

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

no ppp accounting

Syntax Description	default	The name of the method list is created with the aaa accounting command.
Defaults	Accounting is disabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	11.3 T	This command was introduced.
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	<p>The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:</p> <pre>interface async 4 encapsulation ppp ppp accounting charlie</pre>	
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	
<i>protocol1</i> [<i>protocol2...</i>]	At least one of the keywords described in Table 20 .
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
<i>list-name</i>	(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 is created with the aaa authentication ppp command.
callin	(Optional) Authentication on incoming (received) calls only.
one-time	(Optional) The username and password are accepted in the username field.
optional	(Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested.

Defaults PPP authentication is not enabled.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(0.1)	The optional keyword was added.
	12.2(2)XB5	The eap keyword was added to the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS400 platforms.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines When you enable PAP, CHAP, or Extensible Authentication Protocol (EAP) authentication (or all three methods), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked

against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the name of the remote device with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match. EAP works much as CHAP does, except that identity request and response packets are exchanged when EAP starts.

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

**Caution**

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

Table 20 lists the protocols used to negotiate PPP authentication.

Table 20 *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.

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, use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

Examples

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 method 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.
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.

Defaults 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.

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.
<i>list-name</i>	(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.

Defaults

Authorization is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 T	This command was introduced.

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 in interface 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.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

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.

Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specifies “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.

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 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	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------------------	---------------	--

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

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	<p>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.</p> <p>This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.</p>
-------------------------	---

Examples	<p>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.</p>
-----------------	--

```
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.
	ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
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.
---------------	--

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

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.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

Command	Description
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	<i>secret</i>	The secret used to compute the response value for any CHAP challenge from an unknown peer.
---------------------------	---------------	--

Defaults	Enabled
-----------------	---------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	10.3	This command was introduced.

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

<i>string</i>	EAP identity.
---------------	---------------

Defaults

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.

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 reenble 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.

Defaults 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.

Usage Guidelines 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

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

Defaults

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.

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.
---------------------------	---

Defaults	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.	

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.

Defaults

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.

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 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.

Defaults No default behavior or values.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

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

Defaults Remote PAP support disabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command to reenabling 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 specifies 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.
	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.

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} key key
```

```
no pre-shared-key {address address [mask] | hostname hostname} key key
```

Syntax Description

address <i>address</i> [<i>mask</i>]	IP address of the remote peer or a subnet and mask. The <i>mask</i> argument is optional.
hostname <i>hostname</i>	Fully qualified domain name (FQDN) of the peer.
key <i>key</i>	Specifies the secret.

Defaults

No default behaviors or values

Command Modes

Keyring configuration

Command History

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

Usage Guidelines

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

Examples

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

```
crypto keyring vpnkeyring
pre-shared-key address 10.72.23.11 key vpnkey
pre-shared-key hostname www.vpn.com key vpnkey
```

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

<i>name</i>	Name of the primary trustpoint of the router.
-------------	---

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

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:

```
crypto ca trustpoint ka
  enrollment url http://xxx
  primary
  crl optional
```

Related Commands

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

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 configuration file, 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

<i>mode</i>	Configuration mode for the specified command. See Table 21 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.
<i>command-string</i>	Command associated with the specified privilege level. If the all keyword is used, specifies the command and subcommands associated with the privilege level.

Defaults

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.

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.

Table 21 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 21 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
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

Table 21 *mode Argument Options (continued)*

Command	Description
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 Leacs 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
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

Table 21 mode Argument Options (continued)

Command	Description
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 demonstrate 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

<i>level</i>	Privilege level associated with the specified line.
--------------	---

Defaults

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.

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.

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** to level 7 and the **show** 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.

query url



Note

Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **cr1 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]
```

```
query 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).

Defaults

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 cr1 query command.

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 (Example 1: 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** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as 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.

Defaults 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.

radius-server attribute 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6** command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 { **mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value* }

no radius-server attribute 6 { **mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value* }

Syntax Description		
mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.	
on-for-login-auth	Sends the Service-Type attribute in the authentication packets.	
	Note	The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include “Service-Type=Outbound” as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.	
voice <i>value</i>	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.	

