Cisco PDSN Command Reference for IOS Release 12.4(15)XN

This section lists new and revised commands pertaining to the PDSN software. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

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

access list

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

cdma pdsn a10 ahdlc engine

To limit the number of Asynchronous High-Level Data Link Control (AHDLC) channel resources provided by the AHDLC engine, use the **cdma pdsn a10 ahdlc engine** command to in global configuration mode. To reset the number of AHDLC channel resources to the default, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

cdma pdsn a10 ahdlc trailer

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

cdma pdsn a10 ahdlc trailer

no cdma pdsn a10 ahdlc trailer

Syntax Description

There are no arguments or keywords for this command.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
Router (config)# no cdma pdsn a10 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 by default. The default value for **interval** is 3, and the default value for **attempts** is 3.

Command Modes

Global configuration

Command History

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

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

To configure the PDSN so that Point-to-Point Protocol (PPP) negotiation with an MN will start only after the traffic channel is assigned, (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

By default, this CLI is not enabled, therefore, the PDSN will initiate PPP negotiation immediately after a Registration Reply is sent to the initial Registration.Request.

When enabled, the default timeout interval is 10 seconds.

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 will start only after the traffic channel is assigned—after a Registration Request with airlink-start is received. If the airlink start is not received at all, the session will be torn down when timeout occurs.By default, this timeout interval is 10 seconds, or can be configured through the CLI.

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 will be at t1+10. It is likely that the uptime for the call is not more than 10 seconds since t2 > t1. So the call will be checked at the next run (t1+10+10). Thus, the variation is between 1 and 10.

Examples

The following example illustrates 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

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Examples

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

```
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 specifies that the A10 interface will 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 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 police downstream

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

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

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

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

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

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

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

Syntax Description

There are no keywords or variable for this command.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

cdma pdsn a11 dormant sdb-indication gre-flags

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

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

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

Syntax Description

Command	Description
group-number	Specifies the classified match criteria.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

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

Syntax Description

Command	Description
group-number	Specifies the classified match criteria.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

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

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

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

cdma pdsn a11 mandate presence airlink-setup

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

cdma pdsn a11 mandate presence airlink-setup

no cdma pdsn a11 mandate presence airlink-setup

Syntax Description

This command has no keywords or variables.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

```
router# cdma pdsn a11 mandate presence airlink-setup
```

cdma pdsn a11 receive de-reg send-termreq

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

cdma pdsn a11 receive de-reg send-termreq

no cdma pdsn a11 receive de-reg send-termreq

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

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

Examples

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

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

cdma pdsn a11 reject airlink-start active

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

cdma pdsn a11 reject airlink-start active

no cdma pdsn a11 reject airlink-start active

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command Modes

Global configuration

Command History

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

Examples

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

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

cdma pdsn a11 reject airlink-stop dormant

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

cdma pdsn a11 reject airlink-stop dormant

no cdma pdsn a11 reject airlink-stop dormant

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command Modes

Global configuration

Command History

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

Examples

The following example illustrates the **cdma pdsn a11 reject airlink-stop dormant** command:

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

cdma pdsn a11 session-update

To enable the A11 Session update feature on the PDSN, and to send an A11 session update for either the Always On, or 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 enables both the **always-on** and **rn-pdit** attributes:

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

cdma pdsn 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 the 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

This command has no arguments or keywords.

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 illustrates how to configure 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

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example sets the local time in Korea:

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

Related Commands

Command	Description
clock timezone	Specifies the hours and minutes (optional) difference between the local time zone and UTC.
cdma pdsn accounting send start-stop	Causes the PDSN to send: • 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)

cdma pdsn accounting prepaid

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

cdma pdsn accounting prepaid [volume | duration]

no cdma pdsn accounting prepaid [volume | duration]

Syntax Description

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

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

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

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

cdma pdsn accounting prepaid threshold

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

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

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

Syntax Description

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

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Examples

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

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

cdma pdsn accounting send cdma-ip-tech

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History

Release	Modification
12.1XC	This command was introduced.

Examples

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

cdma pdsn accounting send ipv6-flows

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

cdma pdsn accounting send ipv6-flows *number*

no cdma pdsn accounting send ipv6-flows *number*

Syntax Description

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

Examples

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

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

cdma pdsn accounting send start-stop

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

When this feature is enabled, the PDSN will send:

- An Accounting Stop record when it receives an active stop airlink record (dormant state).
- An Accounting Start record when it receives an active start airlink record (active state).

Examples

The following example starts sending PDSN accounting events:

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

Related Commands

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

cdma pdsn accounting time-of-day

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

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

no cdma pdsn accounting time-of-day

Syntax Description

hh:mm:ss	Hour:minutes:seconds.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
clock set	Sets the system clock.
debug cdma pdsn accounting time-of-day	Displays debug information for the command.
show clock	Displays the system clock.
cdma pdsn accounting send start-stop	Causes the PDSN to send: • 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)

cdma pdsn age-idle-users

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

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

no cdma pdsn age-idle-users

Syntax Description

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

Defaults

By default, no idle users are aged out.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

cdma pdsn attribute send

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

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

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

Syntax Description

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

Usage Guidelines

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

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

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

similarly

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

Examples

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

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

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

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

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

cdma pdsn attribute send a3

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

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

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

Syntax Description

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

Defaults

No default values

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX1	This command was introduced.

Examples

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

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

cdma pdsn attribute send meid-optional

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

cdma pdsn attribute send meid-optional

no cdma pdsn attribute send meid-optional

Syntax Description

There are no arguments of keywords for this command.

Defaults

No default values

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX1	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

cdma pdsn cluster controller

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

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

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

Syntax Description

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

Defaults

The timeout default value is 300 seconds.

Command Modes

Global configuration

Command History

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

Examples

The following example enables the cdma cluster controller:

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

cdma pdsn cluster controller closed-rp

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

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

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

Syntax Description

vpdn-group	VPDN group to be used for establishment of the controller-member VPDN tunnels.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example illustrates the **cdma pdsn cluster controller closed-rp** command:

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

cdma pdsn cluster controller member periodic-update

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

cdma pdsn cluster controller member periodic-update

no cdma pdsn cluster controller member periodic-update

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)ZB1	This command was introduced.

Examples

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

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

cdma pdsn cluster controller session-high

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

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

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

Syntax Description

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

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

cdma pdsn cluster controller session-low

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

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

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 illustrates 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* | **queueing** | **timeout** *seconds* [**window** *number*] | **window** *number*]

no cdma pdsn cluster member [**controller** *ipadd* | **interface** *interface-name* | **prohibit** *type* | **queueing** | **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.
queueing	Request queueing for member.
timeout	The time the cluster controller waits to seek a member when there is no reply from that cluster member. The range is between 10 and 600 seconds, and the default value is 300 seconds.
window *number*	The number of sequential seek messages sent to a cluster member before it is presumed offline.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables a cdma pdsn cluster member:

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

cdma pdsn cluster member periodic-update

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

cdma pdsn cluster member periodic-update *time*

no cdma pdsn cluster member periodic-update *time*

Syntax Description

time	The time between when the member sends periodic bulk-updates. The time can be between 300 to 3000 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 illustrates 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. To disable this feature, use the **no** form of the command.

cdma pdsn cluster member prohibit administratively

no cdma pdsn cluster member prohibit administratively

Syntax Description

This command has no arguments or keywords.

Defaults

There are 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 sync. If you choose to not use the HSRP address, and instead use a loopback address, issue this command.

The status of the member will be 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 command illustrates 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 function.

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

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Examples

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

```
router# cdma pdsn compliance is835a
```

cdma pdsn compliance iosv4.1 session-reference

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

cdma pdsn compliance iosv4.1 session-reference

no cdma pdsn compliance iosv4.1 session-reference

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration.

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn debug show-conditions

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

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

cdma pdsn failure-history

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

cdma pdsn failure-history *entries*

no cdma pdsn failure-history

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn ingress-address-filtering

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

cdma pdsn ingress-address-filtering

no cdma pdsn ingress-address-filtering

Syntax Description

This command has no arguments or keywords.

Defaults

Ingress address filtering is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables ingress address filtering:

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

Related Commands

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

cdma pdsn ipv6

To enable the PDSN IPv6 functionality, use the cdma pdsn ipv6 command in global configuration mode. Use the now form of the command to disable this function.

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

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

Syntax Description

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

cdma pdsn maximum pcf

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

cdma pdsn maximum pcf *maxpcf*

no cdma pdsn maximum pcf

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example specifies that 200 PCFs can be sent:

