   Reverse Traffic type (F7) 0    Fundamental Frame size (F8) 0
   Forward Fundamental RC (F9) 0    Reverse Fundamental RC (F10) 0
   DCCH Frame Format (F14) 0    Always On (F15) 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) 173
   In-Bound Mobile IP Signaling Octet Count (G15) 0
   Out-bound Mobile IP Signaling Octet Count (G16) 162
   IP Quality of Service (I1) 0
   Airlink Quality of Service (I4) 0
   Granted QoS (I5)
   R-P Session ID (Y2) 0

 UDR for flow
    Mobile Node IP address 32.1.35.204
    IP Address (B1) 32.1.35.204,  Network Access Identifier (B2)
gSIP1@xxx.com <mailto:gSIP1@xxx.com>
    Correlation ID (C2) ' ' 13158870
    Beginning Session (C4) ' ' 0
    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 G4:1173256572
    Filtered Octet count Terminating (G20)
    Filtered Octet count Originating (G21)
    Packets- in:0 out:0

<Following are new>
    UDR for IPFlow (new: Yes)
    Session ID : 0 Flow ID : 0x05 Direction : Forward
    Serving PCF (D3) 80.0.0.20
   HRPD Subnet (D7):
      Subnet            : 0 | 0 | 0 | 0
      Sector ID         : 0 | 0 | 0 | 0
    Forward Mux Option (F1) 0    Reverse Mux Option (F2) 0
    Service Option (F5) 0    Forward Traffic Type (F6) 0
    Reverse Traffix type (F7) 0    Fundamental Frame size (F8) 0
    Forward Fundamental RC (F9) 0    Reverse Fundamntal RC (F10) 0
    DCCH Frame Format (F14) 0   Flow Status (F24) 0000
    Forward PDCH RC (F16)  0Forward DCCH Mux Option (F17) 0
    Reverse DCCH Mux Option (F18) 0Forward DCCH RC (F19) 0
    Reverse DCCH RC (F20) 0Reverse PDCH RC (F22) 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
```

```
Granted Qos:
Flow direction :0 Flow ID :0
Qos Attribute ID :0 Flow Profile ID :0
Qos Attribute Set ID :0 Traffic Class :0
Peak Rate :0 Bucket Size :0
Token Rate :0 Maximum Latency :0
Max IP Packet Loss Rate :0
Packet Size :0 Delay Variance Sensitive :0
IP Quality of Service (I1) 0
RSVP Signaling Octets Inbound (G22)
RSVP Signaling Octets Outbound (G23)
RSVP Signaling Packets Inbound (G24)
RSVP Signaling Packets Outbound (G25)
Airlink Quality of Service (I4) 0
R-P Session ID (Y2) 0
```

show cdma pdsn accounting session flow

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The counter names appear in abbreviated format.

Examples

The following example shows how to enable the **show cdma pdsn accounting session flow** command:

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

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

PDSN-6500#
```

show cdma pdsn accounting session flow user

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable the **show cdma pdsn accounting session flow user** command:

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

 UDR for flow
    Mobile Node IP address 15.0.0.3

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

Router#
```

show cdma pdsn accounting user

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

show cdma pdsn accounting user [**nai** | **username**] {**detail**}

Syntax Description

user *nai*	Displays accounting information for the specified NAI.
detail	Displays information about existing details.

You can also use a wildcard (*) to view session information for users and NAIs matching the string you specify.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show cdma pdsn accounting user** command:

```
Router# show cdma pdsn accounting user *san* detail
UDR for session
 session ID: 1
 Mobile Station ID IMSI 987654321098766

   Mobile Station ID (A1) IMSI 987654321098766
   ESN (A2)
   MEID (A3)
   Session Continue (C3) ' ' 0
   Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 123412341234 ---------------|-----> new
   HRPD Subnet (D7) SNL 128 --------------------|-----> new
                    SN  00010002000300040000000000000005 ----------------------|-----> new
                    SID 00070008000900100000000000000011 ----------------------|-----> new
   User Zone (E1) 0000
   Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
   Service Option (F5) 59   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    Always On (F15) 0
   Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0
   Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0
   Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 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) 659
  In-Bound Mobile IP Signalling Octet Count (G15) 0
  Out-bound Mobile IP Signalling Octet Count (G16) 0
  Last User Activity Time (G17) 0
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 1

UDR for flow
   Mobile Node IP address 9.1.1.5
   IP Address (B1) 9.1.1.5,  Network Access Identifier (B2) g7SIP1@xxx.com
   Account Session ID (C1) 16
   Correlation ID (C2) ' ' 58
   Beginning Session (C4) ' ' 1
   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 G4:1245923648
   Rsvp Signaling Inbound  Count (G22) 0 Outbound Count (G23) 0
   Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
   Packets- in:0 out:0
   Remote Address Accounting ---------------------|-----> new
   IP Address : 10.10.10.1 Mask : 255.255.255.255 --------------------|-----> new
   Bytes In : 1000 Bytes Out: 0 --------------------|-----> new
   Remote Address Accounting Table Index 1, Summarized ----------------|-----> new
   Bytes In : 1000 Bytes Out: 0


UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x04 Direction : Forward
    Account Session ID (C1) 000D Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 4
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :4
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x05 Direction : Forward
    Account Session ID (C1) 000E Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 5
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :0 Flow ID :5
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x06 Direction : Reverse
    Account Session ID (C1) 000B Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 6
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :6
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2

UDR for IPFlow (new: Yes)
  Session ID : 2 Flow ID : 0x07 Direction : Reverse
    Account Session ID (C1) 000C Correlation (C2) 0
    Service Reference ID (C5) 2 Flow ID (C6) 7
    Serving PCF (D3) 11.1.1.12
    HRPD Subnet (D7) SNL 128 --------------------|-----> new
                     SN  00010002000300040000000000000005 --------------------|-----> new
                     SID 00070008000900100000000000000011 --------------------|-----> new
    Forward Mux Option (F1) 241  Reverse Mux Option (F2) 242
    Service Option (F5) 59   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    Forward PDCH RC (F16) 0
    Forward DCCH Mux (F17) 0    Reverse DCCH Mux (F18) 0
    Forward DCCH RC (F19) 0    Reverse DCCH RC (F20) 0
    Reverse PDCH RC (F22) 0    Flow Status (F24) Active

    Data Octet Count Terminating (G1) 0
    Data Octet Count Originating (G2) 0  Event Time G4:0
    Active Time (G8) 0
    Number of Active Transitions (G9) 1
    SDB Octet Count Terminating (G10) 0
    SDB Octet Count Originating (G11) 0
    Number of SDBs Terminating (G12) 0
    Number of SDBs Originating G13 0
    Granted Qos (I5):
      Flow direction :1 Flow ID :7
      Qos Attribute Set ID :1
      Flow Profile ID :0 Traffic Class :1
      Peak Rate :2 Bucket Size :13
      Token Rate :15 Maximum Latency :1
      Max IP Packet Loss Rate :12
      Packet Size :15 Delay Variance Sensitive :1
  IP Quality of Service (I1) 0
  Airlink Quality of Service (I4) 0
  R-P Session ID (Y2) 2
```

show cdma pdsn ahdlc

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

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP returns the information of each processor as output.

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

Syntax Description

slot_number	Slot number of the AHDLC of interest.
channel [*channel_id*]	Channel on the AHDLC. Possible values are 0 through 8000, or 0 to 20000 depending on the image you are using. If no channel is specified, information for all channels is displayed. In the PDSN 4.0 Release, the possible value is increased to 75000. In the PDSN 5.0 Release, the possible value was increased to 105000 per processor.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.2(8)BY	The possible values for channel ID were extended to 20000.
12.4(15)xx	The possible values for channel ID were extended to 75000.
12.4(22)XR	The possible values for channel ID were extended to 105000.

Examples

The following example shows how to enable 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 cac

To display various call admission control parameters and their status, use the **show cdma pdsn cac** command in Privileged EXEC mode.

Note This command, if executed on PCOP, aggregates the data or statistics from each TCOP and returns output in PCOP.

Syntax Description

There are no keywords or arguments for this command.

Defaults

No default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **show cdma pdsn cac** command:

```
Router# show cdma pdsn cac
Total configured bandwidth 180000 b
 Allocated bandwidth 0 b
 Available bandwidth 180000 b
 CPU Current 0 Threshold 90
 Memory Processor Current 0 Threshold 90
        IO Current 0 Threshold 90
```

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 {**closed rp** | **configuration** | **member** | **session** | **statistics**}

Syntax Description

closed rp	Displays closed rp details.
configuration	Displays configuration information associated with the cluster controller.
statistics	Displays various statistics collected on the cluster controller signaling messages with the cluster member, and redundancy message statistics with the redundancy peer.
member	Displays PDSN cluster member registered with PDSN cluster controller.
session	Displays session records.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.4(22)XR	Support for **queueing** is removed in this release.

Examples

The following example shows how to enable the **show cdma pdsn cluster controller** command:

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

show cdma pdsn cluster controller configuration

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

show cdma pdsn cluster controller configuration

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable 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 (collocated)
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 [*ip addr* | *load* | *prohibited*]

Syntax Description

ipaddr	Specifies the controller member.
session	Specifies the sessions redirected to a particular member on the controller.
load	Specifies the load estimated by PDSN cluster members, recorded in the controller.
prohibited	Specifies members prohibited from being selected for new data sessions

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(8)XW	The **session** keyword was added.
12.4(22)XR	Introduced Group details.

Examples

The following examples show how to enable the **show cdma pdsn cluster controller member** command.

```
Secs until   Seq seeks         Member
(past) seek    no reply      IPv4 Addr      State   Load Weight(max)
--------------------------------------------------------------------
          4       0           2.1.1.1*      ready      1    1(  100)

          7       0           2.1.9.1       ready      1    1(  100)
--------------------------------------------------------------------
                    Controller IPv4 Addr       11.1.1.50
```

Note * indicates collocated member.

In this example, the member has been configured to group 1:

```
PDSN1# show cdma pdsn cluster controller member 2.1.1.1
PDSN cluster member 2.1.1.1 (local) state      ready, Group 1 -------------|-----> new
 registered with PDSN controller 11.1.1.50
 reported load 1 percent, will be sought in 2 seconds

  Member 2.1.1.1 statistics:
  Number of sessions 0
  Controller seek rcvd 6122, Member seek reply rcvd 6122
  Member state changed 0 time to ready
  Member state changed 0 time to Admin prohibited
  Session-Up message rcvd 0, Session-Down message received 0
  Member seek not replied in sequence 0
```

If a member is not part of any group, the output is:

```
pdsn1# show cdma pdsn cluster controller member 2.1.1.1
PDSN cluster member 2.1.1.1 (local) state      ready, Group NONE--------------|-----> new
 registered with PDSN controller 11.1.1.50
 reported load 1 percent, will be sought in 2 seconds

  Member 2.1.1.1 statistics:
  Number of sessions 0
  Controller seek rcvd 6122, Member seek reply rcvd 6122
  Member state changed 0 time to ready
  Member state changed 0 time to Admin prohibited
  Session-Up message rcvd 0, Session-Down message received 0
  Member seek not replied in sequence 0
```

show cdma pdsn cluster controller session

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable the **show cdma pdsn cluster controller session** command:

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

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

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

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

show cdma pdsn cluster controller statistics

To display the IP addresses of the members that registered with a specific controller, and to include new information that displays RRQ's forwarded from the controller for which there was no Session-Up/ Session-Down message received from the member, use the **show cdma pdsn cluster controller statistics** command in privileged EXEC mode.

show cdma pdsn cluster controller statistics

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable the **show cdma pdsn controller statistics** command:

```
Router# show cdma pdsn cluster controller statistics

Sample Output:
Controller-Member Interface:
  Cluster Reg Request rcvd 191, accepted 191, discarded 0
  Cluster Reg Request sent 189
  Cluster Reg Reply rcvd 176, accepted 175, discarded 1

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 1
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0
    Enqueue to master Q fail 0, slave Q fail 0

  Controller seek requests rcvd 63, replies sent 63
  Member seek requests sent 188, replies rcvd 174
  Member state transition msgs rcvd 0, replies sent 0
    ready 0, Administratively prohibited 0
  Total A11 Reg Requests forwarded 38
    A11 Reg Requests orig forwarded 18, retry forwarded 0
    A11 Reg Requests forwarded locally orig 20, retry 0
    Session-Up from member 17, Session-Down from member 0
    Enqueue to SM fail 0 --------------------|-----> new
    Anchor Changes - Remote to local 0, Local to remote 0 --------------------|-----> new
```

```
Controller Redundancy Interface:
    Update rcvd 2 sent 160 orig sent 160 fail 0
    UpdateAck rcvd 0 sent 2
    DownloadReq rcvd 0 sent 61 orig sent 61 fail 0
    DownloadReply rcvd 62 sent 0 orig sent 0 fail 0 drop 0
    DownloadAck rcvd 0 sent 62 drop 0

    Errors: Authentication failed 0 ID mismatch 0
            Ignored due to no redundancy configuration 321
```

show cdma pdsn cluster member

To display configuration and statistics for the PDSN cluster member, including information about RRQs forwarded to the controller member, use the **show cdma pdsn cluster member** command in privileged EXEC mode.

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.4(22)XR	Support for **queueing** is removed in this release.

Examples

The following example shows how to enable the **show cdma pdsn cluster member** command:

```
Router# show cdma pdsn cluster member statistics

Sample Output:
Controller-Member Interface:
  Cluster Reg Request rcvd 191, accepted 191, discarded 0
  Cluster Reg Request sent 189
  Cluster Reg Reply rcvd 176, accepted 175, discarded 1

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 1
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0
    Enqueue to master Q fail 0, slave Q fail 0 ---------------------|-----> new

  Controller seek requests rcvd 122, replies sent 122
  Member seek requests sent 1, replies rcvd 1
  Member state transition msgs sent 0, replies rcvd 0
    ready 0, Administratively prohibited 0
  Session-Up msg sent 0, Session-Down msg sent 0
  Session-Up msg Ack rcvd 0, Session-Down msg Ack rcvd 0
  Controller seek not replied in sequence 0
  Member state not replied in sequence 0
```

The following example shows how to enable the **show cdma pdsn cluster member configuration** command:

```
Router# show cdma pdsn cluster member configuration
    cluster interface GigabitEthernet0/0.341
    IP address of controller is 11.1.1.50  (collocated)
    no prohibit administratively
    timeout to resend status or seek controller = 10 sec or less, randomized
    resend a msg for 2 timeouts sequentially if no reply, then inform operator
    default:  spi 101, Timestamp +/- 0, key ascii hello
    this PDSN cluster member is configured
```

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.

Note Flow information varies for each session. Hence, this command when executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show cdma pdsn flow {mn-ip-address *ip_address* | **mn-ip-address range** *start-ip end-ip*{**detail** | **summary**} | **mn-ipv6-address** *address* | **prepaid** | **msid** *string* | **service-type** | **user** *string*}

Syntax Description

mn- ip-address *ip_address*	Specifies the IP addresses assigned to the mobile numbers in each session.
mn-ipv6-address *address*	Specifies the CDMA PDSN user information by MN IPv6 address.
prepaid	Specifies the CDMA PDSN prepaid flow information.
msid *string*	Specifies the mobile subscriber id number.
service-type	Specifies the CDMA PDSN user information by Service Type.
user *string*	Specifies the CDMA PDSN flow information by user NAI.
mn-ip-address range *start-ip end-ip*	Specifies the CDMA PDSN flow information for the specified range of IP addresses.

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	**mn-ipv6-address** output was introduced.
12.4(22)XR	**mn-ip-address range** option was introduced.

Examples

The following example shows how to enable the **show cdma pdsn flow** command:

```
Router# show cdma pdsn flow

MSID            NAI                                     Type        MN IP Address    St
100000000000099 sim1                                    Simple      100.4.1.1        ACT
200000000000047 sim1                                    Simple      100.4.1.2        ACT
100000000000100 sim1                                    Simple      100.4.1.40       ACT
200000000000048 sim1                                    Simple      100.4.1.3        ACT
100000000000101 sim1                                    Simple      100.4.1.5        ACT
200000000000049 sim1                                    Simple      100.4.1.4        ACT
```

```
100000000000102 sim1                           Simple       100.4.1.6        ACT
200000000000050 sim1                           Simple       100.4.1.7        ACT
100000000000103 sim1                           Simple       100.4.1.9        ACT
200000000000051 sim1                           Simple       100.4.1.8        ACT
100000000000104 sim1                           Simple       100.4.1.11       ACT
200000000000052 sim1                           Simple       100.4.1.10       ACT
100000000000105 sim1                           Simple       100.4.1.12       ACT
200000000000053 sim1                           Simple       100.4.1.13       ACT
300000000000008 sim1                           Simple       100.4.1.14       ACT
100000000000106 sim1                           Simple       100.4.1.15       ACT
200000000000054 sim1                           Simple       100.4.1.16       ACT
300000000000009 sim1                           Simple       100.4.1.17       ACT
100000000000107 sim1                           Simple       100.4.1.19       ACT
200000000000055 sim1                           Simple       100.4.1.18       ACT
100000000000122 sim1                           Simple       100.4.1.21       ACT
200000000000070 sim1                           Simple       100.4.1.20       ACT
300000000000025 sim1                           Simple       100.4.1.22       ACT
100000000000123 sim1                           Simple       100.4.1.24       ACT
200000000000071 sim1                           Simple       100.4.1.23       ACT
300000000000026 sim1                           Simple       100.4.1.25       ACT
100000000000124 sim1                           Simple       100.4.1.26       ACT
200000000000072 sim1                           Simple       100.4.1.27       ACT
300000000000027 sim1                           Simple       100.4.1.28       ACT
100000000000125 sim1                           Simple       100.4.1.29       ACT
200000000000073 sim1                           Simple       100.4.1.30       ACT
300000000000028 sim1                           Simple       100.4.1.31       ACT
100000000000126 sim1                           Simple       100.4.1.33       ACT
200000000000074 sim1                           Simple       100.4.1.32       ACT
300000000000029 sim1                           Simple       100.4.1.34       ACT
100000000000127 sim1                           Simple       100.4.1.36       ACT
200000000000075 sim1                           Simple       100.4.1.35       ACT
300000000000030 sim1                           Simple       100.4.1.37       ACT
100000000000128 sim1                           Simple       100.4.1.39       ACT
200000000000076 sim1                           Simple       100.4.1.38       ACT
300000000000101 sim1                           Simple       100.4.1.41       ACT
100000000000199 sim1                           Simple       100.4.1.43       ACT
200000000000147 sim1                           Simple       100.4.1.42       ACT
300000000000102 sim1                           Simple       100.4.1.44       ACT
100000000000200 sim1                           Simple       100.4.1.46       ACT
 --More--
```

Following is the **mn-ipv6-address** option added in Release 3.0:

```
show cdma pdsn flow mn-ipv6-address ?