Defaults

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The mandatory keyword was added.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router (config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router (config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router (config)# radius-server attribute support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router (config)# radius-server attribute attribute voice 1
```

radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

```
radius-server attribute 8 include-in-access-req
```

```
no radius-server attribute 8 include-in-access-req
```

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 8 include-in-access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the username, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.
- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and “stop” packets will also include the same IP address as in attribute 8.

**Note**

Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

Examples

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (asyncl-pool) has been configured and applied at interface Asyncl.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Asyncl
 peer default ip address pool asyncl-pool
!
ip local pool asyncl-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

radius-server attribute 11 direction default

To specify the default direction of filters from RADIUS, use the **radius-server attribute 11 direction default** command in global configuration mode. To remove this functionality from your configuration, use the **no** form of this command.

radius-server attribute 11 direction default [inbound | outbound]

no radius-server attribute 11 direction default [inbound | outbound]

Syntax Description

inbound	(Optional) Filtering is applied to inbound packets only.
outbound	(Optional) Filtering is applied to outbound packets only.

Defaults

If this command is not enabled, filters are treated as outbound.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **radius-server attribute 11 direction default** command to change the default direction of filters from RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound, which stops traffic from entering a router and prevents resource consumption, rather than keeping the outbound default direction, which waits until the traffic is about to leave the network before filtering occurs.

Examples

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 direction default inbound
```

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "cisco"
    Service-Type = Framed,
    Framed-Protocol = PPP,
    Filter-Id = "myfilter.out"
```

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format (Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **radius-server attribute 44 extend-with-addr** command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.



Note

This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [*vrf vrf-name*]

no radius-server attribute 44 include-in-access-req [*vrf vrf-name*]

Syntax Description

vrf vrf-name (Optional) Per VRF configuration.

Defaults

RADIUS attribute 44 is not sent in access-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(1)DX	The vrf keyword and <i>vrf-name</i> argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

There is no guarantee that the Accounting Session IDs will increment uniformly and consistently. In other words, between two calls, the Accounting Session ID can increase by more than one.

The **vrf vrf-name** keyword and argument specify Accounting Session IDs per Virtual Private Network (VPN) routing and forwarding (VRF), which allows multiple disjointed routing or forwarding tables, where the routes of a user have no correlation with the routes of another user.

Examples

The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
```

radius-server attribute 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description This command has no arguments or keywords.

Defaults This command is not enabled.

Command Modes Global configuration

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

Usage Guidelines Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands	Command	Description
	radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
	radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

radius-server attribute 55 include-in-acct-req

To send the RADIUS attribute 55 (Event-Timestamp) in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 55 is not sent in accounting packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 55 include-in-acct-req** command to send RADIUS attribute 55 (Event-Timestamp) in accounting packets. The Event-Timestamp attribute records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC.



Note

Before the Event-Timestamp attribute can be sent in accounting packets, you *must* configure the clock on the router. (For information on setting the clock on your router, refer to section “Performing Basic System Management” in the chapter “System Management” of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*.)

To avoid configuring the clock on the router every time the router is reloaded, you can enable the **clock calendar-valid** command. (For information on this command, refer to the *Cisco IOS Configuration Fundamentals and Network Management Command Reference*.)

Examples

The following example shows how to enable your router to send the Event-Timestamp attribute in accounting packets. (To see whether the Event-Timestamp was successfully enabled, use the **debug radius** command.)

```
radius-server attribute 55 include-in-acct-req
```

Related Commands

Command	Description
clock calendar-valid	Configures a system as an authoritative time source for a network based on its hardware clock (calendar).
clock set	Manually sets the system software clock.

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** command in global configuration mode. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

radius-server attribute 69 clear

no radius-server attribute 69 clear

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 69 is not sent and encrypted tunnel passwords are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 69 clear** command to receive nonencrypted tunnel passwords, which are sent in RADIUS attribute 69 (Tunnel-Password). This command allows tunnel passwords to be sent in a “string” encapsulated format, rather than the standard tag/salt/string format, which enables the encrypted tunnel password.

Some RADIUS servers do not encrypt Tunnel-Password; however the current NAS (network access server) implementation will decrypt a non-encrypted password that causes authorization failures. Because nonencrypted tunnel passwords can be sent in attribute 69, the NAS will no longer decrypt tunnel passwords.



