cdma pdsn debug show-conditions

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

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

cdma pdsn failure-history

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

cdma pdsn failure-history *entries*

no cdma pdsn failure-history

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn ingress-address-filtering

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

cdma pdsn ingress-address-filtering

no cdma pdsn ingress-address-filtering

Syntax Description

This command has no arguments or keywords.

Defaults

Ingress address filtering is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables ingress address filtering:

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

Related Commands

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

cdma pdsn ipv6

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

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

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

Syntax Description

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

cdma pdsn maximum pcf

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

cdma pdsn maximum pcf *maxpcf*

no cdma pdsn maximum pcf

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example specifies that 200 PCFs can be sent:

```
cdma pdsn maximum pcf 200
```

Related Commands

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

cdma pdsn maximum sessions

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

cdma pdsn maximum sessions *maxsessions*

no cdma pdsn maximum sessions

Syntax Description

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

Defaults

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

Command Modes

Global Configuration.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The maximum number of mobile sessions was raised to 20000.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

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

Examples

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

```
cdma pdsn maximum sessions 100
```

Related Commands

Command	Description
show cdma pdsn session	Displays PDSN session information.

cdma pdsn mobile-advertisement-burst

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

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

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

Syntax Description

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

Defaults

The default number of agent advertisements to send is 5.

The default interval between advertisements is 200 milliseconds.

Command Modes

Interface Configuration.

Command History

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

Usage Guidelines

You must specify at least one of the optional parameters. Otherwise, the command has no effect. When virtual-access interfaces are created from the virtual template, default values will be used for any parameters not already configured on the virtual template.

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

Examples

The following example configures PDSN FA advertisement:

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

Related Commands

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

cdma pdsn msid-authentication

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

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

no cdma pdsn msid-authentication

Syntax Description

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

Defaults

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

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

Command Modes

Global Configuration.

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(2)XC	The **profile-password** keyword was added.
12.2(8)ZB1	The **close-session-on-failure** keyword was added
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

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

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

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

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

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

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

Examples

The following example enables MSID-based authentication and access:

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

Related Commands

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

cdma pdsn pcf default closed-rp

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

cdma pdsn pcf default closed-rp

no cdma pdsn pcf default closed-rp

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default setting is that Closed-RP is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

cdma pdsn radius disconnect

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

cdma pdsn radius disconnect [nai]

no cdma pdsn radius disconnect [nai]

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

cdma pdsn redundancy

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

cdma pdsn redundancy

no cdma pdsn redundancy

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default setting is that PDSN redundancy is disabled.

Command Modes

Global configuration

Command History

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

Examples

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

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

cdma pdsn redundancy accounting send vsa swact

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

cdma pdsn redundancy accounting send vsa swact

no cdma pdsn redundancy accounting send vsa swact

Syntax Description

There are no keywords or arguments for this command.

Defaults

By default, this command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

cdma pdsn redundancy accounting update-periodic

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

cdma pdsn redundancy accounting [update-periodic]

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

Syntax Description

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

Defaults

By default, this command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

cdma pdsn retransmit a11-update

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

cdma pdsn retransmit a11-update *number*

no cdma pdsn retransmit a11-update

Syntax Description

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

Defaults

5 retransmissions.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn secure cluster

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

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

no cdma pdsn secure cluster

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn secure pcf

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

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

no cdma pdsn secure pcf

Syntax Description

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

Defaults

There are no default behavior or values.

Command Modes

Global Configuration

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.2(8)BY1	The **local-timezone** keyword was added.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

cdma pdsn selection interface

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

cdma pdsn selection interface *interface_name*

no cdma pdsn selection interface

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
cdma pdsn selection keepalive	Specifies the keepalive time.

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

cdma pdsn selection keepalive

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

cdma pdsn selection keepalive *value*

no cdma pdsn selection keepalive

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Examples

The following example configures a keepalive value of 200 seconds:

```
cdma pdsn selection keepalive 200
```

Related Commands

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

cdma pdsn selection load-balancing

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

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

no cdma pdsn selection load-balancing

Syntax Description

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

Defaults

The threshold value is 100 sessions.

Command Modes

Global Configuration

Command History

Release	Modification
12.1(3)XS	This command was introduced.
12.2(8)BY	The maximum number of sessions that can be load-balanced was raised to 20000.
12.3(4)T	This command was incorporated in Cisco IOS Release 12.3(4)T.

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn selection session-table-size

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

cdma pdsn selection session-table-size *size*

no cdma pdsn selection session-table-size

Syntax Description

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

Defaults

PDSN selection is disabled.

The default session table size is undefined.

Command Modes

Global Configuration

Command History

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

Examples

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

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

Related Commands

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

cdma pdsn send-agent-adv

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

cdma pdsn send-agent-adv

no cdma pdsn send-agent-adv

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

This command is used with multiple flows.