X:X:X:X::X MN IPv6 address

pdsn2#$n flow mn-ipv6-address 2001:420:10:0:211:20FF:FE43:61C

MSID NAI Type MN IP Address St

00000000000101 mwts-uc1-np-user1 Simple-ipv6

001:420:10:0:211:20FF:FE43:61C ACT
```

A new option, **mn-ip-address range**, is added in Release 5.0:

```
pdsn# show cdma pdsn flow mn-ip-address range 0.0.0.0 1.1.1.1
MSID            NAI                            Type         MN IP Address    St  HA IP
00000000101     san@santel.com                 Simple       0.0.0.0          ACT 0.0.0.0


pdsn# show cdma pdsn flow mn-ip-address range 0.0.0.0 1.1.1.1 summary
```

```
Number of flows having mn-ip-adress between 0.0.0.0 1.1.1.1 :1
Total Number of paks in   :4
Total Number of paks out  :5
Total Number of bytes in  :44
Total Number of bytes out :52

pdsn# show cdma pdsn flow mn-ip-address range 0.0.0.0 1.1.1.1 detail
  Flow service Simple, NAI san@santel.com
    Mobile Node IP address 0.0.0.0
    Packets in 4, bytes in 44
    Packets out 5, bytes out 52
    Radius disconnect enabled

pdsn#
```

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	**simple-ipv6** output was introduced.

Examples

The following example shows how to enable the **show cdma pdsn flow service simple-ipv6** command:

```
Router# show cdma pdsn flow service simple-ipv6

MSID NAI Type MN IP

Address St

00000000000101 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.

Note This command, if executed on PCOP, aggregates the data or statistics from each TCOP and returns output in PCOP.

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(2)XC	The parameters of this command were changed.
12.3(8)XW	The Closed-RP information was added to the example output.
12.4xx	New column was introduced to display the number of auxiliary A10s currently existing to the PCF.
12.4(22)XR	The session information is removed from the output. The output displays only tunnel information, not information about the sessions associated with that PCF.

Examples

The following example shows how to enable 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 5 describes the fields shown in the output of the brief version of the command.

Table 5 show cdma pdsn pcf brief Field Descriptions

Field	Description
PCF IP Address	IP address of the PCF.
Sessions	Number of active sessions.

Table 5 show cdma pdsn pcf brief Field Descriptions (continued)

Field	Description
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 13.1.102.11
PCF 13.1.102.11 has 1 session
  Received 6 pkts (181 bytes), sent 12 pkts (504 bytes)
PCF Session ID 2, Mobile Station ID IMSI 000000000000001
    A10 connection age 00:01:04
    A10 registration lifetime 65535 sec, time since last registration 28 sec
```

Table 6 describes the fields shown in the output of the command when an IP address is specified.

Table 6 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 becomes 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 7 describes the fields shown in the output of the command when the keyword **secure** is specified.

Table 7 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

Table 7 show cdma pdsn pcf secure Field Descriptions (continued)

Field	Description
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

The following example shows the show output for Release 4.0:

```
Router# show cdma pdsn pcf brief
PCF IP Address     Sessions   SFlows   Pkts In     Pkts Out     Bytes In    Bytes Out
1.1.1.1                   1        3    9           12           183          526
Router# show cdma pdsn pcf
PCF 1.1.1.2 has 1 session, 3 service flows, 1 old session, 2 old service flows,
  Received 0 pkts (0 bytes), sent 0 pkts (0 bytes)

  PCF Session ID 1, Mobile Station ID IMSI 123456789012346
    A10 connection age 00:02:19
    A10 registration lifetime 1800 sec, time since last registration 4 sec
```

The following example shows the show output for Release 5.0:

```
PDSN_ACT# show cdma pdsn pcf
PCF 2.2.2.4 has 1 session, 1 service flow ---------------------|-----> new
  Received 382 pkts (9750 bytes), sent 391 pkts (10585 bytes)
PDSN_ACT#
```

show cdma pdsn qos local profile

To display the locally configured subscriber qos profile, use the **show cdma pdsn qos local profile** command in Privileged EXEC mode.

show cdma pdsn qos local profile

Syntax Description

There are no keywords or arguments for this command.

Defaults

No default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4xx	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable the **show cdma pdsn qos local profile** command:

```
Router# PDSN# show cdma pdsn qos ?
  local       CDMA PDSN local qos information

PDSN# show cdma pdsn qos local ?
  profile  CDMA PDSN local qos profile information

PDSN# show cdma pdsn qos local profile ?
  |  Output modifiers
  <cr>

PDSN# show cdma pdsn qos local profile
CDMA PDSN LOCAL QOS PROFILE
  QoS subscriber profile
    Max Aggregate Bandwidth : 8000
    Inter User Priority : 4321
    Maximum Flow Priority : 4
    Number of persistent TFT : 10
    Total link flow : 2
      Service Option : 59
      Service Option : 61
    Flow-profile
      Forward flow-id : 1
      Reverse flow-id : 2
      Bi-direction flow-id : 3
    DSCP
      Allowed-class AF
      Max-selector class 4
```

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.

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show cdma pdsn redundancy

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.
12.4xx	Added details of number of TFTs synced to standby.

Examples

The following example shows how to enable 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
```

The following example shows the show output for the TFT sync information:

```
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                0                   0
SIP Flows               0                   0
MIP Flows               0                   0
PMIP Flows              0                   0
TFT                     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.

Usage Guidelines

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

Examples

The following example shows how to enable 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 6, Down 6, Reregistration 1
  Handoff 5, PPP renegotiation 0

Flow Events
  Simple IP Up 6, Down 6
  Mobile IP Up 0, Down 0
  Proxy Mobile IP Up 0, Down 0

Accouting Events
  Update 0, Flow Start 7, Stop 4
  Active to Dormant 4, Dormant to Active 1
  IPFlow Update 0, Start 0, Stop 0

TFT Events
  TFT Create 0, Update 0
```

show cdma pdsn resource

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

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

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

Syntax Description

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

Defaults

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

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows how to enable 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 session

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

Note Session information varies for each session. Hence, this command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show cdma pdsn session [**brief** | **always-on** | **dormant** | **mn-ip-address** *address* | **mn-ipv6-address** *address* | **msid** *number* | **user** *nai* {brief | summary}| **prepaid** | **summary** | [**lifetime age** {**greater** | **less** | **equals**} *time in hh:mm:ss* | **service-option** *so-value*] {**detail** | **summary** | **brief**}] {**qos** | **tft** | **detail**}

Syntax Description

brief	(Optional) Displays a summary of all sessions.
always-on	(Optional) Displays information about CDMA PDSN always-on sessions
dormant	(Optional) Displays information about dormant PDSN sessions.
lifetime age	(Optional) Displays the session information for the specified criteria.
mn-ip-address *address*	(Optional) Displays user information for the specified IP address.
mn-ipv6-address	(Optional) Displays CDMA PDSN user information by MN IPv6 address.
msid *number*	(Optional) Displays information for the specified MSID.
prepaid	(Optional) Displays information about prepaid flows.
qos	(Optional) Displays information about subscriber quality of service profile.
service-option	Displays information matching with the service option value.
summary	(Optional) Displays a summary of the session output.
tft	(Optional) Displays information about traffic flow templates (tfts).
detail	(Optional) Displays information about existing details.
user *nai*	(Optional) Displays information for the specified NAI.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(2)XC	The parameters of this command were altered.
12.2(8)BY	The **prepaid** variable was introduced.
12.3(8)XW	The **Qos** variables were introduced.
12.3(8)XW1	The Closed-RP session information was included in the examples.
12.3(14)YX	The Simple IPv6 session information was included in the examples.

Release	Modification
12.4xx	QoS and Policing session information was included in the examples. A new column is introduced under the **brief** keyword to display the number of service flows for the session.
12.4(22)XR	The following new commands and options are introduced: • New command statements to view the session output for a specified lifetime age is introduced. • Examples to view session information using wildcard (*) for usernames and NAIs is introduced. • For a user *NAI* | *username*, new keywords (brief and summary) are introduced. The output is similar to that of **show cdma pdsn session {brief | summary}** command except for the session information pertaining to the specified username or IP address. • Detail options are included for msid *number* and for mn-ip-address *mn-ip-address* keywords. • Service-option keyword is introduced. All session information that matches with the value of the **service-option** are displayed. • Output is enhanced to display the following: – Accounting option of a session. The value could be ‘0’, ‘1’, or ‘2’ depending upon the option received. – Remote address accounting details, if RAA is enabled for the session.
12.4(22)XR1	New example is added for the command when CLID is enabled.

Examples

The following example shows how to enable the **show cdma pdsn session** command:

```
PDSN-ACT# show cdma pdsn session

Mobile Station ID IMSI 00123456790
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:00:12,  registration lifetime 100 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime 87 sec
  Always-On enabled for the user
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 8, receive 10
  Using interface Virtual-Access2.1, status OPN
  Using AHDLC engine on slot 0, channel ID 8
  Service Option EV-DO
  This session has 1 flow
  Session Airlink State Active
  This session has 0 TFTs
  Session has accounting option :0 - Accounting option is not
downloaded/configured ---------------------|-----> new
  Flow service Simple, NAI mwtr-sip-user
```

```
    Mobile Node IP address 3.0.0.5
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
    Radius disconnect enabled
   Remote address accounting enabled ---------------------|-----> new
      RAA Table Index : 1
      RAA Table Index : 2, Summarize Enabled
```

The accounting option displays the following values as output based on various scenarios:

- 0 — The accounting option is invalid, has been downloaded or configured.
- 1 — The accounting option is configured only for mainflow.
- 2 — The accounting option is configured only for mainflow, including IP flows.

Note If you have enabled RAA, the RAA table index downloaded during access-accept is displayed.

The following example shows the output for the **show cdma pdsn session** command when CLID is enabled:

```
PDSN_SBY# show cdma pdsn session
Mobile Station ID IMSI 03120983424
  PCF IP Address 1.1.1.1, PCF Session ID 1
  A10 connection time 00:33:56,  registration lifetime 1800 sec
  Number of successful A11 re-registrations 1
  Remaining session lifetime 963 sec
  Always-On not enabled for the user
  Current Access network ID 0001-0101-01
  Last airlink record received is Connection Setup, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit UNKNOWN, receive 708
  Using interface Virtual-Access2.1, status OPN
  Using AHDLC engine on slot 0, channel ID 1
  Service Option 1xRTT Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Setup
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 18000
    Inter User Priority : 1000
    Maximum Flow Priority : 120980

  Flow service Mobile, NAI 03120983424
    RRQ NAI mip-sachin11@ark.com
    Mobile Node IP address 9.1.1.1
    Home Agent IP address 6.1.1.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
```

The following is an example of the summary command:

```
PDSN# show cdma pdsn session summary

Total Number of sessions: 1
Total Number of paks in :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203

PDSN#
```

The following examples show the output of the **cdma pdsn session lifetime age summary** command:

To view session summary for a connection time greater than 0:0:0:

```
PDSN# show cdma pdsn session lifetime age greater 0:0:0 summary

Number of sessions with lifetime greater than the given time: 1
Total Number of paks in :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203
```

To view session summary for a connection time lesser than 110:10:10:

```
PDSN# show cdma pdsn session lifetime age lesser 110:10:10 summary
Number of sessions with lifetime lesser than the given time: 1
Total Number of paks in :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203
```

To view session summary for a connection time that equals 00:17:25:

```
PDSN# show cdma pdsn session lifetime age equals 00:17:25 summary
Number of sessions with lifetime equals to the give time: 1
Total Number of paks in :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203
```

The output that returns when you use the **brief** or **detail** keywords is similar to the output for the **show cdma pdsn session** {**brief | detail**} except for the details pertaining to the specified lifetime age option.
Following is an example for the service-option command with **summary** keyword:

```
SAN-PDSN-4# show cdma pdsn session service-option 59 summary
Number of sessions with service option 59: 1
Total Number of paks in  :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203
```

The output that returns when you use the **brief** or **detail** keywords is similar to the output for the **show cdma pdsn session** {**brief | detail**} except for details pertaining to the specified lifetime age option.

The following example describes the **show cdma pdsn session user** [**username | nai**] {**brief | summary**} command using a wildcard; in this case, *ant* to return usernames such as san@santel.com:

```
PDSN# show cdma pdsn session user *sant* summary
Total Number of sessions: 1
Total Number of paks in :0
Total Number of paks out :8
Total Number of bytes in :0
Total Number of bytes out :203
```

The output for **show cdma pdsn session detail** is similar to:

- **show cdma pdsn msid** *number* **detail**, except for the detail information of a session that matches the given mobile subscriber ID.
- **show cdma pdsn session mn-ip-address** *mn-ip-address* **detail**, except for the detail information of a session that matches the given mobile IP address.

show cdma pdsn statistics

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

Note This command, if executed on PCOP, aggregates the data or statistics from each TCOP and displays the data in PCOP.

show cdma pdsn statistics [**ahdlc** | **rp** [**pcf** *ip address*] | **closed-rp** [**pcf** *ip address*] | **error** | **rm** | **tft** | **ppp** [**pcf** *ip address*] | **prepaid** | **raa** | **qos** | **radius disconnect**]

Syntax Description

rp	Displays all RP interface statistics.
ppp	Displays all PPP interface statistics
ahdlc	Displays all AHDLC statistics. The output of this command with the new option is the framing/deframing statistics of the engine.
tft	Displays all traffic flow templates (tfts) statistics.
error	Displays all CDMA PDSN RP error statistics.
pcf *ip address*	The PCF IP address.
prepaid	Displays the prepaid statistics.
radius disconnect	Displays all RADIUS disconnect statistics.
raa	Displays CDMA PDSN RAA statistics.
sm	Displays CDMA PDSN SM statistics.
qos	Displays QOS statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.3(8)XW	The **error** and **pcf** *ip address* variables were added.
12.3(8)XW1	The **closed-rp** variable was added.
12.3(11)YF	A11 session update statistics were added.
12.3(11)YF1	The **radius disconnect** statistics were added.

Release	Modification
12.4(15)XR	New counters introduced to display the following: • Number of TFTs parsed successfully or failed. • Identify the TFT parsing failure reasons. • Number of Subscriber QoS Profile downloaded from AAA or locally installed. • Consolidation of subscriber qos profile. • Policing installed or uninstalled. • Packets for which the DSCP was remarked based on policy installed.
12.4(15)XR2	The following counters were implemented as a part of the PDSN R 4.1: Invalid attribute format or invalid attribute length in • Served MDN attribute • 3GPP2 DNS server IP address
12.4(22)XR	Introduced RAA, TFT, Prepaid, and SM keywords.
12.4(22)XR1	New example for **ppp pcf** statistics is added.

Examples

The following example shows how to enable the **show cdma pdsn statistics** command:

```
SAN-PDSN# show cdma pdsn statistics
Last clearing of "show cdma pdsn statistics" counters never
RP Interface:
  Reg Request rcvd 156, accepted 156, denied 0, discarded 0
  Initial Reg Request rcvd 9, accepted 9, denied 0, discarded 0, AuxRequest 0
  Re-registration requests rcvd 119, accepted 119, denied 0, discarded 0
  Re-registration requests containing Active-Start 3, Active-Stop 5
  Re-registration requests containing new connections 0, missing connections 0, remapping
flows 0
  Handoff requests rcvd 10, accepted 10, denied 0, discarded 0,AuxRequest 0
  De-registration rcvd 18, accepted 18, denied 0, discarded 0
  De-registration Reg Request with Active-Stop 15
  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
    Max Service Flows 0, Unsupported So 0, Non-Existent A10 0
    Bandwidth Unavailable 0
  Update sent 8, accepted 8, denied 0, not acked 0
  Initial Update sent 8, retransmissions 0
  Acknowledge received 8, discarded 0
  Update reason lifetime expiry 0, PPP termination 8, other 0
  Registration Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0
  Handoff statistics:
    Inter PCF handoff active 10, dormant 0
    Update sent 10, accepted 10, denied 0, not acked 0
    Initial Update sent 10, retransmissions 0
    Acknowledge received 10, discarded 0
    De-registration accepted 10, denied 0
  Handoff Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0
  RP Session Update statistics:
  Update sent 0, accepted 0, denied 0, not acked 0
  Initial Update sent 0, retransmissions 0
  Acknowledge received 0, discarded 0
  Sent reasons Always On 0, RN-PDIT 0, Subscriber Qos 0
  RP Session Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Session parameters not updated 0
    Poorly formed request 0
  Service Option:
    1xEVDO (59) success 156, failure 0
PPP:
  Current Connections 1
  Connection requests 9, success 9, failure 0, aborted 0
  Connection enters stage LCP 10, Auth 10, IPCP 10
  Connection success LCP 10, AUTH 10, IPCP 10
  Failure reason LCP 0, authentication 0, IPCP 0, other 0
  Failure reason lower layer disconnect 0
  A10 release before LCP nego by PDSN 0, by PCF 0
  LCP Stage
    Failure Reasons Options 0, MaxRetry 0, Unknown 0
    LCP Term Req during LCP nego sent 0, rcvd 0
    A10 release during LCP nego by PDSN 0, by PCF 0
  Auth Stage
    CHAP attempt 10, success 10, failure 0, timeout 0
    PAP attempt 0, success 0, failure 0, timeout 0
    MSCHAP attempt 0, success 0, failure 0, timeout 0
    EAP attempt 0, success 0, failure 0
    MSID attempt 0, success 0, failure 0
    AAA timeouts 0, Auth timeouts 0, Auth skipped 0
    LCP Term Req during Auth nego sent 0, rcvd 0
    A10 release during Auth nego by PDSN 0, by PCF 0
  IPCP Stage
    Failure Reasons Options 0, MaxRetry 0, Unknown 0
    Options failure reason MN Rejected IP Address 0
    LCP Term Req during IPCP nego sent 0, rcvd 0
    A10 release during IPCP nego by PDSN 0, by PCF 0
  CCP Stage
    Connection negotiated compression 0
    Compression type Microsoft 0, Stac 0, other 0
    Connections negotiated MRRU 0, IPX 0, IP 10
    Connections negotiated VJ-Compression 0, BAP 0
    PPP bundles 0
    Connections failed to negotiate compression 0
  Renegotiation total 1, by PDSN 1, by Mobile Node 0
  Renegotiation success 1, failure 0, aborted 0
  Renegotiation reason: address mismatch 0, lower layer handoff 0
    GRE key change 0, other 1
  Release total 8, by PDSN 0, by Mobile Node 8
  Release by ingress address filtering 0
  Release reason: administrative 0, LCP termination 8
    Idle timeout 0, echo missed 0
    L2TP tunnel 0, insufficient resources 0
    Session timeout 0, service unavailable 0
    De-Reg from PCF 0, lifetime expiry 0, other 0
  Echo stats
    Request sent 10, resent 0, max retransmit timeout 0
    Response rcvd 10
  Discarded Packets
    Unknown Protocol Errors 0, Bad Packet Length 0
RSVP:
  IEs Parsed 0
  TFTs Created Success 0, Failure 0
  TFTs Updated Success 0, Failure 0
  TFTs Deleted Success 0, Failure 0
  Other Failure 0
    Unknown 0, Unsupported Ie types 0
  Tft Ipv4 Failure Stats
    Tft Unauthorized 0, Unsuccessful Processing 0
    Tft Treatment Unsupported 0
    Packet Filter Add 0, Replace 0
    Packet Filter Precedence Contention 0, Unavailable 0
    Packet Filter Maximum Limit 0, Non-Existent Tft add 0

QOS:
   Total Profile Download Success 0, Failure 0
   Local Profile selected 0
   Failure Reason DSCP 0, Flow Profile ID 0,
   Service option profile 0, Others 0
   Total Consolidated Profile 0, DSCP Remarked 0
   Total policing installed 0, failure 0, removed 0

PDSN related Radius attributes:
  Total Attribute Failure 0
  Failure reason
  3GPP2 Attribute
    DNS server IP address 0

slot 0:
  AHDLC Engine Type: CDMA HDLC SW ENGINE
     Engine is ENABLED
    total channels: 8000, available channels: 7999

  Framing input 5809 bytes, 161 paks
  Framing output 6988 bytes, 161 paks
  Framing errors 0, insufficient memory 0, queue overflow 0
        Invalid size 0

  Deframing input 16884 bytes, 800 paks
  Defaming output 15534 bytes, 214 paks
  Deframing errors 0, insufficient memory 0, queue overflow 0
        Invalid size 0, CRC errors 0

RADIUS DISCONNECT:
  Disconnect Request rcvd 0, accepted 0
  Disconnect Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS Id Mismatch 0
    Session Cxt Not Found 0, Administratively Prohibited 0

RAA: ---------------------|-----> new
  Total RAA index Download 20, Success 20, Failure 0
  Failure Reason Parsing 0, Index match 0

SAN-PDSN#
```

