

deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** command in server group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

no deadtime

Syntax Description	<i>minutes</i>	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
--------------------	----------------	--

Defaults Deadtime is set to 0.

Command Modes Server-group configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

Examples The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
 server 1.1.1.1 auth-port 1645 acct-port 1646
 server 2.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
```

■ **deadtime (server-group configuration)**

Related Commands	Command	Description
	radius-server deadtime	Sets the deadtime value globally.

default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default** command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

command-name Ca-trustpoint configuration subcommand.

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

Examples

The following example shows how to remove the **crl optional** command from your configuration; the default of **crl optional** is off.

```
default crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer aaa [**password** *string* | **suffix** *string*]

no dialer aaa [**password** *string* | **suffix** *string*]

Syntax Description

password <i>string</i>	(Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters.
suffix <i>string</i>	(Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters.

Defaults

This feature is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The password and suffix keywords were added.

Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be “cisco.”



Note

Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 1.1.1.1. The username in the access-request message is “1.1.1.1@ciscoDoD” and the password is “cisco.”

```
interface dialer1
dialer aaa
dialer aaa suffix @ciscoDoD password cisco
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.

dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** command in privileged EXEC mode.

```
disconnect ssh [vty] session-id
```

Syntax Description	
vty	(Optional) Virtual terminal for remote console access.
<i>session-id</i>	The <i>session-id</i> is the number of connection displayed in the show ip ssh command output.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.

Usage Guidelines The **clear line vty n** command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

Related Commands	Command	Description
	clear line vty	Returns a terminal line to idle state using the privileged EXEC command.

dn

To associate the identity of a router with the distinguished name (DN) in the certificate of the router, use the **dn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

```
dn name=string [, name=string]
```

```
no dn name=string [, name=string]
```

Syntax Description

<i>name=string</i>	Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.
--------------------	---

Command Default

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **dn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the DN that the peer used to authenticate itself.



Note

The *name* defined in the **crypto identity** command must match the *string* defined in the **dn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the *name=string*.

Examples

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “green”:

```
crypto map map-to-green 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-green
!
crypto identity to-green
  dn ou=green
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

dnis (authentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

```
dnis [if-avail | required] [accept-stop] [password string]
```

```
no dnis [if-avail | required] [accept-stop] [password string]
```

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.
password string	(Optional) Password to use in the Access-Request packet. The default is cisco.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 group radius
 dnis password Ascend-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

dnis (RADIUS)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

```
dnis [if-avail | required] [accept-stop] [password password]
```

```
no dnis [if-avail | required] [accept-stop] [password password]
```

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as clid or ctype from being tried once preauthentication has succeeded for a call element.
password <i>password</i>	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
  group radius
  dnis required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** command in AAA preauthentication configuration mode. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

```
dnis bypass {dnis-group-name}
```

```
no dnis bypass {dnis-group-name}
```

Syntax Description

<i>dnis-group-name</i>	Name of the defined DNIS group.
------------------------	---------------------------------

Defaults

No DNIS numbers are bypassed for preauthentication.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
  dnis required
  dnis bypass hawaii

dialer dnis group hawaii
 number 12345
 number 12346
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.

dns

To specify the primary and secondary Domain Name Service (DNS) servers, use the **dns** command in (Internet Security Association Key Management Protocol) ISAKMP group configuration mode. To remove this command from your configuration, use the **no** form of this command.

dns *primary-server secondary-server*

no dns *primary-server secondary-server*

Syntax Description

<i>primary-server</i>	Name of the primary DNS server.
<i>secondary-server</i>	Name of the secondary DNS server.

Defaults

A DNS server is not specified.

Command Modes

ISAKMP group configuration

Command History

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

Usage Guidelines

Use the **dns** command to specify the primary and secondary DNS servers for the group.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the **dns** command.

