debug cdma pdsn a10 gre

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

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

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

Syntax Description

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 Modes

Privileged EXEC

Command History

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

Examples

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

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

Router# show debug

CDMA:
  CDMA PDSN A10 GRE events debugging is on for tunnel key 1

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

debug cdma pdsn a10 ppp

To display debug messages for A10 Point-to-Point protocol (PPP) interface errors, events, and packets, use the **debug cdma pdsn a10 ppp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

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

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

Syntax Description

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 Modes

Privileged EXEC

Command History

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

Examples

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

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

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

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

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

debug cdma pdsn a11

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn a11 errors

CDMA PDSN A11 errors debugging is on

Router# show debug

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

```
changed state to up

Router# debug cdma pdsn a11 packets events

Router# show debug

CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001
  CDMA PDSN A11 events debugging is on for mnid 000000000000001

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

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

Router# debug cdma pdsn a11 event mnid 000000000000001

Router# show debug

CDMA:
  CDMA PDSN A11 events debugging is on for mnid 000000000000001

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

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

close the session
Router#
```

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

Router# debug cdma pdsn a11 packet mnid 000000000000001

Router# show debug

CDMA:
  CDMA PDSN A11 packet debugging is on for mnid 000000000000001

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

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

debug cdma pdsn accounting

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

debug cdma pdsn accounting

no cdma pdsn accounting

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn accounting

CDMA PDSN accounting debugging is on
Router#
*Jan  1 00:15:32:CDMA/ACCT:null vaccess in session_start
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[44] len:[3] 01   Processing Y1
*Jan  1 00:15:32:CDMA/ACCT:    Setup airlink record received
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[12]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[41] len:[6] 00 00 00 02 CDMA/ACCT:
Processing Y2
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1A] len:[9]
*Jan  1 00:15:32:CDMA/ACCT:    VSA Vid:5535 type:[42] len:[3] 12 CDMA/ACCT: Processing Y3
*Jan  1 00:15:32:CDMA/ACCT: Current Attribute type:0x[1F] len:[17] 30 30 30 30 30 30 30 30
30 30 30 30 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 debugging output, 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 Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn accounting flow

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

debug cdma pdsn accounting time-of-day

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

debug cdma pdsn accounting time-of-day

no debug cdma pdsn accounting time-of-day

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn accounting time-of-day

CDMA PDSN accounting time-of-day debugging is on

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

debug cdma pdsn cluster

To display the error messages, event messages, and packets received, use the **debug cdma pdsn cluster** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug cdma pdsn cluster {message [**error | events | packets**] **redundancy** [**error | events | packets**]}

no debug cdma pdsn cluster {message [**error | events | packets**] **redundancy** [**error | events | packets**]}

Syntax Description

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 Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# debug cdma pdsn cluster ?

  message     Debug PDSN cluster controller messages
  redundancy  Debug PDSN cluster controller redundancy
```

debug cdma pdsn ipv6

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

debug cdma pdsn ipv6

no debug cdma pdsn ipv6

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

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

Usage Guidelines

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

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

debug cdma pdsn prepaid

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

debug cdma pdsn prepaid

no debug cdma pdsn prepaid

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

```
Router# debug cdma pdsn prepaid

*Mar  1 00:09:38.391: CDMA-PREPAID:  Initialized the authorization request
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added username into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added CLID into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added session id for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added correlation id into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added auth reason for prepaid into A-V list
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added USER_ID for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Added service id for prepaid
*Mar  1 00:09:38.391: CDMA-PREPAID:   Built prepaid VSAs
*Mar  1 00:09:38.391: CDMA-PREPAID:   Sent the request to AAA
*Mar  1 00:09:38.391: CDMA-PREPAID:   Auth_reason: CRB_RSP_PEND_INITIAL_QUOTA
*Mar  1 00:09:38.395: CDMA-PREPAID:   Received prepaid response: status 2
*Mar  1 00:09:38.395: CDMA-PREPAID:   AAA authorised parms being processed
*Mar  1 00:09:38.395: CDMA-PREPAID:   Attr in Grp Prof: crb-entity-type
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: AAA_AT_CRB_ENTITY_TYPE
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: entity type returns 1
*Mar  1 00:09:38.395: CDMA-PREPAID:   Attr in Grp Prof: crb-duration
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: AAA_AT_CRB_DURATION
*Mar  1 00:09:38.395: (0x4B000000) CDMA/PREPAID: duration returns 120
*Mar  1 00:09:38.395: CDMA-PREPAID:   Retrieved attributes successfully
*Mar  1 00:09:38.395: CDMA-PREPAID:   Reset duration to 120, mn 9.3.0.1
*Mar  1 00:09:38.395: CDMA-PREPAID: : Started duration timer for 120 sec
```

debug cdma pdsn qos

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

debug cdma pdsn qos

no debug cdma pdsn qos

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values for this command.

Command History

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

Examples

There are currently no sample outputs for this command.

debug cdma pdsn radius disconnect nai

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

debug cdma pdsn radius disconnect nai

no debug cdma pdsn radius disconnect nai

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

Examples

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

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

Jan 5 12:17:59.671: CDMA-POD: Delete flow for NAI: mwtr-mip-sa2sp1-user1@ispxyz.com

debug cdma pdsn redundancy attributes

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

debug cdma pdsn redundancy attributes

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy errors

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

debug cdma pdsn redundancy errors

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy events

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

debug cdma pdsn redundancy events

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn redundancy packets

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

debug cdma pdsn redundancy packets

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

debug cdma pdsn resource-manager

To display debug messages that help you monitor the resource-manager information, use the **debug cdma pdsn resource-manager** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug cdma pdsn resource-manager [error | events]

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

Syntax Description

errors	Displays Packet Data Service node (PDSN) resource manager errors.
events	Displays PDSN resource manager events.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **debug cdma pds resource-manager** command:

```
Router# debug cdma pdsn resource-manager

   errors  CDMA PDSN resource manager errors
   events  CDMA PDSN resource manager events
```

debug cdma pdsn selection

To display debug messages for the intelligent Packet Data Serving Node (PDSN) selection feature, use the **debug cdma pdsn selection** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn selection events

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

debug cdma pdsn service-selection

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

debug cdma pdsn service-selection

no debug cdma pdsn service-selection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# debug cdma pdsn service-selection

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

debug cdma pdsn session

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

debug cdma pdsn session [errors | events]

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

Syntax Description

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 Modes

Privileged EXEC

Command History

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

Examples

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

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

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

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

debug condition

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

Example 1

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

```
Router# debug condition username user1

Condition 1 set
```

Example 2

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

```
Router# debug condition vcid 1000

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

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

```
Router# debug mpls l2transport vc event

AToM vc event debugging is on

Router# debug mpls l2transport vc fsm

AToM vc fsm debugging is on
```

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

```
Router(config)# interface s3/1/0
Router(config-if)# shut
```

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

```
01:15:59: AToM MGR [13.13.13.13, 1000]: Event local down, state changed from established
to remote ready
01:15:59: AToM MGR [13.13.13.13, 1000]: Local end down, vc is down
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing imposition update, vc_handle 6227BCF0,
update_action 0, remote_vc_label 18
01:15:59: AToM SMGR [13.13.13.13, 1000]: Imposition Disabled
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing disposition update, vc_handle
6227BCF0, update_action 0, local_vc_label 755
01:16:01:%LINK-5-CHANGED: Interface Serial3/1/0, changed state to administratively down
01:16:02:%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1/0, changed state to
down
```

Related Commands

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

debug ip mobile

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

```
Router# debug ip mobile advertise

MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8 )
FA Challenge value:769C808D
```

Table 1 describes the significant fields shown in the display.

Table 1 debug ip mobile advertise Field Descriptions

Field	Description
type	Type of advertisement.
len	Length of extension (in bytes).
seq	Sequence number of this advertisement.
lifetime	Lifetime (in seconds).
flags	Capital letters represent bits that are set; lowercase letters represent unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.
FA Challenge value	Foreign Agent challenge value (randomly generated by the foreign agent.)

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

```
Router# debug ip mobile host

MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA
68.0.0.31 HA 66.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6

MobileIP: HA sent reply to MN 20.0.0.6
```

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

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

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

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

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

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

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

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

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

debug ip mobile cdma ipsec

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

debug ip mobile cdma ipsec

no debug ip mobile cdma ipsec

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command History

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

Examples

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

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

interface cdma-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.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

Examples

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

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

ip mobile authentication ignore-spi

no ip mobile authentication ignore-spi

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

ip mobile bindupdate

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

ip mobile cdma imsi dynamic

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

ip mobile cdma imsi dynamic

no ip mobile cdma imsi dynamic

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Examples

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

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

ip mobile cdma ipsec

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

ip mobile cdma ipsec

no ip mobile cdma ipsec

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

ip mobile foreign-agent

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

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

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

Syntax Description

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

Defaults

reg-wait *seconds*: 15

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on an interface or when no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated. The registration bitflag is handled as described in Table 2. The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending** command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in Table 3). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command).

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

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

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

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

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

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

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

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

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

Table 2 lists mobile node registration request service bitflags.