Note

Once this command is enabled, all tunnel passwords received will be nonencrypted until the command is manually disabled.

Examples

The following example shows how to enable attribute 69 to receive nonencrypted tunnel passwords. (To see whether the Tunnel-Password process is successful, use the **debug radius** command.)

```
radius-server attribute 69 clear
```

radius-server attribute 77

To send connection speed information to the RADIUS server in the access request, use the **radius-server attribute 77** command in global configuration mode. To prevent connection speed information from being included in the access request, use the **no** form of this command.

```
radius-server attribute 77 {include-in-access-req | include-in-acct-req}
```

```
no radius-server attribute 77 {include-in-access-req | include-in-acct-req}
```

Syntax Description

include-in-access-req	Specifies that attribute 77 will be included in access requests.
include-in-acct-req	Specifies that attribute 77 will be included in accounting requests.

Defaults

RADIUS attribute 77 is sent to the RADIUS server in the access request.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)BX	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

RADIUS attribute 77 is sent to the RADIUS server in the access request by default.

RADIUS attribute 77 allows RADIUS authentication based on connection speed. Sessions can be accepted or denied based on the allowed connection speed configured for a particular user on the RADIUS server.

RADIUS attribute 77 includes the following information:

- The accounting start/stop request
- The VC class name defined with the **class-int** command
- The VC class name defined with the **class-vc** command
- The VC class name defined with the **class-range** command

The VC class name may include letters, numbers, and the characters “:” (colon), “;” (semicolon), “-” (hyphen) and “,” (comma).

Examples

The following example disables the inclusion of RADIUS attribute 77 in the access request:

```
no radius-server attribute 77 include-in-access-req
```

Related Commands

Command	Description
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-range	Assigns a VC class to an ATM PVC range.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the **radius-server attribute 188 format non-standard** command in global configuration mode. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the **no** form of this command.

radius-server attribute 188 format non-standard

no radius-server attribute 188 format non-standard

Syntax Description This command has no arguments or keywords.

Defaults RADIUS attribute 188 is not sent in accounting “start” and “stop” records.

Command Modes Global configuration

Command History	Release	Modification
	12.1	This command was introduced.

Usage Guidelines Use this command to send attribute 188 in accounting “start” and “stop” records.

Examples The following example shows a configuration that sends RADIUS attribute 188 in accounting-request packets:

```
radius-server attribute 188 format non-standard
```

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the no form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name Name for an accept or reject list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.



Note

The listname must be the same as the listname defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list “bad-author” for RADIUS authorization and accept list “usage-only” for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 1.1.1.1
Router(config-sg-radius)# authorization reject bad-author
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
```

