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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

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

Examples
The following example enables PDSN service:

```
service cdma pdsn
```
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

**7200-c5 image:**

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

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

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

**7200-c6 image**

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

All registration-update timeout 1 sec, retransmissions 5
Mobile IP registration timeout 300 sec
```
A10 maximum lifetime allowed 1800 sec
GRS sequencing is on
Maximum PCFs limit not set
Maximum sessions limit not set (default 20000 maximum) <<<<< changed
SNMP failure history table size 10
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is disabled
Aging of idle users disabled

Number of pcfs connected 0
Number of sessions connected 0,
  Simple IP flows 0, Mobile IP flows 0,
  Proxy Mobile IP flows 0
show cdma pdsn accounting

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

```
show cdma pdsn accounting
```

**Syntax Description**

This command has no keywords or arguments.

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**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 D4:0000000000000000
  E - E1:0000
  F - F1:00F1 F2:00F2 F3:00F3 F4:00F4 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
Y - Y2:12

UDR for flow
  Mobile Node IP address 15.0.0.3
  B - B1:15.0.0.3 B2:MWTS-MIP-PL-USER121@ispxyz.com
  C - 'C2:36
  D - D1:0.0.0.0
  F - F1:02 F2:01 F3:00
  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-PL-USER122@ispxyz.com
```
show cdma pdsn accounting

Packets in: 0 out: 0
UDR for flow
Mobile Node IP address 15.0.0.5
B - B1:15.0.0.5 B2:mwts-mip-p1-user123@ispxyz.com
C - ' 'C2:38
D - D1:0.0.0.0
F - F11:02 F12:01 F13:00
G - G1:0 G2:0 G4:1023906326
Packets in: 0 out: 0
UDR for session
session ID: 2
Mobile Station ID IMSI 00000000003
A - A1:00000000003
C - ' 'C3:0
D - D3:4.0.0.1 D4:000000000000
E - E1:0000
F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:201 G15:0 G16:0
I - I1:0 I4:0
Y - Y2:2
UDR for flow
Mobile Node IP address 6.0.0.5
B - B1:6.0.0.5 B2:mwt10-sip-user1
C - ' 'C2:39
D - D1:0.0.0.0
F - F11:01 F12:00 F13:00
G - G1:0 G2:0 G4:1023906826
Packets in: 0 out: 0
UDR for session
session ID: 3
Mobile Station ID IMSI 00000000004
A - A1:00000000004
C - ' 'C3:0
D - D3:4.0.0.1 D4:000000000000
E - E1:0000
F - F1:00F1 F2:00F2 F5:00F5 F6:F6 F7:F7 F8:F8 F9:F9 F10:FA F14:00
G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0 G13:0 G14:241 G15:0 G16:0
I - I1:0 I4:0
Y - Y2:3
UDR for flow
Mobile Node IP address 6.0.0.14
B - B1:6.0.0.14 B2:mwt10-sip-user1
C - ' 'C2:40
D - D1:0.0.0.0
F - F11:01 F12:00 F13:00
G - G1:0 G2:0 G4:1023906826
Packets in: 0 out: 0
PDSN-6500#
show cdma pdsn accounting detail

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

show cdma pdsn accounting detail

Syntax Description

This command has no keywords or arguments.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

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 Traffic type (F7) 247 Fundamental Frame size (F8) 248
Forward Fundamental RC (F9) 249 Reverse Fundamental 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
Packet Data Serving Node Commands

```plaintext
show cdma pdsn accounting detail

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 Traffic type (F7) 247 Fundamental Frame size (F8) 248
    Forward Fundamental RC (F9) 249 Reverse Fundamental 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) 0
    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)
mwts10-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 Traffic type (F7) 247 Fundamental Frame size (F8) 248
    Forward Fundamental RC (F9) 249 Reverse Fundamental RC (F10) 250
    DCCH Frame Format (F14) 0
    Bad PPP Frame Count (G3) 0 Active Time (G8) 0
    Number of Active Transitions (G9) 0
```

Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference

MWP-156
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**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 000000000004
UDR for session
  session ID: 3
  Mobile Station ID IMSI 000000000004
    A - A1:000000000004
    C - 'C3:0
    D - D1:4.0.0.1 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 - G1:0 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**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 Traffic type (F7) 247 Fundamental Frame size (F8) 248
Forward Fundamental RC (F9) 249 Reverse Fundamental 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
 mwt10-sip-user1
    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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msid</td>
<td>The ID number of the mobile subscriber.</td>
</tr>
<tr>
<td>mn-ip-address</td>
<td>Specifies the IP addresses assigned to the mobile numbers in each session.</td>
</tr>
<tr>
<td>IP_address</td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

```plaintext
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 - F1:02 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**

<table>
<thead>
<tr>
<th>slot_number</th>
<th>Slot number of the AHDLC of interest.</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)BY</td>
<td>The possible values for channel ID were extended to 20000.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**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 pdn cluster controller

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

`show cdma pdn cluster controller { configuration | statistics }`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>configuration</th>
<th>Displays configuration information associated with the cluster controller.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>statistics</td>
<td>Displays various statistics collected on the cluster controller signaling messages with the cluster member, and redundancy message statistics with the redundancy peer.</td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows output from the `show cdma pdn cluster controller` command:

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

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