Table 2 Mobile Node Registration Request Service Bitflags

Bit Set	Registration Request
S	No operation. Not applicable to foreign agent.
B	No operation. Not applicable to foreign agent.
D	Make sure source IP address belongs to the network of the interface.
M	Deny request. Minimum IP encapsulation is not supported.
G	No operation. GRE encapsulation is supported.
r	Sent as zero; ignored on reception. Do not allocate for any other uses.
V	Reserved.
T	Deny if reverse tunneling is disabled on the foreign agent.
reserved	Deny request. Reserved bit must not be set.

Table 3 lists foreign agent reply codes.

Table 3 Foreign Agent Reply Codes

Code	Reason
64	Reason unspecified.
65	Administratively prohibited.
66	Insufficient resource.
67	Mobile node failed authentication.
68	Home agent failed authentication.
69	Requested lifetime is too long.
70	Poorly formed request.
71	Poorly formed reply.
72	Requested encapsulation is unavailable.
74	Reverse tunnel unsupported.
75	Reverse tunnel is mandatory and T bit is not set.
76	Mobile node too distant.
77	Invalid care-of address.
78	Registration timeout.
79	Delivery style not supported.
80	Home network unreachable (ICMP error received).
81	Home agent host unreachable (ICMP error received).
82	Home agent port unreachable (ICMP error received).
88	Home agent unreachable (other ICMP error received).
98	Missing home agent.
99	Missing home agent address.

Table 3 Foreign Agent Reply Codes (continued)

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

Examples

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

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

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

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

Related Commands

Command	Description
debug ip mobile advertise	Displays advertisement information.
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.
show ip route mobile	Displays the current state of the routing table for mobile routes.

ip mobile foreign-service

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

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

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

Syntax Description

challenge	(Optional) Configures the foreign agent challenge parameters. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
forward-mfce	(Optional) Enables the foreign agent to forward mobile foreign challenge extensions (MFCEs) and mobile node-AAA extensions to the home agent.
timeout *value*	(Optional) Challenge timeout in seconds. Possible values are from 1 to 10.
window *number*	(Optional) Maximum number of valid challenge values to maintain. Possible values are from 1 to 10. The default is 2.
home-access *access-list*	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
limit *number*	(Optional) Number of visitors allowed on the interface. The Busy (B) bit will be advertised when the number of registered visitors reaches this limit. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
registration-required	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
reverse-tunnel [**mandatory**]	(Optional) Enables reverse tunneling on the foreign agent. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

Defaults

Foreign agent service is not enabled.
There is no limit to the number of visitors allowed on an interface.
window *number:* 2
Foreign agent reverse tunneling is not enabled. When foreign agent reverse tunneling is enabled, it is not mandatory by default.

Command Modes

Interface and global configuration

Command History

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

Usage Guidelines

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

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

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

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

Table 4 lists the advertised bitflags.

Table 4 Foreign Agent Advertisement Bitflags

Bit Set	Service Advertisement
T	Set if the **reverse-tunnel** parameter is enabled.
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	Reserved.
reserved	Never set.

Examples

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

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

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

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

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

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

Related Commands

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

ip mobile foreign-service revocation

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

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

Syntax Description

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

Usage Guidelines

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

Examples

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

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

ip mobile prefix-length

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

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

This command has no arguments or keywords.

Defaults

The prefix-length extension is not appended.

Command Modes

Interface and Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
ip mobile prefix-length
```

Related Commands

Command	Description
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, use the **ip mobile proxy-host** command in global configuration mode. To remove the configuration, use the **no** form of this command.

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

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

Syntax Description

nai *username@realm*	Network access identifier.
flags *rrq-flags*	(Optional) Registration request flags.
home-agent *ip-address*	(Optional) IP address of the home agent.
home-addr *home-address*	(Optional) Home IP address of the mobile node.
lifetime *seconds*	(Optional) Global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Values are from 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
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.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T for Packet Data Serving Node (PDSN) platforms.

Usage Guidelines

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

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

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

Examples

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

```
ip mobile proxy-host nai moiproxy1@cisco.com flags 40 home-agent 10.3.3.1 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 or global 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 and global configuration

Command History

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

Usage Guidelines

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** command in global configuration mode. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address [upper-address]* | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix**]

no ip mobile secure {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address [upper-address]* | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix**]

