Authentication, Authorization, and Accounting Commands

This module describes the commands used to configure authentication, authorization, and accounting (AAA) services.

Note All commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router that is introduced from Cisco IOS XR Release 6.3.2. References to earlier releases in Command History tables apply to only the Cisco NCS 5500 Series Router.

Note

- Starting with Cisco IOS XR Release 6.6.25, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 560 Series Routers.
- Starting with Cisco IOS XR Release 6.3.2, all commands applicable for the Cisco NCS 5500 Series Router are also supported on the Cisco NCS 540 Series Router.
- References to releases before Cisco IOS XR Release 6.3.2 apply to only the Cisco NCS 5500 Series Router.
- Cisco IOS XR Software Release 7.0.1 specific updates are not applicable for the following variants of Cisco NCS 540 Series Routers:
  - N540-28Z4C-SYS-A
  - N540-28Z4C-SYS-D
  - N540X-16Z4G8Q2C-A
  - N540X-16Z4G8Q2C-D
  - N540X-16Z8Q2C-D
  - N540-12Z20G-SYS-A
  - N540-12Z20G-SYS-D
  - N540X-12Z16G-SYS-A
  - N540X-12Z16G-SYS-D

For detailed information about AAA concepts, configuration tasks, and examples, see the Configuring AAA Services chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Note Currently, only default VRF is supported. VPNv4, VPNv6 and VPN routing and forwarding (VRF) address families will be supported in a future release.

aaa accounting

To create a method list for accounting, use the **aaa accounting** command in the XR EXEC mode. To remove a list name from the system, use the **no** form of this command.

aaa accounting {**commands** | **exec** | **mobile** | **network** | **subscriber** | **system** } {**default** | **list-name**} {**start-stop** | **stop-only**} {**none** | **method**}
no aaa accounting {**commands** | **exec** | **mobile** | **network**} {**default** | **list-name**}

Syntax Description

commands	Enables accounting for XR EXEC shell commands.
exec	Enables accounting of a XR EXEC session.
mobile	Enables Mobile IP related accounting events.
network	Enables accounting for all network-related service requests, such as Internet Key Exchange (IKE) and Point-to-Point Protocol (PPP).
subscriber	Sets accounting lists for subscribers.
system	Enables accounting for all system-related events.
event manager	Sets the authorization list for XR EXEC.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the accounting method list.
start-stop	Sends a "start accounting" notice at the beginning of a process and a "stop accounting" notice at the end of a process. The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.
stop-only	Sends a "stop accounting" notice at the end of the requested user process. Note: This is not supported with system accounting.
none	Uses no accounting.
method	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Uses the list of all TACACS+ servers for accounting. • **group radius**—Uses the list of all RADIUS servers for accounting. • **group** *named-group*—Uses a named subset of TACACS+ or RADIUS servers for accounting, as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

AAA accounting is disabled.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **aaa accounting** command to create default or named method lists defining specific accounting methods and that can be used on a per-line or per-interface basis. You can specify up to four methods in the method list. The list name can be applied to a line (console, aux, or vty template) to enable accounting on that particular line.

The Cisco IOS XR software supports both TACACS+ and RADIUS methods for accounting. The router reports user activity to the security server in the form of accounting records, which are stored on the security server.

Method lists for accounting define the way accounting is performed, enabling you to designate a particular security protocol that is used on specific lines or interfaces for particular types of accounting services.

For minimal accounting, include the **stop-only** keyword to send a "stop accounting" notice after the requested user process. For more accounting, you can include the **start-stop** keyword, so that TACACS+ or RADIUS sends a "start accounting" notice at the beginning of the requested process and a "stop accounting" notice after the process. The accounting record is stored only on the TACACS+ or RADIUS server.

The requested user process begins regardless of whether the "start accounting" notice was received by the accounting server.

Note This command cannot be used with TACACS or extended TACACS.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define a default commands accounting method list, where accounting services are provided by a TACACS+ security server, with a stop-only restriction:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting commands default stop-only group tacacs+
```

aaa accounting system default

To enable authentication, authorization, and accounting (AAA) system accounting, use the **aaa accounting system default** command in the XR Config mode. To disable system accounting, use the **no** form of this command.

aaa accounting system default {**start-stop** | **stop-only**} {**none** | **method**}
no aaa accounting system default

Syntax Description

start-stop	Sends a "start accounting" notice during system bootup and a "stop accounting" notice during system shutdown or reload.
stop-only	Sends a "stop accounting" notice during system shutdown or reload.
none	Uses no accounting.
method	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Uses the list of all TACACS+ servers for accounting. • **group radius**—Uses the list of all RADIUS servers for accounting. • **group** *named-group*—Uses a named subset of TACACS+ or RADIUS servers for accounting, as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

AAA accounting is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

System accounting does not use named accounting lists; you can define only the default list for system accounting.

The default method list is automatically applied to all interfaces or lines. If no default method list is defined, then no accounting takes place.

You can specify up to four methods in the method list.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to cause a "start accounting" record to be sent to a TACACS+ server when a router initially boots. A "stop accounting" record is also sent when a router is shut down or reloaded.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting system default start-stop group tacacs+
```

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in the XR Config mode. To disable the interim accounting updates, use the **no** form of this command.

aaa accounting update {**periodic** *minutes*}
no aaa accounting update

Syntax Description

periodic *minutes*	(Optional) Sends an interim accounting record to the accounting server periodically, as defined by the *minutes* argument, which is an integer that specifies the number of minutes. The range is from 1 to 35791394 minutes.

Command Default

AAA accounting update is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

When used with the **periodic** keyword, interim accounting records are sent periodically as defined by the *minutes* argument. The interim accounting record contains all the accounting information recorded for that user up to the time the accounting record is sent.

Caution Using the **aaa accounting update** command with the **periodic** keyword can cause heavy congestion when many users are logged into the network.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to send periodic interim accounting records to the RADIUS server at 30-minute intervals:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting update periodic 30
```

aaa authentication (XR-VM)

To create a method list for authentication, use the **aaa authentication** command in the XR Config mode or Admin Configuration modeSystem Admin Config mode. To disable this authentication method, use the **no** form of this command.

aaa authentication {**login** | **ppp**} {**default***list-name*} *method-list*
no aaa authentication {**login** | **ppp**} {**default***list-name*} *method-list*

Syntax Description

login	Sets authentication for login.
ppp	Sets authentication for Point-to-Point Protocol.
default	Uses the listed authentication methods that follow this keyword as the default list of methods for authentication.
subscriber	Sets the authentication list for the subscriber.
list-name	Character string used to name the authentication method list.
method-list	Method used to enable AAA system accounting. The value is one of the following options: • **group tacacs+**—Specifies a method list that uses the list of all configured TACACS+ servers for authentication. • **group radius**—Specifies a method list that uses the list of all configured RADIUS servers for authentication. • **group** *named-group* —Specifies a method list that uses a named subset of TACACS+ or RADIUS servers for authentication, as defined by the **aaa group server tacacs+** or **aaa group server radius** command. • **local**—Specifies a method list that uses the local username database method for authentication. AAA method rollover happens beyond the local method if username is not defined in the local group. • **line**—Specifies a method list that uses the line password for authentication.

Command Default

Default behavior applies the local authentication on all ports.

Command Modes

XR Config mode or Admin Configuration modeSystem Admin Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **aaa authentication** command to create a series of authentication methods, or method list. You can specify up to four methods in the method list. A *method list* is a named list describing the authentication methods (such as TACACS+ or RADIUS) in sequence. The subsequent methods of authentication are used only if the initial method is not available, not if it fails.

The default method list is applied for all interfaces for authentication, except when a different named method list is explicitly specified—in which case the explicitly specified method list overrides the default list.

For console and vty access, if no authentication is configured, a default of local method is applied.

Note

- The **group tacacs+**, **group radius**, and **group** *group-name* forms of this command refer to a set of previously defined TACACS+ or RADIUS servers.
- Use the **tacacs-server host** or **radius-server host** command to configure the host servers.
- Use the **aaa group server tacacs+** or **aaa group server radius** command to create a named subset of servers.
- The **login** keyword, **local** option, and **group** option are available only in Admin Configuration modeSystem Admin Config mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify the default method list for authentication, and also enable authentication for console in XR Config mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa authentication login default group tacacs+
```

aaa authorization (XR-VM)

To create a method list for authorization, use the **aaa authorization** command in the XR Config mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization { **commands** | **eventmanager** | **exec** | **network** | **subscriber** | **nacm** } { **default** *list-name* } { **none** | **local** | **prefer-external** | **only-external** | **group** { **tacacs** + | **radius** *group-name* } }
no aaa authorization { **commands** | **eventmanager** | **exec** | **network** | **subscriber** | **nacm** } { **default** *list-name* }

Syntax Description

commands	Configures authorization for all XR EXEC mode shell commands.
eventmanager	Applies an authorization method for authorizing an event manager (fault manager).
exec	Configures authorization for an interactive (XR EXEC mode) session.
network	Configures authorization for network services, such as PPP or Internet Key Exchange (IKE).
subscriber	Sets the authorization lists for the subscriber.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
none	Uses no authorization. If you specify **none**, no subsequent authorization methods is attempted. However, the task ID authorization is always required and cannot be disabled.
local	Uses local authorization. While this method of authorization is already supported, it is available for command authorization only from Cisco IOS XR Software Release 7.5.1 and later.
prefer-external	Adds the external group names to the list of local group names to determine the access control rules.
only-external	Uses the external group names to determine the access control rules.
group tacacs+	Uses the list of all configured TACACS+ servers for authorization.
group radius	Uses the list of all configured RADIUS servers for authorization. This method of authorization is not available for command authorization.
group *group-name*	Uses a named subset of TACACS+ or RADIUS servers for authorization as defined by the **aaa group server tacacs+** or **aaa group server radius** command.