```
show cdma pdsn cluster controller configuration
```

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

**Defaults**
No default keywords or arguments.

**Command Modes**
Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

controller redundancy:
database in-sync or no need to sync
group: sit_cluster1
```
show cdma pdsn cluster controller member

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load</td>
<td>The load reported by every PDSN member in the cluster, sorted from the lowest load value.</td>
</tr>
<tr>
<td>time</td>
<td>The seek time of the member, sorted from the past to the future.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>Specifies the controller member.</td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>The number of session records on cluster controller.</td>
</tr>
<tr>
<td>age</td>
<td>The number of session records of this age on the cluster controller. Age measured in days.</td>
</tr>
<tr>
<td>oldest</td>
<td>The oldest session record on the cluster controller.</td>
</tr>
<tr>
<td>more 1-20 records</td>
<td>Displays the configured number (from 1 to 20) of the oldest session records on the cluster controller.</td>
</tr>
<tr>
<td>imsi BCDs</td>
<td>Displays the session record with this imsi on the cluster controller.</td>
</tr>
<tr>
<td>more 1-20 records</td>
<td>Displays the configured number (from 1 to 20) of additional session records on the cluster controller.</td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

<table>
<thead>
<tr>
<th>IMSI</th>
<th>Member IPv4 Addr</th>
<th>Age [days]</th>
<th>Anchor changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000007</td>
<td>10.0.0.50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Router# show cdma pdsn clu contr session count

10 session records

Router# show cdma pdsn clu contr session oldest

<table>
<thead>
<tr>
<th>IMSI</th>
<th>Member IPv4 Addr</th>
<th>Age [days]</th>
<th>Anchor changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000002</td>
<td>10.0.0.50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show cdma pdsn cluster controller statistics

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

**show cdma pdsn cluster controller statistics**

**Syntax Description**

There are no arguments or keywords for this command.

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

mwt13-6500c#
```
**show cdma pdsn cluster member**

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>configuration</th>
<th>Display configuration information associated with the cluster member.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>statistics</td>
<td>Displays various statistics collected on cluster member signaling messages with the cluster controller.</td>
</tr>
</tbody>
</table>

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

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

**Syntax Description**

- **mn-ip-address**
  - Specifies the IP addresses assigned to the mobile numbers in each session.

- **ip_address**
  - Specifies the mobile subscriber id number.

- **msid string**
  - Specifies the service type.

- **user string**
  - Specifies the user.

**Defaults**

No default keywords or arguments.

**Command Modes**

Privileged EXEC

**Command History**

**Release** | **Modification**
--- | ---
12.2(8)BY | This command was introduced.
12.3(4)T | This command was incorporated in Cisco IOS Release 12.3(4)T.

**Examples**

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

```
Router# show cdma pdsn flow

MSID       NAI              Type  MN IP Address  St
---------- -----------  -------  ------------  ----
100000000000099 sim1  Simple  100.4.1.1  ACT
200000000000047 sim1  Simple  100.4.1.2  ACT
100000000000100 sim1  Simple  100.4.1.40 ACT
2000000000000048 sim1  Simple  100.4.1.3  ACT
100000000000101 sim1  Simple  100.4.1.5  ACT
2000000000000049 sim1  Simple  100.4.1.4  ACT
100000000000102 sim1  Simple  100.4.1.6  ACT
2000000000000050 sim1  Simple  100.4.1.7  ACT
100000000000103 sim1  Simple  100.4.1.9  ACT
2000000000000051 sim1  Simple  100.4.1.8  ACT
100000000000104 sim1  Simple  100.4.1.11 ACT
2000000000000052 sim1  Simple  100.4.1.10 ACT
100000000000105 sim1  Simple  100.4.1.12 ACT
2000000000000053 sim1  Simple  100.4.1.13 ACT
3000000000000008 sim1  Simple  100.4.1.14 ACT
100000000000106 sim1  Simple  100.4.1.15 ACT
2000000000000054 sim1  Simple  100.4.1.16 ACT
3000000000000009 sim1  Simple  100.4.1.17 ACT
100000000000107 sim1  Simple  100.4.1.19 ACT
2000000000000055 sim1  Simple  100.4.1.18 ACT
100000000000122 sim1  Simple  100.4.1.21 ACT
2000000000000070 sim1  Simple  100.4.1.20 ACT
```
<table>
<thead>
<tr>
<th>ID</th>
<th>Mode</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000000000000025</td>
<td>Simple</td>
<td>100.4.1.22</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000123</td>
<td>Simple</td>
<td>100.4.1.24</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000071</td>
<td>Simple</td>
<td>100.4.1.23</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000026</td>
<td>Simple</td>
<td>100.4.1.25</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000124</td>
<td>Simple</td>
<td>100.4.1.26</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000072</td>
<td>Simple</td>
<td>100.4.1.27</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000027</td>
<td>Simple</td>
<td>100.4.1.28</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000125</td>
<td>Simple</td>
<td>100.4.1.29</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000073</td>
<td>Simple</td>
<td>100.4.1.30</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000028</td>
<td>Simple</td>
<td>100.4.1.31</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000126</td>
<td>Simple</td>
<td>100.4.1.33</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000074</td>
<td>Simple</td>
<td>100.4.1.32</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000029</td>
<td>Simple</td>
<td>100.4.1.34</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000127</td>
<td>Simple</td>
<td>100.4.1.36</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000075</td>
<td>Simple</td>
<td>100.4.1.35</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000030</td>
<td>Simple</td>
<td>100.4.1.37</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000128</td>
<td>Simple</td>
<td>100.4.1.39</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000076</td>
<td>Simple</td>
<td>100.4.1.38</td>
<td>ACT</td>
</tr>
<tr>
<td>30000000000000101</td>
<td>Simple</td>
<td>100.4.1.41</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000199</td>
<td>Simple</td>
<td>100.4.1.43</td>
<td>ACT</td>
</tr>
<tr>
<td>2000000000000147</td>
<td>Simple</td>
<td>100.4.1.42</td>
<td>ACT</td>
</tr>
<tr>
<td>3000000000000102</td>
<td>Simple</td>
<td>100.4.1.44</td>
<td>ACT</td>
</tr>
<tr>
<td>1000000000000200</td>
<td>Simple</td>
<td>100.4.1.46</td>
<td>ACT</td>
</tr>
</tbody>
</table>

---More---
show cdma pdsn flow service

To display flow-based information for a specified service type in each session, use the `show cdma pdsn flow service` command in privileged EXEC mode.