Examples

The following example shows how to define a primary and secondary DNS server for the default group name:

```
crypto isakmp client configuration group default
key cisco
dns 2.2.2.2 2.3.2.3
pool dog
acl 199
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies which group's policy profile will be defined.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.

dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no** form of this command.

dnsix-dmdp retries *count*

no dnsix-dmdp retries *count*

Syntax Description	<i>count</i>	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.
---------------------------	--------------	--

Defaults Retransmits messages up to 4 times, or until acknowledged.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands	Command	Description
		dnsix-nat authorized-redirection
	dnsix-nat primary	Specifies the IP address of the host to which DNSIX audit messages are sent.
	dnsix-nat secondary	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
	dnsix-nat source	Starts the audit-writing module and defines audit trail source address.
	dnsix-nat transmit-count	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

dnsix-nat authorized-redirection

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

dnsix-nat authorized-redirection *ip-address*

no dnsix-nat authorized-redirection *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the host from which redirection requests are permitted.
---------------------------	-------------------	---

Defaults	An empty list of addresses.
-----------------	-----------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	Use multiple dnsix-nat authorized-redirection commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.
-------------------------	---

Examples	The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:
-----------------	--

```
dnsix-nat authorization-redirection 192.168.1.1
```

dnsix-nat primary

To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat primary *ip-address*

no dnsix-nat primary *ip-address*

Syntax Description

<i>ip-address</i>	IP address for the primary collection center.
-------------------	---

Defaults

Messages are not sent.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An IP address must be configured before audit messages can be sent.

Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.1.1.1
```

dnsix-nat secondary

To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat secondary *ip-address*

no dnsix-nat secondary *ip-address*

Syntax Description

<i>ip-address</i>	IP address for the secondary collection center.
-------------------	---

Defaults

No alternate IP address is known.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Examples

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To start the audit-writing module and to define the audit trail source address, use the **dnsix-nat source** command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

dnsix-nat source *ip-address*

no dnsix-nat source *ip-address*

Syntax Description	<i>ip-address</i> Source IP address for DNSIX audit messages.
---------------------------	---

Defaults	Disabled
-----------------	----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	You must issue the dnsix-nat source command before any of the other dnsix-nat commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.
-------------------------	---

Examples	<p>The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:</p> <pre>dnsix-nat source 192.168.2.5 interface ethernet 0 ip address 192.168.2.5 255.255.255.0</pre>
-----------------	---

dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command in global configuration mode. To revert to the default audit message count, use the **no** form of this command.

dnsix-nat transmit-count *count*

no dnsix-nat transmit-count *count*

Syntax Description

<i>count</i>	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.
--------------	---

Defaults

One message is sent at a time.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Examples

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

<i>name</i>	Name of the DNS domain.
-------------	-------------------------

Defaults

A DNS domain is not specified.

Command Modes

ISAKMP group configuration

Command History

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

Usage Guidelines

Use the **domain** command to specify group domain membership.

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that needs to be defined or changed, before enabling the domain command.

Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 2.2.2.2 2.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies which group’s policy profile will be defined.
dns	Specifies the primary and secondary DNS servers.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

enable password [**level** *level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level <i>level</i>	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
<i>password</i>	Password users type to enter enable mode.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default is level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.

**Caution**

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter *abc?123* at the password prompt.

Examples

The following example enables the password “pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “\$1\$i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the enable password command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

enable secret [*level level*] {*password* | [*encryption-type*] *encrypted-password*}

no enable secret [*level level*]

Syntax Description

<i>level level</i>	(Optional) Level for which the password applies. You can specify up to sixteen privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (traditional enable privileges). The same holds true for the no form of the command.
<i>password</i>	Password for users to enter enable mode. This password should be different from the password created with the enable password command.
<i>encryption-type</i>	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available for this command is 5. If you specify <i>encryption-type</i> , the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).
<i>encrypted-password</i>	Encrypted password you enter, copied from another router configuration.

Defaults

No password is defined. The default level is 15.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines



Caution

If neither the **enable password** command nor the **enable secret** command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a non-reversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you paste into this command an encrypted password that you copied from a router configuration file.

**Caution**

If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

**Note**

After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If **service password-encryption** is set, the encrypted form of the password you create here is displayed when a **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters
- Must not have a number as the first character
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password *abc?123*, do the following:
 - Enter **abc**.
 - Type **Ctrl-v**.
 - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter **abc?123** at the password prompt.