Command Default

Authorization is disabled for all actions (equivalent to the method **none** keyword).

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.5.1	The command was modified to make the **local** option available for command authorization as well.
Release 7.4.1	NACM **prefer-external** and **only-external** keywords are introduced.
Release 6.0	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to create method lists defining specific authorization methods that can be used on a per-line or per-interface basis. You can specify up to four methods in the method list.

Note The command authorization mentioned here applies to the one performed by an external AAA server and *not* for task-based authorization.

Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is a named list describing the authorization methods (such as TACACS+), in sequence. Method lists enable you to designate one or more security protocols for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS XR software uses the first method listed to authorize users for specific network services; if that method fails to respond, Cisco IOS XR software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method or until all methods defined have been exhausted.

Note Cisco IOS XR software attempts authorization with the next listed method only when there is no response (not a failure) from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

The Cisco IOS XR software supports the following methods for authorization:

- **none—**The router does not request authorization information; authorization is not performed over this line or interface.
- **local—**Use the local database for authorization.
- **group tacacs+—**Use the list of all configured TACACS+ servers for authorization.
- **group radius—**Use the list of all configured RADIUS servers for authorization.
- **group group-name—**Uses a named subset of TACACS+ or RADIUS servers for authorization.

Method lists are specific to the type of authorization being requested. Cisco IOS XR software supports four types of AAA authorization:

- **Commands authorization—**Applies to the XR EXEC mode commands a user issues. Command authorization attempts authorization for all XR EXEC mode commands.

Note "Command" authorization is distinct from "task-based" authorization, which is based on the task profile established during authentication.

- XR EXEC mode **authorization—**Applies authorization for starting an XR EXEC mode session.

Note The **exec** keyword is no longer used to authorize the fault manager service. The **eventmanager** keyword (fault manager) is used to authorize the fault manager service. The **exec** keyword is used for EXEC authorization.

- **Network authorization—**Applies authorization for network services, such as IKE.
- **Event manager authorization—**Applies an authorization method for authorizing an event manager (fault manager). You are allowed to use TACACS+ or locald.

Note The **eventmanager** keyword (fault manager) replaces the **exec** keyword to authorize event managers (fault managers).

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type. When defined, method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

To know more about command authorization using local user account feature which was introduced in Cisco IOS XR Software Release 7.5.1, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define the network authorization method list named listname1, which specifies that TACACS+ authorization is used:

```
Router# configure
Router(config)# aaa authorization commands listname1 group tacacs+
```

The following examples show how to configure command authorization using local user account:

```
Router#configure
Router(config)#aaa authorization commands default group tacacs+ local
Router(config)#commit
```

or

```
Router(config)#aaa authorization commands default local
Router(config)#commit
```

aaa authorization (System Admin-VM)

To create command rules and data rules on System Admin VM for user authorization, use the **aaa authorization** command in Admin Configuration modeSystem Admin Config mode. To delete the command rules and data rules, use the **no** form of this command.

aaa authorization { **cmdrules cmdrule** { *integer* | **range** *integer* } [**action** *action-type* | **command** *cmd-name* | **context** *context-name* | **group** *group-name* | **ops** *ops-type*] | **commands group** { **none** | **tacacs** } | **datarules datarule** { *integer* | **range** *integer* } [**action** *action-type* | **context** *context-name* | **group** *group-name* | **keypath** *keypath-name* | **namespace** *namespace-string* | **ops** *ops-type*] }

Syntax Description

cmdrules	Configures command rules.
cmdrule *integer*	Specifies the command rule number.
range *integer*	Specifies the range of the command rules or data rules to be configured.
action	Specifies whether users are permitted or not allowed to perform the operation specified for the **ops** keyword.
action-type	Specifies the action type for the command rule or data rule. Available options are: **accept**, **accept_log** and **reject**.
command *cmd-name*	Specifies the command to which the command rule applies. The command must be entered within double-quotes. Example, **get**.
context *context-name*	Specifies to which type of connection the command rule or data rule applies. The connection type can be netconf, cli, or xml.
group *group-name*	Specifies the group to which the command rule or data rule applies. Example, **admin-r**.
ops *ops-type*	Specifies whether the user has read, execute, or read and execute permissions for the command. Available options for command rules are: **r**, rx, and **x**. To know the available options for data rules, use a **?** after the **ops** keyword.
commands group	Sets the command authorization lists for server groups. Available options are **none** that specifies no authorization and **tacacs** that specifies use of the list of all tacacs+ hosts.
datarules	Configures data rules.
datarule *integer*	Specifies the data rule number.
keypath	Specifies the keypath of the data element. If you enter an asterisk '*' for keypath, it indicates that the command rule is applicable to all configuration data.

namespace	Enter asterisk "*" to indicate that the data rule is applicable for all namespace values.

Command Default

None

Command Modes

Admin Configuration modeSystem Admin Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

From Cisco IOS XR Software Release 7.4.1 and later, the system internally maps the users configured on the XR VM to System Admin VM of the router, based on the task table of the user on the XR VM. With this feature, NETCONF and gRPC users can access the admin-related information on the router even if their user profiles do not exist on System Admin VM. For a sample configuration, see the example section.

For more details, see the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

This example shows how to create a command rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 10 action accept command "show
 platform" context cli group group1 ops rx
```

This example shows how to create a data rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 20 action accept context cli
 group group10 keypath * namespace * ops rwx
```

This example shows how to configure a command rule for a NETCONF or gRPC session to allow read access for **admin-r** group users:

```
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 6 context netconf command get
 group admin-r ops rx action accept
```

aaa default-taskgroup

To specify a task group for both remote TACACS+ authentication and RADIUS authentication, use the **aaa default-taskgroup** command in the XR Config mode. To remove this default task group, enter the **no** form of this command.

aaa default-taskgroup *taskgroup-name*
no aaa default-taskgroup

Syntax Description

taskgroup-name	Name of an existing task group.

Command Default

No default task group is assigned for remote authentication.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **aaa default-taskgroup** command to specify an existing task group for remote TACACS+ authentication.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify taskgroup1 as the default task group for remote TACACS+ authentication:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa default-taskgroup taskgroup1
```

aaa enable-cert-authentication

To enable certificate-based authentication for users in the TACACS+ Server or Server Groups, use the **aaa enable-cert-authentication** command in the XR-Config mode.

aaa enable-cert-authentication

Syntax Description

This command has no keywords or arguments.

Command Default

Certificate-based user authentication using TACACS+ server is disabled.

Command Modes

XR-Config mode.

Command History

Release	Modification
Release 7.5.4	This command was introduced.

Usage Guidelines

Enable AAA authorization using **aaa authorization exec** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to configure certificate-based authentication for users configured in the TACACS+ Server or Server Groups:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa enable-cert-authentication
RP/0/RP0/CPU0:router(config)# aaa authorization exec default group tacacs+ local
RP/0/RP0/CPU0:router(config)# commit
```

aaa group server radius

To group different RADIUS server hosts into distinct lists, use the **aaa group server radius** command in the XR Config mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*
no aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

This command is not enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **aaa group server radius** command to group existing server hosts, which allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses or hostnames of the selected server hosts.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and User Datagram Protocol (UDP) port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific authentication, authorization, and accounting (AAA) service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service, for example, accounting, the second host entry acts as an automatic switchover backup to the first host entry. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry on the same device for accounting services. The RADIUS host entries are tried in the order in which they are configured in the server group.

All members of a server group must be the same type, that is, RADIUS.