```
show cdma pdsn flow service {mobile | proxy-mobile | simple | simple-ipv6}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>mobile</th>
<th>Specifies mobile service type.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>proxy-mobile</td>
<td>Specifies the proxy-mobile service type.</td>
</tr>
<tr>
<td></td>
<td>simple</td>
<td>Specifies the simple service type.</td>
</tr>
<tr>
<td></td>
<td>simple-ipv6</td>
<td>Specifies the simple-IPv6 service type.</td>
</tr>
</tbody>
</table>

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)BY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)YX</td>
<td>simple-ipv6 output was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was incorporated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

Examples

The following example shows output from the `show cdma pdsn flow service simple-ipv6` command:

```
Router# show cdma pdsn flow service simple-ipv6
MSID  NAI Type  MN IP  Address St
000000000000101 mwts-ucl-np-user1 Simple-ipv6
```
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(4)T       This command was incorporated in Cisco IOS Release 12.3(4)T.
```

**Examples**

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

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

**Table 6** describes the fields shown in the output of the brief version of the command.

**Table 6  show cdma pdsn pcf brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCF IP Address</td>
<td>IP address of the PCF.</td>
</tr>
<tr>
<td>Sessions</td>
<td>Number of active sessions.</td>
</tr>
<tr>
<td>Pkts In</td>
<td>Total packets received from a PCF.</td>
</tr>
<tr>
<td>Pkts Out</td>
<td>Total packets sent to a PCF.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>Total bytes received from a PCF.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>Total bytes sent to a PCF.</td>
</tr>
</tbody>
</table>

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

Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference
show cdma pdsn pcf

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

Table 7 describes the fields shown in the output of the command when an IP address is specified.

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

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

Table 8 describes the fields shown in the output of the command when the keyword secure is specified.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>The default security associations (used for PCFs that do not have an explicitly configured security association).</td>
</tr>
<tr>
<td>x.x.x.x</td>
<td>IP address of the PCF</td>
</tr>
<tr>
<td>spi spi_value</td>
<td>Security Parameter Index, a 4-byte hex index within the security association that selects the specific security parameters to be used.</td>
</tr>
<tr>
<td>Timestamp +/- value</td>
<td>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.</td>
</tr>
<tr>
<td>key {asciilhex} key</td>
<td>The shared secret key for the security associations</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)YX</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)XW</td>
<td>Prepaid output was included in examples.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

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

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

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

Session Events
  Up 10, Down 39, Reregistration 0
  Handoff 0, PPP renegotiation 0
Flow Events
  Simple IP Up 1, Down 1
  Mobile IP Up 7, Down 7
  Proxy Mobile IP Up 2, Down 2
Accounting Events
  Update 0, Flow Start 0, 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)BY</td>
<td>The possible values for channel ID was extended to 20000.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays a summary of the session table entry.</td>
</tr>
<tr>
<td>msid number</td>
<td>Keyword to indicate that the PDSN selection table entry for a particular MSID is to be displayed.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

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

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

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

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

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(Optional) Displays a summary of all sessions.</td>
</tr>
<tr>
<td>dormant</td>
<td>(Optional) Displays information about dormant PDSN sessions.</td>
</tr>
<tr>
<td>mn-ip-address</td>
<td>address (Optional) Displays user information for the specified IP address.</td>
</tr>
<tr>
<td>msid number</td>
<td>(Optional) Displays information for the specified MSID.</td>
</tr>
<tr>
<td>user nai</td>
<td>(Optional) Displays information for the specified NAI.</td>
</tr>
<tr>
<td>prepaid</td>
<td>(Optional) Displays information about prepaid flows.</td>
</tr>
</tbody>
</table>

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)XC</td>
<td>The parameters of this command were altered.</td>
</tr>
<tr>
<td>12.2(8)BY</td>
<td>The prepaid variable was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

Examples

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