Examples

The following example specifies the enable secret password of “greentree”:

```
enable secret greentree
```

After specifying an enable secret password, users must enter this password to gain access. Any passwords set through enable password will no longer work.

```
Password: greentree
```

The following example enables the encrypted password “\$1\$FaD0\$Xyti5Rkls3LoyxzS8”, which has been copied from a router configuration file, for privilege level 2 using encryption type 5:

```
enable password level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Related Commands	Command	Description
	enable	Enters privileged EXEC mode.
	enable password	Sets a local password to control access to various privilege levels.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

```
encryption { des | 3des | aes | aes 192 | aes 256 }
```

```
no encryption
```

Syntax Description	des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
	3des	168-bit DES (3DES) as the encryption algorithm.
	aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
	aes 192	192-bit AES as the encryption algorithm.
	aes 256	256-bit AES as the encryption algorithm.

Defaults The 56-bit DES-CBC encryption algorithm

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.0(2)T	The 3des option was added.
	12.2(13)T	The following keywords were added: aes , aes 192 , and aes 256 .

Usage Guidelines Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
 encryption method for ISAKMP policy 1
```

Related Commands	Command	Description
	authentication (IKE policy)	Specifies the authentication method within an IKE policy.
	crypto isakmp policy	Defines an IKE policy.
	group (IKE policy)	Specifies the DH group identifier within an IKE policy.
	hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
	lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
	show crypto isakmp policy	Displays the parameters for each IKE policy.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name* *port-num*

Syntax Description

<i>host-name</i>	Defines the proxy server used to get the CA.
<i>port-num</i>	Specifies the port number used to access the CA.

Defaults

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
enrollment url http://kahului
enrollment http-proxy bomborra 8080
crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry count

The **enrollment retry count** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry period

The **enrollment retry period** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

A user may wish to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples

The following example shows how to specify manually certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
  enrollment terminal
  crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-identity)

The **enrollment url (ca-identity)** command is replaced by the **enrollment url (ca-trustpoint)** command. See the **enrollment url (ca-trustpoint)** command for more information.

enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

```
enrollment [mode] [retry period minutes] [retry count number] url url [pem]
```

```
no enrollment [mode] [retry period minutes] [retry count number] url url [pem]
```

Syntax Description

mode	(Optional) Registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period <i>minutes</i>	(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 through 60 minutes.)
retry count <i>number</i>	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 through 100 retries.)
url <i>url</i>	URL of the file system where your router should send certificate requests. For enrollment method options, see Table 15 .
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

Your router does not know the CA URL until you specify it using **url** *url*.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3T	This command was introduced as the enrollment url (ca-identity) command.
12.2(8)T	This command replaced the enrollment url (ca-identity) command. The mode , retry period <i>minutes</i> , and retry count <i>number</i> keywords and arguments were added.
12.2(13)T	The url <i>url</i> option was enhanced to support TFTP enrollment.
12.3(4)T	The pem keyword was added, and the url <i>url</i> option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another

certificate request. By default, the router will send a maximum of 10 requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count number** option) is exceeded.

Use the **pem** keyword to issue certificate requests (using the **crypto pki enroll** command) or receive issued certificates (using the **crypto pki import certificate** command) in PEM-formatted files.

**Note**

When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the **crypto pki authenticate** command.

Use the **url url** option to specify or change the URL of the CA. [Table 15](#) lists the available enrollment methods.

Table 15 Certificate Enrollment Methods

Enrollment Method	Description
bootflash	Enroll via bootflash: file system
cns	Enroll via Cisco Networking Services (CNS): file system
flash	Enroll via flash: file system
ftp	Enroll via FTP: file system
SCEP ¹	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
null	Enroll via null: file system
nvrाम	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
system	Enroll via system: file system
TFTP ²	Enroll via TFTP: file system

1. If you are using SCEP for enrollment, the URL must be in the form `http://CA_name`, where `CA_name` is the host Domain Name System (DNS) name or IP address of the CA.
2. If you are using TFTP for enrollment, the URL must be in the form `tftp://certserver/file_specification`. (The `file_specification` is optional. See the section “TFTP Certificate Enrollment” for additional information.)

TFTP Certificate Enrollment

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the `file_specification` is included in the URL, the router will append an extension onto the file specification. When the **crypto pki authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url url** option does not include a file specification, the FQDN of the router will be used.)

**Note**

The **crypto pki trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all **ca-identity** and **trusted-root** configuration mode commands). If you enter a **ca-identity** or **trusted-root** subcommand, the configuration mode and command will be written back as **pki-trustpoint**.