The following example shows the output for the **show cdma statistics ppp** command:

```
SAN-PDSN# show cdma pdsn statistics ppp
Last clearing of "show cdma pdsn statistics ppp" counters never
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new
PPP:
 Current Connections 0
 Connection requests 0, success 0, failure 0, aborted 0
 Connection enters stage LCP 0, Auth 0, IPCP 0
 Connection success LCP 0, AUTH 0, IPCP 0
 Failure reason LCP 0, authentication 0, IPCP 0, other 0
 Failure reason lower layer disconnect 0

 A10 release before LCP nego by PDSN 0, by PCF 0

 LCP Stage
  Failure Reasons Options 0, MaxRetry 0, Unknown 0
  LCP Term Req during LCP nego sent 0, rcvd 0
  A10 release during LCP nego by PDSN 0, by PCF 0

 Auth Stage
  CHAP attempt 0, success 0, failure 0, timeout 0
  PAP attempt 0, success 0, failure 0, timeout 0
  MSCHAP attempt 0, success 0, failure 0, timeout 0
  EAP attempt 0, success 0, failure 0
  MSID attempt 0, success 0, failure 0
  AAA timeouts 0, Auth timeouts 0, Auth skipped 0
  LCP Term Req during Auth nego sent 0, rcvd 0
  A10 release during Auth nego by PDSN 0, by PCF 0

 IPCP Stage
  Failure Reasons Options 0, MaxRetry 0, Unknown 0
  Options failure reason MN Rejected IP Address 0
  LCP Term Req during IPCP nego sent 0, rcvd 0
  A10 release during IPCP nego by PDSN 0, by PCF 0

 CCP Stage
  Connection negotiated compression 0
  Compression type Microsoft 0, Stac 0, other 0
  Connections negotiated MRRU 0, IPX 0, IP 0
  Connections negotiated VJ-Compression 0, BAP 0
  PPP bundles 0
  Connections failed to negotiate compression 0

 Renegotiation total 0, by PDSN 0, by Mobile Node 0
 Renegotiation success 0, failure 0, aborted 0
 Renegotiation reason: address mismatch 0, lower layer handoff 0
  GRE key change 0, other 0

 Release total 0, by PDSN 0, by Mobile Node 0
 Release by ingress address filtering 0
 Release reason: administrative 0, LCP termination 0
  Idle timeout 0, echo missed 0
  L2TP tunnel 0, insufficient resources 0
  Session timeout 0, service unavailable 0
  De-Reg from PCF 0, lifetime expiry 0, other 0

 Echo stats
  Request sent 0, resent 0, max retransmit timeout 0
  Response rcvd 0

 Discarded Packets
  Unknown Protocol Errors 0, Bad Packet Length 0
Here is an example output for
san-pdsn# show cdma pdsn statistics rp
Last clearing of "show cdma pdsn statistics rp" counters
Last Update received at 00:12:54 UTC Mar 1 2009
RP Interface:
 Reg Request rcvd 0, accepted 0, denied 0, discarded 0
 Initial Reg Request rcvd 0, accepted 0, denied 0, discarded 0, AuxRequest 0
 Re-registration requests rcvd 0, accepted 0, denied 0, discarded 0
 Re-registration requests containing Active-Start 0, Active-Stop 0
 Re-registration requests containing new connections 0, missing connections 0, remapping
flows 0
 Handoff requests rcvd 0, accepted 0, denied 0, discarded 0,AuxRequest 0
 De-registration rcvd 0, accepted 0, denied 0, discarded 0
 De-registration Reg Request with Active-Stop 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
  Max Service Flows 0, Unsupported So 0, Non-Existent A10 0
  Bandwidth Unavailable 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

 Handoff statistics:
  Inter PCF handoff active 0, dormant 0
  Update sent 0, accepted 0, denied 0, not acked 0
  Initial Update sent 0, retransmissions 0
  Acknowledge received 0, discarded 0
  De-registration accepted 0, denied 0
 Handoff Update Errors:
  Unspecified 0, Identification mismatch 0
  Authentication failed 0, Administratively prohibited 0
  Poorly formed request 0

 RP Session Update statistics:
 Update sent 0, accepted 0, denied 0, not acked 0
 Initial Update sent 0, retransmissions 0
 Acknowledge received 0, discarded 0
 Sent reasons Always On 0, RN-PDIT 0, Subscriber Qos 0
 RP Session Update Errors:
  Unspecified 0, Identification mismatch 0
  Authentication failed 0, Session parameters not updated 0
  Poorly formed request 0
```

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

```
SAN-PDSN# show cdma pdsn statistics rp
Last clearing of "show cdma pdsn statistics rp" counters never
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new
RP Interface:
 Reg Request rcvd 0, accepted 0, denied 0, discarded 0
 Initial Reg Request rcvd 0, accepted 0, denied 0, discarded 0, AuxRequest 0
 Re-registration requests rcvd 0, accepted 0, denied 0, discarded 0
 Re-registration requests containing Active-Start 0, Active-Stop 0
 Re-registration requests containing new connections 0, missing connections 0, remapping
flows 0
 Handoff requests rcvd 0, accepted 0, denied 0, discarded 0,AuxRequest 0
 De-registration rcvd 0, accepted 0, denied 0, discarded 0
 De-registration Reg Request with Active-Stop 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
  Max Service Flows 0, Unsupported So 0, Non-Existent A10 0
  Bandwidth Unavailable 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

 Handoff statistics:
  Inter PCF handoff active 0, dormant 0
  Update sent 0, accepted 0, denied 0, not acked 0
  Initial Update sent 0, retransmissions 0
  Acknowledge received 0, discarded 0
  De-registration accepted 0, denied 0
 Handoff Update Errors:
  Unspecified 0, Identification mismatch 0
  Authentication failed 0, Administratively prohibited 0
  Poorly formed request 0

 RP Session Update statistics:
 Update sent 0, accepted 0, denied 0, not acked 0
 Initial Update sent 0, retransmissions 0
 Acknowledge received 0, discarded 0
 Sent reasons Always On 0, RN-PDIT 0, Subscriber Qos 0
 RP Session Update Errors:
  Unspecified 0, Identification mismatch 0
  Authentication failed 0, Session parameters not updated 0
  Poorly formed request 0
```

The following example shows the output for the **show cdma pdsn statistics rp error** command:

```
SAN-PDSN# show cdma pdsn statistics rp error
Last clearing of "show cdma pdsn statistics rp error" counters never
Last Update received at 00:12:54 UTC Mar 1 2009 ----------------------|-----> new
 RP Registration Request Error Reasons:
  Invalid Packet length 0, Protocol 0, Flags 0
  Invalid Connection ID 0, Authentication Key 0, SPI 0, Mismatch SPI 0
  Invalid Mobile ID 0, ID type 0, ID length 0
  Invalid Extension Order 0, VSE type 0, Vendor id 0
  Invalid Application type 0, Sub Application type 0
  Missing extension SSE 0, MHAE 0
  Duplicate Application type 0, GRE Key 0, CVSE 0
  Airlink Retransmission with same sequence number 0
  Airlink Invalid attribute length 0, sequence number 0, record 0
  Airlink Unknown attribute 0, Duplicate attribute 0
  Airlink Initial RRQ No Setup 0, Contains Stop 0, Contains SDB 0
  Airlink Start before Setup 0, Start in De-Registration 0
  Airlink GRE Key change no Setup 0, Rereceive Setup with same GRE Key 0
  Airlink Start rcvd during active 0, Stop rcvd during dormant 0
  De-Registration received for unknown session 0
  Re-Registration received during session disconnect 0
  Processing error due to memory failure 0

 RP Registration Update Ack Error Reasons:
  Invalid Packet length 0, Protocol 0
  Invalid Connection ID 0, Authentication Key 0, SPI 0
  Invalid Mobile ID 0, ID type 0, ID length 0
  Invalid Extension Order 0, VSE type 0
  Missing extension SSE 0, RUAE 0
  Received for unknown session 0, discard memory failure 0
 RP Session Update Ack Error Reasons:
  Invalid Packet length 0, Protocol 0
  Invalid Connection ID 0, Authentication Key 0, SPI 0
  Invalid Mobile ID 0, ID type 0, ID length 0
  Invalid Extension Order 0, VSE type 0
  Missing extension SSE 0, RUAE 0
  Received for unknown session 0, discard memory failure 0

 RP Registration Reply Error Reasons:
  Not sent memory allocation failure 0, Internal error 0
  Reply not sent to PCF security not found/parse error 0

 RP Registration Update Error Reasons:
  Not sent memory allocation failure 0, Internal error 0

 RP Session Update Error Reasons:
  Not sent memory allocation failure 0, Internal error 0

 Other Error Reasons:
  Maximum configured/limit number of session reached 0
```

The following example shows the output for the **show cdma pdsn statistics ppp pcf** command:

```
PDSN1_ACT# show cdma pdsn statistics ppp pcf
  PCF 2.2.2.4, Service Option 33
    Current Connections 0
    Connection requests 21, success 9, failure 10, aborted 2

    A10 release before LCP nego by PDSN 0, by PCF 0

    LCP Stage:
    Failure Reasons Options 0, MaxRetry 0, Unknown 0
    LCP Term Req during LCP nego rcvd 0
    A10 release during LCP nego by PCF 2

    Auth Stage:
    Auth failure 0, AAA Timeouts 0, Unknown 0
    Auth timeouts 0
    LCP Term Req during Auth nego rcvd 0
    A10 release during Auth nego by PCF 0

    IPCP Stage:
    Failure Reasons Options 0, MaxRetry 0, Unknown 9
    No enough IP resource for allocation 0
    LCP Term Req during IPCP nego rcvd 0
    A10 release during IPCP nego by PCF 0

    Renegotiation total 0, by PDSN 0, by Mobile Node 0
    Renegotiation success 0, failure 0, aborted 0
    Renegotiation reason: address mismatch 0, lower layer handoff 0
    GRE key change 0, other 0
```

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

```
SAN-PDSN# show cdma pdsn statistics tft
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new
RSVP:
 IEs Parsed 0
 TFTs Created Success 0, Failure 0
 TFTs Updated Success 0, Failure 0
 TFTs Deleted Success 0, Failure 0
 Other Failure 0
  Unknown 0, Unsupported Ie types 0
 Tft Ipv4 Failure Stats
```

```
  Tft Unauthorized 0, Unsuccessful Processing 0
  Tft Treatment Unsupported 0
  Packet Filter Add 0, Replace 0
  Packet Filter Precedence Contention 0, Unavailable 0
  Packet Filter Maximum Limit 0, Non-Existent Tft add 0
```

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

```
SAN-PDSN# show cdma pdsn statistics qos
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new

QOS:
  Total Profile Download Success 0, Failure 0
  Local Profile selected 0
  Failure Reason DSCP 0, Flow Profile ID 0,
  Service option profile 0, Others 0
  Total Consolidated Profile 0, DSCP Remarked 0
  Total policing installed 0, failure 0, removed 0
```

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

```
SAN-PDSN# show cdma pdsn statistics ahdlc
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new
slot 0:
  AHDLC Engine Type: CDMA HDLC SW ENGINE
     Engine is ENABLED
    total channels: 375000, available channels: 375000

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

  Deframing input 0 bytes, 0 paks
  Defaming output 0 bytes, 0 paks
  Deframing errors 0, insufficient memory 0, queue overflow 0
        Invalid size 0, CRC errors 0
SAN-PDSN#
```

The following example shows the output for the **show cdma pdsn statistics radius disconnect** command:

```
SAN-PDSN# show cdma pdsn statistics radius disconnect
Last Update received at 00:12:54 UTC Mar 1 2002

RADIUS DISCONNECT:
 Disconnect Request rcvd 0, accepted 0
 Disconnect Request Errors:
  Unsupported Attribute 0, Missing Attribute 0
  Invalid Request 0, NAS Id Mismatch 0
  Session Cxt Not Found 0, Administratively Prohibited 0

SAN-PDSN#
```

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

```
PDSN-ssp1-34-RP# show cdma pdsn statistics sm
PPC Stats:
Imsi Create Request to PPC Success 37552, Failure 0
Imsi Delete Request to PPC Success 24, Failure 0
Imsi Response from PPC Success 37551, Failure 0
CCB Create Request to PPC Success 35872, Failure 0
CCB Delete Request to PPC Success 0, Failure 0
CCB HA Create Request to PPC Success 0, Failure 0
CCB HA Delete Request to PPC Success 0, Failure 0
CCB Response from PPC Success 35872, Failure 0
IXP A10 Add Send Success 37552 Failure 0, Received Success 37552 Failure 0
IXP A10 Delete Send Success 24 Failure 0, Received Success 24 Failure 0
IXP CCB Add Send Success 35872 Failure 0, Received Success 35872 Failure 0
IXP CCB Delete Send Success 0 Failure 0, Received Success 0 Failure 0
IXP CCB HA Add Send Success 0 Failure 0, Received Success 0 Failure 0
IXP CCB HA Delete Send Success 0 Failure 0, Received Success 0 Failure 0
IXP Nack terminated session 0 flow 0
Ack timer expiry Imsi 0, Ccb 0

Tunnel PPC Stats:
Tunnel Create Request Rcvd 500, Sent Ack 500 Nack 0
Tunnel Delete Request Rcvd 0, Deleted 0
Invalid Tunnel Request Type Rcvd 0
```

Note The Remote Address Accounting statistics appear only if you have enabled RAA.

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

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.3(8)XW	Prepaid output was included in examples.

Examples

The following example shows how to enable the **show cdma pdsn statistics prepaid** command:

```
Router# show cdma pdsn statistics prepaid
Last Update received at 00:12:54 UTC Mar 1 2009 ---------------------|-----> new
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

Syntax Description

There are no keywords or variables for this command.

Command Modes

EXEC.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to enable the **show ip mobile cdma ipsec** command:

```
Router# show ip mobile cdma ipsec
```

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 keywords or variables for this command.

Command Modes

EXEC

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Usage Guidelines

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

Examples

The following example shows 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** EXEC command.

Note The **show ip mobile proxy registration** command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

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

Syntax Description

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

Command Modes

EXEC.

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.4(22)XR1	The CLID option is added.

Usage Guidelines

None.

Examples

The following example shows how to enable the **show ip mobile proxy host** command:

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

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

The following example shows how to enable the **show ip mobile proxy registration** command:

```
PDSN_ACTIVE# show ip mobile proxy registration

Proxy Mobile Node Registrations:
userpmip1@ispxyz.com:
    Registration accepted 07/02/09 15:01:00
    Next Re-registration 00:01:27
    Registration sequence number 2
    Care-of addr 4.1.1.1, HA addr 4.1.1.2, Home addr 12.1.1.11
    gre cvse enable
    FA provided key 1338165297, HA returned key 3436692080 -------------------|-----> new
    Flags sbdmG-T-, Identification CDF74A2C.365D4
    Lifetime requested 00:03:20 (200), granted 00:03:20, remaining 00:03:07
```

The following example shows the output for **show ip mobile proxy registration** command when CLID is enabled:

```
PDSN_SBY# show ip mob proxy registration

Proxy Mobile Node Registrations:

0312034920249:
    RRQ NAI:Sachin-PMIP@ark.com
    Registration accepted 10/13/09 07:21:04
    Next Re-registration 00:00:15
    Registration sequence number 0
    Care-of addr 6.1.1.8, HA addr 6.1.1.2, Home addr 9.1.1.2
    Flags sbdmg-t-, Identification CE7EA8E0.5A13E880
    Lifetime requested 00:01:00 (60), granted 00:01:00, remaining 00:00:45
```

show ip mobile secure

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

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show ip mobile secure {**home-agent** | **summary** | **visitor**}

Syntax Description

home-agent	Displays Home agent security associations.
summary	Displays a summary of all security associations.
visitor	Displays Mobile visitor security associations.

Command Modes

EXEC.

Command History

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

Usage Guidelines

Multiple security associations can exist for each entity.

Examples

The following example shows how to enable the **show ip mobile secure** command:

```
Router# show ip mobile secure summary

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

Table 8 describes the significant fields shown in the display.