```
router# show cdma pdsn session
Mobile Station ID IMSI 111111111111111
PCF IP Address 2.2.2.100, PCF Session ID 1
A10 connection time 00:00:09, registration lifetime 65535 sec
Number of All re-registrations 0, time since last registration 9 sec
Current Access network ID 0002-0202-64
Last airlink record received is Active Start, airlink is active
GRE sequence number transmit 8, receive 10
Using interface Virtual-Access1, status ACT
Using AHDLC Engine on slot 1, channel ID 2
This session has 1 flow
Flow service Proxy-Mobile, NAI mwts-mipp-np-homeaddr@ispxyz.com
Mobile Node IP address 30.0.0.2
Home Agent IP address 7.0.0.2
Packets in 0, bytes in 0
Packets out 0, bytes out 0
Prepaid duration 36000 secs, used 6500 secs, cumulative 13000 secs
```
show cdma pdsn statistics

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

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

**Syntax Description**

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

**Defaults**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

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

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

AHDLC:

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

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

Deframing input 0 bytes, 0 paks
Deframing output 0 bytes, 0 paks
Deframing errors 0, insufficient memory 0,
   queue overflow 0, invalid size 0, CRC errors 0
show cdma pdsn statistics prepaid

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

```
show cdma pdsn statistics prepaid
```

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

**Defaults**
No default keywords or arguments.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)XW</td>
<td>Prepaid output was included in examples.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)XW</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)XW</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

```
router# show ip mobile cdma ipsec profile
```
show ip mobile proxy

To display information about a proxy Mobile IP host, use the `show ip mobile proxy` command in privileged EXEC mode.

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>host</code></td>
</tr>
<tr>
<td><code>nai string</code></td>
</tr>
<tr>
<td><code>registration</code></td>
</tr>
<tr>
<td><code>traffic</code></td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)XC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T for PDSN platforms.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is available only on Packet Data Serving Node (PDSN) platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

**Examples**

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

```
Router# show ip mobile proxy host

Proxy Host List:

MoIPProxy1@cisco.com:
  Home Agent Address 10.3.3.1
  Lifetime 6000
  Flags :sBdmgvt
```
show ip mobile secure

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Displays security association of the mobile host on the home agent.</td>
</tr>
<tr>
<td>visitor</td>
<td>Displays security association of the mobile visitor on the foreign agent.</td>
</tr>
<tr>
<td>foreign-agent</td>
<td>Displays security association of the remote foreign agents on the home agent.</td>
</tr>
<tr>
<td>home-agent</td>
<td>Displays security association of the remote home agent on the foreign agent.</td>
</tr>
<tr>
<td>proxy-host</td>
<td>Displays security association of the proxy mobile user. This keyword is only available on Packet Data Serving Node (PDSN) platforms running specific PDSN code images.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays number of security associations in table.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address.</td>
</tr>
<tr>
<td>nai string</td>
<td>Network access identifier (NAI).</td>
</tr>
</tbody>
</table>

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)XC</td>
<td>The <code>nai</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <code>proxy-host</code> keyword was added for PDSN platforms.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Multiple security associations can exist for each entity.

The `proxy-host` keyword is only available on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

### Examples

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

```
Router# show ip mobile secure

Security Associations (algorithm,mode,replay protection,key):
10.0.0.6
    SPI 300, MD5, Prefix-suffix, Timestamp +/- 7,
    Key 001123344556677889900112334455