Examples

The following example enables agent advertisements to be sent:

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

Related Commands

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

cdma pdsn timeout

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

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

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

Syntax Description

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

Defaults

a11-session-update default value is 1 second.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

PDSN may initiate the release of an A10 connection by sending an A11 Registration Update message to the PCF. In this case, the PCF is expected to send an A11 Registration Acknowledge message followed by an A11 Registration Request with Lifetime set to 0. If PDSN does not receive an A11 Registration Acknowledge or an A11 Registration Request with Lifetime set to 0, PDSN times out and retransmits the A11 Registration Update. The default timeout is 1 second and is configurable using this command.

Examples

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

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

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

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

Related Commands

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

cdma pdsn timeout mobile-ip-registration

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

cdma pdsn timeout mobile-ip-registration *timeout*

no cdma pdsn timeout mobile-ip-registration

Syntax Description

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

Defaults

5 seconds.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

cdma pdsn virtual-template

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

cdma pdsn virtual-template *virtualtemplate_num*

no cdma pdsn virtual-template *virtualtemplate_num*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global Configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear cdma pdsn cluster controller session records age

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

clear cdma pdsn cluster controller session *records age days*

Syntax Description

days	The number of days of the record age.

Defaults

No default keywords or arguments.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows output from the **clear cdma pdsn cluster controller session** *records age* command:

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

clear cdma pdsn cluster controller statistics

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

clear cdma pdsn cluster controller statistics [queuing | redundancy]

Syntax Description

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

Defaults

There are no default values for this command.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear cdma pdsn cluster member statistics

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

clear cdma pdsn cluster controller statistics [queuing | redundancy]

Syntax Description

queuing	Clear s statistics associated with controller queuing feature.

Defaults

There are no default values for this command.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear cdma pdsn redundancy statistics

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

clear cdma pdsn redundancy statistics

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

EXEC mode

Command History

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

Examples

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

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

clear cdma pdsn selection

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

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

Syntax Description

pdsn *ip-addr*	(Optional) IP address of the PDSN selection session table to be cleared.
msid *number*	(Optional) Identification of the MSID to be cleared.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example clears the pdsn selection session table for PDSN 5.5.5.5:

```
clear cdma pdsn selection pdsn 5.5.5.5
```

Related Commands

Command	Description
cdma pdsn selection session-table-size	Enables the PDSN selection feature and defines the size of the session table.

clear cdma pdsn session

To clear one or more user sessions on the PDSN, use the **clear cdma pdsn session** command in privileged EXEC mode.

clear cdma pdsn session {**all** | **pcf** *ip_addr* | **msid** *number*}

Syntax Description

all	Keyword to clear all sessions on a given PDSN.
pcf *ip_addr*	IP address of the PCF sessions that are to be cleared.
msid *number*	Identification of the MSID to be cleared.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command terminates one or more user sessions. When this command is issued, the PDSN initiates the session release by sending an A11Registration Update message to the PCF.

The keyword **all** clears all sessions on a given PDSN. The keyword **pcf** with an IP address clears all the sessions coming from a given PCF. The keyword **msid** with a number will clear the session for a given MSID.

Examples

The following example clears session MSID 0000000002:

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

Related Commands

Command	Description
show cdma pdsn session	Displays PDSN session information.

clear cdma pdsn statistics

To clear the RAN-to-PDSN interface (RP) or PPP statistics on the PDSN, use the **clear cdma pdsn statistics** command in privileged EXEC mode.

clear cdma pdsn statistics

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

Before counters are reset

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

Note Non-zero values of counters.

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

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

```
  Registration Update Errors:
    Unspecified 0, Identification mismatch 0
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0

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

After the counters are reset

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

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

Note The counter values are zeroes.

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

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

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

Related Commands

Command	Description
show cdma pdsn statistics	Displays PDSN statistics.

clear ip mobile visitor

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

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

Syntax Description

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

Command Modes

EXEC

Command History

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

Usage Guidelines

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

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

If the **nai** *string* **session-id** *string* option is specified, only the visitor entry with that session identifier is cleared. If the **session-id** keyword is not specified, all visitor entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id** *string* value by using the **show ip mobile visitor** command.

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

Examples

The following example administratively stops visitor 172.21.58.16 from visiting:

```
Router# clear ip mobile visitor 172.21.58.16
```

Related Commands

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

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

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

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

no crypto map *map-name seq-num*

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

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.
gdoi	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

Command Default

No crypto maps exist.
Peer discovery is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** *aaalist* keyword and argument combination was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(6)T	The **gdoi** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB without support for the **gdoi** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

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

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named "mymap" is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

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

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

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving the it the highest *seq-num* value of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

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

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

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

Crypto Map Profiles

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

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

Examples

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

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

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

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

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

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

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

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

The following example configures TED on a Cisco router:

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

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

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

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

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

Related Commands

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

crypto map local-address

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

```
interface S0
 crypto map mymap

interface S1
 crypto map mymap

crypto map mymap local-address loopback0
```

Related Commands

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