```
cdma pdsn maximum pcf 200
```

Related Commands

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

cdma pdsn maximum sessions

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

cdma pdsn maximum sessions *maxsessions*

no cdma pdsn maximum sessions

Syntax Description

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

Defaults

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

Command Modes

Global Configuration.

Command History

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

Usage Guidelines

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

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

Examples

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

```
cdma pdsn maximum sessions 100
```

Related Commands

Command	Description
show cdma pdsn session	Displays PDSN session information.

cdma pdsn mobile-advertisement-burst

To configure the number and interval of Agent Advertisements that a PDSN FA can send, use the **cdma pdsn mobile-advertisement-burst** command in 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 will be used for any parameters not already configured on the virtual template.

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

Examples

The following example configures PDSN FA advertisement:

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

Related Commands

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

cdma pdsn msid-authentication

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

cdma pdsn msid-authentication [**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 enables MSID-based authentication and access:

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

Related Commands

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

cdma pdsn 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 illustrates 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 pcf default closed-rp

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

cdma pdsn pcf default closed-rp

no cdma pdsn pcf default closed-rp

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default setting is that Closed-RP is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

cdma pdsn radius disconnect

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

cdma pdsn radius disconnect [nai]

no cdma pdsn radius disconnect [nai]

Syntax Description

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

Defaults

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

Command Modes

Global Configuration

Command History

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

Usage Guidelines

By default the PDSN will not process a Disconnect Request received with only NAI attribute. In a Service provider environment all simple IP sessions can be opened with the same user-name (and in case of Resource Management for sessions), therefore, a session identification attribute will be sent in 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 will set 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 illustrates the **cdma pdsn radius disconnect** command:

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

cdma pdsn redundancy

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

cdma pdsn redundancy

no cdma pdsn redundancy

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default setting is that PDSN redundancy is disabled.

Command Modes

Global configuration

Command History

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

Examples

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

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

cdma pdsn redundancy accounting send vsa swact

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

cdma pdsn redundancy accounting send vsa swact

no cdma pdsn redundancy accounting send vsa swact

Syntax Description

There are no keywords or arguments for this command.

Defaults

By default, this command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

cdma pdsn redundancy accounting update-periodic

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

cdma pdsn redundancy accounting [update-periodic]

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

Syntax Description

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

Defaults

By default, this command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

cdma pdsn retransmit a11-update

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

cdma pdsn retransmit a11-update *number*

no cdma pdsn retransmit a11-update

Syntax Description

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

Defaults

5 retransmissions.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn secure cluster

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

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

no cdma pdsn secure cluster

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn secure pcf

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

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

no cdma pdsn secure pcf

Syntax Description

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

Defaults

There are no default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

cdma pdsn selection interface

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

cdma pdsn selection interface *interface_name*

no cdma pdsn selection interface

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

cdma pdsn selection keepalive

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

cdma pdsn selection keepalive *value*

no cdma pdsn selection keepalive

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Examples

The following example configures a keepalive value of 200 seconds:

```
cdma pdsn selection keepalive 200
```

Related Commands

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

cdma pdsn selection load-balancing

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

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

no cdma pdsn selection load-balancing

Syntax Description

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

Defaults

The threshold value is 100 sessions.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn selection session-table-size

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

cdma pdsn selection session-table-size *size*

no cdma pdsn selection session-table-size

Syntax Description

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

Defaults

PDSN selection is disabled.

The default session table size is undefined.

Command Modes

Global Configuration

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn send-agent-adv

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

cdma pdsn send-agent-adv

no cdma pdsn send-agent-adv

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

This command is used with multiple flows.

Examples

The following example enables agent advertisements to be sent:

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

Related Commands

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

cdma pdsn timeout

To configure a variety of differnent 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 is configurable using this command.

Examples

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

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

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

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 will be retransmitted.
debug cdma pdsn a11	Displays debug messages for A11 interface errors, events, and packets.
show cdma pdsn	Displays the current status and configuration of the PDSN gateway.

cdma pdsn timeout mobile-ip-registration

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

cdma pdsn timeout mobile-ip-registration *timeout*

no cdma pdsn timeout mobile-ip-registration

Syntax Description

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

Defaults

5 seconds.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn virtual-template

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

cdma pdsn virtual-template *virtualtemplate_num*

no cdma pdsn virtual-template *virtualtemplate_num*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear cdma pdsn cluster controller session 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 output from 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

There are no default values for this command.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear cdma pdsn cluster member statistics

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

clear cdma pdsn cluster member statistics [queuing | statistics]

Syntax Description

queuing	Clears statistics associated with member queuing feature.

Defaults

There are no default values for this command.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear cdma pdsn redundancy statistics

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

clear cdma pdsn redundancy statistics

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

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 *1-500*
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 will clear the session for a given MSID.

Examples

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

Before counters are reset

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

Note Non-zero values of counters.

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

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

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

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

After the counters are reset

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

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

Note The counter values are zeroes.

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

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

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

Related Commands

Command	Description
show cdma pdsn statistics	Displays PDSN statistics.

clear ip mobile

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 will be removed for all addresses.
nai *string*	(Optional) Network access identifier of the mobile node.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how counters can be used 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# clear ip mobile traffic

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 will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	Indicates that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
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 will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

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

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

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 SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

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

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the 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 configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

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

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

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

```
Router# crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
```

```
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

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

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

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

```
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. To remove this command from the configuration, use the **no** form of this command.

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

no crypto map *map-name* **local-address** *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 will have its own security association database.
- The IP address of the local interface will be used as the local address for IPSec traffic originating from/destined to that interface.

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

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

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

Examples

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

```
interface S0

 crypto map mymap


interface S1

 crypto map mymap


crypto map mymap local-address loopback0
```

debug cdma pdsn a10 ahdlc

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

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

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

Syntax Description

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

Defaults

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

Command History

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

Examples

The following is sample output from the **debug cdma pdsn a10 ahdlc** command:

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

debug cdma pdsn a10 gre

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

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

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

Syntax Description

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

Defaults

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

Command History

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

Examples

The following is sample output from the **debug cdma pdsn a10 gre events tunnel-key** command:

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

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

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

debug cdma pdsn a10 ppp

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

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

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

Syntax Description

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

Defaults

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

Command History

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

Examples

The following is sample output from the **debug cdma pdsn a10 ppp** command:

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

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

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

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

debug cdma pdsn a11

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

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

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

Syntax Description

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

Defaults

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

Command History

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

Examples

The following is sample output from the **debug cdma pdsn a11**commands:

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


Router#debug cdma pdsn a11 packets events

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

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

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


Router#debug cdma pdsn a11 event mnid 000000000000001

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

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

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

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

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

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

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

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

debug cdma pdsn accounting

To display debug messages for accounting events, use the **debug cdma pdsn accounting** command in privileged EXEC mode. **debug cdma pdsn accounting**

debug cdma pdsn accounting

no debug cdma pdsn accounting

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn accounting** command:

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

debug cdma pdsn accounting flow

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

debug cdma pdsn accounting flow

no debug cdma pdsn accounting flow

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn accounting flow** command:

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

debug cdma pdsn accounting time-of-day

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

debug cdma pdsn accounting time-of-day

no debug cdma pdsn accounting time-of-day

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn accounting time-of-day** command:

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

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

debug cdma pdsn closed-rp

To display the error messages, event messages s and packets received, use the **debug cdma pdsn closed-rp** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug cdma pdsn closed-rp [error | events | packets]

no debug cdma pdsn closed-rp [error | events | packets]

Syntax Description

error	Displays closed-rp error messages.
events	Displays closed-rp events.
packets	Displays closed-rp packets.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn closed-rp** command:

```
Router#debug cdma pdsn closed-rp ?
  errors  CDMA PDSN closed-rp errors
  events  CDMA PDSN closed-rp events
  packet  CDMA PDSN closed-rp packet
```

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 is sample output from the **debug cdma pdsn cluster** command:

```
Router# debug cdma pdsn cluster ?
  message     Debug PDSN cluster controller messages
  redundancy  Debug PDSN cluster controller redundancy
```

debug cdma pdsn ipv6

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

debug cdma pdsn ipv6

no debug cdma pdsn ipv6

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

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

Usage Guidelines

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

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

debug cdma pdsn prepaid

To display debug messages about prepaid flow, use the **debug cdma pdsn prepaid** command in privileged EXEC mode. To disable 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 is sample output from 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^M
*Jan 13 17:46:56: CDMA-PREPAID: Preparing to send on-line Access Request^M
*Jan 13 17:46:56: CDMA-PREPAID: Update Reason: Threshold Reached^M
*Jan 13 17:46:56: CDMA-PREPAID: Added Username: mwtr_sip_user^M
*Jan 13 17:46:56: CDMA-PREPAID: Added Message Authenticator attribute^M
*Jan 13 17:46:56: CDMA-PREPAID: Added CLID: 00000000000002^M
*Jan 13 17:46:56: CDMA-PREPAID: Added Service Option: 245^M
*Jan 13 17:46:56: CDMA-PREPAID: Added Correlation ID: 0000001E^M
*Jan 13 17:46:56: CDMA-PREPAID: Adding PrepaidAccountingQuota(PPAQ):^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_QUOTA_ID_SUBTYPE[1]: value=1^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_SUBTYPE[2]: value=1000^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_OVERFLOW_SUBTYPE[3]: value=0^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_THRESHOLD_OVERFLOW_SUBTYPE[5]: value=0^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_UPDATE_REASON_SUBTYPE[8]: value=3^M
-------------------------------------------------------------------------------------

*Jan 13 17:46:56: CDMA-PREPAID: Received prepaid response: status 2^M
*Jan 13 17:46:56: CDMA-PREPAID: AAA authorised params being processed in on-line Access
Accept^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: addr^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: Framed-Protocol^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: service-type^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: routing^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-prepaid-accounting-capability^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-sess-term-capability^M
*Jan 13 17:46:56: CDMA-PREPAID: Attr received: cdma-prepaid-accounting-quota^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: AAA_AT_CDMA_PREPAID_ACCOUNTING_QUOTA^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_QUOTA_ID_SUBTYPE[1]: value=1^M
```

```
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_QUOTA_SUBTYPE[2]: value=4000^M
*Jan 13 17:46:56: CDMA/PREPAID/AAA: PPAQ_VOLUME_THRESHOLD_SUBTYPE[4]: value=3000^M
*Jan 13 17:46:56: CDMA-PREPAID: Volume Quota received: 4000 bytes with threshold 3000
bytes^M
*Jan 13 17:46:56: CDMA-PREPAID: Access Accept received and retrieved attributes
successfully^M
```

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

There are no default values for this command.

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. Use the **no** form of the command to disable debug messages.

debug cdma pdsn radius disconnect nai

no debug cdma pdsn radius disconnect nai

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

Examples

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

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

debug cdma pdsn redundancy attributes

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

debug cdma pdsn redundancy attributes

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy errors

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

debug cdma pdsn redundancy errors

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy events

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

debug cdma pdsn redundancy events

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy packets

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

debug cdma pdsn redundancy packets

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

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 is sample output from the **debug cdma pdsn resource-manager** command:

```
Router# debug cdma pdsn resource-manager ?
    errors  CDMA PDSN resource manager errors
    events  CDMA PDSN resource manager events
```

debug cdma pdsn selection

To display debug messages for the intelligent PDSN selection feature, use the **debug cdma pdsn selection** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

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

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

Syntax Description

errors	Displays pdsn selection errors.
events	Displays pdsn selection events.
packets	Displays transmitted or received packets.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn selection** command with the keyword **events** specified:

```
Router#debug cdma pdsn selection events
CDMA PDSN selection events debugging is on
Router#
00:27:46: CDMA-PSL: Message(IN) pdsn 51.4.2.40 interface 70.4.2.40
00:27:46:                Keepalive 10
00:27:46:                Count 0
00:27:46:                Capacity 16000
00:27:46:                Weight 0
00:27:46:                Hostname 11 7206-PDSN-2
00:27:46: CDMA-PSL: Reset keepalive, pdsn 51.4.2.40 current 10 new 10
00:27:46: CDMA-PSL: Message processed, pdsn 51.4.2.40 tsize 0 pendings 0
00:27:47: CDMA-PSL: Send KEEPALIVE, len 32
00:27:47: CDMA-PSL: Message(OUT) dest 224.0.0.11
00:27:47:                Keepalive 10
00:27:47:                Count 1
00:27:47:                Capacity 16000
00:27:47:                Weight 0
00:27:47:                Hostname 11 7206-PDSN-1
00:27:47: CDMA-PSL: RRQ sent, s=70.4.1.40 (FastEthernet0/1), d=224.0.0.11
```

debug cdma pdsn service-selection

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

debug cdma pdsn service-selection

no debug cdma pdsn service-selection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

The following is sample output from the **debug cdma pdsn service-selection** command:

```
Router# debug cdma pdsn service-selection
CDMA PDSN service provisioning debugging is on
Router#
1d02h:%LINK-3-UPDOWN:Interface Virtual-Access3, changed state to up
1d02h:Vi3 CDMA-SP:user_class=1, ms_ipaddr_req=1, apply_acl=0
1d02h:Vi3 CDMA-SP:Adding simple ip flow, user=bsip, mn=6.0.0.2,
1d02h:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access3,
changed state to up
```

debug cdma pdsn session

To display debug messages for Session Manager errors, events, and packets, use the **debug cdma pdsn session-manager** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

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

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

Syntax Description

errors	(Optional) Displays session protocol errors.
events	(Optional) Displays session events.

Defaults

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

Command History

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

Examples

The following is sample output from the **debug cdma pdsn session** command:

```
Router# debug cdma pdsn session events
CDMA PDSN session events debugging is on

Router# debug cdma pdsn session errors
CDMA PDSN session errors debugging is on

Router# show debug
CDMA:
  CDMA PDSN session events debugging is on
  CDMA PDSN session errors debugging is on
Router#
*Jan  1 00:22:27:CDMA-SM:create_session 5.5.5.5-4.4.4.5-2
*Jan  1 00:22:27:CDMA-SM:create_tunnel 5.5.5.5-4.4.4.5
*Jan  1 00:22:27:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Jan  1 00:22:29:CDMA-SM:create_flow mn=0.0.0.0, ha=8.8.8.8 nai=l2tp2@cisco.com
*Jan  1 00:22:30:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access1, changed
state to up
```

debug condition calling

To enable conditional debug feature for clustering, use the **debug condition calling** command in privileged EXEC mode. To remove the condition, use the **no** form of the command.

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 will appear without any filtering mechanism.

Command History

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

Examples

The following example illustrates 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 this command to remove the conditions.

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 will appear without any filtering mechanism.

Command History

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

Examples

The following example illustrates 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. Use the **no** form of the command to disable debugging functions.

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 is sample output from 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 unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.

debug ip mobile cdma ipsec

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

debug ip mobile cdma ipsec

no debug ip mobile cdma ipsec

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

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

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

interface cdma-Ix

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

interface cdma-Ix1

no interface cdma-Ix1

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
show interfaces	Displays statistics about the network interfaces.

ip mobile authentication ignore-spi

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

ip mobile authentication ignore-spi

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command Modes

Global configuration.

Command History

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

Examples

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

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

ip mobile bindupdate

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

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

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

Syntax Description

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

Defaults

No default values.

Command Modes

Global configuration.

Command History

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

Examples

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

```
Router# ip mobile bindupdate
```

ip mobile cdma imsi dynamic

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

ip mobile cdma imsi dynamic

no ip mobile cdma imsi dynamic

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF3	This command was introduced.

Examples

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

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

ip mobile cdma ipsec

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

ip mobile cdma ipsec

no ip mobile cdma ipsec

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

ip mobile foreign-agent

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on interface or no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated (**show ip mobile secure visitor** command). The registration bitflag is handled as described in Table 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 deregistration is accepted.

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

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent will 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 will advertise on interfaces configured with the **ip mobile foreign-service** command.

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

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

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

Related Commands

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

ip mobile foreign-service

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

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

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

Syntax Description

home-access *acl*	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99.
limit *number*	(Optional) Number of visitors allowed on interface. The Busy (B) bit will be advertised when the number of registered visitors reach this limit. Range is from 1 to 1000. Default is no limit.
registration-required	(Optional) Solicits registration from the mobile node even if it uses collocated care-of addresses. The Registration-required (R) bit will be advertised.
challenge	(Optional) Configures configure the FA challenge parameters.
timeout *value*	Challenge timeout in seconds. Possible values are 1 through 10.
window *num*	Maximum number of valid challenge values to maintain. Possible values are 1 through 10. The default is 2.
forward-mfce	Enables the FA to forward MFCE and mobile station-AAA to the HA.
reverse-tunnel [**mandatory**]	(Optional) Enables reverse tunneling on the FA.