```

Router(config)# radius-server host 1.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-author
Router(config-radius-attrl)# attribute 22,27-28,56-59

```

**Note**

Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

radius-server attribute nas-port extended

The **radius-server attribute nas-port extended** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server attribute nas-port format

To select the NAS-Port format used for RADIUS accounting features, and to restore the default NAS-Port format, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 5 (NAS-Port) to the RADIUS server, use the **no** form of this command.

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Syntax Description

<i>format</i>	NAS-Port format. Possible values for the format argument are as follows:
	a —Standard NAS-Port format
	b —Extended NAS-Port format
	c —Carrier-based format
	d —PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format
	e —Configurable NAS-Port format

Defaults

Standard NAS-Port format

Command Modes

Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q virtual LANS (VLANs).
12.2(4)T	Format e was introduced.
12.2(11)T	Format e was extended to support PPPoX information.
12.3(3)	Format e was extended to support Session ID U.

Usage Guidelines

The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).

The following NAS-Port formats are supported:

- Standard NAS-Port format—This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format—The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.

- Shelf-slot NAS-Port format—This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format—This NAS-Port format uses 32 bits to indicate the interface, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPP over ATM and PPPoE over ATM, and the interface and VLAN ID for PPPoE over Institute of IEEE standard 802.1Q VLANs.

Format e

The currently supported formats **a** through **c** do not work with new Cisco platforms, such as the AS5400. For this reason, a configurable format **e** was developed. Format **e** requires you to explicitly define the usage of the 32 bits of attribute 25 (Nas-Port). The usage is defined with a given parser character for each Nas-Port field of interest for a given bit field. By configuring a single character in a row, such as **x**, only one bit is assigned to store that given value. Additional characters of the same type, such as **x**, will provide a larger available range of values to be stored. Thus, the ranges may be expanded as follows:

x	0 – 1
xx	0 – 3
xxx	0 – 7
xxxx	0 – F
xxxxx	0 – 1F

and so on.

It is imperative that one know what the valid range is for a given parameter on a platform that one wishes to support. The IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Thus, if one has a parameter that turns out to have a value of 8, but only 3 bits (**xxx**) are configured, 8 and 0x7 will give a result of 0. Therefore, one must always configure enough bits to correctly capture the value required. Care must be taken to ensure that format **e** is configured to properly work for all NAS port types within your network environment.

Currently supported parameters and their representative characters are shown below.

Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 1 to that bit)
DS0 shelf	f
DS0 slot	s
DS0 adapter	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modem line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adapter	A
PPPoX port	P
PPPoX VLAN ID	V

PPPoX VPI	I
PPPoX VCI	C
Session ID	U

All 32 bits that represent the NAS-Port must be set to one of the above characters because this format makes no assumptions for empty fields.

Access Router

The DS0 port on a T1-based card and on a T3-based card will give different results. On T1-based cards, the physical port is equal to the virtual port (as these are the same). So, p and d will give the same information for a T1 card. However, on a T3 system, the port will give you the physical port number (as there can be more than one T3 card for a given platform). As such, d will give you the virtual T1 line (as per configuration on a T3 controller). On a T3 system, p and d will be different, and one should capture both to properly identify the physical device. As a working example for the Cisco AS5400, the following configuration is recommended:

```
Router (config)# radius-server attribute nas-port format e
SSSSPPPPPPPPSSSSpppppddddccccc
```

This will give one an asynchronous slot (0 – 16), asynchronous port (0 – 512), DS0 slot (0 – 16), DS0 physical port (0 – 32), DS0 virtual port (0 – 32), and channel (0 – 32). The parser has been implemented to explicitly require 32-bit support, or it will fail.

Finally, format e is supported for channel-associated signaling (CAS), Primary Rate Interface (PRI), and basic rate interface- (BRI-) based interfaces.



Note

This command replaces the **radius-server attribute nas-port extended** command.

Examples

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Related Commands

Command	Description
vpdn aaa attribute nas-port vpdn-nas	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.

radius-server authorization missing Service-Type

To allow an access server to fully process or deny Access-Accept responses from RADIUS servers that do not send the Service-Type attribute in the Access-Accept packets, use the **radius-server authorization missing Service-Type** command in global configuration mode. To disable the “allow” or “deny” status, use the **no** form of this command.

radius-server authorization [permit | deny] missing Service-Type

no radius-server authorization [permit | deny] missing Service-Type

Syntax Description	permit	(Optional) Allows an access server to fully process Access-Accept responses from RADIUS servers that do not send the Service-Type attribute.
	deny	(Optional) Allows the access server to deny authorization if the Service-Type attribute is not present in the Access-Accept packet. Use this keyword if the permit missing Service-Type keyword has already been configured.

Defaults If this command is not entered, authorization fails if a Service-Type attribute is not present in the RADIUS Access-Accept packet that is received.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.3	This command was replaced by the radius-server attribute 6 command. The radius-server authorization missing Service-Type command continues to perform its normal function in Cisco IOS Release 12.2 T, but it is no longer documented or supported.

Examples The following example shows that the access server has been configured to fully process Access-Accept responses from RADIUS servers that do not send the Service-Type attribute:

```
Router (config)# radius-server authorization permit missing Service-Type
```

The following example shows that the access server has been configured to deny authorization if the Service-Type attribute is not present in the Access-Accept packet:

```
Router (config)# radius-server authorization deny missing Service-Type
```

radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** command in global configuration mode. To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Defaults

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to all users. When the **radius-server challenge-noecho** command is configured, user responses to Access-Challenge packets are not displayed unless the Prompt attribute in the user profile is set to *echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*.

Examples

The following example stops all user responses from displaying on the screen:

```
radius-server challenge-noecho
```

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.



Note

Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you issue a **copy system:running-config nvram:startup-config** command.

Examples The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
radius-server configure-nas
```

Related Commands	Command	Description
	radius-server host non-standard	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server deadtime

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the **radius-server deadtime** command in global configuration mode. To set dead-time to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

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

Defaults

Dead time is set to 0.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to cause the Cisco IOS software to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as “dead” is skipped by additional requests for the duration of *minutes* or unless there are no servers not marked “dead.”