The server group cannot be named radius or tacacs.

This command enters server group configuration mode. You can use the server command to associate a particular RADIUS server with the defined server group.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the configuration of an AAA group server named radgroup1, which comprises three member servers:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius radgroup1
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.5 auth-port 1700 acct-port 1701
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.10 auth-port 1702 acct-port 1703
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.20 auth-port 1705 acct-port 1706
```

Note If the **auth-port** *port-number* and **acct-port** *port-number* keywords and arguments are not specified, the default value of the *port-number* argument for the **auth-port** keyword is 1645 and the default value of the *port-number* argument for the **acct-port** keyword is 1646.

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists, use the **aaa group server tacacs+** command in the XR Config mode. To remove a server group from the configuration list, enter the **no** form of this command.

aaa group server tacacs+ *group-name*
no aaa group server tacacs+ *group-name*

Syntax Description

group-name	Character string used to name a group of servers.

Command Default

This command is not enabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The AAA server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

The **aaa group server tacacs+** command enters server group configuration mode. The **server** command associates a particular TACACS+ server with the defined server group.

A *server group* is a list of server hosts of a particular type. The supported server host type is TACACS+ server hosts. A server group is used with a global server host list. The server group lists the IP addresses or hostnames of the selected server hosts.

The server group cannot be named radius or tacacs.

Note Group name methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers.

From Cisco IOS XR Software Release 7.4.1 and later, you can configure a hold-down timer for TACACS+ server. For details, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the configuration of an AAA group server named tacgroup1, which comprises three member servers:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ tacgroup1
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.226
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.227
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.228
```

aaa password-policy

To define a AAA password security policy, use the **aaa password-policy** command in XR Config mode. To remove the AAA password security policy, use the **no** form of this command.

aaa password-policy *policy-name* { **authen-max-attempts** *authen-max-attempts* | **lifetime** { **years** | **months** | **days** | **hours** | **minutes** | **seconds** } *lifetime* | **lockout-time** { **days** | **hours** | **minutes** | **seconds** } *lockout-time* | **lower-case** *lower-case* | **max-length** *max-length* | **min-char-change** *min-char-change* | **min-length** *min-length* | **numeric** *numeric* | **restrict-consecutive-characters** { **english-alphabet** | **qwerty-keyboard** } *num-of-chars* [**cyclic-wrap**] | **special-char** *special-char* | **upper-case** *upper-case* }

Syntax Description

policy-name	Specifies the name of the password, in characters.
authen-max-attempts	Specifies, in integer, the maximum number of authentication failure attempts allowed for a user, in order to restrict users who authenticate with invalid login credentials.
lifetime	Specifies the maximum lifetime for the password, the value of which is specified in integer, as years, months, days, hours, minutes or seconds.
lockout-time	Specifies, in integer, the duration (in days, hours, minutes or seconds) for which the user is locked out when he exceeds the maximum limit of authentication failure attempts allowed.
lower-case	Specifies the number of lower case alphabets allowed in the password policy, in integer.
max-length	Specifies the maximum length of the password, in integer.
min-char-change	Specifies the number of character change required between subsequent passwords, in integer.
min-length	Specifies the maximum length of the password, in integer.
numeric	Specifies the number of numerals allowed in the password policy, in integer.
restrict-consecutive-characters	Restricts consecutive characters (that includes regular English alphabets, and English alphabets from QWERTY keyboard layout and numbers), for user passwords and secrets.
special-char	Specifies the number of special characters allowed in the password policy, in integer.
upper-case	Specifies the number of upper case alphabets allowed in the password policy, in integer.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.7.1	This command was modified to introduce the **restrict-consecutive-characters** option.
Release 7.2.1	The command options (except a few mentioned in the usage guidelines section) were extended to user secret as well.
Release 6.2.1	This command was introduced.

Usage Guidelines

AAA password security policy works as such for Cisco IOS XR platforms. Whereas, this feature is supported only on XR VM, for Cisco IOS XR 64 bit platforms and Cisco NCS 5500 Series Routers.

For more details on the usage of each option of this command, refer the section on *AAA Password Security for FIPS Compliance* in *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

You must configure both **authen-max-attempts** and **lockout-time** in order for the lock out functionality to take effect.

The **min-char-change** option is effective only for password change through logon, and not for password change by configuration.

Use **username** command along with **password-policy** option, in the XR Config mode, to associate the password policy with a particular user.

From Cisco IOS XR Software Release 7.2.1 and later, most of the options of the **aaa password-policy** command listed in the syntax above are applicable to user password as well as secret. Whereas, the options listed below are supported only for password, and not for secret:

- **max-char-repetition**
- **min-char-change**
- **restrict-password-reverse**
- **restrict-password-advanced**

Among the NCS540 router variants, the **restrict-consecutive-characters** option is applicable only for the following variants:

- N540-28Z4C-SYS-A/D
- N540X-16Z4G8Q2C-A/D
- N540-12Z20G-SYS-A/D
- N540X-12Z16G-SYS-A/D

This table lists the default, maximum and minimum values of various command variables:

Command Variables	Default Value	Maximum Value	Minimum Value
policy-name	None	253	1
max-length	253	253	2

Command Variables	Default Value	Maximum Value	Minimum Value
min-length	2	253	2
special-char	0	253	0
upper-case	0	253	0
lower-case	0	253	0
numeric	0	253	0
For **lifetime** : **years** **months** **days** **hours** **minutes** **seconds**	0 0 0 0 0 0	99 11 30 23 59 59	1 1 1 1 1 1
min-char-change	4	253	0
authen-max-attempts	0	24	1
For **lockout-time** : **days** **hours** **minutes** **seconds**	0 0 0 0	255 23 59 59	1 1 1 1

Task ID

Task ID	Operation
aaa	read, write

This example shows how to define a AAA password security policy:

```
RP/0/RP0/CPU0:router(config)#aaa password-policy test-policy
RP/0/RP0/CPU0:router(config-aaa)#min-length 8
RP/0/RP0/CPU0:router(config-aaa)#max-length 15
RP/0/RP0/CPU0:router(config-aaa)#lifetime months 3
RP/0/RP0/CPU0:router(config-aaa)#min-char-change 5
RP/0/RP0/CPU0:router(config-aaa)#authen-max-attempts 3
```

```
RP/0/RP0/CPU0:router(config-aaa)#lockout-time days 1
```

Related Commands

Command	Description
restrict-consecutive-characters, on page 56	Restricts consecutive characters, including English alphabets and numbers, for user passwords and secrets.
show aaa password-policy	Displays the details of AAA password policy.
username, on page 114	

accounting (line)

To enable authentication, authorization, and accounting (AAA) accounting services for a specific line or group of lines, use the **accounting** command. To disable AAA accounting services, use the **no** form of this command.

accounting {**commands** | **exec**} {**default***list-name*}
no accounting {**commands** | **exec**}

Syntax Description

commands	Enables accounting on the selected lines for all XR EXEC mode shell commands.
exec	Enables accounting of XR EXEC mode session.
default	The name of the default method list, created with the **aaa accounting** command.
list-name	Specifies the name of a list of accounting methods to use. The list is created with the **aaa accounting** command.

Command Default

Accounting is disabled.

Command Modes

Line template configuration

Command History

Release	Modification
Release 6.0	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) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists to the selected line or group of lines. If a method list is not specified this way, no accounting is applied to the selected line or group of lines.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable command accounting services using the accounting method list named *listname2* on a line template named *configure:*

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template configure
RP/0/RP0/CPU0:router(config-line)# accounting commands listname2
```

authorization (line)

To enable authentication, authorization, and accounting (AAA) authorization for a specific line or group of lines, use the **authorization** command in line template configuration mode. To disable authorization, use the **no** form of this command.

authorization {**commands** | **exec** | **eventmanager**} {**default***list-name*}
no authorization {**commands** | **exec** | **eventmanager**}

Syntax Description

commands	Enables authorization on the selected lines for all commands.
exec	Enables authorization for an interactive XR EXEC mode session.
default	Applies the default method list, created with the **aaa authorization** command.
eventmanager	Sets eventmanager authorization method. This method is used for the embedded event manager.
list-name	Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Command Default

Authorization is not enabled.

Command Modes

Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

After you use the **aaa authorization** command to define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or, if none is specified, the default method list) to the selected line or group of lines.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable command authorization using the method list named *listname4* on a line template named *configure:*

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template configure
RP/0/RP0/CPU0:router(config-line)# authorization commands listname4
```

deadtime (server-group configuration)

To configure the deadtime value at the RADIUS server group level, use the **deadtime** command in server-group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*
no deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 (24 hours). The range is from 1 to 1440.