Table 9 describes the significant fields shown in the display.
```
### Table 9  
**show ip mobile secure Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.6</td>
<td>IP address. The NAI is displayed if configured.</td>
</tr>
<tr>
<td>In/Out SPI</td>
<td>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.</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5 authentication algorithm. HMAC-MD5 id displayed if configured.</td>
</tr>
<tr>
<td>Prefix-suffix</td>
<td>Authentication mode.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Replay protection method.</td>
</tr>
<tr>
<td>Key</td>
<td>The shared secret key for the security associations, in hexadecimal format.</td>
</tr>
</tbody>
</table>
show ip mobile traffic

To display protocol counters, use the show ip mobile traffic command in privileged EXEC mode.

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was enhanced to display successful registration requests with NAT detect and to display information about foreign agent reverse tunnels and foreign agent challenge and response extensions.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The command output was enhanced to display the count of UDP Port 434 input packets that were dropped by UDP.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Counters can be reset to zero using the clear ip mobile traffic command, which also allows you to undo the reset.

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

Router# show ip mobile traffic

IP Mobility traffic:
UDP:
  Port: 434 (Mobile IP) input drops: 0
Advertisements:
  Solicitations received 0
  Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
  Register 0, Deregister 0 requests
  Register 0, Deregister 0 replied
  Accepted 0, No simultaneous bindings 0
  Denied 0, Ignored 0
  Unspecified 0, Unknown HA 0
  Administrative prohibited 0, No resource 0
  Authentication failed MN 0, FA 0
  Bad identification 0, Bad request form 0
  Unavailable encap 0, reverse tunnel 0
  Reverse tunnel mandatory 0
  Binding updates received 0, sent 0 total 0 fail 0
  Binding update acks received 0, sent 0
  Binding info request received 0, sent 0 total 0 fail 0
  Binding info reply received 0 drop 0, sent 0 total 0 fail 0
  Binding info reply acks received 0 drop 0, sent 0
  Gratuitous 0, Proxy 0 ARPs sent
  Total incoming requests using NAT detect 1
Foreign Agent Registrations:
Request in 0,
Forwarded 0, Denied 0, Ignored 0
Unspecified 0, HA unreachable 0
Administrative prohibited 0, No resource 0
Bad lifetime 0, Bad request form 0
Unavailable encapsulation 0, Compression 0
Unavailable reverse tunnel 0
Reverse tunnel mandatory
Replies in 0
Forwarded 0, Bad 0, Ignored 0
Authentication failed MN 0, HA 0
Received challenge/gen. authentication extension, feature not enabled 0
Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
Unknown challenge 1, Missing challenge 0, Stale challenge 0

Table 10 describes the significant fields shown in the display.

Table 10  show ip mobile traffic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port: 434 (Mobile IP) input drops</td>
<td>Total number of UDP Port 434 (Mobile IP) packets dropped by UDP processing due to a full input queue. These packets are not processed by the home agent or foreign agent and so are not otherwise counted or displayed by Mobile IP. This count is the same count displayed by using the <code>show ip socket detail</code> command.</td>
</tr>
<tr>
<td>Solicitations received</td>
<td>Total number of solicitations received by the mobility agent.</td>
</tr>
<tr>
<td>Advertisements sent</td>
<td>Total number of advertisements sent by the mobility agent.</td>
</tr>
<tr>
<td>response to solicitation</td>
<td>Total number of advertisements sent by the mobility agent in response to mobile node solicitations.</td>
</tr>
<tr>
<td>Home Agent</td>
<td></td>
</tr>
<tr>
<td>Register requests</td>
<td>Total number of registration requests received by the home agent.</td>
</tr>
<tr>
<td>Deregister requests</td>
<td>Total number of registration requests received by the home agent with a lifetime of zero (requests to deregister).</td>
</tr>
<tr>
<td>Register replied</td>
<td>Total number of registration replies sent by the home agent.</td>
</tr>
<tr>
<td>Deregister replied</td>
<td>Total number of registration replies sent by the home agent in response to requests to deregister.</td>
</tr>
<tr>
<td>Accepted</td>
<td>Total number of registration requests accepted by the home agent (Code 0).</td>
</tr>
<tr>
<td>No simultaneous bindings</td>
<td>Total number of registration requests accepted by the home agent—simultaneous mobility bindings unsupported (Code 1).</td>
</tr>
<tr>
<td>Denied</td>
<td>Total number of registration requests denied by the home agent.</td>
</tr>
<tr>
<td>Ignored</td>
<td>Total number of registration requests ignored by the home agent.</td>
</tr>
<tr>
<td>Unspecified</td>
<td>Total number of registration requests denied by the home agent—reason unspecified (Code 128).</td>
</tr>
<tr>
<td>Unknown HA</td>
<td>Total number of registration requests denied by the home agent—unknown home agent address (Code 136).</td>
</tr>
<tr>
<td>Administrative prohibited</td>
<td>Total number of registration requests denied by the home agent—administratively prohibited (Code 129).</td>
</tr>
</tbody>
</table>
### show ip mobile traffic Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resource</td>
<td>Total number of registration requests denied by the home agent—insufficient resources (Code 130).</td>
</tr>
<tr>
<td>Authentication failed MN</td>
<td>Total number of registration requests denied by the home agent—mobile node failed authentication (Code 131).</td>
</tr>
<tr>
<td>Authentication failed FA</td>
<td>Total number of registration requests denied by the home agent—foreign agent failed authentication (Code 132).</td>