Syntax Description

aaa-download	Downloads security association from AAA at every timer interval.
host	Security association of the mobile host on the home agent.
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. This keyword is only available on Packet Data Serving Node (PDSN) platforms.
lower-address	IP address of a host or lower range of IP address pool.
upper-address	(Optional) Upper range of an IP address pool. If specified, security associations for multiple hosts are configured. The value used in the *upper-address* argument must be greater than that used in the *lower-address* argument.
nai *string*	Network access identifier of the mobile node. The **nai** *string* is valid only for a host, visitor, and proxy host.
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 hex *string*	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Specifies replay protection used on registration packets.
timestamp	(Optional) Validates incoming packets to ensure that they are not being “replayed” by a spoofer using the timestamp method.
number	(Optional) Number of seconds. Registration is valid if received within the router’s clock +/- 7 seconds. This means the sender and receiver are in time synchronization (NTP can be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
hmac-md5	(Optional) Hash-based message authentication code (HMAC) 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	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added and this command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

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

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

The HMAC-MD5 authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), and foreign-home authentication (FHAE)

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

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

The **nai** keyword is valid only for a host, visitor, and proxy host.

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

Note NTP is not required for operation but NTP can be used to synchronize time for all parties.

Examples

The following example shows mobile node 10.0.0.4, which has a key that is generated by the MD5 hash of the string:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

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

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** command in global configuration mode. To disable the setting of tunnels created by Mobile IP, use the **no** form of this command.

ip mobile tunnel {**crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag*}

no ip mobile tunnel {**crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag*}

Syntax Descriptionl

crypto map	Enables encryption or decryption on new tunnels. This keyword is only available on platforms running specific Packet Data Serving Node (PDSN) code images.
map-name	The name of the crypto map. This argument is available only on platforms running specific PDSN code images.
route-cache	Sets tunnels to fast-switching mode.
cef	Sets tunnels to Cisco Express Forwarding (CEF) switching mode if CEF is enabled on the router.
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.
route-map *map-tag*	Defines a meaningful name for the route map.

Defaults

Disabled.

If enabled, default value for the *minutes* argument is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	The **nat**, **inside**, and **outside** keywords were added.
12.2T	The **cef** keyword was added.
12.2(13)T	The **route-map** keyword and *map-tag* argument were added.
12.3(4)T	The **crpto map** keyword and *map-name* argument were added for PDSN platforms.

Usage Guidelines

Path MTU Discovery is used by end stations to find a packet size that does not need to be fragmented when being sent between the end stations. Tunnels must adjust their MTU to the smallest MTU interior to achieve this condition, as described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from a case where suboptimum MTU existed at time of discovery. It is reset to the outgoing MTU of the interface.

The **no ip mobile tunnel route-cache** command disables fast switching and CEF switching (if CEF is enabled) on Mobile IP tunnels. The **no ip mobile tunnel route-cache cef** command disables CEF switching only.

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

The **crypto map** *map-name* keyword and argument combination are available only on platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Examples

The following example sets the discovered tunnel MTU to expire in 10 minutes (600 seconds):

```
ip mobile tunnel path-mtu-discovery age-timer 600
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.
show ip mobile tunnel	Displays active tunnels.

ppp authentication

To enable at least one PPP authentication protocol and to specify the order in which the protocols are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

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

no ppp authentication

Syntax Description

protocol1 [*protocol2...*]	At least one of the keywords described in Table 5.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if authentication has already been provided. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with authentication, authorization, and accounting (AAA). Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command.
default	(Optional) Name of the method list created with the **aaa authentication ppp** command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(1)	The **optional** keyword was added.
12.1(3)XS	The **optional** keyword was added.
12.2(2)XB5	Support for the **eap** authentication protocol was added on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS5400 platforms.
12.2(13)T	The **eap** authentication protocol support introduced in Cisco IOS Release 12.2(2)XB5 was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you enable Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

You can enable CHAP, Microsoft CHAP (MS-CHAP), PAP, or EAP in any order. If you enable all four methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the ability of the remote device to correctly negotiate the appropriate method and on the level of data-line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

Caution If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 5 lists the protocols used to negotiate PPP authentication.

Table 5 ppp authentication Protocols

chap	Enables CHAP on a serial interface.
eap	Enables EAP on a serial interface.
ms-chap	Enables MS-CHAP on a serial interface.
pap	Enables PAP on a serial interface.

Enabling or disabling PPP authentication does not affect the ability of the local router to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

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

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

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

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

The following example enables EAP on dialer interface 1:

```
interface dialer 1
 encapsulation ppp
 ppp authentication eap
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
autoselect	Configures a line to start an ARAP, PPP, or SLIP session.
encapsulation	Sets the encapsulation method used by the interface.
ppp accm	Identifies the ACCM table.
username	Establishes a username-based authentication system, such as PPP, CHAP, and PAP.