Examples

The following example shows how to declare a CA named “ka” and specify the URL of the CA as “http://kahului:80”:

```
crypto pki trustpoint ka
enrollment url http://kahului:80
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

evaluate *name*

no evaluate *name*

Syntax Description

<i>name</i>	The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the permit (reflexive) command.
-------------	---

Defaults

Reflexive access lists are not evaluated.

Command Modes

Access-list configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit** (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Examples

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
  description Access to the Internet via this interface
  ip access-group inboundfilters in
!
ip access-list extended inboundfilters
  permit 190 any any
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
```

Related Commands

Command	Description
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

fqdn (ca-trustpoint)

To specify a fully qualified domain name (FQDN) that will be included as “unstructuredName” in the certificate request, use the **fqdn** command in ca-trustpoint configuration mode. To remove the FQDN, use the **no** form of this command.

```
fqdn {name | none}
```

```
no fqdn {name | none}
```

Syntax Description

<i>name</i>	FQDN that will be included as “unstructuredName” in the certificate request.
none	Router FQDN will not be included in the certificate request.

Defaults

The FQDN is not configured. The router FQDN will be included as “unstructuredName” in the certificate request.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **fqdn** command is a subcommand that allows you to specify a certificate enrollment parameter. Use the **fqdn** command to include a different FQDN from that of the router in the certificate request or to specify that a FQDN should not be included in the certificate request.

Examples

The following example shows that the FQDN “jack.cisco.com” will be included in the certificate request instead of the router FQDN:

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  fqdn none
  subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US
```

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  fqdn jack.cisco.com
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

fqdn (crypto identity)

To associate the identity of the router with the host name that the peer used to authenticate itself, use the **fqdn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

fqdn *name*

no fqdn *name*

Syntax Description

<i>name</i>	Identity used to restrict access to peers with specific certificates.
-------------	---

Defaults

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

Use the **fqdn** command to associate the identity of the router, which is defined in the **crypto identity** command, with the distinguished name (DN) in the certificate of the router. This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DN, from having access to selected encrypted interfaces.



Note

The name argument defined in the **crypto identity** command must match the *name* argument defined in the **fqdn** command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

Examples

The following example shows how to configure a crypto map that can be used only by peers that have been authenticated by hostname and if the certificate belongs to “little.com”:

```
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
```

■ fqdn (crypto identity)

Related Commands	Command	Description
	crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
	crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.

group (authentication)

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

```
group {tacacs+ server-group}
```

```
no group {tacacs+ server-group}
```

Syntax Description

tacacs+	Uses a TACACS+ server for authentication.
<i>server-group</i>	Name of the server group to use for authentication.

Defaults

No method list is configured.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (IKE policy)

To specify the Diffie-Hellman group identifier within an Internet Key Exchange (IKE) policy, use the **group** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

group {1 | 2}

no group

Syntax Description	1	2
	Specifies the 768-bit Diffie-Hellman group.	Specifies the 1024-bit Diffie-Hellman group.

Defaults 768-bit Diffie-Hellman (group 1)

Command Modes ISAKMP policy configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

Examples The following example configures an IKE policy with the 1024-bit Diffie-Hellman group (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 group 2
 exit
```

Related Commands	Command	Description
	authentication (IKE policy)	Specifies the authentication method within an IKE policy.
	crypto isakmp policy	Defines an IKE policy.
	encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
	hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
	lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
	show crypto isakmp policy	Displays the parameters for each IKE policy.

group (RADIUS)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

```
group server-group
```

```
no group server-group
```

Syntax Description

<i>server-group</i>	Specifies a AAA RADIUS server group.
---------------------	--------------------------------------

Defaults

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
  server 1.1.1.1
  server 2.2.2.2
  server 3.3.3.3

aaa preauth
  group maestro
  dnis required
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.

Command	Description
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

group-lock

To allow you to enter your extended authentication (Xauth) username, including the group name, when preshared key authentication is used with Internet Key Exchange (IKE), use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

group-lock

no group-lock

Syntax Description This command has no arguments or keywords.

Defaults Group lock is not configured.

Command Modes ISAKMP group configuration

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines When the group-lock command is enabled, you may enter your Xauth username as name/group, name\group, name@group, or name%group. The group specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.

Examples The following example shows that group lock is configured:

```
crypto isakmp client configuration group cisco
  group-lock
```

Command	Description
acl	Specifies which policy profile of a group will be defined.