Command Default

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The value of the deadtime set in the server groups overrides the deadtime that is configured globally. If the deadtime is omitted from the server group configuration, the value is inherited from the primary list. If the server group is not configured, the default value of 0 applies to all servers in the group. If the deadtime is set to 0, no servers are marked dead.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example specifies a one-minute deadtime for RADIUS server group **group1** when it has failed to respond to authentication requests for the **deadtime** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.1.1.1 auth-port 1645 acct-port 1646
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.2.2.2 auth-port 2000 acct-port 2001
RP/0/RP0/CPU0:router(config-sg-radius)# deadtime 1
```

description (AAA)

To create a description of a task group or user group during configuration, use the **description** command in task group configuration or user group configuration mode. To delete a task group description or user group description, use the **no** form of this command.

description *string*
no description

Syntax Description

string	Character string describing the task group or user group.

Command Default

None

Command Modes

Task group configuration

User group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **description** command inside the task or user group configuration submode to define a description for the task or user group, respectively.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the creation of a task group description:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup alpha
RP/0/RP0/CPU0:router(config-tg)# description this is a sample taskgroup
```

The following example shows the creation of a user group description:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# usergroup alpha
RP/0/RP0/CPU0:router(config-ug)# description this is a sample user group
```

group (AAA)

To add a user to a group, use the **group** command in username configuration mode. To remove the user from a group, use the **no** form of this command.

group {**cisco-support** | **maintenance** | **netadmin** | **operator** | **provisioning** | **retrieve** | **root-lr** | **serviceadmin** | **sysadmin***group-name*}
no group {**cisco-support** | **maintenance** | **netadmin** | **operator** | **provisioning** | **retrieve** | **root-lr** | **serviceadmin** | **sysadmin***group-name*}

Syntax Description

cisco-support	Adds the user to the predefined Cisco support personnel group. **Note** Starting from IOS XR 6.0 release, the cisco-support group is combined with the root-system group. This means a user who is part of the root-system group can also access commands that are included in the cisco-support group.
maintenance	Adds the user to the predefined maintenance group.
netadmin	Adds the user to the predefined network administrators group.
operator	Adds the user to the predefined operator group.
provisioning	Adds the user to the predefined provisioning group.
retrieve	Adds the user to the predefined retrieve group.
root-lr	Adds the user to the predefined root-lr group. Only users with root-lr authority may use this option.
serviceadmin	Adds the user to the predefined service administrators group.
sysadmin	Adds the user to the predefined system administrators group.
group-name	Adds the user to a named user group that has already been defined with the **usergroup** command.

Command Default

None

Command Modes

Username configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **group** command in username configuration mode. To access username configuration mode, use the username, on page 114 command in XR Config mode.

If the **group** command is used in Admin Configuration modeSystem Admin Config mode, only cisco-support keywords can be specified.

The privileges associated with the cisco-support group are now included in the root-system group. The cisco-support group is no longer required to be used for configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to assign the user group operator to the user named user1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# group operator
```

holddown-time (TACACS+)

To specify a duration for which an unresponsive TACACS+ server is to be marked as down, and not be used for sending further client requests for that duration, use the **holddown-time** command in various configuration modes. To disable this feature, use the **no** form of this command or configure the hold down timer value as zero.

holddown-time *time*

Syntax Description

time	Specifies the hold-down timer value, in seconds. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.

Command Default

By default, the TACACS+ hold-down timer is disabled.

Command Modes

TACACS server

TACACS+ server group

TACACS+ private server

Command History

Release	Modification
Release 7.4.1	This command was introduced.

Usage Guidelines

Note To set the hold-down timer at global level, use the **tacacs-server holddown-time** command in XR Config mode.

While selecting the timer at various configuration levels, the system gives preference to the one which is more specific to the server. That is, the server-level timer has the highest precedence, followed by server group-level and finally, the global-level.

Also, see the *Guidelines for Configuring Hold-Down Timer for TACACS+* section in the *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to mark an unresponsive TACACS+ server as being down, and not to use it for sending further client requests for a duration of 35 seconds:

```
Router(config)#tacacs-server host 10.105.236.102 port 2020
Router(config-tacacs-host)#holddown-time 35
```

This example shows how to set a hold-down timer at global level:

```
Router#configure
Router(config)#tacacs-server holddown-time 30
```

This example shows how to set a hold-down timer at server-group level:

```
Router#configure
Router(config)#aaa group server tacacs+ test-group
Router(config-sg-tacacs)#holddown-time 40
```

This example shows how to set a hold-down timer at private server level:

```
Router(config)#aaa group server tacacs+ test-group
Router(config-sg-tacacs)#server-private 10.105.236.109 port 2020
Router(config-sg-tacacs-private)#holddown-time 55
Router(config-sg-tacacs-private)#commit
```

Related Commands

Command	Description
aaa group server tacacs+, on page 20	Groups different TACACS+ server hosts into distinct lists.
server-private (TACACS+), on page 66	Configures the IP address of the private TACACS+ server for the group server.
tacacs-server host, on page 98	Configures a TACACS+ host server.

inherit taskgroup

To enable a task group to derive permissions from another task group, use the **inherit taskgroup** command in task group configuration mode.

inherit taskgroup {*taskgroup-name* | **netadmin** | **operator** | **sysadmin** | **cisco-support** | **root-lr** | **serviceadmin**}

Syntax Description

taskgroup-name	Name of the task group from which permissions are inherited.
netadmin	Inherits permissions from the network administrator task group.
operator	Inherits permissions from the operator task group.
sysadmin	Inherits permissions from the system administrator task group.
cisco-support	Inherits permissions from the cisco support task group.
root-lr	Inherits permissions from the root-lr task group.
serviceadmin	Inherits permissions from the service administrators task group.

Command Default

None

Command Modes

Task group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **inherit taskgroup** command to inherit the permissions (task IDs) from one task group into another task group. Any changes made to the taskgroup from which they are inherited are reflected immediately in the group from which they are inherited.

Task ID

Task ID	Operations
aaa	read, write

Examples

In the following example, the permissions of task group tg2 are inherited by task group tg1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup tg1
RP/0/RP0/CPU0:router(config-tg)# inherit taskgroup tg2
RP/0/RP0/CPU0:router(config-tg)# end
```

inherit usergroup

To enable a user group to derive characteristics of another user group, use the **inherit usergroup** command in user group configuration mode.

inherit usergroup *usergroup-name*

Syntax Description

usergroup-name	Name of the user group from which permissions are to be inherited.

Command Default

None

Command Modes

User group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Each user group is associated with a set of task groups applicable to the users in that group. A task group is defined by a collection of task IDs. Task groups contain task ID lists for each class of action. The task permissions for a user are derived (at the start of the EXEC or XML session) from the task groups associated with the user groups to which that user belongs.

User groups support inheritance from other user groups. Use the **inherit usergroup** command to copy permissions (task ID attributes) from one user group to another user group. The "destination" user group inherits the properties of the inherited group and forms a union of all task IDs specified in those groups. For example, when user group A inherits user group B, the task map of the user group A is a union of that of A and B. Cyclic inclusions are detected and rejected. User groups cannot inherit properties from predefined groups, such as root-system users, root-sdr users, netadmin users, and so on. Any changes made to the usergroup from which it is inherited are reflected immediately in the group from which it is inherited.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable the purchasing user group to inherit properties from the sales user group:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# usergroup purchasing
RP/0/RP0/CPU0:router(config-ug)# inherit usergroup sales
```

key (TACACS+)

To specify an authentication and encryption key shared between the AAA server and the TACACS+ server, use the **key (TACACS+)** command in TACACS host configuration mode. To disable this feature, use the **no** form of this command.

key { **0** *clear-text-key* | **6** *encrypted-type6-key* | **7** *encrypted-key* | **Encrypt6** *encrypted-key clear-text-key* | **clear** *clear-text-key* | **encrypted** *encrypted-key* }

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
6 *encrypted-type6-key*	Specifies an type 6 encrypted shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
Encrypt6 *encrypted-key*	Specifies an unencrypted (cleartext) shared key to be encrypted in type6.
clear-text-key	Specifies an unencrypted (cleartext) user password.
clear *clear-text-key*	Specifies an unencrypted (cleartext) shared key. **Note** This option is decrypted from release 7.4.1. Use keyword **0**
encrypted *encrypted-key*	Specifies an encrypted shared key. **Note** This option is decrypted from release 7.4.1. Use keyword **7**

Command Default

None

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The TACACS+ packets are encrypted using the key, and it must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the **tacacs-server key** command for this server only.

The key is used to encrypt the packets that are going from TACACS+, and it should match with the key configured on the external TACACS+ server so that the packets are decrypted properly. If a mismatch occurs, the result fails.