When the RADIUS Server Is Marked As Dead

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

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

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

Examples

The following example specifies five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

```
radius-server deadtime 5
```

Related Commands	Command	Description
	deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
	radius-server host	Specifies a RADIUS server host.
	radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
	radius-server timeout	Sets the interval for which a router waits for a server host to reply.

radius-server dead-criteria

To force one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [*time seconds*] [*tries number-of-tries*]

no radius-server dead-criteria [*time seconds*] [*tries number-of-tries*]

Syntax Description

time <i>seconds</i>	<p>(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met.</p> <ul style="list-style-type: none"> If the <i>seconds</i> argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. <p>Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.</p>
tries <i>number-of-tries</i>	<p>(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packet will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted.</p> <ul style="list-style-type: none"> If the <i>number-of-tries</i> argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. <p>Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.</p>

Defaults

If the *seconds* argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server.

If the *number-of-tries* argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration

Command History

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

Usage Guidelines**Note**

Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is indicated, both time and tries will be set to their defaults.
- If either the *seconds* or the *number-of-tries* arguments is indicated, the one indicated (time or tries) will be set to its default. The other will be left unchanged.
- If both the *seconds* and the *number-of-tries* arguments are indicated, both time and tries will be set to their defaults.

Examples

The following example shows that the router will be considered dead after 5 seconds and four tries:

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

radius-server directed-request

To allow users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication, use the **radius-server directed-request** command in global configuration mode. To disable the directed-request feature, use the **no** form of this command.

radius-server directed-request [restricted]

no radius-server directed-request [restricted]

Syntax Description

restricted (Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Defaults

User cannot log into a Cisco NAS to select a RADIUS server for authentication.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the “@” symbol to the host specified after the “@” symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling the **radius-server directed-request** command causes the whole string, both before and after the “@” symbol, to be sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response that it gets from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

The **no radius-server directed-request** command causes the entire username string to be passed to the default RADIUS server.



Note

When **no radius-server directed-request restricted** is entered, only the “restricted” flag is removed, and the “directed-request” flag is retained. To disable the directed-request feature, you must also issue the **no radius-server directed-request** command.

Examples

The following example verifies that the RADIUS server is selected based on the directed request:

```
aaa new-model
aaa authentication login default radius
radius-server host 192.168.1.1
radius-server host 172.16.56.103
```

```
radius-server host 172.31.40.1  
radius-server directed-request
```

radius-server domain-stripping

To enable Virtual Route Forwarding (VRF)-aware domain-stripping, use the **radius-server domain-stripping** command in global configuration mode. To remove VRF-aware domain-stripping, use the **no** form of this command.

```
radius-server domain-stripping [vrf vrf-name]
```

```
no radius-server domain-stripping [vrf vrf-name]
```

Syntax Description

<code>vrf vrf-name</code>	(Optional) Per VRF configuration.
---------------------------	-----------------------------------

Defaults

This functionality is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **radius-server domain-stripping** command to strip or truncate the domain from a username. For example, if the username is `user1@cisco.com` and the **radius-server domain-stripping** command is configured, only “user1” is sent out as the username.

To configure domain-stripping only to a specified VRF, use the **vrf vrf-name** option.