</tr>
<tr>
<td>Bad identification</td>
<td>Total number of registration requests denied by the home agent—identification mismatch (Code 133).</td>
</tr>
<tr>
<td>Bad request form</td>
<td>Total number of registration requests denied by the home agent—poorly formed request (Code 134).</td>
</tr>
<tr>
<td>Unavailable encap</td>
<td>Total number of registration requests denied by the home agent—unavailable encapsulation (Code 139).</td>
</tr>
<tr>
<td>Reverse tunnel mandatory</td>
<td>Total number of registration requests denied by the home agent—reverse tunnel is mandatory and the “T” bit is not set (Code 138).</td>
</tr>
<tr>
<td>Unavailable reverse tunnel</td>
<td>Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 137).</td>
</tr>
<tr>
<td>Binding updates</td>
<td>A Mobile IP standby message sent from the active router to the standby router when a registration request comes into the active router.</td>
</tr>
<tr>
<td>Binding update acks</td>
<td>A Mobile IP standby message sent from the standby router to the active router to acknowledge the reception of a binding update.</td>
</tr>
<tr>
<td>Binding info request</td>
<td>A Mobile IP standby message sent from a router coming up from reboot/or a down interface. The message is a request to the current active router to send the entire Mobile IP binding table.</td>
</tr>
<tr>
<td>Binding info reply</td>
<td>A reply from the active router to the standby router that has part or all of the binding table (depending on size).</td>
</tr>
<tr>
<td>Binding info reply acks</td>
<td>An acknowledge message from the standby router to the active router that it has received the binding info reply.</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Total number of gratuitous ARPs sent by the home agent on behalf of mobile nodes.</td>
</tr>
<tr>
<td>Proxy ARPs sent</td>
<td>Total number of proxy ARPs sent by the home agent on behalf of mobile nodes.</td>
</tr>
<tr>
<td>Total incoming registration requests...</td>
<td>Total number incoming registration requests using NAT detect.</td>
</tr>
</tbody>
</table>

### Foreign Agent

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request in</td>
<td>Total number of registration requests received by the foreign agent.</td>
</tr>
<tr>
<td>Forwarded</td>
<td>Total number of registration requests relayed to the home agent by the foreign agent.</td>
</tr>
<tr>
<td>Denied</td>
<td>Total number of registration requests denied by the foreign agent.</td>
</tr>
<tr>
<td>Ignored</td>
<td>Total number of registration requests ignored by the foreign agent.</td>
</tr>
<tr>
<td>Unspecified</td>
<td>Total number of registration requests denied by the foreign agent—reason unspecified (Code 64).</td>
</tr>
</tbody>
</table>
Table 10  show ip mobile traffic Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA unreachable</td>
<td>Total number of registration requests denied by the foreign agent—home agent unreachable (Codes 80-95).</td>
</tr>
<tr>
<td>Administrative prohibited</td>
<td>Total number of registration requests denied by the foreign agent—administratively prohibited (Code 65).</td>
</tr>
<tr>
<td>No resource</td>
<td>Total number of registration requests denied by the home agent—insufficient resources (Code 66).</td>
</tr>
<tr>
<td>Bad lifetime</td>
<td>Total number of registration requests denied by the foreign agent—requested lifetime too long (Code 69).</td>
</tr>
<tr>
<td>Bad request form</td>
<td>Total number of registration requests denied by the home agent—poorly formed request (Code 70).</td>
</tr>
<tr>
<td>Unavailable encapsulation</td>
<td>Total number of registration requests denied by the home agent—unavailable encapsulation (Code 72).</td>
</tr>
<tr>
<td>Unavailable compression</td>
<td>Total number of registration requests denied by the foreign agent—requested Van Jacobson header compression unavailable (Code 73).</td>
</tr>
<tr>
<td>Unavailable reverse tunnel</td>
<td>Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 74).</td>
</tr>
<tr>
<td>Reverse tunnel mandatory</td>
<td>Total number of registration requests denied by the foreign agent—reverse tunnel is mandatory and the “T” bit is not set (Code 75).</td>
</tr>
<tr>
<td>Replies in</td>
<td>Total number of well-formed registration replies relayed to the mobile node by the foreign agent.</td>
</tr>
<tr>
<td>Bad</td>
<td>Total number of registration replies denied by the foreign agent—poorly formed reply (Code 71).</td>
</tr>
<tr>
<td>Ignored</td>
<td>Total number of registration replies ignored by the foreign agent.</td>
</tr>
<tr>
<td>Authentication failed MN</td>
<td>Total number of registration requests denied by the home agent—mobile node failed authentication (Code 67).</td>
</tr>
<tr>
<td>Authentication failed HA</td>
<td>Total number of registration replies denied by the foreign agent—home agent failed authentication (Code 68).</td>
</tr>
<tr>
<td>Received challenge/gen.</td>
<td>Total number of registration requests dropped by the foreign agent—received challenge/generalized-authentication extension in registration request but Mobile IP foreign agent challenge/response extension is not enabled.</td>
</tr>
<tr>
<td>authentication extension, feature not enabled</td>
<td></td>
</tr>
<tr>
<td>Unknown challenge</td>
<td>Total number of registration requests denied by the foreign agent—unknown challenge (Code 104).</td>
</tr>
<tr>
<td>Missing Challenge</td>
<td>Total number of registration requests denied by the foreign agent—missing challenge (Code 105).</td>
</tr>
<tr>
<td>Stale Challenge</td>
<td>Total number of registration requests denied by the foreign agent—stale challenge (Code 106).</td>
</tr>
</tbody>
</table>
show ip mobile violation

To display information about security violations, use the `show ip mobile violation` command in privileged EXEC mode.

