

ppp accounting through quit

- ppp accounting, on page 3
- ppp authentication, on page 4
- ppp authentication ms-chap-v2, on page 7
- ppp authorization, on page 9
- ppp chap hostname, on page 10
- ppp chap password, on page 12
- ppp chap refuse, on page 14
- ppp chap wait, on page 16
- ppp eap identity, on page 18
- ppp eap local, on page 19
- ppp eap password, on page 21
- ppp eap refuse, on page 22
- ppp eap wait, on page 23
- ppp link, on page 24
- ppp pap refuse, on page 26
- ppp pap sent-username, on page 27
- preempt, on page 29
- pre-shared-key, on page 30
- pre-shared-key (IKEv2 keyring), on page 32
- prf, on page 36
- primary, on page 38
- priority (firewall), on page 39
- private-hosts, on page 40
- private-hosts layer3, on page 41
- private-hosts mac-list, on page 42
- private-hosts mode, on page 44
- private-hosts promiscuous, on page 46
- private-hosts vlan-list, on page 48
- privilege, on page 50
- privilege level, on page 55
- profile (GDOI local server), on page 57
- profile (profile map configuration), on page 58
- propagate sgt, on page 59

- propagate sgt (config-if-cts-dot1x), on page 61
- proposal, on page 63
- protection (zone), on page 64
- protocol, on page 65
- protocol (config-filter-list), on page 66
- proxy, on page 67
- publickey, on page 69
- qos-group (PVS Bundle Member), on page 70
- query certificate, on page 71
- query url, on page 73
- quit, on page 75

ppp accounting

To enable authentication, authorization, and accounting (AAA) accounting services on the selected interface, use the **ppp accounting** command in interface configuration mode. To disable AAA accounting services, use the **no** form of this command.

ppp accounting {**default***listname*}
no ppp accounting

Syntax Description

default	The name of the method list is created with the **aaa accounting** command.
listname	A specified method list.

Command Default

Accounting is disabled.

Command Modes

Interface 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.(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.
Cisco IOS XE Release 2.6	The *listname* argument was added.

Usage Guidelines

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp accounting list1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ppp authentication

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

`ppp authentication` *protocol1* [*protocol2...*] [`if-needed`*list-name*|`default`|`callin`|`one-time`|`optional`]
no ppp authentication

Syntax Description

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

Command Default

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

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

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

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

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



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

The table below lists the protocols used to negotiate PPP authentication.

Table 1: ppp authentication Protocols

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

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

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

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

Caution In Cisco IOS Release 15.0(1)S and later releases, enabling CHAP authentication only for incoming (received) calls is not supported in scenarios where the VPDN tunnel is established over a pseudowire, using the L2TP or L2TPv3 protocols. Enabling CHAP authentication only for incoming calls by using the **ppp authentication chap callin** command is not supported unless used in conjunction with the **ppp direction callout** command.

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

```
ppp authentication chap pap optional
```

Examples

The following example configures virtual-template interface 4:

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

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

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

The following example enables EAP on dialer interface 1:

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

Related Commands

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

ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

ppp authentication ms-chap-v2
no ppp authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Command Default

MSCHAP V2 authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth**command must be configured to allow at least two authentication retries and the **radius-server vsa send**command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

Examples

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
```

```
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 exit
aaa authentication ppp default group radius
 radius-server host 10.0.0.2 255.0.0.0
 radius-server key secret
 radius-server vsa send authentication
```

Related Commands

Command	Description
debug aaa authentication	Displays information on AAA/TACACS+ authorization.
debug ppp	Displays information on traffic and exchanges in a network that is implementing PPP.
debug radius	Displays information associated with RADIUS.
ppp max-bad-auth	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
radius-server vsa send	Configures the network access server to recognize and use VSAs.

ppp authorization

To enable authentication, authorization, and accounting (AAA) authorization on the selected interface, use the **ppp authorization**command in interface configuration mode. To disable authorization, use the no form of this command.

ppp authorization [**default***list-name*]
no ppp authorization

Syntax Description

default	(Optional) The name of the method list is created with the **aaa authorization** command.
list-name	(Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Command Default

Authorization is disabled.

Command Modes

Interface 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.(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

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Examples

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4
 encapsulation ppp
 ppp authorization charlie
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname**command ininterface configuration mode. To disable this function, use the **no** form of this command.

ppp chap hostname *hostname*
no ppp chap hostname *hostname*

Syntax Description

hostname	The name sent in the CHAP challenge.

Command Default

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.



Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the Multilink PPP (MLP) bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Examples

The following example shows how to identify dialer interface 0 as the dialer rotary group leader and specify ppp as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username ISPCorp will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password**command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

ppp chap password *secret*
no ppp chap password *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

Examples

The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
 encapsulation ppp
 ppp chap password 7 1234567891
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.

Command	Description
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

ppp chap refuse [**callin**]
no ppp chap refuse [**callin**]

Syntax Description

callin	(Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.

Command	Description
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap wait	Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router.

ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

ppp chap wait *secret*
no ppp chap wait *secret*

Syntax Description

secret	The secret used to compute the response value for any CHAP challenge from an unknown peer.

Command Default

Enabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.

Command	Description
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp chap refuse	Refuses CHAP authentication from peers requesting it.

ppp eap identity

To specify the Extensible Authentication Protocol (EAP) identity, use the **ppp eap identity** command in interface configuration mode. To remove the EAP identity from your configuration, use the **no** form of this command.

ppp eap identity *string*
no ppp eap identity *string*

Syntax Description

string	EAP identity.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap identity** command to configure the client to use a different identity when requested by the peer.

Examples

The following example shows how to enable EAP on dialer interface 1 and set the identity to “cat”:

```
interface dialer 1
 encapsulation ppp
 ppp eap identity cat
```

ppp eap local

To authenticate locally instead of using the RADIUS back-end server, use the **ppp eap local** command in interface configuration mode. To reenable proxy mode (which is the default), use the **no** form of this command.

ppp eap local
no ppp eap local

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication is performed via proxy mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

By default, Extensible Authentication Protocol (EAP) runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the network access server (NAS) to a back-end server that may reside on or be accessed via a RADIUS server. To disable proxy mode (and thus to authenticate locally instead of via RADIUS), use the **ppp eap local**command .

In local mode, the EAP session is authenticated using the MD5 algorithm and obeys the same authentication rules as does Challenge Handshake Authentication Protocol (CHAP).

Examples

The following example shows how to configure EAP to authenticate locally:

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

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap password

To set the Enhanced Authentication Protocol (EAP) password for peer authentication, use the **ppp eap password** command in interface configuration mode. To disable the password, use the **no** form of this command.

ppp eap password [*number*] *string*
no ppp eap password [*number*] *string*

Syntax Description

number	(Optional) Encryption type, including values 0 through 7; 0 means no encryption.
string	Character string that specifies the EAP password.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For remote EAP authentication only, you can configure your router to create a common EAP password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor or from an older running version of the Cisco IOS software) to which a new (that is, unknown) router has been added, the common password will be used to respond to the new router. The **ppp eap password**command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

Examples

The following example shows how to set the EAP password “7 141B1309” on the client:

```
ppp eap identity user
ppp eap password 7 141B1309
```

ppp eap refuse

To refuse Enhanced Authentication Protocol (EAP) from peers requesting it, use the **ppp eap refuse** command in interface configuration mode. To return to the default, use the **no** form of this command.

ppp eap refuse [**callin**]
no ppp eap refuse [**callin**]

Syntax Description

callin	(Optional) Authentication is refused for incoming calls only.

Command Default

The server will not refuse EAP authentication challenges received from the peer.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap refuse** command to disable EAP authentication for all calls. If the **callin** keyword is used, the server will refuse to answer EAP authentication challenges received from the peer but will still require the peer to answer any EAP challenges the server sends.

Examples

The following example shows how to refuse EAP authentication on incoming calls from the peer:

```
ppp authentication eap
ppp eap local
ppp eap refuse callin
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp eap wait

To configure the server to delay the Enhanced Authentication Protocol (EAP) authentication until after the peer has authenticated itself to the server, use the **ppp eap wait** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ppp eap wait
no ppp eap wait

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ppp eap wait**command to specify that the server will not authenticate to a peer requesting EAP authentication until after the peer has authenticated itself to the server.

Examples

The following example shows how to configure the server to wait for the peer to authenticate itself first:

```
ppp authentication eap
ppp eap local
ppp eap wait
```

Related Commands

Command	Description
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

ppp link

To generate the Point-to-Point Protocol (PPP) Link Control Protocol (LCP) down and keepalive-failure link traps or enable calls to the interface-reset vector, use the **ppp link**command in interface configuration mode. To disable the PPP LCP down and keepalive-failure link traps or calls to the interface-reset vector, use the **no** form of this command.

ppp link {**reset** | **trap**}
no ppp link {**reset** | **trap**}

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down and keepalive-failure link traps.

Command Default

The defaults are as follows:

- The calls are sent to the interface-reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **no ppp link trap** command disables the sending of the link traps when the LCP goes down.

In the event that the PPP calls the interface-reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface-reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **no ppp link reset**command to disable calls to the interface-reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface-reset vector:

```
Router(config-if)#
ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface-reset vector:

```
Router(config-if)#
```

```
no ppp link reset
Router(config-if)#
```

This example shows how to generate the PPP LCP down/keepalive-failure link traps:

```
Router(config-if)#
ppp link trap
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)#
no ppp link trap
Router(config-if)#
```

ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol (PAP), use the ppp pap refuse command in interface configuration mode. To disable the refusal, use the no form of this command.

ppp pap refuse
no ppp pap refuse

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

Examples

The following example shows how to enable the ppp pap command to refuse a peer request for remote authentication:

```
interface dialer 0 encapsulation ppp ppp pap refuse
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+.
encapsulation ppp	Sets PPP as the encapsulation method used by a serial or ISDN interface.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp pap sent-username	Reenables remote PAP support for an interface and uses the sent-username and password in the PAP authentication request packet to the peer.

ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

ppp pap sent-username *username* **password** *password*
no ppp pap sent-username

Syntax Description

username	Username sent in the PAP authentication request.
password	Password sent in the PAP authentication request.
password	Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.

Command Default

Remote PAP support disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to reenable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. *ISPCorp*is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.

Command	Description
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp authentication ms-chap-v2	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
ppp chap password	Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer.

preempt

To enable preemption on the redundancy group, use the **preempt**command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt
no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

pre-shared-key

To define a preshared key to be used for Internet Key Exchange (IKE) authentication, use the **pre-shared-key**command in keyring configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-addressipv6-prefix*}} **key** *key*
no pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-addressipv6-prefix*}} **key** *key*

Syntax Description

address *address [mask]*	IP address of the remote peer or a subnet and mask. The *mask*argument is optional.
hostname *hostname*	Fully qualified domain name (FQDN) of the peer.
ipv6	Specifies that an IPv6 address of a remote peer will be used.
ipv6-address	IPv6 address of the remote peer. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
ipv6-prefix	IPv6 prefix of the remote peer.
key *key*	Specifies the secret.

Command Default

None

Command Modes

Keyring configurati
on (config-keyring)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(2)T	This command was modified so that output for the **pre-shared-key**command will show that the preshared key is either encrypted or unencrypted.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **ipv6** keyword and the *ipv6-address* and *ipv6-prefix* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before configuring preshared keys, you must configure an Internet Security Association and Key Management Protocol (ISAKMP) profile.