Defaults

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

Command Modes

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 will be set in the agent advertisement, which is appended to the IRDP router advertisement whenever the foreign agent or home agent service is enabled on the interface.

Note The Registration-required bit only tells the visiting mobile node to register even if the visiting mobile node is using a 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 enables foreign agent service for up to 100 visitors:

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

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
cdma pdsn mobile-advertisement -burst	Configures FA advertisements.
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. To disable this feature, use the **no** form of the command.

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 illustrates the **ip mobile foreign-service revocation** command:

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

ip mobile prefix-length

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

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

This command has no arguments or keywords.

Defaults

The prefix-length extension is not appended.

Command Modes

Interface 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 appends 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. To remove the configuration, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No security association is specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip mobile 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 will be denied.

Examples

The following example sets the registration lifetime to 10 minutes on interface Ethernet 1 and 1 hour on interface Ethernet 2:

```
interface e1
ip mobile registration-lifetime 600
interface e2
ip mobile registration-lifetime 3600
```

Related Commands

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

ip mobile tunnel

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

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

Syntax Description

crypto map	Enables encryption/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 assigns and specifically names a crypto map:

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

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

ppp accm

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

ppp accm *number*

no ppp accm

Syntax Description

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

Defaults

The default value is 000A0000.

Command Modes

Interface Configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ppp accm 00000000
```

Related Commands

Command	Description
ppp authentication	Specifies CHAP or PAP authentication.

ppp authentication

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

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

no ppp authentication

Syntax Description

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

Defaults

PPP authentication is not enabled.

Command Modes

Interface Configuration

Command History

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

Usage Guidelines

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

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

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

Related Commands

Command	Description
ppp accm	Identifies the ACCM table.

service cdma pdsn

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

service cdma pdsn

no service cdma pdsn

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables PDSN service:

```
service cdma pdsn
```

Related Commands

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

show cdma pdsn

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

show cdma pdsn

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router#show cdma pdsn
PDSN software version 3.0, 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 20000 maximum)
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is disabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability disabled
Closed RP Capability not enabled
Number of pcfs connected 0,
Number of pcfs 3GPP2-RP 0, Closed-RP 0,
Number of sessions connected 0,
Number of sessions 3GPP2-RP 0, Closed-RP 0,
Number of sessions Active 0, Dormant 0,
Number of sessions using HDLCoGRE 0, using PPPoGRE 0
Simple IP flows 0, Mobile IP flows 0,
Proxy Mobile IP flows 0, VPDN flows 0
```

This example shows the new PPPoGRE counter statistics.

```
Router#show cdma pdsn
PDSN software version 2.0, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 5 sec
  A10 maximum lifetime allowed 65534 sec
  GRE sequencing is on
  Maximum PCFs limit not set
  Maximum sessions limit not set (default 20000 maximum)
  SNMP failure history table size 100
  MSID Authentication is disabled
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation is disabled
  Allow CI_ADD option during IPCP Phase  is disabled
  Aging of idle users disabled
  Radius Disconnect Capability disabled
  Closed RP Capability not enabled

  Number of pcfs connected 0,
  Number of sessions connected 0,
  Number of sessions using HDLCoGRE 0, using PPPoGRE 0
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 0, VPDN flows 0
```

The counter HDLCoGRE and PPPoGRE indicates number of sessions opened with AHDLC enabled and disabled respectively.

```
Router#show cdma pdsn session
Mobile Station ID IMSI 000000000000001
  PCF IP Address 13.1.102.17, PCF Session ID 1
  A10 connection time 00:00:07,  registration lifetime 65534 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime 65526 sec
  Always-On not enabled for the user
  Current Access network ID 000D-0166-11
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x880B
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.1, status OPN
  Service Option 1xEV-DO
  This session has 1 flow

  Flow service Simple, NAI sip1
    Mobile Node IP address 11.112.1.0
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
```

The GRE Protocol type field indicates if this is an PPPoGRE (0x880B) or HDLCoGRE (0x8881) session.

Cisco PDSN Release 3.0 adds the simple IPV6 information in the show output:

```
router# show cdma pdsn

PDSN software version 3.0, service is enabled
A11 registration-update timeout 1 sec, retransmissions 5
Mobile IP registration timeout 60 sec
A10 maximum lifetime allowed 65535 sec
GRE sequencing is on
Maximum PCFs limit not set
Maximum sessions limit not set (default 20000 maximum)
```

```
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is enabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability disabled
Closed RP Capability not enabled
IPv6 feature enabled
Number of pcfs connected 1,
Number of pcfs 3GPP2-RP 1, Closed-RP 0,
Number of sessions connected 1,
Number of sessions 3GPP2-RP 1, Closed-RP 0,
Number of sessions Active 1, Dormant 0,
Number of sessions using HDLCoGRE 1, using PPPoGRE 0
Simple IP flows 1, Mobile IP flows 0,
Proxy Mobile IP flows 0, VPDN flows 0
router#
```

Here is an example for the Cisco PDSN Release 3.5:

```
Router# show cdma pdsn

PDSN software version 3.5, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 10 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCF's limit set to 2000
  Maximum sessions limit not set (default 974 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 enabled
  Allow CI_ADD option during IPCP Phase  is disabled
  Aging of idle users disabled
  Radius Disconnect Capability enabled

  Number of pcfs connected 0,
  Number of pcfs 3GPP2-RP 0,
  Number of sessions connected 0,
  Number of sessions 3GPP2-RP 0,
  Number of sessions Active 0, Dormant 0,
  Number of sessions using HDLCoGRE 0, using PPPoGRE 0
```

show cdma pdsn accounting

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

show cdma pdsn accounting

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(14)YX	IPV6 UDR show output was added.

Usage Guidelines

The counter names appear in abbreviated format.

Examples

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

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

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

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

 UDR for flow
    Mobile Node IP address 15.0.0.4

    B - B1:15.0.0.4 B2:mwts-mip-p1-user122@ispxyz.com
```

```
   C - ' 'C2:37
   D - D1:0.0.0.0
   F - F11:02 F12:01 F13:00
   G - G1:0 G2:0 G4:1023906326
   Packets- in:0 out:0

UDR for flow
   Mobile Node IP address 15.0.0.5

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

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

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

UDR for flow
   Mobile Node IP address 6.0.0.5

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

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

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

UDR for flow
   Mobile Node IP address 6.0.0.14

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

PDSN-6500#
```

Release 3.0 includes the following IPv6 UDR information:

- Include the IPv4 or IPv6 address of the Mobile Node
- B3 – IPv6 prefix (64-bits)
- B4 – IPv6 interface-id (64-bits)

```
UDR for session

    session ID: 1
    Mobile Station ID IMSI 00000000000101

    A - A1:00000000000101 A2:
    C - C3:0
    D - D3:4.0.0.1 D4:000000000000
    E - E1:0000
    F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00 F15:0
    G - G3:0 G8:0 G9:1 G10:0 G11:0 G12:0 G13:0 G14:530 G15:0 G16:0
    I - I1:0 I4:0
    Y - Y2:1

UDR for flow

    Mobile Node IP address 2001:420:10:0:211:20FF:FE43:61C

    B - B2:mwts-uc1-np-user1 B3: 2001:420:10:0 B4: 211:20FF:FE43:61C
    C - C1:0011 C2:7 C4:0
    D - D1:0.0.0.0
    F - F11:01 F12:00 F13:00
    G - G1:0 G2:0 G4:1131720576

    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.