```
show ip mobile violation [address | nai string]
```

**Syntax Description**

- `address` (Optional) Displays violations from a specific IP address.
- `nai string` (Optional) Network access identifier.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)XC</td>
<td>The <code>nai</code> keyword and associated parameters were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, which are the violators without security associations. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the `logging` global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the `show logging` command.

**Examples**

The following is sample output from the `show ip mobile violation` command:

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1: Violations: 1, Last time: 06/18/97 01:16:47
SPI: 300, Identification: B751B5R1.77FD0E40
Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

Table 11 describes significant fields shown in the display.

**Table 11  `show ip mobile violation` Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the violator. The network access identifier (NAI) is displayed if configured.</td>
</tr>
<tr>
<td>Violations</td>
<td>Total number of security violations for this peer.</td>
</tr>
<tr>
<td>Last time</td>
<td>Time of the most recent security violation for this peer.</td>
</tr>
</tbody>
</table>
Table 11  show ip mobile violation Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI</td>
<td>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.</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification used in request or reply of the most recent security violation for this peer.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Error code in request or reply.</td>
</tr>
<tr>
<td>Reason Codes</td>
<td>Reason for the most recent security violation for this peer. Possible reasons are:</td>
</tr>
<tr>
<td></td>
<td>• (1) No mobility security association</td>
</tr>
<tr>
<td></td>
<td>• (2) Bad authenticator</td>
</tr>
<tr>
<td></td>
<td>• (3) Bad identifier</td>
</tr>
<tr>
<td></td>
<td>• (4) Bad SPI</td>
</tr>
<tr>
<td></td>
<td>• (5) Missing security extension</td>
</tr>
<tr>
<td></td>
<td>• (6) Other</td>
</tr>
</tbody>
</table>
show ip mobile visitor

To display the visitor table that contains information on mobile nodes (MNs) using this foreign agent (FA), use the `show ip mobile visitor` command in privileged EXEC mode.