Table 8 show ip mobile secure Field Descriptions

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

show ip mobile traffic

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

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show ip mobile traffic

Syntax Description

There are no keywords or variables for this command.

Command Modes

EXEC.

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable the **show ip mobile traffic** command:

```
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 102
    Advertisements sent 13758, response to solicitation 102
Foreign Agent Registrations:
    Register requests rcvd 8580, valid 7243, forwarded 7243, denied 1009, ignored 328
    Register requests valid initial 7242, re-register 0, de-register 1
    Register requests forwarded initial 7242, re-register 0, de-register 1
    Register requests denied initial 1009, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0,  de-register 0
    Register replies rcvd 7242, forwarded 7234, bad 0, ignored 8
    Register replies rcvd initial 7241, re-register 0, de-register 1
    Register replies forwarded initial 7233, re-register 0, de-register 1
    Registration Errors:
      Unspecified 1005, HA unreachable 0
      Administrative prohibited 0, No resource 0
      Bad lifetime 0, Bad request form 0
      Unavailable encapsulation 0, Compression 0
      Unavailable reverse tunnel 0, Reverse tunnel mandatory 0
      Authentication failed MN 4, HA 0
      Received challenge/gen. authentication extension, feature not enabled 0
      Unknown challenge 1001, Missing challenge 0, Stale challenge 4
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
```

show ip mobile violation

To display information about security violations, use the **show ip mobile violation** EXEC command.

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show ip mobile violation [*address* | **nai** *string*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC.

Command History

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

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. The oldest violations are 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 example shows how to enable 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 9 describes significant fields shown in the display.

Table 9 show ip mobile violation Field Descriptions

Field	Description
20.0.0.1	IP address of the violator.
Violations	Total number of security violations for this peer.

Table 9 show ip mobile violation Field Descriptions (continued)

Field	Description
Last time	Time of the most recent security violation for this peer.
SPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the Mobile-Home Authentication Extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply.
Reason	Reason for the most recent security violation for this peer. Possible reasons are: • No mobility security association • Bad authenticator • Bad identifier • Bad SPI • Missing security extension • Other

show ip mobile visitor

To display the table containing the visitor list of the foreign agent, use the **show ip mobile visitor** EXEC command.

Note This command, if executed on PCOP, does not aggregate the data or statistics. Instead, using the RCAL functionality, PCOP displays the information of each processor as output.

show ip mobile visitor [[**pending**] [*address* | **summary**| **brief**]] | [[**nai** *string* | **ha-addr** *address*][brief]]

Syntax Description

pending	(Optional) Displays the pending registration table.
address	(Optional) IP address.
summary	(Optional) Displays all values in the table.
nai *string*	(Optional) Network access identifier.
ha-addr *address*	(Optional) ha-ip-address.
brief	Displays information about all mobile ip visitors.

Command Modes

EXEC.

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.4(22)XR	The **brief** command was introduced.
12.4(22)XR1	The CLID option is introduced.

Usage Guidelines

The foreign agent updates the table containing the visitor list of the foreign agent in response to registration events from mobile nodes.

Examples

The following example shows how to enable the **show ip mobile visitor** command:

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
20.0.0.1:
    Interface Ethernet1/2, MAC addr 0060.837b.95ec
    IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
    HA addr 66.0.0.5, Identification B7510E60.64436B38
    Lifetime 08:20:00 (30000) Remaining 08:19:16
    Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
    gre cvse enable
    FA provided key 771596863, HA returned key 3746886318 --------------|-----> new
    Routing Options - (T)Reverse-tunnel
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip mobile visitor Field Descriptions

Field	Description
Total	1
IP address	Home IP address of a visitor.
Interface	Name of the interface.
MAC addr	MAC address of the visitor.
IP src	Source IP address the Registration Request of a visitor.
IP dest	Destination IP address of Registration Request of a visitor. When a foreign agent sends a reply to a visitor, the IP source address is set to this address, unless it is multicast or broadcast, in which case it is set to IP address of the output interface.
UDP src port	Source UDP port of Registration Request of the visitor.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime granted to the mobile node for this registration.
Remaining	The number of seconds remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE is be displayed in the Routing Options field.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Possible options are: • (S) Mult-binding • (B) Broadcast • (D) Direct-to-mobile station • (M) MinIP • (G) GRE • (V) VJH-compress • (T) Reverse-tunnel

The following example shows the output for the **show ip mobile visitor** command when CLID is enabled:

```
PDSN_SBY# show ip mobile visitor
Mobile Visitor List:
Total 1
03120983424:
    Home addr 9.1.1.1 RRQNAI:mip-sachin11@ark.com
    Interface Virtual-Access2.1, MAC addr 0000.0000.0000
    IP src 0.0.0.0, dest 6.1.1.8, UDP src port 434
    HA addr 6.1.1.2, Identification CE7EA193.10000
    Lifetime 00:10:00 (600) Remaining 00:09:47
    Tunnel0 src 6.1.1.8, dest 6.1.1.2, reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse Tunneling
```

The following example shows the output for the **show ip mobile visitor ha-addr** command:

```
pdsn# show ip mobile visitor ha-addr 5.5.5.2 brief
Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
    Home addr 9.9.9.2
    MAC addr 0000.0000.0000
    HA addr 5.5.5.2
    Lifetime 00:10:00 (600) Remaining 00:04:07
pdsn#

PDSN_ACT# show ip mobile visitor ha-addr 6.6.6.2
Mobile Visitor List:
Total 1
arkumar11@ark.com:
    Home addr 9.9.9.2
    Interface Virtual-Access2.1, MAC addr 0000.0000.0000
    IP src 0.0.0.0, dest 6.6.6.1, UDP src port 434
    HA addr 6.6.6.2, Identification CD6C5449.10000
    Lifetime INFINITE
    Tunnel0 src 6.6.6.1, dest 6.6.6.2, reverse-allowed
    Routing Options -
PDSN_ACT#
```

The following example shows the output for the **show ip mobile visitor brief** command:

```
pdsn# show ip mobile visitor brief
Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
    Home addr 9.9.9.2
    MAC addr 0000.0000.0000
    HA addr 5.5.5.2
    Lifetime 00:10:00 (600) Remaining 00:04:07
pdsn#
```

show ipc sctp statistics

To display ipc sctp statistics, use the **show ipc sctp statistics** command.

show ipc sctp statistics

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to enable 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#
```

show policy-map apn realm

To display the statistics of the flow-based marking for a particular NAI, use the **show policy-map apn realm command** in privileged EXEC mode**.**

show policy-map apn realm [nai]

Syntax Description

nai	Displays the statistics of the flow based marking for a particular nai.

Defaults

There are no keywords or variables for this command.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show policy-map apn realm [nai]** command:

```
ACTIVE_PDSN# show policy-map apn realm mipuser1
MSID            NAI                            Type         MN IP Address    St  HA
IP05363805481     mipuser1                       Mobile       9.9.9.11         ACT 6.6.6.2
  Service-policy input: sdb-in
    Class-map: sdb (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp af11
          Packets marked 0
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
  Service-policy output: sdb-out
    Class-map: sdb (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp af11
          Packets marked 0
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
```

show redundancy history

To display the Redundancy Facility (RF) history, use the **show redundancy history** command in privileged EXEC mode**.**

show redundancy history

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show redundancy history** command:

```
PDSN_STDBY# sh redundancy history
10 client added: RF_INTERNAL_MSG(0) seq=0
10 client added: RF_LAST_CLIENT(65000) seq=351
10 client added: CHKPT RF(25) seq=69
94 client added: Bouncer Config Sync client(5) seq=137
96 client added: DHCPD(101) seq=178
96 client added: DHCPC(100) seq=177
96 client added: History RF Client(35) seq=199
97 client added: SNMP RF Client(34) seq=190
105 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
105 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) CHKPT RF(25) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) Bouncer Config Sync client(5) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) DHCPC(100) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) DHCPD(101) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) SNMP RF Client(34) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) History RF Client(35) op=0 rc=11
105 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) op=0 rc=11
105 *my state = NEGOTIATION(3) peer state = DISABLED(1)
2968 client added: SingleIP RF(121) seq=180
2976 client added: IPRM(76) seq=229
2978 client added: CCM RF(82) seq=198
3228 client added: FH_RF_Event_Detector_stub(50) seq=237
3379 RF_STATUS_PEER_PRESENCE(400) op=0 rc=0
3379 RF_STATUS_PEER_COMM(401) op=0 rc=0
3500 Configuration parsing complete
4884 RF_STATUS_PEER_PRESENCE(400) op=0 rc=0
4884 RF_STATUS_PEER_COMM(401) op=0 rc=0
5964 System initialization complete
6160 RF_STATUS_PEER_PRESENCE(400) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=1 rc=0
```

```
6160 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=1 rc=0
6160 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) DHCPC(100) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) DHCPD(101) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) CCM RF(82) op=1 rc=0
6160 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=1 rc=0
6160 *my state = NEGOTIATION(3) *peer state = UNKNOWN(0)
6160 *my state = NEGOTIATION(3) *peer state = ACTIVE(13)
6160 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=100 rc=0
6160 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=100 rc=0
6160 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=100 rc=0
8790 RF_EVENT_GO_STANDBY(513) op=0 rc=0
8790 *my state = STANDBY COLD(4) peer state = ACTIVE(13)
8790 RF_PROG_STANDBY_COLD(101) RF_INTERNAL_MSG(0) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) CHKPT RF(25) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) Bouncer Config Sync client(5) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) DHCPC(100) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) DHCPD(101) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) SingleIP RF(121) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) SNMP RF Client(34) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) CCM RF(82) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) History RF Client(35) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) IPRM(76) op=0 rc=11
8790 RF_PROG_STANDBY_COLD(101) FH_RF_Event_Detector_stub(50) op=0 rc=11
8790 RF_EVENT_START_PROGRESSION(501) RF_INTERNAL_MSG(0) op=0 rc=0
8790 RF_PROG_STANDBY_COLD(101) RF_LAST_CLIENT(65000) op=0 rc=11
8792 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=5 rc=0
8792 *my state = STANDBY COLD-CONFIG(5) peer state = ACTIVE(13)
8792 RF_EVENT_CLIENT_PROGRESSION(503) Bouncer Config Sync client(5) op=5 rc=0
8792 RF_EVENT_CLIENT_PROGRESSION(503) Bouncer Config Sync client(5) op=5 rc=11
8797 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=6 rc=0
8797 *my state = STANDBY COLD-FILESYS(6) peer state = ACTIVE(13)
8797 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=7 rc=0
8797 *my state = STANDBY COLD-BULK(7) peer state = ACTIVE(13)
8797 RF_EVENT_CLIENT_PROGRESSION(503) DHCPC(100) op=7 rc=0
8797 RF_EVENT_CLIENT_PROGRESSION(503) DHCPC(100) op=7 rc=11
8797 RF_EVENT_CLIENT_PROGRESSION(503) DHCPD(101) op=7 rc=0
8797 RF_EVENT_CLIENT_PROGRESSION(503) DHCPD(101) op=7 rc=11
8797 RF_EVENT_CLIENT_PROGRESSION(503) CCM RF(82) op=7 rc=0
8797 RF_EVENT_CLIENT_PROGRESSION(503) CCM RF(82) op=7 rc=11
8797 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=8 rc=0
8797 *my state = STANDBY HOT(8) peer state = ACTIVE(13)
8797 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=8 rc=0
8797 RF_PROG_STANDBY_HOT(105) RF_LAST_CLIENT(65000) op=8 rc=0
8797 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=8 rc=0
Jul  9 11:52:19.556 Changing to system clock timestamps at uptime 314840
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul  9 11:52:19.556 *my state = STANDBY HOT(8) *peer state = DISABLED(1)
Jul  9 11:52:19.556 Reloading peer (peer presence lost)
Jul  9 11:52:19.556 *my state = ACTIVE-FAST(9) peer state = DISABLED(1)
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) CHKPT RF(25) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) Bouncer Config Sync client(5) op=0
rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) DHCPC(100) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) DHCPD(101) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) SNMP RF Client(34) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) CCM RF(82) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_MAINTENANCE_ENABLE(403) FH_RF_Event_Detector_stub(50) op=0
rc=0
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) RF_INTERNAL_MSG(0) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) CHKPT RF(25) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) Bouncer Config Sync client(5) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) DHCPC(100) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) DHCPD(101) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) SingleIP RF(121) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) SNMP RF Client(34) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) CCM RF(82) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) History RF Client(35) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) IPRM(76) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_FAST(200) RF_LAST_CLIENT(65000) op=0 rc=11
Jul  9 11:52:19.556 *my state = ACTIVE-DRAIN(10) peer state = DISABLED(1)
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) RF_INTERNAL_MSG(0) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) CHKPT RF(25) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) Bouncer Config Sync client(5) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) DHCPC(100) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) DHCPD(101) op=0 rc=11
Jul  9 11:52:19.556 RF_PROG_ACTIVE_DRAIN(201) SingleIP RF(121) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) DHCPC(100) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) DHCPD(101) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) CCM RF(82) op=0 rc=0
Jul  9 11:52:19.556 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul  9 11:52:19.556 Reloading peer (communication down)
Jul  9 11:52:19.556 RF_EVENT_GO_ACTIVE(512) op=0 rc=0
Jul  9 11:52:27.556 RF_EVENT_LOCAL_PROG_DONE(505) SingleIP RF(121) op=201 rc=0
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) SNMP RF Client(34) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) CCM RF(82) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) History RF Client(35) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) IPRM(76) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_DRAIN(201) RF_LAST_CLIENT(65000) op=0 rc=11
Jul  9 11:52:27.556 *my state = ACTIVE_PRECONFIG(11) peer state = DISABLED(1)
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) RF_INTERNAL_MSG(0) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) CHKPT RF(25) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) Bouncer Config Sync client(5) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) DHCPC(100) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) DHCPD(101) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) SingleIP RF(121) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) SNMP RF Client(34) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) CCM RF(82) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) History RF Client(35) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) IPRM(76) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_PRECONFIG(202) RF_LAST_CLIENT(65000) op=0 rc=11
Jul  9 11:52:27.556 *my state = ACTIVE_POSTCONFIG(12) peer state = DISABLED(1)
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) RF_INTERNAL_MSG(0) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) CHKPT RF(25) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) Bouncer Config Sync client(5) op=0
rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) DHCPC(100) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) DHCPD(101) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) SingleIP RF(121) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) SNMP RF Client(34) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) CCM RF(82) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) History RF Client(35) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) IPRM(76) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) FH_RF_Event_Detector_stub(50) op=0 
rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE_POSTCONFIG(203) RF_LAST_CLIENT(65000) op=0 rc=11
Jul  9 11:52:27.556 *my state = ACTIVE(13) peer state = DISABLED(1)
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) RF_INTERNAL_MSG(0) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) CHKPT RF(25) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) Bouncer Config Sync client(5) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) DHCPC(100) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) DHCPD(101) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) SingleIP RF(121) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) SNMP RF Client(34) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) CCM RF(82) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) History RF Client(35) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) IPRM(76) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul  9 11:52:27.556 RF_PROG_ACTIVE(204) RF_LAST_CLIENT(65000) op=0 rc=11
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) DHCPC(100) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) DHCPD(101) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) CCM RF(82) op=1 rc=0
Jul 10 04:38:35.038 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=1 rc=0
Jul 10 04:38:35.038 *my state = ACTIVE(13) *peer state = UNKNOWN(0)
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(0) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) CHKPT RF(25) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) Bouncer Config Sync client(5) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) DHCPC(100) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) DHCPD(101) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) SingleIP RF(121) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) SNMP RF Client(34) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) CCM RF(82) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) History RF Client(35) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) IPRM(76) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul 10 04:38:35.038 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=0 rc=0
Jul 10 04:38:35.038 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=100 rc=0
Jul 10 04:38:35.038 *my state = ACTIVE(13) *peer state = NEGOTIATION(3)
Jul 10 04:38:35.042 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=300 rc=0
Jul 10 04:39:03.426 RF_EVENT_START_PROGRESSION(501) op=0 rc=0
Jul 10 04:39:03.438 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=5 rc=0
Jul 10 04:39:03.438 RF_PROG_STANDBY_CONFIG(102) RF_INTERNAL_MSG(0) op=0 rc=11
Jul 10 04:39:03.438 RF_PROG_STANDBY_CONFIG(102) CHKPT RF(25) op=0 rc=11
Jul 10 04:39:03.438 RF_PROG_STANDBY_CONFIG(102) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:39:03.438 RF_EVENT_CLIENT_PROGRESSION(503) Bouncer Config Sync client(5) op=5 
rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul 10 04:39:22.537 *my state = ACTIVE(13) *peer state = DISABLED(1)
Jul 10 04:39:22.537 Reloading peer (peer presence lost)
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) DHCPC(100) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) DHCPD(101) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) CCM RF(82) op=0 rc=0
Jul 10 04:39:22.537 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul 10 04:39:22.537 Reloading peer (communication down)
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) DHCPC(100) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) DHCPD(101) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) CCM RF(82) op=1 rc=0
Jul 10 04:48:50.264 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=1 rc=0
Jul 10 04:48:50.264 *my state = ACTIVE(13) *peer state = UNKNOWN(0)
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) RF_INTERNAL_MSG(0) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) CHKPT RF(25) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) Bouncer Config Sync client(5) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) DHCPC(100) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) DHCPD(101) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) SingleIP RF(121) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) SNMP RF Client(34) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) CCM RF(82) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) History RF Client(35) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) IPRM(76) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) FH_RF_Event_Detector_stub(50) op=0 rc=11
Jul 10 04:48:50.264 RF_PROG_PLATFORM_SYNC(300) RF_LAST_CLIENT(65000) op=0 rc=0
Jul 10 04:48:50.264 RF_EVENT_CLIENT_PROGRESSION(503) RF_LAST_CLIENT(65000) op=100 rc=0
Jul 10 04:48:50.264 *my state = ACTIVE(13) *peer state = NEGOTIATION(3)
Jul 10 04:48:50.264 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=300 rc=0
Jul 10 04:49:17.132 RF_EVENT_START_PROGRESSION(501) op=0 rc=0
Jul 10 04:49:17.144 RF_EVENT_STANDBY_PROGRESSION(502) RF_INTERNAL_MSG(0) op=5 rc=0
Jul 10 04:49:17.144 RF_PROG_STANDBY_CONFIG(102) RF_INTERNAL_MSG(0) op=0 rc=11
Jul 10 04:49:17.144 RF_PROG_STANDBY_CONFIG(102) CHKPT RF(25) op=0 rc=11
Jul 10 04:49:17.144 RF_PROG_STANDBY_CONFIG(102) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:49:17.144 RF_EVENT_CLIENT_PROGRESSION(503) Bouncer Config Sync client(5) op=5
rc=0
Jul 10 04:49:22.456 *my state = ACTIVE(13) *peer state = STANDBY COLD-CONFIG(5)
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) CHKPT RF(25) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) DHCPC(100) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) DHCPD(101) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) SNMP RF Client(34) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) CCM RF(82) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_PRESENCE(400) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul 10 04:49:37.492 *my state = ACTIVE(13) *peer state = DISABLED(1)
Jul 10 04:49:37.492 Reloading peer (peer presence lost)
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) CHKPT RF(25) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) Bouncer Config Sync client(5) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) DHCPC(100) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) DHCPD(101) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) SNMP RF Client(34) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) CCM RF(82) op=0 rc=0
Jul 10 04:49:37.492 RF_STATUS_PEER_COMM(401) FH_RF_Event_Detector_stub(50) op=0 rc=0
Jul 10 04:49:37.492 Reloading peer (communication down)
PDSN_STDBY#
```

show redundancy inter-device

To display redundancy inter-device operational state and statistics, use the **show redundancy inter-device** command.

show redundancy inter-device

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.3(8)XW	This command was introduced.

Examples

The following example shows how to enable the **show redundancy inter-device** command:

```
Redundancy inter-device state: RF_INTERDEV_STATE_ACT
  Scheme: standby
      Groupname: SB Group State: Active
  Peer present: RF_INTERDEV_PEER_NOT_PRESENT
```

show redundancy states

To display the redundancy states, use the **show redundancy states** command in privileged EXEC mode**.**

show redundancy states

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show redundancy states** command:

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
        Unit ID = 0
Maintenance Mode = Disabled
   Manual Swact = Enabled
 Communications = Up
   client count = 9
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

show sami standby

To display the SAMI Standby HSRP-Relay information, use the **show sami standby** command in privileged EXEC mode**.**

show sami standby

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show sami standby** command:

```
PDSN_STDBY# sh sami standby
HSRP-Relay Group : PDSN-SCDMA,  State : Active
HSRP-State Relay Statistics:
PROC#4  Tx Success:4            Tx Errors:0
PROC#5  Tx Success:4            Tx Errors:0
PROC#6  Tx Success:4            Tx Errors:0
PROC#7  Tx Success:4            Tx Errors:0
PROC#8  Tx Success:4            Tx Errors:0
PCOP ACTIVE_DRAIN Wait Time : 10
PROC#4  ACT-DRAIN Info Rx :1
PROC#5  ACT-DRAIN Info Rx :1
PROC#6  ACT-DRAIN Info Rx :1
PROC#7  ACT-DRAIN Info Rx :1
PROC#8  ACT-DRAIN Info Rx :1
PDSN_STDBY#
```

show standby

To display the Hot Standby Router Protocol (HSRP) information, use the **show standby** command in privileged EXEC mode**.**

show standby

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Examples

The following example shows how to enable the **show standby** command:

```
PDSN_STDBY# show  standby ?
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  all              Include groups in disabled state
  brief            Brief output
  capability       HSRP capability
  delay            Group initialisation delay
  internal         Internal HSRP information
  neighbors        HSRP neighbors
  redirect         HSRP ICMP redirect information
  |                Output modifiers
  <cr>
PDSN_STDBY#

Router# show standby
Ethernet0/0 - Group 10
  State is Active
    2 state changes, last state change 6d05h
  Virtual IP address is 10.1.1.20
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.080 secs
  Preemption disabled
  Active router is local
  Standby router is 10.1.1.1, priority 100 (expires in 8.976 sec)
  Priority 100 (default 100)
  Group name is "test-group" (cfgd)
```

show tech-support cdma pdsn

To display PDSN information that is useful to Cisco Customer Engineers for diagnosing problems, use the **show tech-support cdma pdsn** command in privileged EXEC mode.

show tech support cdma pdsn

Syntax Description

There are no keywords or variables for this command.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.1(3)XS	This command was modified to include PDSN status.

Usage Guidelines

This command displays the output of several **show** commands. We recommend that you attach the output of this command whenever you submit a PDSN problem report.

Examples

The following example shows how to enable the **show tech-support cdma pdsn** command:

```
pdsn-6500# show tech-support cdma pdsn

------------------ show version ------------------

Cisco Internetwork Operating System Software
IOS (tm) 6500 Software (C6500-C5IS-M), Experimental Version 12.2(20020306:074931)
[user-dw91527 104]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 06-Mar-02 22:21 by user
Image text-base:0x600088E0, data-base:0x6169A000

ROM:System Bootstrap, Version 12.0(19990210:195103) [12.0XE 105], DEVELOPMENT SOFTWARE
BOOTLDR:6500 Software (C6500-BOOT-M), Version 12.0(3)T,  RELEASE SOFTWARE (fc1)

mwt10-7206a uptime is 20 minutes
System returned to ROM by reload at 23:17:59 UTC Wed Mar 6 2002
System image file is "tftp://223.255.254.254/user/c6500-c5is-mz.dw91527"

cisco 7206VXR (NPE300) processor (revision D) with 229376K/65536K bytes of memory.
Processor board ID 21302179
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.1

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
```

```
8 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
125K bytes of non-volatile configuration memory.

8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0


------------------ show running-config ------------------


Building configuration...

Current configuration :3015 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
!
hostname mwt10-7206a
!
aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default group radius
aaa authentication ppp VPDN group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network VPDN group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 10
aaa accounting network pdsn start-stop group radius
aaa session-id common
enable secret 5 <removed>
enable password <removed>
!
username abc password 0 <removed>
ip subnet-zero
no ip gratuitous-arps
ip cef
ip cef accounting per-prefix non-recursive prefix-length
!
!
!
ip ftp source-interface Ethernet2/0
no ip domain-lookup
!
vpdn enable
vpdn authen-before-forward
virtual-profile aaa
!
!
!
!
```

```
!
!
!
interface Loopback0
 ip address 6.0.0.1 255.0.0.0
!
interface CDMA-Ix1
 ip address 5.0.0.1 255.0.0.0
 tunnel source 5.0.0.1
 tunnel key 0
 tunnel sequence-datagrams
!
interface FastEthernet1/0
 ip address 4.0.0.101 255.0.0.0
 duplex half
 speed auto
 no cdp enable
!
interface Ethernet2/0
 ip address 7.0.0.1 255.0.0.0
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 150.1.10.4 255.255.0.0
 duplex half
 no cdp enable
!
interface Ethernet2/2
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/4
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/5
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/6
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/7
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface ATM4/0
 no ip address
 no ip mroute-cache
 shutdown
 no atm ilmi-keepalive
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip mobile foreign-service challenge
 ip mobile foreign-service reverse-tunnel
 ip mobile registration-lifetime 65535
 no peer default ip address
 ppp authentication chap pap optional
!
Router mobile
!
ip local pool ispabc-pool1 9.0.0.1 9.0.0.255
ip classless
ip route 10.0.0.0 255.0.0.0 7.0.0.2
no ip http server
ip pim bidir-enable
ip mobile foreign-agent care-of Ethernet2/0
ip mobile proxy-host nai mwts-mipp-np-user1@ispxyz.com flags 42
!
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
!
!
radius-server host 150.1.0.1 auth-port 1645 acct-port 1646 key <removed>
radius-server retransmit 3
radius-server optional-passwords
radius-server key <removed>
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdlc-engine 5 usable-channels 8000
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn msid-authentication
cdma pdsn selection interface Ethernet2/0
cdma pdsn secure pcf default spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 1000 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
```

```
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password <removed>
!
!
end


------------------ show cdma pdsn ------------------


PDSN software version 1.2, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 300 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCFs limit not set, maximum sessions limit not set
  SNMP failure history table size 100
  MSID Authentication is enabled
      Network code digits for IMSI 5, MIN 6, IRM 4
      Profile Password is cisco
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is disabled
  Aging of idle users disabled

  Number of pcfs connected 1
  Number of sessions connected 1,
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 1


------------------ show ip interface brief ------------------


Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet1/0            4.0.0.101       YES NVRAM  up                    up
Ethernet2/0                7.0.0.1         YES manual up                    up
Ethernet2/1                150.1.10.4      YES NVRAM  up                    up
Ethernet2/2                unassigned      YES NVRAM  administratively down down
Ethernet2/3                unassigned      YES NVRAM  administratively down down
Ethernet2/4                unassigned      YES NVRAM  administratively down down
Ethernet2/5                unassigned      YES NVRAM  administratively down down
Ethernet2/6                unassigned      YES NVRAM  administratively down down
Ethernet2/7                unassigned      YES NVRAM  administratively down down
ATM4/0                     unassigned      YES NVRAM  administratively down down
Loopback0                  6.0.0.1         YES NVRAM  up                    up
CDMA-Ix1                   5.0.0.1         YES NVRAM  up                    up
Virtual-Template1          6.0.0.1         YES unset  down                  down
Virtual-Access1            unassigned      YES unset  up                    up
Mobile0                    unassigned      YES unset  up                    up
Tunnel0                    unassigned      YES unset  up                    up
Tunnel1                    7.0.0.1         YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
Virtual-Access3            unassigned      YES unset  up                    up
```

```
Virtual-Access3.1          6.0.0.1         YES unset  up                    up

------------------ show ip route ------------------


Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    4.0.0.0/8 is directly connected, FastEthernet1/0
C    5.0.0.0/8 is directly connected, CDMA-Ix1
C    6.0.0.0/8 is directly connected, Loopback0
C    7.0.0.0/8 is directly connected, Ethernet2/0
S    10.0.0.0/8 [1/0] via 7.0.0.2
C    150.1.0.0/16 is directly connected, Ethernet2/1
     30.0.0.0/32 is subnetted, 1 subnets
C       30.0.0.1 is directly connected, Virtual-Access3.1

------------------ show cdma pdsn session brief ------------------

MSID            PCF IP Address          PSI      Age  St Flows Interface
11122000050031  4.0.0.1                   1 00:19:57 ACT     1 Virtual-Access3.1


------------------ show cdma pdsn session ------------------


Mobile Station ID IMSI 11122000050031
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:19:57,  registration lifetime 1800 sec
  Number of A11 re-registrations 1, time since last registration 1193 sec
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE sequence number transmit 12, receive 12
  Using interface Virtual-Access3.1, status ACT
  Using AHDLC engine on slot 5, channel ID 0
  This session has 1 flow

  Flow service Proxy-Mobile, NAI mwts-mipp-np-user1@ispxyz.com
    Mobile Node IP address 30.0.0.1
    Home Agent IP address 7.0.0.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0


------------------ show cdma pdsn pcf brief ------------------

PCF IP Address     Sessions      Pkts In     Pkts Out     Bytes In    Bytes Out
4.0.0.1                   1            0           12            0          396


------------------ show cdma pdsn pcf ------------------


PCF 4.0.0.1 has 1 session
  Received 0 pkts (0 bytes), sent 12 pkts (396 bytes)

  PCF Session ID 1, Mobile Station ID IMSI 11122000050031
```

```
    A10 connection age 00:19:58
    A10 registration lifetime 1800 sec, time since last registration 1194 sec



------------------ show cdma pdsn selection summary ------------------


CDMA PDSN selection summary:
    Hostname         PDSN             Session-count  Max-sessions
   *mwt10-7206a      5.0.0.1              1              8000
    mwt10-7206b      12.0.0.1             0              8000

    Hostname         Keepalive    Interface       Load-factor
   *mwt10-7206a          30       7.0.0.1            0.00
    mwt10-7206b          30       7.0.0.2            0.00

------------------ show ip mobile traffic ------------------

IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0 , Dropped 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0, active HA 0
    Bad identification 0, Bad request form 0
    Unavailable encap 0, reverse tunnel 0
    Reverse tunnel mandatory 0
    Binding Updates received 0, sent 0 total 0 fail 0
    Binding Update acks received 0 sent 0
    Binding info requests received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Reverse tunnel mandatory 0
    Replies in 1
    Forwarded 0, Bad 0, Ignored 1
    Authentication failed MN 0, HA 0
    Received challenge/gen. authentication extension, feature not enabled 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Unknown challenge 0, Missing challenge 0, Stale challenge 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
```

```
------------------ show ip mobile globals ------------------

IP Mobility global information:
Home Agent is not enabled

Foreign Agent

    Pending registrations expire after 15 secs
    Care-of addresses advertised
        Ethernet2/0 (7.0.0.1) - up

0 interfaces providing service
Encapsulations supported:IPIP and GRE
Tunnel fast switching enabled
Tunnel path MTU discovery aged out after 10 min

------------------ show ip mobile interface ------------------

IP Mobility interface information:

------------------ show vpdn tunnel ------------------



------------------ show cdma pdsn resource ------------------


Resource allocated/available in the resource manager

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

snmp-server enable traps cdma

To enable network management traps for CDMA, use the **snmp-server enable traps cdma** command in global configuration mode. To disable network management traps for CDMA, use the **no** form of this command.

snmp-server enable traps cdma

no snmp-server enable traps cdma

Syntax Description

There are no keywords or variables for this command.

Defaults

Network management traps disabled.

Command Modes

Global Configuration.

Command History

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

Examples

The following example shows how to enable network management traps for CDMA:

```
snmp-server enable traps cdma
```

snmp-server enable traps ipmobile

To configure Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the no form of this command.

snmp-server enable traps ipmobile

no snmp-server enable traps ipmobile

Syntax Description

There are no keywords or variables for this command.

Defaults

SNMP notifications are disabled.

Command Modes

Global Configuration.

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at

http://tools.cisco.com/ITDIT/MIBS/servlet/index

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 shows how to enable 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
```

subscriber redundancy rate

To configure the Cluster Control Manager to sync the number_sessions calls to the standby at a configuring interval, use the **subscriber redundancy rate** command in global configuration mode. The periodic rate is applicable for both dynamic and bulk sync. Use the **no** form of the command to disable this feature.

subscriber redundancy rate [**number_sessions**] [**number_period**]

no subscriber redundancy rate

Syntax Description

Command	Description
number_sessions	Specifies the number of calls synched to the standbv.
number_period	Specifies the number in seconds between synch attempts.

Defaults

No default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(14)YX6	This command was introduced to the PDSN image.

Usage Guidelines

Note You should only configure this command with the following values:

subscriber redundancy rate 500 1

Examples

The following example shows how to enable the **subscriber redundancy rate** command:

```
Router(config)# subscriber redundancy rate 500 1
```

tft-allowed (service flows qos subscriber profile sub-mode)

To configure allowed number of persistent TFTs parameter, use the **tft-allowed** command in service flows qos subscriber profile sub-mode. Use the **no** form of the command to disable this feature.

tft-allowed *value*

no tft-allowed *value*

Syntax Description

value	The allowed number of persistent TFTs. The valid range is 1-255.

Defaults

No default values.

Command Modes

Service flows qos subscriber profile sub-mode.

Command History

Release	Modification
12.4(15)hxx	This command was introduced.

Examples

The following example shows how to enable the **tft-allowed** command:

```
Router#(config-qos-profile)# tft-allowed ?
  <1-255>  Value

Router#(config-qos-profile)# tft-allowed 22 ?
```

vpdn debug show-conditions

When username or IMSI conditional debugging is enabled for a VPDN session, use the **vpdn debug show-conditions** command to show the condition as part of L2TP and VPDN call event debugs. Use the **no** form of the command to disable this feature.

vpdn debug show-conditions

no vpdn debug show-conditions

Syntax Description

There are no keywords or variables for this command.

Defaults

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(22)XR1	This command is introduced.

Examples

The following example shows how to enable the **vpdn debug show-conditions** command:

```
Lac(config)# vpdn debug ?
  show-conditions  Show Conditions (IMSI/Username) with debug messages

Lac(config)# vpdn debug show-conditions ?
<cr>

Lac# show debugging
VPN:
  VPDN call event debugging is on
```

Osler Commands

The Operator Interface for Multiple Service blades for the Single IP PDSN is introduced in this release to provide a single Operations, Administration, and Maintenance (OAM) viewpoint for a defined set of functions. Using this interface, the operator can view the entire chassis as a black box without having to independently deal with multiple service blades containing multiple processors, and active and standby configurations. By using this interface, you can reduce dependencies on customer OAM deployments and provide real-time diagnostics for quick and proactive problem resolution. It also helps in ongoing verification of dimensioning parameters, such as network predictability, and repair and recovery based on problem identification.

The interface covers four commands:

- show subscriber, page 316
- monitor subscriber, page 334
- show subscriber session, page 343
- bulk statistics collection, page 346

show subscriber

To query the subscriber on the Osler interface, use **show subscriber command.** Multiple CLI commands are executed on the processors that run the active PDSN instances to query the subscriber, for a match based on one or more conditions.

show subscriber {**summary** | **brief** | **verbose**} [**all** | **card** *value* | **cpu** *separated SAMI card, cpu ID* | **age** {**greater** | **lesser** | **equals**} *time in hh:mm:ss* | **fa-chassis** | **fa-member** | **ha-user** *ip address* | **address space** *ip address range* | **calltype** *service-option* | **user** *nai*]

Syntax Description

summary	Displays the total number of subscribers that match the display policy.
brief	Displays the information, in the one-line-of-output-per-subscriber format, for each subscriber matching the display policy.
verbose	Displays the information, in the multiple-lines-of-output-per-subscriber format, for each subscriber matching the display policy.
all	Displays the summary of all sessions of users on the chassis.
card	Displays the summary of all user sessions on a particular card or slot or blade.
cpu	Displays the summary of all CPU users.
age	Displays the summary of all users with a Connect Time that is greater then, less than, or equal to a time value.
fa-chassis	Displays the summary of all visitors on FAs within the PDSN.
fa-member	Displays the summary of all FA users specific within the PDSN.
ha-user	Displays the summary of all users registered with a particular Home Agent.
address space	Displays the summary of all users in the specified address space.
calltype	Displays the summary of all users for a specified Call Type.
user	Displays the summary of all users for a specified NAI.

Defaults

No default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

The display options can be used in the command to filter the subscriber details.

Examples

The examples below show how to enable the **show subscriber summary** command for the following CLIs used on processors:

- **show ip mobile visitor summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):    1

SHOW SUBSCRIBER SUMMARY <-> (FA-Chasis Visitors)
-------------------------------
FA-Chasis visitors List:
Total 1
```