Examples

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

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

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

 UDR for flow
    Mobile Node IP address 15.0.0.3

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

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

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

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

 UDR for flow
    Mobile Node IP address 6.0.0.5

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

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

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

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

 UDR for flow
    Mobile Node IP address 6.0.0.14

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

PDSN-6500#
```

show cdma pdsn accounting session

To display the accounting information for the session identified by the msid, and the 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 output from the **show cdma pdsn accounting session** command:

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

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

 UDR for flow
    Mobile Node IP address 6.0.0.14

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

show cdma pdsn accounting session detail

To display the accounting information (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.

Usage Guidelines

The counter names appear in abbreviated format.

Examples

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

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

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

```
 UDR for flow
    Mobile Node IP address 6.0.0.14

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

PDSN-6500#
```

show cdma pdsn accounting session flow

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The counter names appear in abbreviated format.

Examples

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

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

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

PDSN-6500#
```

show cdma pdsn accounting session flow user

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

 UDR for flow
    Mobile Node IP address 15.0.0.3

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

PDSN-6500#
```

show cdma pdsn ahdlc

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

show cdma pdsn cluster controller

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

show cdma pdsn cluster controller {**closed rp** | **configuration** | **member** | **queueing** | **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.
queueing	Displays statistics for request queueing on the 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.

Examples

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

```
Router# show cdma pdsn cluster controller configuration
sh cdma pdsn cluster controller config
cluster interface FastEthernet0/0
no R-P signaling proxy
timeout to seek member = 10 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
this PDSN cluster controller is configured

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

show cdma pdsn cluster controller member

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

show cdma pdsn cluster controller member *ipaddr* [**session** | **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.

Examples

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

```
Router# show cdma pdsn cluster controller member 1.2.3.4 session
Session Rec ID: 00000100003   Member-Ack received:  TRUE   Age: 24 secs
Session Rec ID: 00000100004   Member-Ack received:  TRUE   Age: 24 secs
Session Rec ID: 00000100005   Member-Ack received:  TRUE   Age: 24 secs
```

show cdma pdsn cluster controller session

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

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

Syntax Description

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

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

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

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

show cdma pdsn cluster controller statistics

To display the IP addresses of the members that registered with a specific controller, 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 output from the **show cdma pdsn controller statistics** command:

```
Router# show cdma pdsn cluster controller statistics

Sample Output:
Controller-Member Interface:
  Cluster Reg Request rcvd 12, accepted 3, discarded 9
  Cluster Reg Request sent 0
  Cluster Reg Reply rcvd 0, accepted 0, discarded 0

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 9
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0

  Controller seek requests rcvd 3, replies sent 3
  Member seek requests sent 0, replies rcvd 0
  Member state transition msgs rcvd 0, replies sent 0
    ready 0, Administratively prohibited 0
  Total A11 Reg Requests forwarded 0
    A11 Reg Requests orig forwarded 0, retry forwarded 0
    Session-Up from member 0, Session-Down from member 0
    No Acknowledgement from member 0

Controller Redundancy Interface:
    Update rcvd 0 sent 6 orig sent 3 fail 0
```

```
UpdateAck rcvd 1 sent 0
DownloadReq rcvd 0 sent 11 orig sent 10 fail 0
DownloadReply rcvd 11 sent 0 orig sent 0 fail 0 drop 0
DownloadAck rcvd 0 sent 11 drop 0

Errors: Authentication failed 0 ID mismatch 0
        Ignored due to no redundancy configuration 0
```

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** | **queueing** | **statistics**}

Syntax Description

configuration	Displays configuration information associated with the cluster member.
queueing	Displays statistics for request queueing on the member.
statistics	Displays various statistics collected on cluster member signaling messages with the cluster controller.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show cdma pdsn cluster member statistics

Sample Output:
Controller-Member Interface:
  Cluster Reg Request rcvd 10, accepted 10, discarded 0
  Cluster Reg Request sent 23
  Cluster Reg Reply rcvd 11, accepted 11, discarded 0

  Cluster Reg message errors:
    Reg Request rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0, Unrecognized application type 0
    Unrecognized data type 0

    Reg Reply rcvd: Authentication failed 0, ID mismatch 0
    Unrecognized extension 0

  Reg Req not sent: Interface cdma-Ix not configured 0
  Invalid Reg message type 0

  Controller seek requests rcvd 10, replies sent 10
  Member seek requests sent 23, replies rcvd 11
  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
```

show cdma pdsn flow

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

show cdma pdsn flow {mn-ip-address *ip_address* **| 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.

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.

Examples

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

```
Router# show cdma pdsn flow

MSID            NAI                                Type         MN IP Address    St
100000000000099 sim1                               Simple       100.4.1.1        ACT
200000000000047 sim1                               Simple       100.4.1.2        ACT
100000000000100 sim1                               Simple       100.4.1.40       ACT
200000000000048 sim1                               Simple       100.4.1.3        ACT
100000000000101 sim1                               Simple       100.4.1.5        ACT
200000000000049 sim1                               Simple       100.4.1.4        ACT
100000000000102 sim1                               Simple       100.4.1.6        ACT
200000000000050 sim1                               Simple       100.4.1.7        ACT
100000000000103 sim1                               Simple       100.4.1.9        ACT
200000000000051 sim1                               Simple       100.4.1.8        ACT
100000000000104 sim1                               Simple       100.4.1.11       ACT
200000000000052 sim1                               Simple       100.4.1.10       ACT
100000000000105 sim1                               Simple       100.4.1.12       ACT
200000000000053 sim1                               Simple       100.4.1.13       ACT
300000000000008 sim1                               Simple       100.4.1.14       ACT
100000000000106 sim1                               Simple       100.4.1.15       ACT
200000000000054 sim1                               Simple       100.4.1.16       ACT
```

```
300000000000009 sim1                            Simple       100.4.1.17       ACT
100000000000107 sim1                            Simple       100.4.1.19       ACT
200000000000055 sim1                            Simple       100.4.1.18       ACT
100000000000122 sim1                            Simple       100.4.1.21       ACT
200000000000070 sim1                            Simple       100.4.1.20       ACT
300000000000025 sim1                            Simple       100.4.1.22       ACT
100000000000123 sim1                            Simple       100.4.1.24       ACT
200000000000071 sim1                            Simple       100.4.1.23       ACT
300000000000026 sim1                            Simple       100.4.1.25       ACT
100000000000124 sim1                            Simple       100.4.1.26       ACT
200000000000072 sim1                            Simple       100.4.1.27       ACT
300000000000027 sim1                            Simple       100.4.1.28       ACT
100000000000125 sim1                            Simple       100.4.1.29       ACT
200000000000073 sim1                            Simple       100.4.1.30       ACT
300000000000028 sim1                            Simple       100.4.1.31       ACT
100000000000126 sim1                            Simple       100.4.1.33       ACT
200000000000074 sim1                            Simple       100.4.1.32       ACT
300000000000029 sim1                            Simple       100.4.1.34       ACT
100000000000127 sim1                            Simple       100.4.1.36       ACT
200000000000075 sim1                            Simple       100.4.1.35       ACT
300000000000030 sim1                            Simple       100.4.1.37       ACT
100000000000128 sim1                            Simple       100.4.1.39       ACT
200000000000076 sim1                            Simple       100.4.1.38       ACT
300000000000101 sim1                            Simple       100.4.1.41       ACT
100000000000199 sim1                            Simple       100.4.1.43       ACT
200000000000147 sim1                            Simple       100.4.1.42       ACT
300000000000102 sim1                            Simple       100.4.1.44       ACT
100000000000200 sim1                            Simple       100.4.1.46       ACT
 --More--
```

A new option, **mn-ipv6-address**, is 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
```

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 output from the **show cdma pdsn flow service simple-ipv6** command:

```
Router# show cdma pdsn flow service simple-ipv6

MSID NAI Type MN IP

Address St

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.

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

Examples

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

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

Table 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.
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 will be active.

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

Table 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
spi *spi_value*	Security Parameter Index, a 4-byte hex index within the security association that selects the specific security parameters to be used.
Timestamp +/- *value*	Maximum difference allowed between the timestamp received in the A11 message and the system time on the PDSN for the A11 message to be accepted.
key {ascii|hex} *key*	The shared secret key for the security associations

show cdma pdsn redundancy

To show whether or not the PDSN redundancy feature is enabled or not, use the **show cdma pdsn redundancy** command in Privileged EXEC mode.

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example illustrates the output for the **show cdma pdsn redundancy** command:

```
router# show cdma pdsn redundancy

CDMA PDSN Redundancy is enabled
CDMA PDSN Session Redundancy system status
PDSN state = ACTIVE
PDSN-peer state = STANDBY HOT
CDMA PDSN Session Redundancy Statistics
Last clearing of cumulative counters never
Synced to standby Current
since peer up Connected
Sessions 1 2
SIP Flows 0 0
MIP Flows 1 0
PMIP Flows 0 0
```

show cdma pdsn redundancy statistics

To display a variety of information about the sessions and the associated flows that have been/are synchronized to/from the standby/active, use show **cdma pdsn redundancy statistics** command in privileged EXEC mode.

show cdma pdsn redundancy statistics

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(8)XW	Prepaid output was included in examples.

Usage Guidelines

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

Examples

The following output is displayed with the **show cdma pdsn redundancy statistics** command:

```
Router# show cdma pdsn redundancy statistics
Last clearing of cumulative counters never Number of messages sent to standby:

Session Events
Up 10, Down 39, Reregistration 0
Handoff 0, PPP renegotiation 0
Flow Events
Simple IP Up 1, Down 1
Mobile IP Up 7, Down 7
Proxy Mobile IP Up 2, Down 2
Accouting Events
Update 0, Flow Start0, Stop 0
Active to Dormant 0, Dormant to Active 0
```

show cdma pdsn resource

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

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

Syntax Description

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

Defaults

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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


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

show cdma pdsn session

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

show cdma pdsn session [**brief** | **always-on** | **dormant** | **mn-ip-address** *address* | **mn-ipv6-address** *address* | **msid** *number* | **user** *nai* | **prepaid**]

Syntax Description

brief	(Optional) Displays a summary of all sessions.
always-on	Displays CDMA PDSN always-on sessions information
dormant	(Optional) Displays information about dormant PDSN sessions.
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.
user *nai*	(Optional) Displays information for the specified NAI.
prepaid	(Optional) Displays information about prepaid flows.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(2)XC	The parameters of this command were altered.
12.2(8)BY	The **prepaid** variable was introduced.
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.
12.4(15)XN	QoS and Policing session information was included in the examples.

Examples

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

```
Router#show cdma pdsn session
Mobile Station ID IMSI 00000000001
PCF IP Address 13.1.102.11, ID local 31994, remote 18555
Session ID local 2, remote 17, state established
  A10 connection time 00:00:07,  registration lifetime 65535 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime INFINITE
  Current Access network ID 000D-010A-6A
  Last airlink record received is Active Start, airlink is active
  GRE sequence number transmit 7, receive 0
  Using interface Virtual-Access2.1, status ACT
```

```
  Using AHDLC engine on slot 0, channel ID 0
  Service Option Undefined
  Policier Upstream CIR(bps) 8000,
                   Normal Burst(bytes) 4000,
                   Excess Burst(bytes) 8000
           Downstream CIR(bps) 8000,
                     Normal Burst(bytes) 4000,
                     Excess Burst(bytes) 8000
  This session has 1 flow

  Flow service Simple, NAI nai-qos1
    Mobile Node IP address 11.2.1.1
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0
    Quota Details of Prepaid Service based on Volume:
      Quota Id : 257
      Allocated: 50000 bytes
      Threshold: 40000 bytes
      Consumed : 20000 bytes

    Quota Details of Prepaid Service based on Duration:
      Quota Id : 4522002
      Allocated: 60 sec
      Threshold: 45 sec
      Consumed : 41 sec

    Qos Allowed Diffserv class A,E,O
        Max Class Selection Marking 40
        Reverse Tunneling Marking 26
```

Cisco PDSN Release 3.0 adds the following Simple IPV6 information:

```
Router#show cdma pdsn session
Mobile Station ID IMSI 00000000000101
PCF IP Address 4.0.0.1, PCF Session ID 1
A10 connection time 00:03:55, 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 0004-0000-01
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 11, receive 0
Using interface Virtual-Access2.1, status OPN
Using AHDLC engine on slot 0, channel ID 5
Service Option Undefined
This session has 1 flow
Flow service Simple-ipv6, NAI mwts-uc1-np-user1
Mobile Node IPv6 address 2001:420:10:0:211:20FF:FE43:61C
IPv6 Packets in 0, bytes in 0
IPv6 Packets out 0, bytes out 0
router#
```

This example shows the PDSN 3.5 session related subscriber QoS profile and policing details:

```
Router#show cdma pdsn session
Mobile Station ID IMSI 123456789123457
  PCF IP Address 5.1.1.46, PCF Session ID 1
  A10 connection time 119:19:10, registration lifetime 1800 sec
  Number of successful A11 re-registrations 357
  Remaining session lifetime 650 sec
  Always-On not enabled for the user
  Current Access network ID 0005-0101-2E
  Last airlink record received is Unknown, airlink is active
```

```
GRE protocol type is 0x8881
GRE sequence number transmit 9, receive 7
Using interface Virtual-Access2.1, status OPN
Using AHDLC engine on slot 0, channel ID 4381
Service Option Ev-DO
Police Downstream CIR(bps) 8000,
  Normal Burst(bytes) 1500, Excess Burst(bytes) 3000
  Packets Conformed 0 Exceeded 0 Dropped packets 0
This session has 1 flow
Session Airlink State Active
QoS Parameters:
  Max Aggregate Bandwidth: 8000
  Home Area              : 10
  Inter User Priority    : 15

Flow service Simple, NAI NAI gSIP1@xxx.com
  Mobile Node IP address 32.1.35.203
  Packets in 0, bytes in 0
  Packets out 0, bytes out
```

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.

show cdma pdsn statistics [**ahdlc** | **rp** [**pcf** *ip address*] | **closed-rp** [**pcf** *ip address*] | **error**] [**ppp** [**pcf** *ip address*] [**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.
error	Displays all CDMA PDSN RP error statistics.
pcf *ip address*	The PCF IP address.
radius disconnect	Displays all RADIUS disconnect 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.

Examples

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

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

    Update sent 2, accepted 2, denied 0, not acked 0
    Initial Update sent 2, retransmissions 0
    Acknowledge received 2, discarded 0
    Update reason lifetime expiry 1, PPP termination 0, other 1
```

```
    Error: Unspecified 23 Administratively prohibited 0
      Authentication failed 4, Identification mismatch 4
      Poorly formed request 2


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

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

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

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

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

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

AHDLC:

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

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

  Deframing input 0 bytes, 0 paks
  Defaming output 0 bytes, 0 paks
```

```
  Deframing errors 0, insufficient memory 0,
        queue overflow 0, invalid size 0, CRC errors 0

RADIUS Disconnect:

router#show cdma pdsn statistics radius disconnect

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
```

In R3.0, the **show cdma pdsn statistics** command has been enhanced to include Closed-RP statistics. Here is a sample output:

```
PDSN#show cdma pdsn statistics ?
  ahdlc      AHDLC information
  closed-rp  CDMA PDSN closed-rp statistics
  ppp        CDMA PDSN ppp statistics
  prepaid    CDMA PDSN prepaid statistics
  radius     CDMA PDSN traffic statistics
  rp         CDMA PDSN RP statistics
  |          Output modifiers
  <cr>

PDSN#show cdma pdsn statistics
Last clearing of 'show cdma pdsn statistics' counters never

RP Interface:
    Reg Request rcvd 0, accepted 0, denied 0, discarded 0
    Initial Reg Request rcvd 0, accepted 0, denied 0, discarded 0
    Re-registration requests rcvd 0, accepted 0, denied 0, discarded 0
    Re-registration requests containing Active-Start 0, Active-Stop 0
    Handoff requests rcvd 0, accepted 0, denied 0, discarded 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
    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
    RP Session Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Session parameters not updated 0
    Poorly formed request 0

Service Option:

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

slot 0:
    AHDLC Engine Type: CDMA HDLC SW ENGINE
    Engine is ENABLED
    total channels: 20000, available channels: 20000
    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

Bandwidth policing:
  Policing installed 0 failure 0 uninstalled 0

ClosedRP Interface:
    Control packets rcvd 0, sent 0, resent 0, dropped 0
    ZLB rcvd 0, sent 0, resent 0, dropped 0
    SCCRQ rcvd 0, sent 0, resent 0, dropped 0
    SCCRP rcvd 0, sent 0, resent 0, dropped 0
    SCCCN rcvd 0, sent 0, resent 0, dropped 0
    StopCCN rcvd 0, sent 0, resent 0, dropped 0
    CDN rcvd 0, sent 0, resent 0, dropped 0
    Hello rcvd 0, sent 0, resent 0, dropped 0
    ICRQ rcvd 0, sent 0, resent 0, dropped 0
    ICRP rcvd 0, sent 0, resent 0, dropped 0
    ICCN rcvd 0, sent 0, resent 0, dropped 0
```

show cdma pdsn statistics prepaid

To display statistics related to all prepaid enabled flows, use the **show cdma pdsn statistics prepaid** command in Privileged EXEC mode.

show cdma pdsn statistics prepaid

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)XW	Prepaid output was included in examples.