Output for the **pre-shared-key** command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
pre-shared-key address 10.1.0.1 key test123
```

An output example for a type 6 encrypted preshared key would be as follows:

pre-shared-key address 10.1.0.1 key 6 RHZE[JACMUI\bcbTdELISAAB

Examples

The following example shows how to configure a preshared key using an IP address and hostname:

```
Router(config)# crypto keyring vpnkeyring
Router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
Router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

Related Commands

Command	Description
crypto keyring	Defines a crypto keyring to be used during IKE authentication.

pre-shared-key (IKEv2 keyring)

To define a preshared key for an Internet Key Exchange Version 2 (IKEv2) peer, use the **pre-shared-key** command in IKEv2 keyring peer configuration mode. To disable the preshared key, use the **no** form of this command.

pre-shared-key {**local** | **remote**}[**0** | **6***line* | **hex** *hexadecimal-string*]
no pre-shared-key {**local** | **remote**}

Syntax Description

local	Specifies the signing key.
remote	Specifies the verifying key.
0	Specifies that the password is unencrypted.
6	Specifies that the password is encrypted.
line	Specifies an unencrypted user password.
hex *hexadecimal-string*	Specifies the preshared key is in hexadecimal format.

Command Default

The default is a symmetric key.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(3)T	This command was modified. The **hex** *hexadecimal-string* keyword-argument pair was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to specify the preshared key for the peer. Use the **local** or **remote** keywords to specify an asymmetric key.

When specifying a pre-shared key that includes the ! delimiter combined with the characters h, l, or r, enclose the entire key string in double quotation marks ("). This ensures the key is parsed correctly by the system. Without the quotations, the pre-shared key will be lost after a reload.

Examples

The following examples show how to configure a preshared key in different scenarios.

IKEv2 Keyring with Symmetric Preshared Keys Based on the IP Address

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key key-1
```

IKEv2 Keyring with Asymmetric Preshared Keys Based on the IP Address

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.1
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer2
Router(config-ikev2-keyring-peer)# description peer2 with asymmetric keys
Router(config-ikev2-keyring-peer)# address 10.0.0.3
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

IKEv2 Keyring with Asymmetric Preshared Keys Based on the Hostname

The following is the keyring on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host1
Router(config-ikev2-keyring-peer)# description host1 in abc domain
Router(config-ikev2-keyring-peer)# host host1.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-1
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-2
```

The following is the keyring on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer host2
Router(config-ikev2-keyring-peer)# description host2 in example domain
Router(config-ikev2-keyring-peer)# host host2.example.com
Router(config-ikev2-keyring-peer)# pre-shared-key local key-2
Router(config-ikev2-keyring-peer)# pre-shared-key remote key-1
```

IKEv2 Keyring with Symmetric Preshared Keys Based on the Identity

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-ikev2-keyring)# peer abc
Router(config-ikev2-keyring-peer)# description example domain
Router(config-ikev2-keyring-peer)# identity fqdn example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-1
Router(config-ikev2-keyring-peer)# exit
Router(config-ikev2-keyring)# peer user1
Router(config-ikev2-keyring-peer)# description user1 in example domain
Router(config-ikev2-keyring-peer)# identity email user1@example.com
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-2
Router(config-ikev2-keyring-peer)# exit
Router(config-ikev2-keyring)# peer user1-remote
Router(config-ikev2-keyring)# description user1 abc remote users
Router(config-ikev2-keyring-peer)# identity key-id abc
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key-3
```

IKEv2 Keyring with a Wildcard Key

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description ABCdomain
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key abc-key
```

IKEv2 Keyring with a Hexadecimal Key

The following is the configuration on the initiator:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key hex 0x6A6B6C
```

The following is the configuration on the responder:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0
Router(config-ikev2-keyring-peer)# pre-shared-key jkl
```

Because the hexadecimal equivalent of each character in the string **jkl** is **0x6A6B6C**, the preshared key matches.

Related Commands

Command	Description
address (IKEv2 keyring)	Specifies the IPv4 address or the range of the peers in the IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (IKEv2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.

Command	Description
hostname (IKEv2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (IKEv2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.

prf

To specify one or more Pseudo-Random Function (PRF) algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **prf** command in IKEv2 proposal configuration mode. To remove the PRF algorithm, use the **no** form of this command.

prf *prf-algorithm...*
no prf

Syntax Description

prf-algorithm...	Specifies the type of PRF algorithm.

Command Default

The PRF algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.4(2)T	This command was introduced.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S.

Usage Guidelines

Use this command to specify the PRF algorithm to be used in an IKEv2 proposal. The PRF algorithm can be one of the following:

PRF Type	Description
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the PRF algorithm.
sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the PRF algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the PRF algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the PRF algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the PRF algorithm.

The PRF algorithm is required if the encryption type is Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM)—**aes-gmc-128** or **aes-gmc-256**, If the encryption algorithm is not AES-GCM, the PRF algorithm is the same as the specified integrity algorithm. However, you can specify a PRF algorithm, if required.

Examples

The following example configures an IKEv2 proposal with the 3DES encryption algorithm:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# encryption aes-cbc-256
Device(config-ikev2-proposal)# prf sha256 sha512
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (IKEv2 proposal)	Specifies one or more encryption algorithms for an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH group identifier in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

primary *name*

Syntax Description

name	Name of the primary trustpoint of the router.

Command Default

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the primary command to specify a given trustpoint as primary.

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

Examples

The following example shows how to configure the trustpoint “ka” as the primary trustpoint:

```
cr
ypto ca trustpoint ka
 enrollment url http://xxx
 primary
 crl option
al
```

Related Commands

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

priority (firewall)

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]
no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

private-hosts

To globally enable the Private Hosts feature, use the **private-hosts** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts
no private-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into the Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Issue this command to enable the Private Hosts feature on the router. Then, use the **private-hosts mode** command to enable Private Hosts on individual interfaces (ports).

Examples

The following example globally enables the Private Hosts feature on the router:

```
Router(config)# private-hosts
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts mode	Specifies the operating mode for a Private Hosts port.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

private-hosts layer3

To globally enable Layer 3 routing on private hosts, use the **private-hosts layer3** command in global configuration mode. To disable the feature, use the **no** form of this command.

private-hosts layer3
no private-hosts layer3

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD	This command was introduced.