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default SHA-1 hash algorithm, use the **no** form of this command.

```
hash {sha | md5}
```

```
no hash
```

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Defaults

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

identity

To set the identity to the crypto map, use the **identity** command in crypto map configuration mode.

identity *name*

Syntax Description	<i>name</i>	Identity used to permit or restrict access for a host to a crypto map.
Defaults	If this command is not enabled, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.	
Command Modes	Crypto map configuration	
Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines Use the **identity** command to set the identity to the configured crypto maps. When this command is applied, only the hosts that match a configuration listed within the *name* argument can use that crypto map.

Examples The following example shows how to configure two IP Security (IPSec) crypto maps and apply the identity to each crypto map. That is, the identity is set to “to-bigbiz” for the first crypto map and “to-little-com” for the second crypto map.

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
!
```

Related Commands	Command	Description
	crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
	crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
	crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
	fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

initiate-mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the **initiate-mode** command in ISAKMP profile configuration mode. To remove the mode that was configured, use the **no** form of this command.

initiate-mode aggressive

no initiate-mode aggressive

Syntax Description

aggressive	Aggressive mode is initiated.
-------------------	-------------------------------

Defaults

IKE initiates main mode.

Command Modes

ISAKMP profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

```
crypto isakmp profile vpnprofile
  initiate-mode aggressive
```

ip-address (ca-trustpoint)

To specify a dotted IP address or an interface that will be included as “unstructuredAddress” in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address { *ip-address* | *interface* | **none** }

no ip-address

Syntax Description

<i>ip-address</i>	Specifies a dotted IP address that will be included as “unstructuredAddress” in the certificate request.
<i>interface</i>	Specifies an interface, from which the router can get an IP address, that will be included as “unstructuredAddress” in the certificate request.
none	Specifies that an IP address is not to be included in the certificate request.

Defaults

An IP address is not configured. You will be prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca | pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command is a subcommand that allows you to specify a certificate enrollment parameter.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you will not be prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint “frog”:

```
crypto ca trustpoint frog
  enrollment url http://frog.phoobin.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet-0
```

The following example shows that an IP address is not to be included in the certificate request:

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  fqdn none
```

```
ip-address none
subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

ip audit

To apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction, use the **ip audit** command in interface configuration mode. To disable auditing of the interface for the specified direction, use the **no** version of this command.

```
ip audit audit-name {in | out}
```

```
no ip audit audit-name {in | out}
```

Syntax Description

<i>audit-name</i>	Name of an audit specification.
in	Inbound traffic.
out	Outbound traffic.

Defaults

No audit specifications are applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit** interface configuration command to apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction.

Examples

In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
 ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
 no ip audit MARCUS in
```

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** command in global configuration mode. To set the default action for attack signatures, use the **no** form of this command.

```
ip audit attack {action [alarm] [drop] [reset]}
```

```
no ip audit attack
```

Syntax Description	action	Specifies an action for the attack signature to take in response to a match.
	alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
	drop	(Optional) Drops the packet. Used with the action keyword.
	reset	(Optional) Resets the TCP session. Used with the action keyword.

Defaults The default action is **alarm**.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **ip audit attack** global configuration command to specify the default actions for attack signatures.

Examples In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```

ip audit info

To specify the default actions for info signatures, use the **ip audit info** command in global configuration mode. To set the default action for info signatures, use the **no** form of this command.

```
ip audit info { action [alarm] [drop] [reset] }
```

```
no ip audit info
```

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
drop	(Optional) Drops the packet. Used with the action keyword.
reset	(Optional) Resets the TCP session. Used with the action keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit info** global configuration command to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** command in global configuration mode. To delete an audit rule, use the **no** form of this command.

```
ip audit name audit-name {info | attack} [list standard-acl] [action [alarm] [drop] [reset]]
```

```
no ip audit name audit-name {info | attack}
```

Syntax Description

<i>audit-name</i>	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	(Optional) Specifies an ACL to attach to the audit rule.
<i>standard-acl</i>	(Optional) Integer representing an access control list. Use with the list keyword.
action	(Optional) Specifies an action or actions to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the action keyword.
drop	(Optional) Drops the packet. Use with the action keyword.
reset	(Optional) Resets the TCP session. Use with the action keyword.