Examples

Here is sample output of the **show cdma pdsn statistics prepaid** command:

```
router# show cdma pdsn statistics prepaid
Prepaid-related statistics:
Total prepaid flows opened: 0
Volume-based 0, Duration-based 0
Simple IP 0, VPDN 0, Proxy Mobile IP 0, Mobile IP 0
Total online Access Requests sent 0
Total online Access Response received 0
Accepted 0, Discarded 0, Timeout 0
Online Access Requests sent with Update Reason:
Pre-Initialization 0
Initial Request 0
Threshold Reached 0
Quota Reached 0
Remote Forced Disconnect 0
Client Service Termination 0
Main SI Released 0
SI not established 0
Tariff Switch Update 0
```

show ip mobile cdma ipsec

To display if IS835 IPSec security is enabled, use the **show ip mobile cdma ipsec** command in EXEC mode.

show ip mobile cdma ipsec

Syntax Description

There are no arguments or keywords for this command.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

Examples

The following example illustrates how to enable the **show ip mobile cdma ipsec** 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 arguments or keywords 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 illustrates how to enable the **show ip mobile cdma ipsec profile** command:

```
router# show ip mobile cdma ipsec profile
```

show ip mobile proxy

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

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

Syntax Description

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

Command Modes

EXEC

Command History

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

Usage Guidelines

None.

Examples

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

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

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

show ip mobile secure

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

show ip mobile secure {**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 is sample output from 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, then outbound SPI will be used when a response is sent.
MD5	Message Digest 5 authentication algorithm.
Prefix-suffix	Authentication mode.

Table 8 show ip mobile secure Field Descriptions

Field	Description
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

show ip mobile traffic

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

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ip mobile traffic

IP Mobility traffic:
Advertisements:
    Solicitations received 102
    Advertisements sent 13758, response to solicitation 102
Foreign Agent Registrations:
    Register requests rcvd 8580, valid 7243, forwarded 7243, denied 1009, ignored 328
    Register requests valid initial 7242, re-register 0, de-register 1
    Register requests forwarded initial 7242, re-register 0, de-register 1
    Register requests denied initial 1009, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0,  de-register 0
    Register replies rcvd 7242, forwarded 7234, bad 0, ignored 8
    Register replies rcvd initial 7241, re-register 0, de-register 1
    Register replies forwarded initial 7233, re-register 0, de-register 1
    Registration Errors:
      Unspecified 1005, HA unreachable 0
      Administrative prohibited 0, No resource 0
      Bad lifetime 0, Bad request form 0
      Unavailable encapsulation 0, Compression 0
      Unavailable reverse tunnel 0, Reverse tunnel mandatory 0
      Authentication failed MN 4, HA 0
      Received challenge/gen. authentication extension, feature not enabled 0
      Unknown challenge 1001, Missing challenge 0, Stale challenge 4
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
```

show ip mobile violation

To display information about security violations, use the **show ip mobile violation** EXEC command.

show ip mobile violation [*address* | **nai** *string*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC

Command History

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

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the **logging** global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the **show logging** command.

Examples

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

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1:
    Violations: 1, Last time: 06/18/97 01:16:47
    SPI: 300, Identification: B751B581.77FD0E40
    Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

Table 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.
Last time	Time of the most recent security violation for this peer.

Table 9 show ip mobile violation Field Descriptions (continued)

Field	Description
SPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the Mobile-Home Authentication Extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply.
Reason	Reason for the most recent security violation for this peer. Possible reasons are: • 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.

show ip mobile visitor [[**pending**] [*address* | **summary**] | **nai** *string*]

Syntax Description

pending	(Optional) Displays the pending registration table.
address	(Optional) IP address.
summary	(Optional) Displays all values in the table.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC

Command History

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

Usage Guidelines

The foreign agent updates the table containing the visitor list of the foreign agent in response to registration events from mobile nodes.

Examples

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

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
20.0.0.1:
    Interface Ethernet1/2, MAC addr 0060.837b.95ec
    IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
    HA addr 66.0.0.5, Identification B7510E60.64436B38
    Lifetime 08:20:00 (30000) Remaining 08:19:16
    Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
    Routing Options - (T)Reverse-tunnel
```

Table 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.

Table 10 show ip mobile visitor Field Descriptions (continued)

Field	Description
IP dest	Destination IP address of Registration Request of a visitor. When a foreign agent sends a reply to a visitor, the IP source address is set to this address, unless it is multicast or broadcast, in which case it is set to IP address of the output interface.
UDP src port	Source UDP port of Registration Request of the visitor.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime granted to the mobile node for this registration.
Remaining	The number of seconds remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Possible options are: • (S) Mult-binding • (B) Broadcast • (D) Direct-to-mobile station • (M) MinIP • (G) GRE • (V) VJH-compress • (T) Reverse-tunnel

show ipc sctp statistics

To display ipc sctp statistics, use the **show ipc sctp statistics** command.

show ipc sctp statistics

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

Sample show output for the **show ipc sctp** command:

```
router # show ipc sctp statistics
IPC default Zone:
 IPC association Id: 1
   SCTP Protocol Local: port: 6602 ip: 10.2.86.26
     keepalive  1500
     retransmit-timeout  300  600
     bundling 20
     cumulative-sack 200
     path-retransmit 4
     assoc-retransmit 4
     max-inbound-streams 2
     init-timeout 1000
     init-retransmit 8
     receive-window 24000
   SCTP Protocol Remote: port: 22 ip: 10.2.87.26
router #
```

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

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

Sample show output for 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 tech-support cdma pdsn

To display PDSN information that is useful to Cisco Customer Engineers for diagnosing problems, use the **show tech-support cdma pdsn** command in privileged EXEC mode.

show tech support cdma pdsn

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XS	This command was modified to include PDSN status.

Usage Guidelines

This command displays the output of several **show** commands. We recommend that you attach the output of this command whenever you submit a PDSN problem report.