Usage Guidelines

Use this command on the router to enable layer 3 routing on private hosts.

Examples

The following example shows the layer 3 configuration enabled on private hosts:

```
Router(config)# private-hosts layer3
Router(config)# end
Router# show private-hosts configuration
Private hosts disabled. BR INDEX 65536
Layer-3 switching on Private Hosts is enabled
Missing config: MAC list, VLAN list, MAC list association, Enable command, Atlea
st one Promiscuous/Mixed port
Privated hosts vlans lists:
None
```

Related Commands

Command	Description
private-hosts mac list	Creates a MAC address list that identifies the content servers providing broadband services to isolated hosts.
private-hosts promiscuous	Identifies the content servers and receiving hosts for broadband services.
private-hosts vlan-list	Identifies the VLANs whose hosts need to be isolated.
show private-hosts configuration	Displays Private Hosts configuration information for the router.

private-hosts mac-list

To identify the content servers that provide broadband services to isolated hosts, create a MAC address list by using the **private-hosts mac-list** command in global configuration mode. To delete an address from the MAC address list and remove that device from the list of content servers providing services for the Private Hosts feature, use the **no** form of this command.

private-hosts mac-list *mac-list-name mac-address* [**remark** *device-namecomment*]
no private-hosts mac-list *mac-list-name mac-address*

Syntax Description

mac-list-name	A name to assign to the address list (up to 80 characters).
mac-address	The MAC address of a Broadband Remote Access Server (BRAS), multicast server, or video server that provides broadband services for the Private Hosts feature. **Note** If the server is not directly connected to the networking device, specify the MAC address of the core network device that provides access to the server.
remark *device-name* | *comment*	(Optional) Specifies an optional device name or comment to assign to this MAC address list.

Command Default

The MAC address list is not populated with content servers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of MAC addresses that identify the content servers being used to provide broadband services to isolated hosts in the Private Hosts configuration. The Private Hosts feature uses port-based Protocol-Independent MAC ACLs (PACLs) to provide Layer 2 isolation between hosts on trusted ports within a purely Layer 2 domain. The PACLs isolate the hosts by imposing Layer 2 forwarding constraints on the router ports.

Use this command to specify the MAC address of every content server that provides broadband services for the Private Hosts feature. A *content server* is any BRAS, multicast server, or video server that provides services to the isolated hosts in your network.

You can assign all of the content servers to a single MAC address list or you can create multiple MAC address lists, each identifying the content server for a particular type of broadband service or set of services. When you configure the promiscuous ports for Private Hosts, you specify a MAC address list and VLAN list to identify the server and receiving hosts for broadband services.

If you plan to deliver different types of broadband services to different sets of hosts, create multiple MAC address lists to identify the servers for each type of service. You can also create multiple VLAN lists to identify different sets of isolated hosts. When you configure promiscuous ports, you can specify different combinations of MAC address lists and VLAN lists to identify the servers and receiving hosts for each type of service.



Note The MAC address list is deleted when the last address in the list is deleted.

Examples

This example creates a MAC address list named BRAS1 that identifies the MAC address of the upstream BRAS. The optional remark names the MAC address list BRAS1.

```
Router(config)# private-hosts mac-list BRAS1 0000.1111.1111 remark BRAS1
```

Related Commands

Command	Description
show private-hosts mac-list	Displays a list of the MAC addresses that identify the content servers that are providing broadband defined for Private Hosts.

private-hosts mode

To enable Private Hosts on an interface (port) and specify the mode in which the port is to operate, use the **private-hosts mode** command in interface configuration mode. To disable Private Hosts on the port, use the **no** form of this command.

private-hosts mode {**promiscuous** | **isolated** | **mixed**}
no private-hosts

Syntax Description

promiscuous	Configures the port for promiscuous mode. Use this mode for ports that face upstream. These are the ports that connect the router to the servers providing broadband services (Broadband Remote Access Server [BRAS], multicast, or video), or to the core network devices providing access to the servers.
isolated	Configures the port for isolated mode. Use this mode for ports that face the DSL access multiplexer (DSLAM) to which the isolated hosts are connected.
mixed	Configures the port for mixed mode. Use this mode for ports that connect to other networking devices, typically in a ring topology. The behavior of this port can change depending on the Spanning Tree Protocol (STP) topology.

Command Modes

This command is disabled by default.
The default for the **mode** keyword is promiscuous.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use this command, you must globally enable the Private Hosts feature on the router by issuing the **private-hosts** command.

Use this command to enable the Private Hosts feature on individual ports and to define the mode of operation for the port. A port's mode determines which type of Protocol-Independent MAC ACLs (PACL) will be assigned to the port in order to restrict the type of traffic that is allowed to pass through the port. Each type of PACL restricts the traffic flow for a different type of traffic (for example, from content servers to isolated hosts, from isolated hosts to servers, and traffic between isolated hosts). Use the **show private-hosts interface configuration** command to display the mode assigned to Private Hosts ports.

Examples

The following command example enables Private Hosts on an interface (port) and configures the port for isolated mode:

```
Router(config-if)# private-hosts mode isolated
```

Related Commands

Command	Description
private-hosts	Enables or configures the private hosts feature.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts	Displays the private hosts information.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts promiscuous

To identify the content servers and receiving hosts for broadband services, use the **private-hosts promiscuous** command in global configuration mode. To remove a promiscuous ports setting, use the **no** form of this command.

private-hosts promiscuous *mac-list-name* [**vlan** *vlan-ids*]
no private-hosts promiscuous *mac-list-name*

Syntax Description

mac-list-name	The name of MAC address list that identifies the content servers (Broadband Remote Access Server [BRAS], multicast, or video) providing broadband services for the Private Hosts feature.
vlan *vlan-ids*	(Optional) The VLAN or set of VLANs whose hosts will be allowed to receive services from the content servers identified by the MAC address list. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25). **Note** If no VLAN list is specified, the global VLAN list is used.