- **execute-on** *slot PPC3* **show ip mobile visitor summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11): 2
>> Now enter the Card number for FA-Member visitors:1
SHOW SUBSCRIBER SUMMARY <-> (FA-Member Visitors: 1)
-------------------------------
FA-Member Visitors List:
Total 1
```

- **show ip mobile visitor ha-addr** *ha-ip* **brief**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   3
>> Now enter the HA-User address (Home Agent IP) :5.5.5.2
```

```
SHOW SUBSCRIBER SUMMARY <-> (HA-User IP: 5.5.5.2)
-------------------------------
HA User Subscriber List:
Total 1
```

- **show cdma pdsn flow mn-ip-address range** *startIP*, *endIP* **summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   4
>> Now enter the ',' separated starting IP address & end IP address(e.g.
10.114.200.49,10.114.200.180) :
9.9.9.1,9.9.9.10

SHOW SUBSCRIBER SUMMARY <-> (Subscriber in address range: 9.9.9.1 9.9.9.10)
-------------------------------
Number of flows having mn-ip-adress between 9.9.9.1 9.9.9.10 : 1
Total Number of Paks in :0
Total Number of Paks out :0
Total Number of bytes in :0
Total Number of bytes out :0
```

- **show cdma pdsn session service-option** *service-option* **summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   5
Select Service Type:
1.   EVDO
2.   1xRTT
3.   Quit
Enter the your service Type choice from the above menu (1/2/3):1

SHOW SUBSCRIBER SUMMARY <-> With CallType Option 59
-------------------------------
Total Number of sessions with service option 59:3
Total Number of Paks in :14
Total Number of Paks out :40
Total Number of bytes in :906
Total Number of bytes out :1915
```

- **show cdma pdsn session lifetime age** *lesser* | *greater* | *equals hh:mm:ss* **summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   6
>> Now enter the lifetime (hh:mm:ss format): 0:20:3
>> Enter the valuetype for Lifetime Record(e.g: greater|lesser|equals): lesser
SHOW SUBSCRIBER SUMMARY <-> (With specified lifetime: 0:20:3)
-------------------------------
Total  Number of sessions with lifetime lesser than the give time :3
Total  Number of Paks in :16
Total  Number of Paks out :42
Total  Number of bytes in :922
Total  Number of bytes out :1949
```

- **show cdma pdsn session user** *patt** **summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   7
>> Now enter the NAI (wild-carded or specific): scdma_*.*
```

Note You can use a wildcard (*) to view **show subscriber summary** for users matching the string you specify.

```
SHOW SUBSCRIBER SUMMARY <-> (Matching NAI: scdma_*.*)
-------------------------------
Total  Number of sessions with user scdma_*.* :1
Total  Number of Paks in :8
Total  Number of Paks out :14
Total  Number of bytes in :802
Total  Number of bytes out :798
```

- **execute-on** *slot PPC3* **show cdma pdsn session summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
```

```
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   8
>> Now enter the SAMI Card ID ([1-13]):1
SHOW SUBSCRIBER SUMMARY <-> (All Subscribers on the Card: 1)
-------------------------------
Total  Number of sessions :1
Total  Number of Paks in :8
Total  Number of Paks out :14
Total  Number of bytes in :802
Total  Number of bytes out :798
```

- **execute-on** *slot PPC3* **execute-on** *processor* **show cdma pdsn session summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   9
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,3):1,4
SHOW SUBSCRIBER SUMMARY <-> (All Subscribers on the Slot,CPU: [1,4])
-------------------------------
Total  Number of sessions :1
Total  Number of Paks in :8
Total  Number of Paks out :14
Total  Number of bytes in :802
Total  Number of bytes out :805
```

- **show cdma pdsn session summary**

```
PDSN-DEV-7600-4# showSummary
Show Subscriber Summary ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   10
SHOW SUBSCRIBER SUMMARY
-------------------------------
Total  Number of sessions :1
Total  Number of Paks in :8
Total  Number of Paks out :14
Total  Number of bytes in :802
Total  Number of bytes out :805
```

The examples below show how to enable the **show subscriber verbose** command for the following CLIs used on processors:

- **show ip mobile visitor**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):    1

----------- Slot 1/CPU 4, show ip mobile visitor -------------
Total 1
------------------------------------
scdma_osler3@ark.com:
Home addr 9.9.9.1
Interface Virtual-Access2.2, MAC addr 0000.0000.0000
IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
HA addr 5.5.5.2, Identification CD9926F3.10000
Lifetime 00:10:00 (600) Remaining 00:09:58
Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
Routing Options - (T)Reverse Tunneling
```

- **execute-on** *slot PPC3* **show ip mobile visitor**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):    2
>> Now enter the Card number for FA-Member visitors: 1
----------- Slot 1/CPU 4, show ip mobile visitor -------------
Total 1
------------------------------------
scdma_osler3@ark.com:
Home addr 9.9.9.1
Interface Virtual-Access2.2, MAC addr 0000.0000.0000
IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
HA addr 5.5.5.2, Identification CD9926F3.10000
Lifetime 00:10:00 (600) Remaining 00:08:41
Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
Routing Options - (T)Reverse Tunneling
```

- **show ip mobile visitor ha-addr** *ha-ip*

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
```

```
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   3
>> Now enter the HA-User address (Home Agent IP) :5.5.5.2

----------- Slot 1/CPU 4, show ip mobile visitor ha-addr 5.5.5.2-------------
Total 1
------------------------------------
scdma_osler3@ark.com:
Home addr 9.9.9.1
Interface Virtual-Access2.2, MAC addr 0000.0000.0000
IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
HA addr 5.5.5.2, Identification CD9926F3.10000
Lifetime 00:10:00 (600) Remaining 00:07:39
Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
Routing Options - (T)Reverse Tunneling
```

- **show cdma pdsn flow mn-ip-address range** *startIP,endIP* **detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   4
>> Now enter the ',' separated starting IP address & end IP address(e.g.
10.114.200.49,10.114.200.180) :
9.9.9.1,9.9.9.10

-------- Slot 1/CPU 4, show cdma pdsn flow mn-ip-address range 9.9.9.1 9.9.9.10
detail--
  Flow service Mobile, NAI scdma_osler3@ark.com
    Mobile Node IP address 9.9.9.1
    Home Agent IP address 5.5.5.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0

  Qos per flow : scdma_osler3@ark.com
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Number of Persistent Tft : 34567
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
```

- **show cdma pdsn session service-option** *service-option* **detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   5
Select Service Type:
1.   EVDO
2.   1xRTT
3.   Quit
Enter the your service Type choice from the above menu (1/2/3):1

----------- Slot 1/CPU 4, show cdma pdsn session service-option 59 detail
-------------
Mobile Station ID IMSI 09003004953
  PCF IP Address 6.6.6.5, PCF Session ID 4951
  A10 connection time 00:04:42,  registration lifetime 65535 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.2, status OPN
  Using AHDLC engine on slot 0, channel ID 1
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs

  Qos subscriber profile
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505

  Flow service Mobile, NAI scdma_osler3@ark.com
    Mobile Node IP address 9.9.9.1
    Home Agent IP address 5.5.5.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
  Qos per flow : scdma_osler3@ark.com
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Number of Persistent Tft : 34567
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
```

- **show cdma pdsn session lifetime age** *lesser* | *greater* | *equals hh:mm:ss* **detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   6
>> Now enter the lifetime (hh:mm:ss format): 0:20:3
>> Enter the valuetype for Lifetime Record(e.g: greater|lesser|equals): lesser
----------- Slot 1/CPU 4, show cdma pdsn session lifetime age lesser 0:20:2  detail
---------
Mobile Station ID IMSI 09003004953
  PCF IP Address 6.6.6.5, PCF Session ID 4951
  A10 connection time 00:06:38,  registration lifetime 65535 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.2, status OPN
  Using AHDLC engine on slot 0, channel ID 1
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 1

    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
  Flow service Mobile, NAI scdma_osler3@ark.com
    Mobile Node IP address 9.9.9.1
    Home Agent IP address 5.5.5.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0

  Qos per flow : scdma_osler3@ark.com
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Number of Persistent Tft : 34567
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
```

- **show cdma pdsn session user** *patt** **detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   7
>> Now enter the NAI (wild-carded or specific): scdma_*.*
```

Note You can use a wildcard (*) to view **show subscriber detail** for users matching the string you specify.

```
----------- Slot 1/CPU 4, show cdma pdsn session user scdma_*.* detail -------------

Mobile Station ID IMSI 09003004953
  PCF IP Address 6.6.6.5, PCF Session ID 4951
  A10 connection time 00:08:05,  registration lifetime 65535 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.2, status OPN
  Using AHDLC engine on slot 0, channel ID 1
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505

  Flow service Mobile, NAI scdma_osler3@ark.com
    Mobile Node IP address 9.9.9.1
    Home Agent IP address 5.5.5.2
    Packets in 0, bytes in 0

    Packets out 0, bytes out 0
  Qos per flow : scdma_osler3@ark.com
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Number of Persistent Tft : 34567
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
```

- **execute-on** *slot PPC3* **show cdma pdsn session detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   8
>> Now enter the SAMI Card ID ([1-13]):1

----------- Slot 1/CPU 4, show cdma pdsn session detail -------------
Mobile Station ID IMSI 09003004953
  PCF IP Address 6.6.6.5, PCF Session ID 4951
  A10 connection time 00:09:27,  registration lifetime 65535 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.2, status OPN
  Using AHDLC engine on slot 0, channel ID 1
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505

  Flow service Mobile, NAI scdma_osler3@ark.com
    Mobile Node IP address 9.9.9.1
    Home Agent IP address 5.5.5.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0

  Qos per flow : scdma_osler3@ark.com
    Max Aggregate Bandwidth : 1
    Inter User Priority : 1000
    Maximum Flow Priority : 120980
    Number of Persistent Tft : 34567
    Forward profile-id : 4660
    Forward profile-id : 9097
    Forward profile-id : 14454
    Reverse profile-id : 6295
    Reverse profile-id : 17185
    Bidirectional profile-id : 22136
    Bidirectional profile-id : 26505
```

- **execute-on** *slot PPC3* **execute-on** *processor* **show cdma pdsn session detail**

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   9
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,3):4,4
----------- Slot 4/CPU 4, show cdma pdsn session detail-------------
Mobile Station ID IMSI 123456789123457
  PCF IP Address 51.1.1.1, PCF Session ID 1
  A10 connection time 01:04:29,  registration lifetime 50 sec
  Number of successful A11 re-registrations 117
  Remaining session lifetime 41 sec
  Always-On not enabled for the user
  Current Access network ID 0033-0101-01
  Last airlink record received is Connection Setup, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 13, receive 12
  Using interface Virtual-Access2.1, status OPN

  Using AHDLC engine on slot 0, channel ID 11
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Setup
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 20000
    Number of Persistent Tft : 1

  Flow service Simple, NAI ddhayalasip
    Mobile Node IP address 20.2.0.6
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
    Radius disconnect enabled
```

- show cdma pdsn session detail

```
PDSN-DEV-7600-4# showVerbose
Show Subscriber Detail ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   10

----------- Slot 4/CPU 4, show cdma pdsn session detail -------------
Mobile Station ID IMSI 123456789123457
  PCF IP Address 51.1.1.1, PCF Session ID 1
  A10 connection time 01:03:35,  registration lifetime 50 sec
  Number of successful A11 re-registrations 115
  Remaining session lifetime 30 sec
  Always-On not enabled for the user
  Current Access network ID 0033-0101-01
  Last airlink record received is Connection Setup, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 13, receive 12
  Using interface Virtual-Access2.1, status OPN
  Using AHDLC engine on slot 0, channel ID 11
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Setup
  This session has 0 TFTs
  Qos subscriber profile
    Max Aggregate Bandwidth : 20000
    Number of Persistent Tft : 1

  Flow service Simple, NAI ddhayalasip
    Mobile Node IP address 20.2.0.6
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
    Radius disconnect enabled
```

The examples below show how to enable the **show subscriber brief** command for the following CLIs used on processors:

- **show ip mobile visitor brief**

```
pdsn-dev-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):    1
----------- Slot 1/CPU 7, show ip mobile visitor brief -------------
Total 1
------------------------------------
scdma_osler3@ark.com:
    Home addr 9.9.9.1

    MAC addr 0000.0000.0000
    HA addr 5.5.5.2
    FA addr 5.5.5.1
    Lifetime 00:10:00 (600) Remaining 00:09:53
```

- **execute-on** *slot PPC3* **show ip mobile visitor brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):    2
>> Now enter the Card number for FA-Member visitors:1
----------- Slot 1/CPU 7, show ip mobile visitor brief -------------
Total 1
------------------------------------
scdma_osler3@ark.com:
Home addr 9.9.9.1
MAC addr 0000.0000.0000
HA addr 5.5.5.2
FA addr 5.5.5.1
Lifetime 00:10:00 (600) Remaining 00:09:07
```

- **show ip mobile visitor ha-addr** *ha-ip* **brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
```

```
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   3
>> Now enter the HA-User address (Home Agent IP) :5.5.5.2
----------- Slot 1/CPU 7, show ip mobile visitor ha-addr 5.5.5.2 brief -------------
Total 1
------------------------------------
scdma_osler3@ark.com:
Home addr 9.9.9.1
MAC addr 0000.0000.0000
HA addr 5.5.5.2
FA addr 5.5.5.1
Lifetime 00:10:00 (600) Remaining 00:08:07
```

- **show cdma pdsn flow mn-ip-address range** *startIP, endIP*

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   4
>> Now enter the ',' separated starting IP address & end IP address(e.g.
10.114.200.49,10.114.200.180) :
9.9.9.1,9.9.9.4
----------- Slot 1/CPU 7, show cdma pdsn flow mn-ip-address range 9.9.9.1
9.9.9.4---------
MSID            NAI                            Type         MN IP Address    St  HA IP
09003000453     scdma_osler3@ark.com           Mobile       9.9.9.1          ACT
5.5.5.2
```

- **show cdma pdsn session service-option** *service-option* **brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   5
Select Service Type:
1.   EVDO
2.   1xRTT
3.   Quit
Enter the your service Type choice from the above menu (1/2/3):1

----------- Slot 1/CPU 7, show cdma pdsn session service-option 59 brief -------------
```

```
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000453     6.6.6.5                 451 00:03:25 OPN      0     1
Virtual-Access2.1
```

- **show cdma pdsn session lifetime age** *lesser* | *greater* | *equals hh:mm:ss* **brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   6
>> Now enter the lifetime (hh:mm:ss format): 0:23:34
>> Enter the valuetype for Lifetime Record(e.g: greater|lesser|equals): lesser

----------- Slot 1/CPU 7, show cdma pdsn session lifetime age lesser 0:23:33  brief
--------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000453     6.6.6.5                 451 00:04:15 OPN      0     1
Virtual-Access2.1

---------- Slot 4/CPU 7, show cdma pdsn session lifetime age lesser 0:23:33  brief
--------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
123456789123457 51.1.1.1                  1 00:00:01 OPN      1     1
Virtual-Access2.1
123456789123507 51.1.1.1                 51 00:00:01 OPN      1     1
Virtual-Access2.2
123456789123557 51.1.1.1                101 00:00:01 OPN      1     1
Virtual-Access2.3
```

- **show cdma pdsn session user** *patt** **brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):   7
>> Now enter the NAI (wild-carded or specific): scdma*
```

Note You can use a wildcard (*) to view **show subscriber brief** for users matching the string you specify.