Examples

The following example shows typical output of the **show tech-support cdma pdsn** command:

```
pdsn-6500#show tech-support cdma pdsn

------------------ show version ------------------

Cisco Internetwork Operating System Software
IOS (tm) 6500 Software (C6500-C5IS-M), Experimental Version 12.2(20020306:074931)
[user-dw91527 104]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 06-Mar-02 22:21 by user
Image text-base:0x600088E0, data-base:0x6169A000

ROM:System Bootstrap, Version 12.0(19990210:195103) [12.0XE 105], DEVELOPMENT SOFTWARE
BOOTLDR:6500 Software (C6500-BOOT-M), Version 12.0(3)T,  RELEASE SOFTWARE (fc1)

mwt10-7206a uptime is 20 minutes
System returned to ROM by reload at 23:17:59 UTC Wed Mar 6 2002
System image file is "tftp://223.255.254.254/user/c6500-c5is-mz.dw91527"

cisco 7206VXR (NPE300) processor (revision D) with 229376K/65536K bytes of memory.
Processor board ID 21302179
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.1

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
```

```
8 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
1 ATM network interface(s)
125K bytes of non-volatile configuration memory.

8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0


------------------ show running-config ------------------


Building configuration...

Current configuration :3015 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service cdma pdsn
!
hostname mwt10-7206a
!
aaa new-model
!
!
aaa authentication login default none
aaa authentication ppp default group radius
aaa authentication ppp VPDN group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network VPDN group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 10
aaa accounting network pdsn start-stop group radius
aaa session-id common
enable secret 5 <removed>
enable password <removed>
!
username abc password 0 <removed>
ip subnet-zero
no ip gratuitous-arps
ip cef
ip cef accounting per-prefix non-recursive prefix-length
!
!
!
ip ftp source-interface Ethernet2/0
no ip domain-lookup
!
vpdn enable
vpdn authen-before-forward
virtual-profile aaa
!
!
!
!
```

```
!
!
!
interface Loopback0
 ip address 6.0.0.1 255.0.0.0
!
interface CDMA-Ix1
 ip address 5.0.0.1 255.0.0.0
 tunnel source 5.0.0.1
 tunnel key 0
 tunnel sequence-datagrams
!
interface FastEthernet1/0
 ip address 4.0.0.101 255.0.0.0
 duplex half
 speed auto
 no cdp enable
!
interface Ethernet2/0
 ip address 7.0.0.1 255.0.0.0
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 ip address 150.1.10.4 255.255.0.0
 duplex half
 no cdp enable
!
interface Ethernet2/2
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/4
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/5
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet2/6
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
```

```
 no cdp enable
!
interface Ethernet2/7
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface ATM4/0
 no ip address
 no ip mroute-cache
 shutdown
 no atm ilmi-keepalive
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip mobile foreign-service challenge
 ip mobile foreign-service reverse-tunnel
 ip mobile registration-lifetime 65535
 no peer default ip address
 ppp authentication chap pap optional
!
router mobile
!
ip local pool ispabc-pool1 9.0.0.1 9.0.0.255
ip classless
ip route 10.0.0.0 255.0.0.0 7.0.0.2
no ip http server
ip pim bidir-enable
ip mobile foreign-agent care-of Ethernet2/0
ip mobile proxy-host nai mwts-mipp-np-user1@ispxyz.com flags 42
!
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
no cdp run
!
!
radius-server host 150.1.0.1 auth-port 1645 acct-port 1646 key <removed>
radius-server retransmit 3
radius-server optional-passwords
radius-server key <removed>
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdlc-engine 5 usable-channels 8000
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn msid-authentication
cdma pdsn selection interface Ethernet2/0
cdma pdsn secure pcf default spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii test
cdma pdsn secure pcf 4.0.0.1 spi 1000 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
```

```
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password <removed>
!
!
end


------------------ show cdma pdsn ------------------


PDSN software version 1.2, service is enabled

  A11 registration-update timeout 1 sec, retransmissions 5
  Mobile IP registration timeout 300 sec
  A10 maximum lifetime allowed 65535 sec
  GRE sequencing is on
  Maximum PCFs limit not set, maximum sessions limit not set
  SNMP failure history table size 100
  MSID Authentication is enabled
      Network code digits for IMSI 5, MIN 6, IRM 4
      Profile Password is cisco
  Ingress address filtering is disabled
  Sending Agent Adv in case of IPCP Address Negotiation  is disabled
  Aging of idle users disabled

  Number of pcfs connected 1
  Number of sessions connected 1,
    Simple IP flows 0, Mobile IP flows 0,
    Proxy Mobile IP flows 1


------------------ show ip interface brief ------------------


Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet1/0            4.0.0.101       YES NVRAM  up                    up
Ethernet2/0                7.0.0.1         YES manual up                    up
Ethernet2/1                150.1.10.4      YES NVRAM  up                    up
Ethernet2/2                unassigned      YES NVRAM  administratively down down
Ethernet2/3                unassigned      YES NVRAM  administratively down down
Ethernet2/4                unassigned      YES NVRAM  administratively down down
Ethernet2/5                unassigned      YES NVRAM  administratively down down
Ethernet2/6                unassigned      YES NVRAM  administratively down down
Ethernet2/7                unassigned      YES NVRAM  administratively down down
ATM4/0                     unassigned      YES NVRAM  administratively down down
Loopback0                  6.0.0.1         YES NVRAM  up                    up
CDMA-Ix1                   5.0.0.1         YES NVRAM  up                    up
Virtual-Template1          6.0.0.1         YES unset  down                  down
Virtual-Access1            unassigned      YES unset  up                    up
Mobile0                    unassigned      YES unset  up                    up
Tunnel0                    unassigned      YES unset  up                    up
Tunnel1                    7.0.0.1         YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
Virtual-Access3            unassigned      YES unset  up                    up
```

```
Virtual-Access3.1          6.0.0.1         YES unset  up                    up

------------------ show ip route ------------------


Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    4.0.0.0/8 is directly connected, FastEthernet1/0
C    5.0.0.0/8 is directly connected, CDMA-Ix1
C    6.0.0.0/8 is directly connected, Loopback0
C    7.0.0.0/8 is directly connected, Ethernet2/0
S    10.0.0.0/8 [1/0] via 7.0.0.2
C    150.1.0.0/16 is directly connected, Ethernet2/1
     30.0.0.0/32 is subnetted, 1 subnets
C       30.0.0.1 is directly connected, Virtual-Access3.1

------------------ show cdma pdsn session brief ------------------

MSID            PCF IP Address          PSI      Age  St Flows Interface
11122000050031  4.0.0.1                   1 00:19:57 ACT     1 Virtual-Access3.1


------------------ show cdma pdsn session ------------------


Mobile Station ID IMSI 11122000050031
  PCF IP Address 4.0.0.1, PCF Session ID 1
  A10 connection time 00:19:57,  registration lifetime 1800 sec
  Number of A11 re-registrations 1, time since last registration 1193 sec
  Current Access network ID 0004-0000-01
  Last airlink record received is Active Start, airlink is active
  GRE sequence number transmit 12, receive 12
  Using interface Virtual-Access3.1, status ACT
  Using AHDLC engine on slot 5, channel ID 0
  This session has 1 flow

  Flow service Proxy-Mobile, NAI mwts-mipp-np-user1@ispxyz.com
    Mobile Node IP address 30.0.0.1
    Home Agent IP address 7.0.0.2
    Packets in 0, bytes in 0
    Packets out 0, bytes out 0


------------------ show cdma pdsn pcf brief ------------------

PCF IP Address     Sessions      Pkts In     Pkts Out     Bytes In    Bytes Out
4.0.0.1                   1            0           12            0          396


------------------ show cdma pdsn pcf ------------------


PCF 4.0.0.1 has 1 session
  Received 0 pkts (0 bytes), sent 12 pkts (396 bytes)

  PCF Session ID 1, Mobile Station ID IMSI 11122000050031
```

```
    A10 connection age 00:19:58
    A10 registration lifetime 1800 sec, time since last registration 1194 sec



------------------ show cdma pdsn selection summary ------------------


CDMA PDSN selection summary:
    Hostname         PDSN            Session-count  Max-sessions
   *mwt10-7206a      5.0.0.1             1              8000
    mwt10-7206b      12.0.0.1            0              8000

    Hostname         Keepalive    Interface       Load-factor
   *mwt10-7206a          30       7.0.0.1            0.00
    mwt10-7206b          30       7.0.0.2            0.00

------------------ show ip mobile traffic ------------------

IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0 , Dropped 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0, active HA 0
    Bad identification 0, Bad request form 0
    Unavailable encap 0, reverse tunnel 0
    Reverse tunnel mandatory 0
    Binding Updates received 0, sent 0 total 0 fail 0
    Binding Update acks received 0 sent 0
    Binding info requests received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Reverse tunnel mandatory 0
    Replies in 1
    Forwarded 0, Bad 0, Ignored 1
    Authentication failed MN 0, HA 0
    Received challenge/gen. authentication extension, feature not enabled 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Unknown challenge 0, Missing challenge 0, Stale challenge 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
    Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0

------------------ show ip mobile globals ------------------

IP Mobility global information:
```

```
Home Agent is not enabled

Foreign Agent

    Pending registrations expire after 15 secs
    Care-of addresses advertised
        Ethernet2/0 (7.0.0.1) - up

0 interfaces providing service
Encapsulations supported:IPIP and GRE
Tunnel fast switching enabled
Tunnel path MTU discovery aged out after 10 min

------------------ show ip mobile interface ------------------

IP Mobility interface information:

------------------ show vpdn tunnel ------------------



------------------ show cdma pdsn resource ------------------


Resource allocated/available in the resource manager

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

snmp-server enable traps cdma

To enable network management traps for CDMA, use the **snmp-server enable traps cdma** command in global configuration mode. To disable network management traps for CDMA, use the **no** form of this command.

snmp-server enable traps cdma

no snmp-server enable traps cdma

Syntax Description

This command has no arguments or keywords.

Defaults

Network management traps disabled.

Command Modes

Global Configuration

Command History

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

Examples

The following example enables network management traps for CDMA:

```
snmp-server enable traps cdma
```

snmp-server enable traps ipmobile

To configure Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the no form of this command.

snmp-server enable traps ipmobile

no snmp-server enable traps ipmobile

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global Configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at

http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

subscriber redundancy rate

To configure the Cluster Control Manager to sync the number_sessions calls to the standby at a configurable interval, use the **subscriber redundancy rate** command in global configuration mode. The periodic rate will be applicable for both dynamic and bulk sync. To disable this feature, use the **no** form of the command.

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

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX6	This command was introduced to the PDNS image.

Usage Guidelines

Note You should only configure this command with the following values:

subscriber redundancy rate 500 1

Examples

The following example illustrates the **subscriber redundancy rate** command:

```
router(config)# subscriber redundancy rate 500 1
```