The minimum character length of the key is 1 and maximum character length of the key is 48.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the encrypted key to anykey

```
RP/0/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)# key anykey
```

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line template configuration mode. To return to the default authentication settings, use the **no** form of this command.

login authentication {**default***list-name*}
no login authentication

Syntax Description

default	Default list of AAA authentication methods, as set by the **aaa authentication login** command.
list-name	Name of the method list used for authenticating. You specify this list with the **aaa authentication login** command.

Command Default

This command uses the default set with the **aaa authentication login** command.

Command Modes

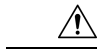
Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **login authentication** command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login.



Caution If you use a *list-name* value that was not configured with the **aaa authentication login** command, the configuration is rejected.

Entering the **no** form of the **login authentication** command has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the **aaa authentication login** command.

Task ID

Task ID	Operations
aaa	read, write
tty-access	read, write

Examples

The following example shows that the default AAA authentication is used for the line template *template1*:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# line template template1
RP/0/RP0/CPU0:router(config-line)# login authentication default
```

The following example shows that the AAA authentication list called *list1* is used for the line template *template2*:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template template2
RP/0/RP0/CPU0:router(config-line)# login authentication list1
```

nacm enable-external-policies

To enable dynamic NETCONF Access Control Model (NACM) policy authorization on a router, use the **nacm enable-external-policies** command in the XR Config mode. To remove the configuration, use the **no** form of this command.

nacm enable-external-policies

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.8.1	This command was introduced.

Usage Guidelines

If this configuration is not present, update the NACM policies manually on each router.

Task ID

Task ID	Operation
nacm	read, write

This example shows how to enable the dynamic NACM on a router.

```
Router#configure
Router(config)# nacm enable-external-policies
Router(config)# commit
```

password (AAA)

To create a login password for a user, use the **password** command in username configuration mode or line template configuration mode. To remove the password, use the **no** form of this command.

password {[**0**] | **7** *password*}
no password {**0** | **7** *password*}

Syntax Description

0	(Optional) Specifies that an unencrypted clear-text password follows.
7	Specifies that an encrypted password follows.
password	Specifies the unencrypted password text to be entered by the user to log in, for example, “lab”. If encryption is configured, the password is not visible to the user. Can be up to 253 characters in length.

Command Default

The password is in unencrypted clear text.

Command Modes

Username configuration

Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

You can specify one of two types of passwords: encrypted or clear text.

When an XR EXEC modeprocess is started on a line that has password protection, the process prompts for the password. If the user enters the correct password, the process issues the prompt. The user can try three times to enter a password before the process exits and returns the terminal to the idle state.

Passwords are two-way encrypted and should be used for applications such as PPP that need decryptable passwords that can be decrypted.

Note The **show running-config** command always displays the clear-text login password in encrypted form when the **0** option is used.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the unencrypted password *pwd1* for user. The output from the **show** command displays the password in its encrypted form.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# password 0 pwd1
RP/0/RP0/CPU0:router(config-un)# commit
RP/0/RP0/CPU0:router(config-un)# show running-config
Building configuration...
username user1
 password 7 141B1309
```

policy (AAA)

To configure a policy that is common for user password as well as secret, use the **policy** command in username configuration mode. To remove this configuration, use the **no** form of this command.

policy *policy-name*

Syntax Description

policy-name	Specifies the name of the policy that is common for user password as well as secret.

Command Default

None

Command Modes

username

Command History

Release	Modification
Release 7.2.1	This command was introduced.

Usage Guidelines

For detailed usage guidelines for this command, see the *Guidelines to Configure Password Policy for User Secret* section in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure a password policy that applies to both the password and the secret of the user.

```
Router#configure
Router(config)#username user1
Router(config-un)#policy test-policy1
Router(config-un)#secret 10
$6$dmwuW0Ajicf98W0.$y/vzynWF1/OcGxwBwHs79VAy5ZZLhoHd7TicR4mOo8IIVriYCGAKW0A.w1JvTPO7IbZry.DxHrE3SN2BBzBJe0
Router(config-un)#commit
```

Related Commands

Command	Description
username, on page 114	

aaa display-login-failed-users

aaa display-login-failed-users

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default

Command Modes

Global configuration mode

Command History

Release	Modification
Release 7.10.1	The command was introduced to make the **display-login-failed-users** option available to display user ID for failed user login attempts.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

This example shows how to enable the functioanlity to display the username for a failed authentication:

```
Router#Configure
Router(config)# aaa display-login-failed-users
Router(config)#commit
```

radius-server dead-criteria time

To specify the 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, use the **radius-server dead-criteria time** command in XR Config mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria time *seconds*
no radius-server dead-criteria time *seconds*

Syntax Description

seconds Length of time, in seconds. The range is from 1 to120 seconds. If the *seconds* argument is not configured, the number of seconds ranges from 10 to 60, depending on the transaction rate of the server.

Note The time criterion must be met for the server to be marked as dead.

Command Default

If this command is not used, the number of seconds ranges from 10 to 60 seconds, depending on the transaction rate of the server.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Note If you configure the **radius-server dead-criteria time** command before the **radius-server deadtime** command, the **radius-server dead-criteria time** command may not be enforced.

If a packet has not been received since the router booted and there is a timeout, the time criterion is treated as though it were met.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the time for the dead-criteria conditions for a RADIUS server to be marked as dead for the **radius-server dead-criteria time** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server dead-criteria time 5
```

radius-server dead-criteria tries

To specify the number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead, use the **radius-server dead-criteria tries** command in the XR Config mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria *tries*
no radius-server dead-criteria *tries*

Syntax Description

tries Number of timeouts from 1 to 100. If the *tries* argument is not configured, the number of consecutive timeouts ranges from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Note The tries criterion must be met for the server to be marked as dead.

Command Default

If this command is not used, the number of consecutive timeouts ranges from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

If the server performs both authentication and accounting, both types of packet are included in the number. Improperly constructed packets are counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, are counted.

Note If you configure the **radius-server dead-criteria tries** command before the **radius-server deadtime** command, the **radius-server dead-criteria tries** command may not be enforced.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the number of tries for the dead-criteria conditions for a RADIUS server to be marked as dead for the **radius-server dead-criteria tries** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server dead-criteria tries 4
```

radius-server deadtime (BNG)

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

radius-server deadtime *value*
no radius-server deadtime *value*

Syntax Description

value	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 (24 hours). The range is from 1 to 1440. The default value is 0.

Command Default

Dead time is set to 0.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

A RADIUS server marked as dead is skipped by additional requests for the duration of minutes unless all other servers are marked dead and there is no rollover method.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example specifies five minutes of deadtime for RADIUS servers that fail to respond to authentication requests for the **radius-server deadtime** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server deadtime 5
```

radius-server host

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

radius-server host *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**dtls-server trustpoint** *string*] [**radsec-server trustpoint** *string*]

Syntax Description

ip-address	IP address of the RADIUS server host. IPv6 address is not supported.
auth-port *port-number*	(Optional) Specifies the RADIUS authentication port for authentication requests; the host is not used for authentication if set to 0.
acct-port *port-number*	(Optional) Specifies the RADIUS accounting port for accounting requests; the host is not used for accounting if set to 0.
timeout *seconds*	(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 from 1 to 1000. The default is 5.
retransmit *retries*	(Optional) The number of times a RADIUS request is resent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used. Enter a value in the range from 1 to 100. The default is 3.
key *string*	(Optional) Specifies the authentication and encryption key used between the router and the 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.
dtls-server trustpoint *string*	(Optional) Specifies the details for RADIUS over DTLS support. The trustpoint is a text string that matches the Trustpoint to be used for RADIUS over DTLS configuration. The default destination port for RADIUS over DTLS is UDP 2083 for authentication and accounting.
radsec-server trustpoint *string*	(Optional) Specifies the details for RADIUS over TLS support. The trustpoint is a text string that matches the Trustpoint to be used for RADIUS over TLS configuration. The default destination port for RADIUS over TLS is TCP 2083 for authentication and accounting.

Command Default

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

Command Modes

Global Configuration mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The Cisco IOS XR 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.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to establish the host with IP address 172.29.39.46 as the RADIUS server, use ports 1612 and 1616 as the authorization and accounting ports, set the timeout value to 6, set the retransmit value to 5, and set “rad123” as the encryption key, matching the key on the RADIUS server:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# 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.