```
----------- Slot 1/CPU 7, show cdma pdsn session user scdma* brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
```

```
09003000453     6.6.6.5                 451 00:07:04 OPN      0     1
Virtual-Access2.1
```

- **execute-on** *slot PPC3* **show cdma pdsn session brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):  8
>> Now enter the SAMI Card ID ([1-13]):1

----------- Slot 1/CPU 7, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000453     6.6.6.5                 451 00:07:45 OPN      0     1
Virtual-Access2.1
```

- **execute-on** *slot PPC3* **execute-on** *processor* **show cdma pdsn session brief**

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):  9
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,3):1,7
----------- Slot 1/CPU 7, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000453     6.6.6.5                 451 00:09:40 OPN      0     1
Virtual-Access2.1
```

- show cdma pdsn session brief

```
PDSN-DEV-7600-4# showBrief
Show Subscriber in Brief ...
1.   Show all visitors serviced in FA chasis
2.   Show all visitors serviced in FA in specific service card
3.   Show subscribers registered for a particular HA
4.   Show subscribers within given address space
5.   Show subscribers with particular CallType
6.   Show subscribers with lifetime of
7.   Show subscribers with matching NAI
8.   Show subscribers in a Card
9.   Show subscribers in a CPU
10.  Show all subscribers
11.  Quit
Enter the choice from the above menu (1/2/3/../11):  10
----------- Slot 1/CPU 4, show cdma pdsn session brief -------------
```

```
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000453     6.6.6.5                 451 00:00:05 OPN      0     1
Virtual-Access2.1
```

monitor subscriber

To monitor the subscriber, use traces commands. The subscriber is identified based on the NAI, the assigned IP address, or the IMSI. To trace the subscriber, the monitor subscriber policy invokes multiple commands on one or more processors that run the active and standby PDSN to set conditional debugs using existing IOS commands for that subscriber. The set of conditional debugs is based on AAA, CDMA,PPP, SSS and so on that will invoke multiple commands on the processors. By using conditional debugs, an operator does not need to set the debug conditions on all the processors.

To enable the inclusion of the username in the traces, use the **ip mobile debug include username** command to configure each SAMI processor in config mode.

traces {**start tracing** | **stop tracing** | **show open traces** | **clear all traces**}{**brief** | **verbose**}{**all** | **session** | **accounting** | **tft** | **vpdn** | **mip** | **pmip**}

Syntax Description

start tracing	Starts tracing details on a subscriber.
stop tracing	Stops tracing details on a subscriber.
show open traces	Shows traces that are open.
clear all traces	Clears details of all traces.
exit	Quits the tracing activity.
brief	Displays information, using the one-line-of-output-per-subscriber format, for each subscriber matching the debug condition.
verbose	Displays information, using the multiple-lines-of-output-per-subscriber format, for each subscriber matching the debug condition.
all	Displays all details of the user on the chassis.
session	Displays session details of the user on the chassis.
accounting	Displays accounting details of the user on the chassis.
tft	Displays TFT details of the users on the chassis.
vpdn	Displays VPDN details of the users on the chassis.
mip	Displays MIP details of the user on the chassis.
pmip	Displays PMIP details of the users on the chassis.

Defaults

No default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

The subscriber is identified either by NAI or IMSI. When you use the trace command, options to work with traces appear, followed by the display option, and then the debugging conditions. Based on a combination of these, multiple commands are run on the processors and the output is returned.

Examples

The following example shows how to enable the **start tracing** command:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:1
Specify the NAI/IMSI: osler1@cisco.com

Trace mode...
  1. Brief
  2. Verbose
  Please choose the trace mode: 2

Traces options...
  1. Session
  2. Accounting
  3. TFT
  4. VPDN
  5. MIP
  6. PMIP
  7. All
  Please choose the trace option(s): 1 2
Checking console logging severity level...
Checking debugs on supervisor card...
Checking available space in disk0:/pdsn_traces directory...
Directory disk0:/pdsn_traces can contain upto 50 trace log files only
Transferred osler1@cisco.com_2009_Mar_16_11_16_31.log file to external host
Deleted the osler1@cisco.com_2009_Mar_16_11_16_31.log file from disk0:/pdsn_traces
directory
Enabling the trace conditions...
Enter the telnet username for slot 4 processor 3: admin
Enter the telnet password for slot 4 processor 3: admin
Enter the enable password for slot 4 processor 3: lab
Enter the telnet username for slot 8 processor 3: admin
Enter the telnet password for slot 8 processor 3: admin
Enter the enable password for slot 8 processor 3: lab


Starting the tracing of subscriber 09003000001
Monitored traces shall be stored in disk0:/pdsn_traces/
09003000001_2009_Mar_9_12_06_56.log file

SAMI 8/3: Apr 17 11:14:57.254
CDMA-RP:
extension type=38, len=0
extension type=38, len=0
extension type=38, len=0
extension type=134, len=10
00 00 00 00 15 9F 09 01 00 3B
extension type=32, len=20
00 00 01 01 73 69 FD D7 5B 2E 77 04 3B 81 9C 12
54 A1 AE 98
(req) process_rp_req, homeagent=77.77.77.1 coaddr=6.6.6.2
```

```
lifetime=65535 id=CD24088E-4ED91065 IMSI=09003000001
(req) rp_req_create, ha=77.77.77.1, coa=6.6.6.2, key=1 IMSI=09003000001
CDMA-SM:
cdma_sm_create_session_common pdsn=77.77.77.1, pcf=6.6.6.2, key=1
cdma_sm_create_session_common session subblock allocated, sb=0x42D111B0 session=0x42D111BC
CDMA-HDLC:
cdma_hdlc_create_session init ahdlc for session 77.77.77.1-6.6.6.2-1
CDMA-SM:
Access IE handle=0x12000005 allocated for session 77.77.77.1-6.6.6.2-1
SSS switch handle allocated for session 77.77.77.1-6.6.6.2-1 sss_circuit=0x42D51DCC,
sss_switch_handle=0x3A000005
SSS sss_sip_service_request succeeds for session 77.77.77.1-6.6.6.2-1
CDMA-RP:
(out) rp_reply session=77.77.77.1-6.6.6.2-1, lifetime=65535
(out) Setup RP message, ha=77.77.77.1 coa=6.6.6.2 key=1 dst=6.6.6.2
PDSN sending Registration Reply to PCF 6.6.6.2
CDMA-SM:
Received SSS response=1 for session 77.77.77.1-6.6.6.2-1, state=4
PPP bind request succeeds for session 77.77.77.1-6.6.6.2-1
PPP:
Send Message[Dynamic Bind Response]
Using default call direction
Treating connection as a dedicated line
Session handle[C1000007] Session id[5]
Phase is ESTABLISHING, Active Open
LCP:
O CONFREQ [Closed] id 1 len 21
ACCM 0x00000000 (0x020600000000)
AuthProto CHAP (0x0305C22305)
MagicNumber 0x009B750F (0x0506009B750F)
```

The following example shows how to enable the **stop tracing** command:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:2
Specify the NAI/IMSI address: osler1@cisco.com
Do you want to transfer the trace log file of subscriber osler1@cisco.com to external host
(y/n)? y
Successfully sent the trace stop request for subscriber osler1@cisco.com
```

The following example shows how to enable the **show open traces** command:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:3
Total number of trace sessions: 2
Tracing is on for subscriber(s): osler1@cisco.com, scdma_osler3@ark.com
```

The following example shows how to enable the **clear all traces** command:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:4

Tracing is on for subscriber(s): osler1@cisco.com, scdma_osler3@ark.com
This option shall stop all trace sessions
Do you want to stop all trace sessions (y/n)? y

Sending stop request to trace session(s)...
Do you want to transfer the trace log file of subscriber osler1@cisco.com to external host
(y/n)? y
Disabling the trace conditions of subscriber osler1@cisco.com...
Successfully sent the trace stop request for subscriber osler1@cisco.com
Do you want to transfer the trace log file of subscriber scdma-osler3@ark.com to external
host (y/n)? y
Disabling the trace conditions of subscriber scamd_osler3@ark.com...
Releasing the resources...
Successfully sent the trace stop request for subscriber scdma_olser3@cisco.com
```

The following example shows how to enable the **start tracing** command using NAI as subscriber identifier:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:1
Specify the NAI/IMSI: abc@xyz.com

Trace mode...
  1. Brief
  2. Verbose
  Please choose the trace mode: 1

Traces options...
  1. Session
  2. Accounting
  3. TFT
  4. VPDN
  5. MIP
  6. PMIP
  7. All
  Please choose the trace option(s): 1
SAMI 1/4: *Mar  3 17:59:55.371:
------------------------------
CDMA-RP:
    Sending Registration Update to 6.6.6.2
    Sending Registration Update to 6.6.6.2
    (ack) process_rp_update_ack, homeagent=0.0.0.0 coaddr=6.6.6.2
      lifetime=0 id=CD9697BE-4245 IMSI=09003000001
    PDSN sending Registration Reply to PCF 6.6.6.2
CDMA-SM:
    cdma_sm_delete_session1 key=1 imsi=09003000001
    delete flow osler1@cisco.com in session 09003000001

SAMI 1/4: *Mar  3 17:59:56.591:
------------------------------
RADIUS
    Send Access-Request to 1.1.1.111:1645 id 45512/3, len 104
     Vendor, 3GPP2       [26]  16
```

```
      cdma-correlation-id[44]  10  "00000022"
     Calling-Station-Id  [31]  13  "09003000001"
     Framed-Protocol     [7]   6   PPP                       [1]
     User-Name           [1]   18  "osler1@cisco.com"
     CHAP-Password       [3]   19  *
     Service-Type        [6]   6   Framed                    [2]
     NAS-IP-Address      [4]   6   1.1.1.110

SAMI 1/4: *Mar  3 17:59:56.595:
------------------------------
    Received from id 45512/3 1.1.1.111:1645, Access-Accept, len 104
     Vendor, 3GPP2       [26]  12
      cdma-int-usr-pri   [139] 6   1000
     Vendor, 3GPP2       [26]  12
      cdma-num-persistent[89]  6   34567
     Vendor, 3GPP2       [26]  12
      cdma-max-flow-prior[133] 6   120980

SAMI 1/4: *Mar  3 17:59:56.599:
------------------------------
CDMA-RP:
    simple ip visitor added, mn=4.4.4.3, ha=0.0.0.0
    (out) send session update, session=77.77.77.1-6.6.6.2-1 IMSI=09003000001

SAMI 1/4: *Mar  3 17:59:56.603:
------------------------------
    process session upd ack, homeagent=0.0.0.0 coaddr=6.6.6.2
      lifetime=0 id=CD9697BF-FEF995C5 IMSI=09003000001
    CDMA SM process RP Session Upd Ack : Session Upd Denied by PCF 6.6.6.2 - (85H)
Identification mismatch
    (out) send session update, session=77.77.77.1-6.6.6.2-1 IMSI=09003000001
    process session upd ack, homeagent=0.0.0.0 coaddr=6.6.6.2
      lifetime=0 id=CD9697BF-4245 IMSI=09003000001
```

The following example shows how to enable the **start tracing** command using IMSI as subscriber identifier:

```
PDSN-OSLER# traces
  Trace option...
  1. Start tracing
  2. Stop tracing
  3. Show open traces
  4. Clear all traces
  5. Exit
  Please make a choice:1
Specify the NAI/IMSI: 09003000555

Trace mode...
  1. Brief
  2. Verbose
  Please choose the trace mode: 1

Traces options...
  1. Session
  2. Accounting
  3. TFT
  4. VPDN
  5. MIP
  6. PMIP
  7. All
  Please choose the trace option(s): 2

SAMI 1/4: *Mar  1 02:25:29.455:
------------------------------
```

```
CDMA-SM:
    cdma_sm_create_session_common pdsn=77.77.77.1, pcf=6.6.6.5, key=551

SAMI 1/4: *Mar  1 02:25:29.459:
------------------------------
CDMA-ACCT:
    Generating Accounting Record for ipflow 255
    Setup airlink record received
    Generating Accounting Record for ipflow 255
    Start airlink record received
CDMA-RP:
    PDSN sending Registration Reply to PCF 6.6.6.5
      IMSI create timer stopped
PPP:
    Phase is ESTABLISHING, Active Open
LCP:
    O CONFREQ [Closed] id 1 len 21
    ACCM 0x00000000 (0x020600000000)
    AuthProto CHAP (0x0305C22305)
    MagicNumber 0x00C633A8 (0x050600C633A8)

SAMI 1/4: *Mar  1 02:25:29.463:
------------------------------
    I CONFREQ [REQsent] id 1 len 16
    ACCM 0x00000000 (0x020600000000)
    MagicNumber 0x0695773D (0x05060695773D)
    O CONFACK [REQsent] id 1 len 16
    ACCM 0x00000000 (0x020600000000)
    MagicNumber 0x0695773D (0x05060695773D)
    I CONFACK [ACKsent] id 1 len 21
    ACCM 0x00000000 (0x020600000000)
    AuthProto CHAP (0x0305C22305)
    MagicNumber 0x00C633A8 (0x050600C633A8)
    State is Open
PPP:
    Phase is AUTHENTICATING, by this end
CHAP:
    O CHALLENGE id 1 len 31 from "PDSN_OSLER"
    I RESPONSE id 1 len 36 from "osler@cisco.com"
PPP:
    Phase is FORWARDING, Attempting Forward
    Phase is AUTHENTICATING, Unauthenticated User
    Phase is FORWARDING, Attempting Forward

SAMI 1/4: *Mar  1 02:25:29.479:
------------------------------
    Phase is FORWARDED, Session Forwarded
CDMA-RP:
    simple ip visitor added, mn=0.0.0.0, ha=0.0.0.0
CDMA-ACCT:
    calling accounting flow start
      C - ' 'C2:226 C3:0 C4:1 C5:1 C6:255
      I - I1:0 I4:0 I5:00 00 00 00 00 00 00 00 00 00 00
RADIUS
    Best Local IP-Address 1.1.1.110 for Radius-Server 1.1.1.111
    Send Accounting-Request to 1.1.1.111:1646 id 45513/108, len 448
     Acct-Session-Id     [44]  10  "0000002B"
     Calling-Station-Id  [31]  13  "09003000555"
     Vendor, 3GPP2       [26]  23
      cdma-esn           [52]  17  "000400050006558"
     Vendor, 3GPP2       [26]  16
      cdma-correlation-id[44]  10  "000000E2"
     Vendor, 3GPP2       [26]  12
      cdma-ha-ip-addr    [7]   6   0.0.0.0
     User-Name           [1]   17  "osler@cisco.com"
     Vendor, Cisco       [26]  32
      Cisco AVpair       [1]   26  "connect-progress=Call Up"
     Vendor, 3GPP2       [26]  22
      cdma-meid          [116] 16  "              "
     Framed-IP-Address   [8]   6   0.0.0.0
     Vendor, 3GPP2       [26]  12
      cdma-begin-session [51]  6   1
     Vendor, 3GPP2       [26]  12
      cdma-pcf-ip-addr   [9]   6   6.6.6.5
     Vendor, 3GPP2       [26]  20
      cdma-bs-msc-addr   [10]  14  "000000000000"
     Vendor, 3GPP2       [26]  12
      cdma-user-id       [11]  6   0
     Vendor, 3GPP2       [26]  12
      cdma-forward-mux   [12]  6   241
     Vendor, 3GPP2       [26]  12
      cdma-reverse-mux   [13]  6   242
     Vendor, 3GPP2       [26]  12
      cdma-service-option[16]  6   59
     Vendor, 3GPP2       [26]  12
      cdma-forward-type  [17]  6   246
     Vendor, 3GPP2       [26]  12
      cdma-reverse-type  [18]  6   247
     Vendor, 3GPP2       [26]  12
      cdma-frame-size    [19]  6   248
     Vendor, 3GPP2       [26]  12
      cdma-forward-rc    [20]  6   249
     Vendor, 3GPP2       [26]  12
      cdma-reverse-rc    [21]  6   250
     Vendor, 3GPP2       [26]  12
      cdma-ip-tech       [22]  6   1
     Vendor, 3GPP2       [26]  12
      cdma-comp-flag     [23]  6   Non Secure Tunnel         [1]
     Vendor, 3GPP2       [26]  12
      cdma-dcch-frame-siz[50]  6   0
     Vendor, 3GPP2       [26]  12
      cdma-ip-qos        [36]  6   0
     Vendor, 3GPP2       [26]  12
      cdma-airlink-qos   [39]  6   0
     Vendor, 3GPP2       [26]  12
      cdma-rp-session-id [41]  6   551

SAMI 1/4: *Mar  1 02:25:29.483:
------------------------------
     Acct-Authentic      [45]  6
     Acct-Status-Type    [40]  6   Start                     [1]
     NAS-Port-Type       [61]  6   Virtual                   [5]
     NAS-Port            [5]   6   0
     NAS-Port-Id         [87]  11  "CDMA-IX/0"
     Service-Type        [6]   6   Framed                    [2]
     NAS-IP-Address      [4]   6   1.1.1.110
     Acct-Delay-Time     [41]  6
CDMA-RP:
    process session upd ack, homeagent=0.0.0.0 coaddr=6.6.6.5
      lifetime=0 id=CDAD09FA-1B5B IMSI=09003000555
RADIUS
    Received from id 45513/108 1.1.1.111:1646, Accounting-response, len 20

SAMI 1/4: *Mar  1 02:27:32.995:
------------------------------
RADIUS
    Orig. component type = PDSN
    Config NAS IP: 0.0.0.0
```

```
sending
Best Local IP-Address 1.1.1.110 for Radius-Server 1.1.1.111
Send Accounting-Request to 1.1.1.111:1646 id 45513/119, len 617
 Acct-Session-Id     [44]  10  "0000002B"
 Calling-Station-Id  [31]  13  "09003000555"
 Vendor, 3GPP2       [26]  23
  cdma-esn           [52]  17  "000400050006558"
 Vendor, 3GPP2       [26]  16
  cdma-correlation-id[44]  10  "000000E2"
 Vendor, 3GPP2       [26]  12
  cdma-ha-ip-addr    [7]   6   0.0.0.0
 User-Name           [1]   17  "osler@cisco.com"
 Vendor, Cisco       [26]  32
  Cisco AVpair       [1]   26  "connect-progress=Call Up"
 Vendor, 3GPP2       [26]  22
  cdma-meid          [116] 16  "              "
 Framed-IP-Address   [8]   6   0.0.0.0
 Vendor, 3GPP2       [26]  12
  cdma-pcf-ip-addr   [9]   6   6.6.6.5
 Vendor, 3GPP2       [26]  20
  cdma-bs-msc-addr   [10]  14  "000000000000"
 Vendor, 3GPP2       [26]  12
  cdma-user-id       [11]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-forward-mux   [12]  6   241
 Vendor, 3GPP2       [26]  12
  cdma-reverse-mux   [13]  6   242
 Vendor, 3GPP2       [26]  12
  cdma-service-option[16]  6   59
 Vendor, 3GPP2       [26]  12
  cdma-forward-type  [17]  6   246
 Vendor, 3GPP2       [26]  12
  cdma-reverse-type  [18]  6   247
 Vendor, 3GPP2       [26]  12
  cdma-frame-size    [19]  6   248
 Vendor, 3GPP2       [26]  12
  cdma-forward-rc    [20]  6   249
 Vendor, 3GPP2       [26]  12
  cdma-reverse-rc    [21]  6   250
 Vendor, 3GPP2       [26]  12
  cdma-ip-tech       [22]  6   1
 Vendor, 3GPP2       [26]  12
  cdma-comp-flag     [23]  6   Non Secure Tunnel         [1]
 Vendor, 3GPP2       [26]  12
  cdma-dcch-frame-siz[50]  6   0
 Acct-Input-Octets   [42]  6   50
 Acct-Output-Octets  [43]  6   58
 Acct-Input-Packets  [47]  6   4
 Acct-Output-Packets [48]  6   5
 Vendor, 3GPP2       [26]  12
  cdma-bad-frame-coun[25]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-active-time   [49]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-num-active    [30]  6   1
 Vendor, 3GPP2       [26]  12
  cdma-sdb-input-octe[31]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-sdb-output-oct[32]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-numsdb-input  [33]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-numsdb-output [34]  6   0
 Vendor, 3GPP2       [26]  12
```

```
  cdma-hdlc-layer-byt[43]  6   202
 Vendor, 3GPP2       [26]  12
  cdma-moip-inbound  [46]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-moip-outbound [47]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-ip-qos        [36]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-airlink-qos   [39]  6   0
 Vendor, 3GPP2       [26]  12
  cdma-rp-session-id [41]  6   551
 Acct-Authentic      [45]  6   RADIUS                    [1]
 Vendor, Cisco       [26]  31
  Cisco AVpair       [1]   25  "nas-tx-speed=1229102904"
 Acct-Session-Time   [46]  6   124
 Acct-Status-Type    [40]  6   Watchdog                  [3]
 NAS-Port-Type       [61]  6   Virtual                   [5]
 NAS-Port            [5]   6   0
 NAS-Port-Id         [87]  11  "CDMA-IX/0"
 Service-Type        [6]   6   Framed                    [2]
 NAS-IP-Address      [4]   6   1.1.1.110
 Acct-Delay-Time     [41]  6   0
Received from id 45513/119 1.1.1.111:1646, Accounting-response, len 20
```

show subscriber session

The **show subscriber session** commands are used to determine the service blade that hosts the subscriber, executes the set of IOS commands, collates and presents the results in a single coherent output format.