```
show ip mobile visitor [[pending] [ip-address | summary] | nai string [session-id string]]
```

### Syntax Description

- **pending** (Optional) Displays the pending registration table.
- **ip-address** (Optional) IP address of visiting MNs.
- **summary** (Optional) Displays all values in the table.
- **nai string** (Optional) Network access identifier (NAI).
- **session-id string** (Optional) Session identifier. The string value must be fewer than 25 characters.

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(2)XC</td>
<td>The <code>nai</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <code>session-id</code> keyword was added.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The output was enhanced to display UDP tunneling.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to find out information on MNs that are registered with their (home agent) HA via this FA. The FA updates the visitor table that contain a list of the MNs using a FA.

A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

### Examples

The following is sample output from the `show ip mobile visitor` command:

```
Router# show ip mobile visitor

Mobile Visitor List:
Total 1
10.0.0.1:
  Interface Ethernet1/2, MAC addr 0060.837b.95ec
  IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
  HA addr 66.0.0.5, Identification B7510E60.64436B38
  Lifetime 08:20:00 (30000) Remaining 08:19:16
  Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
  Routing Options - (T)Reverse-tunnel
```
If the mobile node has visited and is associated with a session identifier, then the visitor entry for the mobile node shows the session identifier as shown below:

Router# show ip mobile visitor

Mobile Visitor List:
Total 1
user01@cisco.com
    Home addr 100.100.100.17
    Interface Ethernet3/3, MAC addr 0004.6d25.b857
    IP src 0.0.0.0, dest 100.100.100.1, UDP src port 434
    HA addr 100.100.100.100, Identification BC189864.B2FE6CC4
    Lifetime 00:33:20 (2000) Remaining 00:33:06
    Tunnel0 src 70.70.70.2, dest 100.100.100.100, reverse-allowed
    Routing Options - (B)Broadcast
    Session identifier PD

The following sample output shows that the MN is registering with the HA (at the FA):

Router# show ip mobile visitor

Mobile Visitor List:
Total 1
10.99.100.2:
    Interface FastEthernet3/0, MAC addr 00ff.ff80.002b
    IP src 10.99.100.2, dest 30.5.3.5, UDP src port 434
    HA addr 200.1.1.1, Identification BCE7E391.A09E8720
    Lifetime 01:00:00 (3600) Remaining 00:30:09
    Tunnel1 src 200.1.1.5, dest 200.1.1.1, reverse-allowed
    Routing Options - (T)Reverse Tunneling

Table 12 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Number of mobile nodes visiting the foreign agent.</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>Home IP address of a visitor. The NAI is displayed if configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface the FA received the MN’s registration on.</td>
</tr>
<tr>
<td>MAC addr</td>
<td>MAC address of the visitor.</td>
</tr>
<tr>
<td>IP src</td>
<td>Source IP address of the registration request of a visitor.</td>
</tr>
<tr>
<td>IP dest</td>
<td>Destination IP address of the registration request of a visitor. A MN solicits an advertisement from the FA, and the FA uses the output interface’s address (where it received the solicitation) as the source IP address in the advertisement. The MN picks up on this address and sends in a RRQ to it. This tells you which destination address the MN used when it sent in its registration request to the FA (typically the interface address). If it had sent the registration request to a broadcast or multicast address, or advertised address (not knowing the interface address), the FA will reply using the output interface address (typically the interface where it received the RRQ).</td>
</tr>
<tr>
<td>UDP src port</td>
<td>UDP src port used by the visiting mobile node in its registration request.</td>
</tr>
<tr>
<td>HA addr</td>
<td>Home agent IP address for that visiting mobile node.</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification used in that registration by the mobile node.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The lifetime (in hh:mm:ss) granted to the mobile node for this registration.</td>
</tr>
</tbody>
</table>
Table 12  show ip mobile visitor Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remaining</td>
<td>The time (in hh:mm:ss) remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The options are IPIN, GRE, and UDP. The default is IPIN encapsulation.</td>
</tr>
<tr>
<td>Routing Options</td>
<td>Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Options are:</td>
</tr>
<tr>
<td></td>
<td>• (S) Multi-binding (not supported on home agent)</td>
</tr>
<tr>
<td></td>
<td>• (B) Broadcast</td>
</tr>
<tr>
<td></td>
<td>• (D) Direct-to-mobile node</td>
</tr>
<tr>
<td></td>
<td>• (M) MinIP (not supported on home agent)</td>
</tr>
<tr>
<td></td>
<td>• (G) GRE</td>
</tr>
<tr>
<td></td>
<td>• (T) Reverse-tunnel</td>
</tr>
<tr>
<td>Session identifier</td>
<td>Session identifier can be the device name or MAC address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip mobile</td>
<td>Displays IP mobility activities.</td>
</tr>
<tr>
<td>ip mobile foreign-agent nat traversal</td>
<td>Enables NAT UDP traversal support for MIP FAs.</td>
</tr>
<tr>
<td>ip mobile home-agent nat traversal</td>
<td>Enables NAT UDP traversal support for MIP HAs.</td>
</tr>
<tr>
<td>show ip mobile binding</td>
<td>Displays the mobility binding table.</td>
</tr>
<tr>
<td>show ip mobile globals</td>
<td>Displays global information about MIP HAs, FAs, and MNs.</td>
</tr>
<tr>
<td>show ip mobile tunnel</td>
<td>Displays information about UDP tunneling.</td>
</tr>
</tbody>
</table>
show ipc sctp

To display ipc sctp statistics, use the show ipc sctp command.

show ipc sctp

Syntax Description
This command has no keywords or arguments.

Defaults
No default keywords or arguments.

Command Modes
Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)XW</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
</tbody>
</table>

Examples
Sample show output for the show ipc sctp command:

```
router # show ipc sctp statistics
IPC default Zone:
  IPC association Id: 1
    SCTP Protocol Local: port: 6602 ip: 10.2.86.26
    keepalive 1500
    retransmit-timeout 300 600
    bundling 20
    cumulative-sack 200
    path-retransmit 4
    assoc-retransmit 4
    max-inbound-streams 2
    init-timeout 1000
    init-retransmit 8
    receive-window 24000
    SCTP Protocol Remote: port: 22 ip: 10.2.87.26
router #
```
**snmp-server enable traps cdma**

To enable network management traps for CDMA, use the `snmp-server enable traps cdma` command in global configuration mode. To disable network management traps for CDMA, use the `no` form of this command.

```
  snmp-server enable traps cdma
  no snmp-server enable traps cdma
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Network management traps disabled.

**Command Modes**

Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(3)XS</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was incorporated in Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Examples**

The following example enables network management traps for CDMA:

```
  snmp-server enable traps cdma
```
snmp-server enable traps ipmobile

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the `snmp-server enable traps ipmobile` command in global configuration mode. To disable SNMP notifications for Mobile IP, use the `no` form of this command.

```
snmp-server enable traps ipmobile
```

```
no snmp-server enable traps ipmobile
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

SNMP notifications are disabled by default.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. This command enables Mobile IP Authentication Failure notifications. This notification is defined in RFC2006-MIB.my as the `mipAuthFailure` notification type `{mipMIBNotifications 1}`. This notification, when enabled, is triggered when there is an authentication failure for the Mobile IP entity during validation of the mobile registration request or reply.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The `snmp-server enable traps ipmobile` command is used in conjunction with the `snmp-server host` command. Use the `snmp-server host` global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one `snmp-server host` command.

**Examples**

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of an SNMP notification operation.</td>
</tr>
<tr>
<td>snmp-server trap-source</td>
<td>Specifies the interface from which an SNMP trap should originate.</td>
</tr>
</tbody>
</table>