This example shows how to configure RADIUS with DTLS protection.

```
Router# configure
Router(config)#radius-server host 209.165.201.1
Router(config-radius-host)#retransmit 5
Router(config-radius-host)#timeout 10
Router(config-radius-host)#dtls-server trustpoint test
Router(config-radius-host)#commit
```

This example shows how to configure RADIUS with TLS protection.

```
Router# configure
Router(config)#radius-server host 209.165.201.1 auth-port 2083 acct-port 2083 radsec-server
Router(config-radius-host)#trustpoint test
Router(config-radius-host)#commit
```

Related Commands

Command	Description
aaa accounting subscriber	Creates a method list for accounting.
aaa authentication subscriber	Creates a method list for authentication.
aaa authorization subscriber	Creates a method list for authorization.

Command	Description
radius-server key (BNG)	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit (BNG), on page 53	Specifies how many times Cisco IOS XR software retransmits packets to a server before giving up.
radius-server timeout (BNG), on page 54	Sets the interval a router waits for a server host to reply.

radius-server key (BNG)

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 the XR Config mode. To disable the key, use the **no** form of this command.

radius-server key { **0** *clear-text-key* | **6** *encrypted-type6-key* | **7** *encrypted-key* | **Encrypt6** *encrypted-key clear-text-key* | **clear** *clear-text-key* | **encrypted** *encrypted-key* }

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
6 *encrypted-type6-key*	Specifies an type 6 encrypted shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
Encrypt6 *encrypted-key*	Specifies an unencrypted (cleartext) shared key to be encrypted in type6.
clear-text-key	Specifies an unencrypted (cleartext) user password.
clear *clear-text-key*	Specifies an unencrypted (cleartext) shared key. **Note** This option is decrypted from release 7.4.1. Use keyword **0**
encrypted *encrypted-key*	Specifies an encrypted shared key. **Note** This option is decrypted from release 7.4.1. Use keyword **7**

Command Default

The authentication and encryption key is disabled.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The key entered must match the key used on the RADIUS server. 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.

The minimum character length of the key is 1 and maximum character length of the key is 48.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to set the cleartext key to “samplekey”:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server key 0 samplekey
```

This example shows how to set the encrypted shared key to “anykey”:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server key 7 anykey
```

radius-server retransmit (BNG)

To specify the number of times the Cisco IOS XR software retransmits a packet to a server before giving up, use the **radius-server retransmit** command in the XR Config mode. The **no** form of this command sets it to the default value of 3 .

radius-server retransmit {*retries* **disable**}
no radius-server retransmit {*retries* **disable**}

Syntax Description

retries	Maximum number of retransmission attempts. The range is from 1 to 100. Default is 3.
disable	Disables the radius-server transmit command.

Command Default

The RADIUS servers are retried three times, or until a response is received.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The RADIUS client tries all servers, allowing each one to time out before increasing the retransmit count.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to specify a retransmit counter value of five times:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server retransmit 5
```

radius-server timeout (BNG)

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

radius-server timeout *seconds*
no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. Range is from 1 to 1000.

Command Default

The default radius-server timeout value is 5 seconds.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **radius-server timeout** command to set the number of seconds a router waits for a server host to reply before timing out.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to change the interval timer to 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius-server timeout 10
```

radius source-interface (BNG)

To force RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets, use the **radius source-interface** command in the XR Config mode. To prevent only the specified interface from being the default and not from being used for all outgoing RADIUS packets, use the **no** form of this command.

radius source-interface *interface* [**vrf** *vrf_name*]
no radius source-interface *interface*

Syntax Description

interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-id*	Specifies the name of the assigned VRF.

Command Default

If a specific source interface is not configured, or the interface is down or does not have an IP address configured, the system selects an IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **radius source-interface** command to set the IP address of the specified interface or subinterface for all outgoing RADIUS packets. This address is used as long as the interface or subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

The specified interface or subinterface must have an IP address associated with it. If the specified interface or subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the interface or subinterface or bring the interface to the up state.

The **radius source-interface** command is especially useful in cases in which the router has many interfaces or subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to make RADIUS use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# radius source-interface loopback 10 vrf vrf1
```

restrict-consecutive-characters

To restrict consecutive characters (that includes regular English alphabets, and English alphabets from QWERTY keyboard layout and numbers), for user passwords and secrets, use the **restrict-consecutive-characters** command in *aaa password-policy* configuration mode. To disable the feature, use the **no** form of the command.

restrict-consecutive-characters { **english-alphabet** | **qwerty-keyboard** } *num-of-chars* [**cyclic-wrap**]

Syntax Description

english-alphabet	Restricts consecutive English alphabets for user passwords and secrets. For example, "abcd", "wxyz", and so on.
qwerty-keyboard	Restricts consecutive English alphabets from QWERTY keyboard layout and numbers, for user passwords and secrets. For example, "qwer", "mnbv", "7890", and so on.
num-of-chars	Specifies the number of consecutive characters to be restricted for user passwords and secrets. Range is 2 to 26, for **english-alphabet**. Range is 2 to 10, for **qwerty-keyboard**.
cyclic-wrap	Restricts cyclic wrapping of the alphabet or the number for user passwords and secrets. For example, "yzab", "opqw", "9012", and so on.

Command Default

Disabled, by default.

Command Modes

aaa password-policy configuration mode

Command History

Release	Modification
Release 7.7.1	This command was introduced.

Usage Guidelines

All password policies are applicable only to locally configured users.

After creating the password policy, you must explicitly apply that policy to the user profiles so that the password policy take effect in the password and secret configuration.

For more details about the feature and configuration task, see the section *Enhanced Security for User Passwords and Secrets* in *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Among the NCS540 router variants, this command is applicable only for the following variants:

- N540-28Z4C-SYS-A/D
- N540X-16Z4G8Q2C-A/D
- N540-12Z20G-SYS-A/D

- N540X-12Z16G-SYS-A/D

Task ID

Task ID	Operation
aaa	read, write

This example shows how to configure a AAA password policy that restricts cyclic wrapping of four consecutive English alphabets and six consecutive characters from QWERTY keyboard.

```
Router(config)#aaa password-policy test-policy
Router(config-pp)#restrict-consecutive-characters english-alphabet 4 cyclic-wrap
Router(config-pp)#restrict-consecutive-characters qwerty-keyboard 6
```

This example shows how to apply the password policy to the user profile, *user1*:

```
Router(config)#username user1
Router(config-un)#policy test-policy
Router(config-un)#commit
```

Related Commands

Command	Description
aaa password-policy, on page 22	Defines the FIPS-compliant AAA password security policy.

secret

To configure an encrypted or clear-text password for the user, use the **secret** command in username configuration mode or line template configuration mode. To remove this configuration, use the **no** form of this command.

secret [**0** [**enc-type** *enc-type-value*] | **5** | **8** | **9** | **10**] *secret-login*
no secret

Syntax Description

0	(Optional) Specifies that an unencrypted (clear-text) password follows. The password will be encrypted for storage in the configuration using an MD5 encryption algorithm. Otherwise, the password is not encrypted.
5	Specifies that an encrypted MD5 password (secret) follows.
8	(Optional) Specifies that SHA256-encrypted password follows.
9	(Optional) Specifies that scrypt-encrypted password follows.
10	(Optional) Specifies that SHA512-encrypted password follows.
secret-login	Text string in alphanumeric characters that is stored as the MD5-encrypted password entered by the user in association with the user's login ID. Can be up to 253 characters in length. **Note** The characters entered must conform to MD5 encryption standards.
enc-type	(Optional) Configures the encryption type for a password entered in clear text.
enc-type-value	Specifies the encryption type to be used.

Command Default

No password is specified.

Command Modes

Username configuration

Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.0.1	Added the support for Type 8 (SHA256), Type 9 (scrypt) and Type 10 (SHA512) encryption for **secret** configuration.
Release 7.0.1	Added the support for **enc-type** option under **secret 0** to specify the type of encryption for password entered in clear-text format.

Usage Guidelines

From Release 7.0.1 and later, Type 10 encryption is applied as the default encryption type for the **secret** on Cisco IOS XR 64-bit operating systems. Prior to this, Type 5 (MD5) was the default one.

Prior to Release 7.0.1, Cisco IOS XR software allows you to configure only Message Digest 5 (MD5) encryption for username logins and passwords. MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear-text passwords. Therefore, MD5 encrypted passwords cannot be used with protocols that require the clear-text password to be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).

Prior to Release 7.0.1, you can specify only one of two types of secure secret IDs: encrypted (5) or clear text (0). If you do not select either 0 or 5, the clear-text password you enter is not encrypted.

When an XR EXEC mode process is started on a line that has password protection, the process prompts for the secret. If the user enters the correct secret, the process issues the prompt. The user can try entering the secret thrice before the terminal returns to the idle state.

Secrets are one-way encrypted and should be used for login activities that do not require a decryptable secret.

To verify that MD5 password encryption has been enabled, use the **show running-config** command. The "username name secret 5" line in the command output indicates the same.

Note The **show running-config** command does not display the login password in clear text when the **0** option is used to specify an unencrypted password. See the "Examples" section.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to establish the clear-text secret "lab" for the user *user2*:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user2
RP/0/RP0/CPU0:router(config-un)# secret 0 lab
RP/0/RP0/CPU0:router(config-un)# commit
RP/0/RP0/CPU0:router(config-un)# show running-config
Building configuration...
username user2
 secret 5 $1$DTmd$q7C6fhzje7Cc7Xzmu2Frx1
!
end
```

The following examples show how to configure a Type 10 (SHA512) password for the user, *user10*. You can also see the examples and usage of the username, on page 114 command.