Command Default

Promiscuous ports are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The MAC address list and VLAN list define the content servers and receiving hosts for broadband services. If no VLAN list is specified, the system uses the global VLAN list created with the **private-hosts vlan-list** command.

You can issue this command multiple times to specify multiple combinations of MAC and VLAN lists, each defining the server and receiving hosts for a particular type of service. For example, the BRAS at xxxx.xxxx.xxxx could be used to deliver a basic set of services over VLANs 20, 25, and 30, and the BRAS at yyyy.yyyy.yyyy could be used to deliver a premium set of services over VLANs 5, 10, and 15.

Examples

The following example configures the broadband services provided by the content servers defined in the BRASlist address list to be delivered to the isolated hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts promiscuous BRASlist vlan 10,12,15,200-300
```

Related Commands

Command	Description
private-hosts vlan-list	Creatse a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services).
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show private-hosts interface configuration	Displays Private Hosts configuration information for individual interfaces.

private-hosts vlan-list

To create a VLAN list to be used to identify the VLANs whose hosts need to be isolated from each other (so that the VLANs can be used to deliver broadband services) use the **private-hosts vlan-list** command in global configuration mode. To remove a VLAN from the list of VLANs requiring host isolation, use the **no** form of this command.

private-hosts vlan-list *vlan-ids*
no private-hosts vlan-list *vlan-ids*

Syntax Description

vlan-ids	A list of the VLANs whose hosts need to be isolated from each other. Use commas to separate individual VLANs and hyphens to specify a range of VLANs (for example, 1,3,5,20-25).

Command Default

A VLAN is not included in the list of VLANs requiring host isolation.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command creates a list of VLANs whose hosts need to be isolated through the Private Hosts feature. The VLAN list should include all of the VLANs that are being used to deliver broadband services to multiple end users (isolated hosts).

If you plan to deliver different types of broadband services to different sets of hosts, you can create multiple VLAN lists and multiple MAC address lists. When you configure promiscuous ports, you can specify different combinations of MAC and VLAN lists to identify the content servers and receiving hosts for each type of service.

If you do not specify a VLAN list when you configure promiscuous ports, the system uses the global VLAN list created by this command.

Note The Private Hosts feature isolates the hosts in all of the VLANs included in VLAN lists; therefore, VLAN lists should include only those VLANs that are being used to deliver broadband services.

Examples

This example shows how to configure the Private Hosts feature to isolate the hosts in VLANs 10, 12, 15, and 200 through 300:

```
Router(config)# private-hosts vlan-list 10,12,15,200-300
```

Related Commands

Command	Description
show private-hosts configuration	Displays Private Hosts configuration information for the router.

privilege

To configure a new privilege level for users and associate commands with that privilege level, use the **privilege**command in global configuration mode. To reset the privilege level of the specified command or commands to the default and remove the privilege level configuration from the running configurationfile, use the **no**form of this command.



Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*
no privilege *mode* [**all**] {**level** *level* | **reset**} *command-string*

Syntax Description

mode	Configuration mode for the specified command. See the table in the "Usage Guidelines" section for a list of options for this argument.
all	(Optional) Changes the privilege level for all the suboptions to the same level.
level *level*	Specifies the privilege level you are configuring for the specified command or commands. The level argument must be a number from 0 to 15.
reset	Resets the privilege level of the specified command or commands to the default and removes the privilege level configuration from the running configuration file. **Note** For Cisco IOS software releases earlier than Release 12.3(6) and Release 12.3(6)T, you use the **no** form of this command to reset the privilege level to the default. The default form of this command will still appear in the configuration file. To completely remove a privilege configuration, use the **reset** keyword.
command-string	Command associated with the specified privilege level. If the **all** keyword is used, specifies the command and subcommands associated with the privilege level.

Command Default

User EXEC mode commands are privilege level 1.

Privileged EXEC mode and configuration mode commands are privilege level 15.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(22)S, 12.2(13)T	The **all** keyword was added.
12.3(6), 12.3(6)T	The **no** form of the command performs the same function as the **reset** keyword.

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

Usage Guidelines

The password for a privilege level defined using the **privilege**global configuration command is configured using the **enable secret**command.

Level 0 can be used to specify a more-limited subset of commands for specific users or lines. For example, you can allow user "guest" to use only the **show users**and **exit** commands.



Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included.

When you set the privilege level for a command with multiple words, note that the commands starting with the first word will also have the specified access level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip**commands are automatically set to privilege level 15--unless you set them individually to different levels. This is necessary because you can't execute, for example, the **show ip** command unless you have access to **show** commands.

To change the privilege level of a group of commands, use the **all** keyword. When you set a group of commands to a privilege level using the **all** keyword, all commands which match the beginning string are enabled for that level, and all commands which are available in submodes of that command are enabled for that level. For example, if you set the **show ip** keywords to level 5, show and ip will be changed to level 5 and all the options that follow the **show ip** string (such as **show ip accounting**, **show ip aliases**, **show ip bgp**, and so on) will be available at privilege level 5.

The table below shows some of the keyword options for the mode argument in the **privilege**command. The available mode keywords will vary depending on your hardware and software version. To see a list of available mode options on your system, use the **privilege ?**command.

Table 2: mode Argument Options

Command	Description
accept-dialin	VPDN group accept dialin configuration mode
accept-dialout	VPDN group accept dialout configuration mode
address-family	Address Family configuration mode
alps-ascu	ALPS ASCU configuration mode
alps-circuit	ALPS circuit configuration mode
atm-bm-config	ATM bundle member configuration mode
atm-bundle-config	ATM bundle configuration mode

Command	Description
atm-vc-config	ATM virtual circuit configuration mode
atmsig_e164_table_mode	ATMSIG E164 Table
cascustom	Channel-associated signalling (cas) custom configuration mode
config-rtr-http	RTR HTTP raw request Configuration
configure	Global configuration mode
controller	Controller configuration mode
crypto-map	Crypto map config mode
crypto-transform	Crypto transform config modeCrypto transform configuration mode
dhcp	DHCP pool configuration mode
dspfarm	DSP farm configuration mode
exec	Exec mode
flow-cache	Flow aggregation cache configuration mode
gateway	Gateway configuration mode
interface	Interface configuration mode
interface-dlci	Frame Relay DLCI configuration mode
ipenacl	IP named extended access-list configuration mode
ipsnacl	IP named simple access-list configuration mode
ip-vrf	Configure IP VRF parameters
lane	ATM Lan Emulation Lecs Configuration Table
line	Line configuration mode
map-class	Map class configuration mode
map-list	Map list configuration mode
mpoa-client	MPOA Client
mpoa-server	MPOA Server
null-interface	Null interface configuration mode
preaut	AAA Preauth definitions
request-dialin	VPDN group request dialin configuration mode
request-dialout	VPDN group request dialout configuration mode

Command	Description
route-map	Route map configuration mode
router	Router configuration mode
rsvp_policy_local	
rtr	RTR Entry Configuration
sg-radius	RADIUS server group definition
sg-tacacs+	TACACS+ server group
sip-ua	SIP UA configuration mode
subscriber-policy	Subscriber policy configuration mode
tcl	Tcl mode
tdm-conn	TDM connection configuration mode
template	Template configuration mode
translation-rule	Translation Rule configuration mode
vc-class	VC class configuration mode
voiceclass	Voice Class configuration mode
voiceport	Voice configuration mode
voipdialpeer	Dial Peer configuration mode
vpdn-group	VPDN group configuration mode

Examples

The following example shows how to set the **configure** command to privilege level 14 and establish SecretPswd14 as the password users must enter to use level 14 commands:

```
privilege exec level 14 configure
enable secret level 14 SecretPswd14
```

The following example shows how to set the **show**and **ip**keywords to level 5. The suboptions coming under **ip** will also be allowed to users with privilege level 5 access:

```
Router(config)# privilege exec all level 5 show ip
```

The following two examples demonstate the difference in behavior between the **no** form of the command and the use of the **reset** keyword when using Cisco IOS software releases earlier than Releases 12.3(6) and Release 12.3(6)T.

Note As of Cisco IOS Releases 12.3(6) and 12.3(6)T, the **no** form of the **privilege** command and the **reset** keyword perform the same functions.

```
! show currently configured privilege commands
Router# show running-config | include priv

privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no privilege exec level 3 configure terminal
Router(config)# end
! show currently configured privilege commands
Router# show running-config | include priv
privilege configure all level 3 interface
privilege exec level 15 configure terminal
privilege exec level 15 configure
```

Note that in the **show running-config**output above, the privilege command for "configure terminal" still appears, but now has the default privilege level assigned.

To remove a previously configured privilege command entirely from the configuration, use the **reset** keyword, as shown in the following example:

```
! show currently configured privilege commands
Router# show running-config | include priv

privilege configure all level 3 interface
privilege exec level 3 configure terminal
privilege exec level 3 configure
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# privilege exec reset configure terminal
Router(config)#
Router# show running-config | include priv

privilege configure all level 3 interface
Router#
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege level	Sets the default privilege level for a line.

privilege level

To set the default privilege level for a line, use the **privilege level** command in line configuration mode. To restore the default user privilege level to the line, use the **no** form of this command.

privilege level *level*
no privilege level

Syntax Description

level	Privilege level associated with the specified line.

Command Default

Level 15 is the level of access permitted by the enable password.

Level 1 is normal EXEC-mode user privileges.

Command Modes

Line configuration

Command History

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

Usage Guidelines

Users can override the privilege level you set using this command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level.

You can use level 0 to specify a subset of commands for specific users or lines. For example, you can allow user “guest” to use only the **show users** and **exit** commands.

You might specify a high level of privilege for your console line to restrict line usage.

Note Before Cisco IOS Release 12.2SXI, it was mandatory that a privilege level of 15 needed to be configured in the Access Control System (ACS) for Webauth (web authentication) to succeed. After this release, privilege configurations in the ACS are no longer mandatory.

Note Some CLI commands are not supported with the **privilege level** command. For example, commands such as **router bgp**, and **default interface**, etc cannot be associated with a privilege level. Though the global configuration CLI may accept the privilege-level assignment for these unsupported commands, they do not become part of the router's running-configuration.

Examples

The following example configures the auxiliary line for privilege level 5. Anyone using the auxiliary line has privilege level 5 by default:

```
line aux 0
 privilege level 5
```

The following example sets all **show ip** commands, which includes all **show** commands, to privilege level 7:

```
privilege exec level 7 show ip route
```

This is equivalent to the following command:

```
privilege exec level 7 show
```

The following example sets the **show ip route** command to level 7 and **show ip** commands to level 1:

```
privilege exec level 7 show ip route
privilege exec level 1 show ip
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.

profile (GDOI local server)

To define the IP security (IPsec) security association (SA) policy for a Group Domain of Interpretation (GDOI) group, use the **profile** command in GDOI local server configuration mode. To disable the IPsec SA policy that was defined, use the **no** form of this command.

profile *ipsec-profile-name*
no profile *ipsec-profile-name*

Syntax Description

ipsec-profile-name	Name of the IPsec profile.

Command Default

An IPsec SA policy is not defined for the GDOI group.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example shows that the IPsec SA policy has been defined as “group1234”:

```
profile group1234
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

profile (profile map configuration)

To define or modify an individual authentication and authorization cache profile, use the **profile** command in profile map configuration mode. To disable a cache profile, use the **no** form of this command.

profile *name* [**no-auth**]
no profile *name*

Syntax Description

name	Text string that is an exact match to an existing username.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No profiles are defined.