Defaults

If an action is not specified, the default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Any signatures disabled with the **ip audit signature** command do not become a part of the audit rule created with the **ip audit name** command.

Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:

```
ip audit signature 1000 disable
ip audit name INFO.3 info action alarm drop reset
```

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

```
ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
```

ip audit notify

To specify the method of event notification, use the **ip audit notify** command in global configuration mode. To disable event notifications, use the **no** form of this command.

ip audit notify {nr-director | log}

no ip audit notify {nr-director | log}

Syntax Description

nr-director	Send messages in NetRanger format to the NetRanger Director or Sensor.
log	Send messages in syslog format.

Defaults

The default is to send messages in syslog format.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director's Post Office transport parameters using the **ip audit po remote** command.

Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

Related Commands

Command	Description
ip audit po local	Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.
ip audit po remote	Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.

ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** command in global configuration mode. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip audit po local hostid *id-number* **orgid** *id-number*

no ip audit po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description

hostid	Specifies a NetRanger host ID.
<i>id-number</i>	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.
orgid	Specifies a NetRanger organization ID.
<i>id-number</i>	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the group to which the local host belongs. The default organization ID is 1.

Defaults

The default organization ID is 1. The default host ID is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

Examples

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```

ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip audit po max-events** command in global configuration mode. To set the number of recipients to the default setting, use the **no** version of this command.

```
ip audit po max-events number-of-events
```

```
no ip audit po max-events
```

Syntax Description

number-of-events Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Defaults

The default number of events is 100.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```

ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** command in global configuration mode. To remove network addresses from the protected network list, use the **no** form of this command.

ip audit po protected *ip-addr* [**to** *ip-addr*]

no ip audit po protected [*ip-addr*]

Syntax Description	<i>ip-addr</i>	IP address of a network host.
	to <i>ip-addr</i>	(Optional) Specifies a range of IP addresses.

Defaults If no addresses are defined as protected, then all addresses are considered outside the protected network.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not.

If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

Examples In the following example, a range of addresses is added to the protected network list:

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```

ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** command in global configuration mode. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

```
ip audit po remote hostid host-id orgid org-id rmtaddress ip-address localaddress ip-address
[port port-number] [preference preference-number] [timeout seconds] [application {director
| logger}]
```

```
no ip audit po remote hostid host-id orgid org-id rmtaddress ip-address
```

Syntax	Description
hostid	Specifies a NetRanger host ID.
<i>host-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.
orgid	Specifies a NetRanger organization ID.
<i>org-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. The default organization ID is 1.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
<i>ip-address</i>	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the rmtaddress and localaddress keywords.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
<i>port-number</i>	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. The default UDP port number is 45000.
preference	(Optional) Specifies a route preference for communication.
<i>preference-number</i>	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. The default preference is 1.
timeout	(Optional) Specifies a timeout value for Post Office communications.
<i>seconds</i>	(Optional) Integer representing the heartbeat timeout value for Post Office communications. The default timeout is 5 seconds.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages. The default application is director.
director	(Optional) Specifies that the receiving application is the NetRanger Director interface.
logger	(Optional) Specifies that the receiving application is a NetRanger Sensor.

Defaults

The default organization ID is 1.

The default host ID is 1.

The default UDP port number is 45000.

The default preference is 1.

The default heartbeat timeout is 5 seconds.

The default application is **director**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

Examples

In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1
preference 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
10 application director
```

ip audit signature

To attach a policy to a signature, use the **ip audit signature** command in global configuration mode. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

```
ip audit signature signature-id { disable | list acl-list }
```

```
no ip audit signature signature-id
```

Syntax Description		
	<i>signature-id</i>	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
	disable	Disables the ACL associated with the signature.
	list	Specifies an ACL to associate with the signature.
	<i>acl-list</i>	Unique integer specifying a configured ACL on the router. Use with the list keyword.

Defaults No policy is attached to a signature.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines This command allow you to set two policies: disable the audit of a signature or qualify the audit of a signature with an access list.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the **ip audit name** command and apply it to an interface with the **ip audit** command.

Examples In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99

access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the **ip audit smtp** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description	Command	Description
	spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
	<i>number-of-recipients</i>	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default is 250 recipients.

Defaults The default number of recipients is 250.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **ip audit smtp** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

Examples In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```