You can specify Type as '10' under the **secret** keyword, to explicitly configure Type 10 password.

```
Router#configure
Router(config)#username user10 secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
Router(config-un)#commit
```

You can also use the **enc-type** keyword under the **secret 0** option, to specify Type 10 as the encryption for a password entered in clear text.

```
Router#configure
Router(config)#username user10 secret 0 enc-type 10 testpassword
Router(config-un)#commit
```

server (RADIUS)

To associate a particular RADIUS server with a defined server group, use the **server** command in RADIUS server-group configuration mode. To remove the associated server from the server group, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The *port-number* argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. Default is 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The *port-number* argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0. Default is 1646.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **server** command to associate a particular RADIUS server with a defined server group.

There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server based on their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service, for example, accounting, the second host entry configured acts as an automatic switchover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to use two different host entries on the same RADIUS server that are configured for the same services—authentication and accounting. The second host entry configured acts as switchover backup to the first one.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.1.1.1 auth-port 1645 acct-port 1646
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.2.2.2 auth-port 2000 acct-port 2001
```

server (TACACS+)

To associate a particular TACACS+ server with a defined server group, use the **server** command in TACACS+ server-group configuration mode. To remove the associated server from the server group, use the **no** form of this command.

server {*hostnameip-address*}
no server {*hostnameip-address*}

Syntax Description

hostname	Character string used to name the server host.
ip-address	IP address of the server host.

Command Default

None

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **server** command to associate a particular TACACS+ server with a defined server group. The server need not be accessible during configuration. Later, you can reference the configured server group from the method lists used to configure authentication, authorization, and accounting (AAA).

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to associate the TACACS+ server with the IP address 192.168.60.15 with the server group tac1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ tac1
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the AAA group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
no server-private *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The *port-number* argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0. The default value is 1645.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The *port-number* argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0. The default value is 1646.
timeout *seconds*	(Optional) Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting. The setting overrides the global value of the **radius-server timeout** command. If no timeout is specified, the global value is used. The *seconds* argument specifies the timeout value in seconds. The range is from 1 to 1000. If no timeout is specified, the global value is used.
retransmit *retries*	(Optional) Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly. The setting overrides the global setting of the **radius-server transmit** command. The *retries* argument specifies the retransmit value. The range is from 1 to 100. If no retransmit value is specified, the global value is used.
key *string*	(Optional) Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the 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.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. Possible overlapping of IP addresses between VRF instances are permitted. Private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (for example, default radius server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the configuration and the definitions of private servers.

Both the **auth-port** and **acct-port** keywords enter RADIUS server-group private configuration mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to define the group1 RADIUS group server, to associate private servers with it, and to enter RADIUS server-group private configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 timeout 5
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 retransmit 3
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 key coke
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)# exit
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 timeout 5
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 retransmit 3
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 key coke
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)#

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)# exit
(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)#
```

server-private (TACACS+)

To configure the IP address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ server-group configuration mode. To remove the associated private server from the AAA group server, use the **no** form of this command.

server-private {*hostnameip-address*} [**holddown-time** *time*][**port** *port-number*] [**timeout** *seconds*] [**key** *string*]
no server-private {*hostnameip-address*}

Syntax Description

hostname	Character string used to name the server host.
ip-address	IP address of the TACACS+ server host. Both IPv4 and IPv6 addresses are supported.
holddown-time *time*	Specifies a duration, in seconds, for which an unresponsive TACACS+ server is to be marked as DOWN. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.
timeout *seconds*	(Optional) Specifies, in seconds, a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server. This option overrides the global timeout value set with the **tacacs-server timeout** command for only this server. The range is from 1 to 1000. The default is 5.
key *string*	(Optional) Specifies the authentication and encryption key that is used between the router and the TACACS+ daemon running on the TACACS+ server. This key overrides the global setting of the **tacacs-server key** command. If no key string is specified, the global value is used.

Command Default

The *port-name* argument, if not specified, defaults to the standard port 49.

The *seconds* argument, if not specified, defaults to 5 seconds.

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.4.1	This command was modified to include **holddown-time** option.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. Possible overlapping of IP addresses between VRF instances are permitted. Private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (for example, default tacacs+ server group) can still be referred by IP addresses and port

numbers. Therefore, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

For details on TACACS+ hold-down timer, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to define the myserver TACACS+ group server, to associate private servers with it, and to enter TACACS+ server-group private configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 timeout 5
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 key a_secret
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 port 51
RP/0/RP0/CPU0:router(config-sg-tacacs-private)# exit
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 timeout 5
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 key coke
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 port 300
RP/0/RP0/CPU0:router(config-sg-tacacs-private)#
```

show aaa (XR-VM)

To display information about an Internet Key Exchange (IKE) Security Protocol group, user group, local user, login traces, or task group; to list all task IDs associated with all IKE groups, user groups, local users, or task groups in the system; or to list all task IDs for a specified IKE group, user group, local user, or task group, use the **show aaa** command in the XR EXEC mode.

show aaa {**ikegroup** *ikegroup-name* | **login trace** | **usergroup** [*usergroup-name*] | **trace** | **userdb** [*username*] | **task supported** | **taskgroup** [**root-lr** | **netadmin** | **operator** | **sysadmin** | **root-system** | **service-admin** | **cisco-support** | *taskgroup-name*]}

Syntax Description

ikegroup	Displays details for all IKE groups.
ikegroup-name	(Optional) IKE group whose details are to be displayed.
login trace	Displays trace data for login subsystem.
usergroup	Displays details for all user groups.
root-lr	(Optional) Usergroup name.
netadmin	(Optional) Usergroup name.
operator	(Optional) Usergroup name.
sysadmin	(Optional) Usergroup name.
root-system	(Optional) Usergroup name.
cisco-support	(Optional) Usergroup name.
usergroup-name	(Optional) Usergroup name.
trace	Displays trace data for AAA subsystem.
userdb	Displays details for all local users and the usergroups to which each user belongs.
username	(Optional) User whose details are to be displayed.
task supported	Displays all AAA task IDs available.
taskgroup	Displays details for all task groups. **Note** For taskgroup keywords, see optional usergroup name keyword list.
taskgroup-name	(Optional) Task group whose details are to be displayed.

Command Default

Details for all user groups, or all local users, or all task groups are listed if no argument is entered.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show aaa** command to list details for all IKE groups, user groups, local users, AAA task IDs, or task groups in the system. Use the optional *ikegroup-name*, *usergroup-name*, *username*, or *taskgroup-name* argument to display the details for a specified IKE group, user group, user, or task group, respectively.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is from the **show aaa** command, using the **ikegroup** keyword:

```
RP/0/RP0/CPU0:router# show aaa ikegroup

IKE Group ike-group
        Max-Users = 50
IKE Group ikeuser
        Group-Key = test-password
        Default Domain = cisco.com
IKE Group ike-user
```

The following sample output is from the **show aaa** command, using the **usergroup** command:

```
RP/0/RP0/CPU0:router# show aaa usergroup operator

User group 'operator'
  Inherits from task group 'operator'
User group 'operator' has the following combined set
of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