Command Modes

Profile map configuration (config-profile-map)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **profile** command to define or modify an authentication and authorization cache profile. The *name* argument in this command must be an exact match to a username being queried by an authentication or authorization service request.

Using the **profile** command with the *name* argument, as opposed to using the **regexp** or **all** command, is the recommended way to cache information.

Examples

The following example defines a cache profile that includes no user authentication and is a part of the localusers cache profile group:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# profile user101 no auth
```

Related Commands

Command	Description
aaa cache profile	Creates a named authentication and authorization cache profile group.
all	Specifies that all authentication and authorization requests be cached.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

propagate sgt

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS manual interface configuration mode (config-if-cts-manual)

Command History

Release	Modification
4.1(2)	This command was introduced on the Cisco Nexus 7000 series switches.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.

Usage Guidelines

SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on Gigabit Ethernet interface 0:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# cts manual
Router(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Router#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
show cts interface	Displays information about CTS interfaces.

propagate sgt (config-if-cts-dot1x)

To enable Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface, use the **propagate sgt** command in CTS dot1x interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt
no propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

SGT processing propagation is enabled.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

SGT propagation (SGT tag encapsulation) is enabled by default in both CTS dot1x and CTS manual interface configuration modes. A TrustSec-capable port can support Layer-2 MACsec and SGT encapsulation, and negotiates the most secure mode with the peer for the transmittal of the SGT tag and data. MACsec is an 802.1AE standard-based link-to-link protocol used by switches and servers. A peer can support MACsec, but not SGT encapsulation. In such a case, it is recommended that this Layer 2 SGT propagation be disabled with the **no propagate sgt** CTS Dot1x interface configuration command.

To re-enable the SGT propagation enter the **propagate sgt** command. Use the **show cts interface** command to verify the state of SGT propagation. Only the disabled state is saved in the nonvolatile generation (NVGEN) process.

Examples

The following example enables SGT propagation on a TrustSec-capable interface:

```
Device(config)# interface gigabit 6/1
Device(config-if)# cts dot1x
Device(config-if-cts-dot1x)# propagate sgt
Device# show cts interface gigabit 6/1

Global Dot1x feature is Enabled

Interface GigabitEthernet6/1:

    CTS is enabled, mode:    DOT1X

    IFC state:               INIT

SAP Status:              UNKNOWN

Configured pairwise ciphers:

 gcm-encrypt

 null
```

```
        Replay protection:      enabled

        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:          Enabled
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
sap mode-list (config-if-cts-dot1x)	Configures CTS Security Association Protocol (SAP) authentication.
show cts interface	Displays CTS interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.
timer reauthentication (config-if-cts-dot1x)	Configures the reauthentication timer for a CTS device.

proposal

To specify the proposals in an Internet Key Exchange Version 2 (IKEv2) policy, use the **proposal** command in IKEv2 policy configuration mode. To delete the proposal from the policy, use the **no** form of this command.

proposal *name*
no proposal *name*

Syntax Description

name	Proposal name.

Command Default

The default proposal is used with the default policy.

Command Modes

IKEv2 policy configuration (config-ikev2-policy)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this option to specify the proposals to use with the policy. One proposal must be specified at least and additional proposals can be specified with one proposal for each statement. The proposals are prioritized in the order of listing.

Note The specified proposals must be defined. Use the **crypto ikev2 proposal** command to define a proposal.

Examples

The following example shows how to specify a proposal in an IKEv2 policy:

```
Router(config)# crypto ikev2 policy policy1
Router(config-ikev2-policy)# proposal proposal1
```

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
show crypto ikev2 policy	Displays the default or user-defined IKEv2 policy.

protection (zone)

To configure TCP synchronization (SYN) cookie protection against SYN-flood attacks, use the **protection** command in security zone configuration mode. To disable the SYN cookie protection, use the **no** form of this command.

protection *parameter-map-name*
no protection *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map.

Command Default

SYN cookie protection is not configured.

Command Modes

Security zone configuration (config-sec-zone)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

You must configure the **zone security** command before you can configure the **protection** command.

You can use the **protection** command to bind an inspect zone-type parameter map to a zone.

TCP SYN-flooding attacks are a type of denial-of-service (DoS) attack. Usually, TCP SYN packets are sent to a targeted end host or a range of subnet addresses behind the firewall.

Examples

The following example shows how to configure the TCP SYN cookie protection:

```
Router(config)# zone security zone1
Router(config-sec-zone)# protection zone-pmap
Router(config-sec-zone)# end
```

Related Commands

Command	Description
zone security	Creates a security zone and enters security zone configuration mode.

protocol

To define a protocol instance in a redundancy group, use the **protocol**command in redundancy application configuration mode. To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*
no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

protocol (config-filter-list)

To specify a protocol instance in a sensor protocol filter list, use the **protocol** command in filter list configuration mode. To remove the protocol instance form the sensor protocol filter list, use the **no** form of this command.

protocol *protocol-name*
no protocol *protocol-name*

Syntax Description

protocol-name	Specifies the protocol name. Valid values are: • **cdp** • **dhcp** • **h323** • **http** • **lldp** • **mdns** • **sip**

Command Default

A protocol instance is not specified in the sensor protocol filter list.

Command Modes

Filter list configuration (config-filter-list)

Command History

Release	Modification
15.2(2)E	This command was introduced prior to Cisco IOS Release 15.2(2)E.