Examples

The following example shows a configuration that strips the domain name from the VRF “abc”:

```
radius-server domain-stripping vrf abc
```

radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command for more information.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

```
radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]
[timeout seconds] [retransmit retries] [key string] [alias{hostname | ip-address}]
```

```
no radius-server host {hostname | ip-address}
```

Syntax Description

<i>hostname</i>	Domain Name System (DNS) name of the RADIUS server host.
<i>ip-address</i>	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
<i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
<i>port-number</i>	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
<i>seconds</i>	(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
<i>retries</i>	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
<i>string</i>	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The alias keyword was added on the Cisco AS5300 and AS5800 universal access servers.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Examples

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named *host1*:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 172.29.39.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server *host1* be used for accounting but not for authentication, and that RADIUS server *host2* be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 172.1.1.1:

```
radius-server host 172.1.1.1 acct-port 1645 auth-port 1646
radius-server host 172.1.1.1 alias 172.16.2.1 172.17.3.1 172.16.4.1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

radius-server host {*host-name* | *ip-address*} **non-standard**

no radius-server host {*host-name* | *ip-address*} **non-standard**

Syntax Description	
<i>host-name</i>	DNS name of the RADIUS server host.
<i>ip-address</i>	IP address of the RADIUS server host.

Defaults No RADIUS host is specified.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines The **radius-server host non-standard** command enables you to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*.

Examples The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
radius-server host alcatraz non-standard
```

Related Commands	Command	Description
	radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.
	radius-server host	Specifies a RADIUS server host.

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

```
radius-server key {0 string | 7 string | string}
```

```
no radius-server key
```

Syntax Description

0	Specifies that an unencrypted key will follow.
<i>string</i>	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
<i>string</i>	The hidden shared key.
<i>string</i>	The unencrypted (cleartext) shared key.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	The <i>string</i> argument was modified as follows: <ul style="list-style-type: none"> • 0 <i>string</i> • 7 <i>string</i> • <i>string</i>

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.



Note

Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
radius-server key dare to go
```

The following example sets the authentication and encryption key to “anykey.” The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key will be displayed as follows:

```
Router# show running-config
!
!
radius-server key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server optional-passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries Maximum number of retransmission attempts. The default is 3 attempts.

Defaults

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.

Examples

The following example specifies a retransmit counter value of five times:

```
radius-server retransmit 5
```

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the **radius-server retry method reorder** command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

If the **radius-server retry method reorder** command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples

The following example shows that RADIUS server retry has been configured:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 1.2.3.4 key rad123
radius-server host 4.5.6.7 key rad123
```

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server source-ports extended

To enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode. To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

radius-server source-ports extended

no radius-server source-ports extended

Syntax Description This command has no arguments or keywords.

Defaults Ports 1645 and 1646 are used as the source ports for RADIUS requests.

Command Modes Global configuration

Command History	Release	Modification
	12.3(4)	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The identifier field of the RADIUS packet is 8 bits long, and yields 256 unique identifiers. A NAS uses one port (1645) as the source port to send out access requests to the RADIUS server and one port (1646) as the source port to send out accounting requests to the RADIUS server. This scheme allows for 256 outstanding access requests and 256 outstanding accounting requests.

If the number of outstanding access requests or accounting requests exceeds 256, the port and ID space will wrap, and all subsequent RADIUS requests will be forced to reuse ports and IDs that are already in use. When the RADIUS server receives a request that uses a port and ID that is already in use, it treats the request as a duplicate. The RADIUS server then drops the request.

The **radius-server source-ports extended** command allows you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Examples The following example shows how to configure a NAS to use 200 ports in the range from 21645 to 21844 as the source ports for RADIUS requests:

```
Router(config)# radius-server source-ports extended
```

radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description	<i>seconds</i>	Number that specifies the timeout interval, in seconds. The default is 5 seconds.
--------------------	----------------	---

Defaults	5 seconds
----------	-----------

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

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	Use this command to set the number of seconds a router waits for a server host to reply before timing out.
------------------	--

Examples	The following example changes the interval timer to 10 seconds:
----------	---

```
radius-server timeout 10
```

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.	

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the **radius-server transaction max-retries** command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number Total number of transmissions per transaction. The default is eight.

Defaults

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reordeer
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 1.2.3.4
radius-server host 5.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server vsa send [**accounting** | **authentication**]

no radius-server vsa send [**accounting** | **authentication**]

Syntax Description

accounting	(Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes.
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just accounting attributes. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just authentication attributes.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a “NAS Prompt” user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

```
radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.