To get the session and accounting details from the SAMI cards, run the following commands on all the active SAMI cards:

- For NAI-based session information:

  show cdma pdsn session user *NAI* **detail**

  show cdma pdsn accounting user *NAI*

- For IP address-based session information:

  show cdma pdsn session mn-ip-address *IP-Address* **detail**

  show cdma pdsn accounting mn-ip-addr *IP-Address*

- For IMSI-based session information:

  show cdma pdsn session msid *IMSI_value* **detail**

  show cdma pdsn accounting session *IMSI_value*

Syntax Description

session	Displays session details on the user on the chassis.
accounting	Displays accounting details on the user on the chassis.
user	Displays summary of all users for a specified NAI.
nai	Network access identifier.
ip-address	Specifies the IP addresses assigned to the mobile numbers in each session.
msid	Specifies the mobile subscriber ID number
imsi_value	Displays the International Mobile Station Identifier number

Defaults

No default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

The display options can be used in the command to filter the subscriber details.

Examples

The following example shows how to enable the **show subscriber session summary** command:

```
User ID: osler1@cisco.com    [Slot:1 CPU:3]
Session Details:
   Mobile Station ID IMSI 09003000001
   PCF IP Address 6.6.6.2, PCF Session ID 1
   A10 connection time 00:00:12,  registration lifetime 65535 sec
   Number of successful A11 re-registrations 0
   Remaining session lifetime INFINITE
   Always-On not enabled for the user
   Current Access network ID 0006-0606-02
   Last airlink record received is Active Start, airlink is active
   GRE protocol type is 0x8881
   GRE sequence number transmit 14, receive 7
   Using interface Virtual-Access2.1, status OPN
   Using AHDLC engine on slot 0, channel ID 3
   Service Option EV-DO Flow Discrimination 0 DSCP Included 0
   Flow Count forward 0 reverse 0
   This session has 1 flow
   This session has 0 service flows
   Session Airlink State Active
   This session has 0 TFTs
   Qos subscriber profile
   Max Aggregate Bandwidth : 1
   Inter User Priority : 1000
   Maximum Flow Priority : 120980
   Forward profile-id : 4660
   Forward profile-id : 9097
   Forward profile-id : 14454
   Reverse profile-id : 6295
   Reverse profile-id : 17185
   Bidirectional profile-id : 22136
   Bidirectional profile-id : 26505
   Flow service Simple, NAI osler1@cisco.com
   Mobile Node IP address 4.4.4.1
   Packets in 0, bytes in 0
   Packets out 0, bytes out 0
   Qos per flow : osler1@cisco.com
   Max Aggregate Bandwidth : 1
   Inter User Priority : 1000
   Maximum Flow Priority : 120980
   Number of Persistent Tft : 34567
   Forward profile-id : 4660
   Forward profile-id : 9097
   Forward profile-id : 14454
   Reverse profile-id : 6295
   Reverse profile-id : 17185
   Bidirectional profile-id : 22136
   Bidirectional profile-id : 26505
Accounting Details:
   UDR for session
   session ID: 1
   Mobile Station ID IMSI 09003000001
   A - A1:09003000001 A2: A3:
   C - C3:0
   D - D3:6.6.6.2 D4:000000000000
   E - E1:0000
   F - F1:00F1 F2:00F2 F5:003B F6:F6 F7:F7 F8:F8
   F9:F9 F10:FA F14:00 F15:0
   F16:00 F17:00 F18:00
   F19:00 F20:00 F22:00
   G - G3:0 G8:0 G9:1 G10:0 G11:0 G12:0
   G13:0 G14:245 G15:0 G16:270 G17:0
   I - I1:0 I4:0
```

```
Y - Y2:1
UDR for flow
Mobile Node IP address 4.4.4.1
B - B1:4.4.4.1 B2:osler1@cisco.com
C - C1:000F C2:7 C4:0
D - D1:0.0.0.0
F - F11:01 F12:00 F13:00
G - G1:0 G2:0 G4:1232699771
G22:0 G23:0 G24:0 G25:0
Packets- in:0 out:0
```

bulk statistics collection

The Bulk Statistics Collection feature is similar to Home Agent Bulk Statistics Collection feature.

Statistics are collected using the SNMP MIB bulk statistics feature available on the Cisco router. With the help of Osler commands, SNMP MIB object list is configured on the control processor. After enabling the bulk statistics feature, the statistics is collected for a specified time interval, and sent to the configured TFTP server. If TFTP file transfer failed, then the statistics are sent to the SUP disk specified in the secondary URL.

Following are the commands available for the Bulk Statistics Collection:

- Start Bulk Statistics: The Start Bulk Statistics command configures SNMP MIB objects on all the control processors. When you run this command, do not use the telnet connection since it affects the configuring of SNMP MIB objects on each PCOP.

  Following are the Start Bulk Statistics commands:

  - **no snmp mib bulkstat object-list** *object_name*
  - **snmp mib bulkstat object-list** *object_name*
  - **add** *oids*
  - **poll-interval** *time_interval*
  - **buffer-size** *bytes*
  - **instance exact oid 0**
  - **no snmp mib bulkstat schema** *schema_name*
  - **snmp mib bulkstat schema** *schema_name*
  - **no snmp mib bulkstat transfer** *transfer_name*
  - **snmp mib bulkstat transfer** *transfer_name*
  - **format** *transfer_format* (For example, the format can be *ASCII)*
  - **transfer-interval** *periodicity*
  - **url primary** *url*
  - **url secondary** *url*
  - **retain** *time_interval*
  - **retry** *max-number_try*

- Stop Bulk Statistics: The Stop Bulk Statistics command removes the SNMP MIB objects configuration on all the control processors. When you run this command, do not telnet to any processor, since it affects the removal of the SNMP MIB objects configuration from the processors.

  Following are the Stop Bulk Statistics commands:

  - **snmp mib bulkstat transfer** *transfer_name*
  - **no enable**
  - **no snmp mib bulkstat transfer** *transfer_name*
  - **no snmp mib bulkstat schema** *schema_name*
  - **no snmp mib bulkstat object-list** *object_name*

- Update Statistics Mapping file: The Update Statistics Mapping file option enables you to add new OIDs to the mapping file.

For configuring SNMP MIB object list, a mapping file containing all the OIDs with Cisco Object Name, Vendor Object Name, and Object ID is available. Run the command **updateStatsMap** to update the file with new OIDs that are to be included in the global statistics.

Syntax Description

no snmp mib bulkstat object-list *object_name*	Removes the configuration of the object-list.
snmp mib bulkstat object-list *object_name*	Configures the object-list.
add *oids*	Configurse the SNMP objects.
poll-interval *time_interval*	Configures the poll interval.
buffer-size *bytes*	Configures the maximum buffer size of the statistics file.
instance exact oid 0	Configures the instances.
no snmp mib bulkstat schema *schema_name*	Removes the configuration of the statistics schema.
snmp mib bulkstat schema *schema_name*	Configures the statistics schema.
no snmp mib bulkstat transfer *transfer_name*	Removes the configuration of the Bulk Statistics Transfer Option.
snmp mib bulkstat transfer *transfer_name*	Configures the Bulk Statistics Transfer Option.
format *transfer_format*	Configures the format of the transfer option. For example, the format can be ASCII.
transfer-interval *periodicity*	Configures the transfer-interval of the transfer option.
url primary *url*	Configures the primary URL of the transfer option.
url secondary *url*	Configures the secondary URL of the transfer option.
retain *time_interval*	Configures the retain period (in seconds) of the transfer option.
retry *max-number_try*	Configures the retry option of the transfer option.
snmp mib bulkstat transfer *transfer_name*	Changes the directory to bulk statistics transfer option.
no enable	Disables the bulk statistics transfer option.

no snmp mib bulkstat transfer *transfer_name*	Removes the configuration of the bulk statistics transfer option.
no snmp mib bulkstat schema *schema_name*	Removes the configuration of the statistics schema.
no snmp mib bulkstat object-list *object_name*	Removes the configuration of the statistics object list.
updateStatsMap	Updates the file with new OIDs that are to be included in the global statistics.

Defaults

No default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(22)XR	This command was introduced.

Usage Guidelines

The display options can be used in the command to filter the subscriber details.

Examples

The following example shows how to enable the **bulk statistics collection summary** commands:

```
Schema-def osler_stats_schema "%u, %s ,%u, %u, %u, %d, %u, %u, %u, %u, %u, %d, %u, %u, %u,
%u, %u, %u,  %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u, %u,
%u, %u, %u, %u, %u, %u, %u, %u, %u, %u , %d, %u, %s, %u, %u, %d, %u, %u, %u, %u, %d, %d,
%s, %u"
  2         epochtime instanceOID    cCdmaActiveSessions
cCdmaDormantSessions     cCdmaEstablishedSessions    cCdmaFormatE rrorNotifEnabled
cCdmaHDLCoGRESessionTotal   cCdmaMSIDFlowTotal   cCdmaMobileIpFlowTotal
cCdmaPPPoGRESessionTotal      cCdma PcfMaxAllowed   cCdmaPcfMaxAllowedNotifEnabled
cCdmaPcfSoRpDeRegAcptdReqs   cCdmaPcfSoRpDeRegAirlinkStops    cCdmaPcfSoRpDeRegDeniedReqs
cCdmaPcfSoRpDeRegDiscardedReqs   cCdmaPcfSoRpDeRegRcvdReqs
cCdmaPcfSoRpHandoffRegAcptdReqs  cCdmaPcfSoRpHandoffRegDeniedReqs
cCdmaPcfSoRpHandoffRegDiscardedReqs
cCdmaPcfSoRpHandoffRegRcvdReqs   cCdmaPcfSoRpInitRegAcptdRe qs
cCdmaPcfSoRpInitRegDeniedReqs     cCdmaPcfSoRpInitRegDiscardedReqs
cCdmaPcfSoRpInitRegRcvdReqs      cCdmaPcfSoRpReRegAcpt dReqs
cCdmaPcfSoRpReRegAirlinkStarts      cCdmaPcfSoRpReRegAirlinkStops
cCdmaPcfSoRpReRegDeniedReqs         cCdmaPcfSoRpReRegDis cardedReqs
cCdmaPcfSoRpReRegRcvdReqs        cCdmaPcfSoRpRegAcptdReqs cCdmaPcfSoRpRegAdmnFails
cCdmaPcfSoRpRegBadCVSEFails cCdmaPcfSoRpRegBadReqFails         cCdmaPcfSoRpRegDeniedReqs
cCdmaPcfSoRpRegDiscardedReqs         cCdmaPcfSoRpRegIdMismatFails
cCdmaPcfSoRpRegMNAuthFails   cCdmaPcfSoRpRegNoRevTunFails cCdmaPcfSoRpRegNoRsrcFails
cCdmaPcfSoRpRegPcfUnknwnFails cCdmaPcfSoRpRegRcvdReqs        cCdmaPcfSoRpRegTBitNSetFails
cCdmaPcfSoRpRegUnkPdsnFails           cCdmaPcfTotal    cCdmaProxyMobileIpFlowTota l
cCdmaRegReqFailedNotifEnabled      cCdmaReleasedSessions     cCdmaServingPdsnHostname
cCdmaSessionFailTotal  cCdmaSessionMaxAllowed     cCdmaSessionMaxNotifEnabled
```

```
cCdmaSessionPdsnAuthenTimer     cCdmaSessionPdsnMaxFailHistory       cCdmaSessionTotal
cCdmaSimpleIpFlowTotal  cCdmaSrEnabled  cCdmaSystemStatus  cCdmaSystemVersion
cCdmaVPDNFlowTotal
     3  Schema-def GLOBAL "%s, %s, %u, %u, %u, %u, %u"
     4         hostname date timeofday sysuptime cpu5min cpu1min cpu5sec
     5  pdsn_osler_stats_schema: 1231339742, .0, 1, 0, 10, 2, 1, 0, 0, 0, 0, 2, ~, ~, ~,
~, ~, ~, ~, ~, ~, ~, ~, ~,  ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~,
1, 0, 2, 9, PDSN_OSLER, 0, 25000, 2, 6000, 100, 1, 1, 1, 1, 4.0, 0
     6  pdsn_osler_stats_schema: 1231340042, .0, 1, 0, 10, 2, 1, 0, 0, 0, 0, 2, ~, ~, ~,
~, ~, ~, ~, ~, ~, ~, ~, ~,  ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~,
1, 0, 2, 9, PDSN_OSLER, 0, 25000, 2, 6000, 100, 1, 1, 1, 1, 4.0, 0
     7  pdsn_osler_stats_schema: 1231340342, .0, 1, 0, 10, 2, 1, 0, 0, 0, 0, 2, ~, ~, ~,
~, ~, ~, ~, ~, ~, ~, ~, ~,  ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~, ~,
1, 0, 2, 9, PDSN_OSLER, 0, 25000, 2, 6000, 100, 1, 1, 1, 1, 4.0, 0
     8 Global: PDSN_OSLER, 20090107, 150252, 200509, 0%, 0%, 0%
```

RCAL Functionality

For some of the show commands it is not possible to send bulk data using IPC. Though there is a facility to send data continuously, it is not feasible when more data must be sent to PCOP. For these types of show outputs, RCAL functionality is used.

The debug commands are executed on the TCOPs and the trace gets displayed from the PCOP. RCAL functionality is used to display the debug outputs. You need to look into the session information and find out if it is feasible to send the session related information using IPC; if not, you need the RCAL functionality to display the information.

The sample output of RCAL:

Let us assume there are 10 sessions opened and they are distributed among the TCOPs:

```
Router# show cdma pdsn session brief

----------- Slot 7/CPU 4, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09880456745     50.1.1.1                451 00:00:41 OPN      0     1 Virtual-Access2.1
09880456795     50.1.1.1                501 00:00:22 OPN      0     1 Virtual-Access2.2



----------- Slot 7/CPU 5, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09880456345     50.1.1.1                 51 00:05:28 OPN      0     1 Virtual-Access2.1
09880456395     50.1.1.1                101 00:04:42 OPN      0     1 Virtual-Access2.2



----------- Slot 7/CPU 6, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09880456445     50.1.1.1                151 00:04:22 OPN      0     1 Virtual-Access2.1
09880456495     50.1.1.1                201 00:03:52 OPN      0     1 Virtual-Access2.2



----------- Slot 7/CPU 7, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09880456295     50.1.1.1                  1 00:06:05 OPN      0     1 Virtual-Access2.1



----------- Slot 7/CPU 8, show cdma pdsn session brief -------------
MSID            PCF IP Address          PSI      Age  St SFlows Flows Interface
09880456545     50.1.1.1                251 00:03:15 OPN      0     1 Virtual-Access2.1
09880456595     50.1.1.1                301 00:02:57 OPN      0     1 Virtual-Access2.2
09880456645     50.1.1.1                351 00:02:33 OPN      0     1 Virtual-Access2.3


Router#
```

Following commands, when executed, displays the respective outputs as shown in the sample RCAL output.

- show alignment
- show aaa sessions
- show aaa subscriber profile
- show aaa user all

- show buffers
- show ccm
- show checkpoint
- show cdma pdsn accounting
- show cdma pdsn ahdlc
- show cdma pdsn flow
- show cdma pdsn redundancy
- show cdma pdsn resource
- show cdma pdsn session
- show fastblk
- show idb
- show interfaces
- show ip mobile proxy
- show ip mobile secure
- show ip mobile violation
- show ip mobile visitor
- show ip route
- show ip interface
- show ip mobile interface
- show ip mobile globals
- show ip traffic
- show ip local policy
- show ip vrf
- show ip mobile visitor ha-addr
- show ip mobile tunnel
- show ip mobile traffic
- show memory
- show policy-map apn
- show processes
- show l2tp counter tunnel
- show l2tp tunnel
- show l2tp session
- show l2tp class
- show l2tp memory
- show l2tp counters tunnel id
- show l2tun session
- show l2tun tunnel
- show l2tun counters tunnel l2tp all

- show l2tun counters tunnel l2tp id
- show radius statistics
- show radius server-group all
- show sami health-monitoring
- show sss sessions
- show sss circuits
- show tech-support page
- show tech-support password page
- show tech-support
- show vpdn session
- show vpdn tunnel
- show vpdn history failure
- show vrf

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 11 describes the product documentation that is available.

Table 11 Product Documentation

Document Title	Available Formats
Command Reference for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR1	• PDF on the documentation CD-ROM • On Cisco.com at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/command/reference_xr1/pdsn_5_1cr.html

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 12 describes the additional documentation that is available.

Table 12 Related Documentation

Document Title	Available Formats
Cisco Packet Data Serving Node Release 5.1 for Cisco IOS Release 12.4(22)XR1	• PDF on the documentation CD-ROM • On Cisco.com at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/feature/guide/pdsn5_1_fcs.html
Release Notes for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR1	• PDF on the documentation CD-ROM • On Cisco.com at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/release/notes/124_22xr1rn.html