Examples

The following example shows how to configure a protocol instance in a sensor protocol filter list:

```
Device# configure terminal
Device(config)# access-session accounting attributes filter-list list mylist
Device(config-filter-list)# protocol http
Device(config-filter-list)# end
```

Related Commands

Command	Description
access-session accounting	Adds access-session protocol data to accounting records and generates additional accounting events when new sensor data is detected.

proxy

To configure proxy parameters for an Easy VPN remote device, use the **proxy** command in ISAKMP browser proxy configuration mode. To disable the parameters, use the **no** form of this command.

proxy *proxy-parameter*
no *proxy-parameter*

Syntax Description

proxy-parameter	Proxy parameter. See the table below for a list of acceptable proxy parameters.

Command Default

Proxy parameters are not set.

Command Modes

ISAKMP browser proxy configuration (config-ikmp-browser-proxy)

Command History

Release	Modification
12.4(2)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 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a subcommand of the **crypto isakmp client configuration browser-proxy** command.

The table below lists acceptable proxy parameters.

Table 3: Proxy Parameters

Proxy Parameter	Result
auto-detect	Automatically detects proxy settings.
by-pass-local	Bypasses proxy server for local addresses.
exception-list	Semicolon- (;) delimited list of IP addresses.
none	No proxy settings.
server	Proxy server IP and port number (ip:port number).

Examples

The following example shows various browser-proxy parameter settings for a browser proxy named “bproxy.”:

```
crypto isakmp client configuration browser-proxy bproxy
 proxy auto-detect
crypto isakmp client configuration browser-proxy bproxy
 proxy none
crypto isakmp client configuration browser-proxy bproxy
```

```
proxy server 10.1.1.1:2000
proxy exception-list 10.2.2.*,www.*org
proxy by-pass-local
```

Related Commands

Command	Description
crypto isakmp client configuration browser-proxy	Configures browser-proxy parameters for an Easy VPN remote device.

publickey

To configure the location of the 512-byte public key that is used for encrypting the session key used for Cloud Web Security header encryption, use the **publickey** command in parameter-map type inspect configuration mode. To remove the location of the public key, use the **no** form of this command.

publickey *filesystem*
no publickey *filesystem*

Syntax Description

filesystem	The location of the local file system.

Command Default

The location of the public key for encryption is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The Cisco IOS Release 15.2(1)T supports only local file systems such as slot, disk, flash, nvram, and so on.

Examples

The following example shows how to configure the flash file system as the location of the public key:

```
Device(config)# parameter-map type cws global
Device(config-profile)# publickey flash:
```

Related Commands

Command	Description
parameter-map type inspect cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

qos-group (PVS Bundle Member)

To associate a quality of service (QoS) group or groups with a permanent virtual circuit (PVC) bundle-member, use the **qos-group**command in PVC bundle member configuration mode. To remove a QoS-group from a PVC bundle member, use the **no** form of this command.

qos-group *group number*
no qos-group *group number*

Syntax Description

group number *<0-99>*	Associates a QoS-group with a PVC bundle member. You can associate one QoS group, a range of QoS groups, or any combination of QoS groups and ranges of QoS groups, separated by commas, with a PVC bundle member. When a range of QoS groups is associated with a PVC bundle, only the starting and ending QoS group number need to be listed, separated by a hyphen. For example, 1-5. When multiple-non contiguous QoS groups or non-contiguous ranges of QoS groups are associated with a PVC bundle, separate the groups. For example, 1, 3, 8-10, 12-14. When a QoS group is associated with a bundle member, use a number from 0 to 99. When a QoS group is not associated with a PVC bundle, use numbers greater 100 and greater.
other	All non-configured QoS groups.

Command Default

By default, QoS groups are not associated with PVC bundle members.

Command Modes

PVC bundle-member configuration mode

Command History

Release	Modification
12.4(4)T	This command was introduced to associate a QoS-group with a permanent virtual circuit (PVC) bundle member, using the **qos-group** command in ATM VC bundle-member configuration mode.
12.2(31)SB2	This command was integrated into the Cisco IOS Release 12.2(31)SB2.
12.4(9)XJ	This command modification was integrated into the Cisco IOS Special Release 12.4(9)XJ.
12.4(15)T	This command modification was integrated into the Cisco IOS Release 12.4(6th)T and associates a QoS-group with a permanent virtual circuit (PVC) bundle member in PVC bundle member configuration mode.

Examples

The following example shows the configuration of which QoS groups will use RBE:

```
Router(config-if-atm-member)# qos group 5
```

query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

query certificate
no query certificate

Syntax Description

This command has no arguments or keywords.

Command Default

Query certificates are stored in NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was incorporated into Relese 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to prevent certificates from being stored locally; instead, they are retrieved from a specified certification authority (CA) trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

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

Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified truspoint will not be written into NVRAM, and the certificate query will be attempted during the next reload of the router.

Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certicate query** command is used, any previously query certificate configuration will be removed from all trustpoints, and any query in progress will be halted and the feature disabled.

Examples

The following example shows how to configure a trustpoint and initiate query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
 enrollment url http://trustpoint1
 crl query ldap://trustpoint1
 query certificate
 exit
```

Related Commands

Command	Description
crypto ca certificate query	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint.
crypto ca trustpoint	Declares the CA that your router should use.

query url

Note Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **crl query** command.

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **query url**command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete (LDAP) URL, use **no** form of this command.

query url ldap://*hostname*
:[*port*]
noquery url ldap://*hostname*[**:**[*port*]]

Syntax Description

ldap :// hostname	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
: port	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Command Default

No enabled. If **query url ldap ://** *hostname* **:**[*port*] is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap:myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	This command was replaced by the **crl query** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)
- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://** *hostname* **:**[*port*} keywords and arguments are used to provide this information.

Note The **crypto ca trustpoint**commandreplaces 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, theconfiguration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
 enrollment url http://bar.cisco.com
 query url ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

quit

To exit from the key-string mode while defining the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **quit** command in public key configuration mode.

quit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Public key configuration

Command History

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

Usage Guidelines

Use this command to exit text mode while defining the RSA public key.

Examples

The following example shows that the RSA public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.