The following sample output is from the **show aaa** command, using the **taskgroup** keyword for a task group named netadmin:

```
RP/0/RP0/CPU0:router# show aaa taskgroup netadmin

Task group 'netadmin'

Task group 'netadmin' has the following combined set
  of task IDs (including all inherited groups):

Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:                 cgn  : READ    WRITE    EXECUTE    DEBUG
Task:         config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:     config-services  : READ    WRITE    EXECUTE    DEBUG
Task:              crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                diag  : READ    WRITE    EXECUTE    DEBUG
Task:             drivers  : READ
Task:                dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                 eem  : READ    WRITE    EXECUTE    DEBUG
Task:   ethernet-services  : READ
Task:          ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:              fabric  : READ    WRITE    EXECUTE    DEBUG
Task:           fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:          filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:            firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                  fr  : READ    WRITE    EXECUTE    DEBUG
Task:                hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:       host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:           interface  : READ    WRITE    EXECUTE    DEBUG
Task:           inventory  : READ
Task:         ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                isis  : READ    WRITE    EXECUTE    DEBUG
Task:               l2vpn  : READ    WRITE    EXECUTE    DEBUG
Task:                  li  : READ    WRITE    EXECUTE    DEBUG
Task:             logging  : READ    WRITE    EXECUTE    DEBUG
Task:                lpts  : READ    WRITE    EXECUTE    DEBUG
Task:             monitor  : READ
Task:           mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:         mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:           multicast  : READ    WRITE    EXECUTE    DEBUG
Task:             netflow  : READ    WRITE    EXECUTE    DEBUG
Task:             network  : READ    WRITE    EXECUTE    DEBUG
Task:                ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                ouni  : READ    WRITE    EXECUTE    DEBUG
Task:            pkg-mgmt  : READ

Task:                 ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                 qos  : READ    WRITE    EXECUTE    DEBUG
Task:                 rib  : READ    WRITE    EXECUTE    DEBUG
Task:                 rip  : READ    WRITE    EXECUTE    DEBUG
Task:             root-lr  : READ                          (reserved)
Task:           route-map  : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                snmp  : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:              static  : READ    WRITE    EXECUTE    DEBUG
Task:              sysmgr  : READ
Task:              system  : READ    WRITE    EXECUTE    DEBUG
Task:           transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:              tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:           universal  : READ                          (reserved)
Task:                vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                vrrp  : READ    WRITE    EXECUTE    DEBUG
```

The following sample output is from the **show aaa** command, using the **taskgroup** keyword for an operator. The task group operator has the following combined set of task IDs, which includes all inherited groups:

```
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

The following sample output is from the show aaa task group displaying the different task groups:

```
  Task IDs included directly by this group:
  Task:                  aaa  : READ
  Task:                  acl  : READ
  Task:                admin  : READ
  Task:       basic-services  : READ
  Task:                 boot  : READ
  Task:        cisco-support  : READ                                (reserved)
  Task:          config-mgmt  : READ
  Task:      config-services  : READ
  Task:               crypto  : READ
  Task:                 dwdm  : READ
  Task:    ethernet-services  : READ
  Task:               fabric  : READ
  Task:           fault-mgr  : READ
  Task:          filesystem  : READ
  Task:                 hdlc  : READ
  Task:        host-services  : READ
  Task:                 hsrp  : READ
  Task:           interface  : READ
  Task:           inventory  : READ
  Task:          ip-services  : READ
  Task:                 ipv4  : READ
  Task:                 ipv6  : READ
  Task:              logging  : READ
  Task:              mpls-te  : READ
```

The following sample output is from **show aaa** command with the **userdb** keyword:

```
RP/0/RP0/CPU0:router# show aaa userdb

Username lab (admin plane)
User group root-system
User group cisco-support
Username acme
User group root-system
```

The following sample output is from the **show aaa** command, using the **task supported** keywords. Task IDs are displayed in alphabetic order.

```
RP/0/RP0/CPU0:router# show aaa task supported

aaa
acl
admin
atm
basic-services
bcdl
bfd
bgp
boot
```

```
bundle
cdp
cef
cisco-support
config-mgmt
config-services
crypto
diag
disallowed
drivers
ext-access
fabric
fault-mgr
filesystem
firewall
fr
hdlc
host-services
hsrp
interface
inventory
ip-services
ipv4
ipv6
isis
logging
lpts
monitor
mpls-ldp
mpls-static
mpls-te
multicast
netflow
network
ospf
ouni
pkg-mgmt

ppp
qos
rib
rip
User group root-systemlrlr
root-system
route-map
route-policy
sbc
snmp
sonet-sdh
static
sysmgr
system
transport
tty-access
tunnel
universal
vlan
vrrp
```

show aaa accounting

To display command history with the date and time for AAA sub-system, use the **show aaa accounting** command in the System Admin EXEC mode. You must have a group aaa-r or root-system on System Admin VM.

show aaa accounting

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

System Admin EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read

This is the sample output of the **show aaa accounting** command:

```
sysadmin-vm:0_RP0#show aaa accounting
Mon Nov  3  13:37:21.573 UTC

Detail audit log information
  Time                      Username          Session-ID     Node-Information     Command
-------------------------------------------------------------------------------------------------
2014-11-03.13:14:27 UTC      root                  17         System        logged in from
 the CLI with aaa disabled
..
…
2014-11-03.13:37:01 UTC      cisco                 57          0/RP0         assigned to
groups: root-system
2014-11-03.13:37:03 UTC      cisco                 57          0/RP0         CLI 'config
terminal'
2014-11-03.13:37:03 UTC      cisco                 57          0/RP0         CLI done
2014-11-03.13:37:09 UTC      cisco                 57          0/RP0         CLI 'aaa
authentication users user temp'
2014-11-03.13:37:09 UTC      cisco                 57          0/RP0         CLI done
2014-11-03.13:37:11 UTC      cisco                 57          0/RP0         CLI 'password
 ****
2014-11-03.13:37:11 UTC      cisco                 57          0/RP0         CLI done
2014-11-03.13:37:12 UTC      cisco                 57          0/RP0         CLI 'commit'
2014-11-03.13:37:14 UTC      cisco                 57          0/RP0         CLI done
2014-11-03.13:37:16 UTC      cisco                 57          0/RP0         CLI 'exit'
2014-11-03.13:37:16 UTC      cisco                 57          0/RP0         CLI done
2014-11-03.13:37:18 UTC      cisco                 57          0/RP0         CLI 'exit'
2014-11-03.13:37:18 UTC      cisco                 57          0/RP0         CLI done
```

```
2014-11-03.13:37:21 UTC      cisco                  57          0/RP0          CLI 'show aaa
 accounting'
```

show aaa password-policy

To display the details of AAA password policy configured in a system, use the **show aaa password-policy** command in XR EXEC mode.

show aaa password-policy [*policy-name*]

Syntax Description

policy-name	Specifies the name of password policy.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

If the option *policy-name* is not specified, the command output displays the details of all password policies configured in the system.

Refer **aaa password-policy** command details of each field in this command output.

Task ID

Task ID	Operation
aaa	read

This is a sample out of **show aaa password-policy** command:

```
RP/0/RP0/CPU0:router#show aaa password-policy test-policy

Fri Feb  3 16:50:58.086 EDT
Password Policy Name : test-policy
  Number of Users : 1
  Minimum Length : 2
  Maximum Length : 253
  Special Character Len : 0
  Uppercase Character Len : 0
  Lowercase Character Len : 1
  Numeric Character Len : 0
  Policy Life Time :
    seconds : 0
    minutes : 0
    hours : 0
    days : 0
    months : 0
    years : 0
  Lockout Time :
    seconds : 0
    minutes : 0
    hours : 0
    days : 0
```

```
  months : 0
  years : 0
Character Change Len : 4
Maximum Failure Attempts : 0
```

Related Commands

Command	Description
aaa password-policy, on page 22	Defines the FIPS-compliant AAA password security policy.

show radius

To display information about the RADIUS servers that are configured in the system, use the **show radius** command in the XR EXEC mode.

show radius

Syntax Description

This command has no keywords or arguments.

Command Default

If no radius servers are configured, no output is displayed.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show radius** command to display statistics for each configured RADIUS server.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius** command:

```
RP/0/RP0/CPU0:router# show radius

Global dead time: 0 minute(s)

Server: 10.1.1.1/1645/1646  is UP
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
  Authentication:
    0 requests, 0 pending, 0 retransmits
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt

Server: 10.2.2.2/1645/1646  is UP
  Timeout: 10 sec, Retransmit limit: 3
  Authentication:
    0 requests, 0 pending, 0 retransmits
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
```

```
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 1: show radius Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Timeout	Number of seconds the router waits for a server host to reply before timing out.
Retransmit limit	Number of times the Cisco IOS XR software searches the list of RADIUS server hosts before giving up.

show radius accounting

To obtain information and detailed statistics for the RADIUS accounting server and port, use the **show radius accounting** command in the XR EXEC mode

show radius accounting

Syntax Description

This command has no keywords or arguments.

Command Default

If no RADIUS servers are configured on the router, the output is empty. If the default values are for the counter (for example, request and pending), the values are all zero because the RADIUS server was just defined and not used yet.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is displayed on a per-server basis for the **show radius accounting** command:

```
RP/0/RP0/CPU0:router# show radius accounting

Server: 12.26.25.61, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.26.49.12, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.38.28.18, port: 29199
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 2: show radius accounting Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.

show radius authentication

To obtain information and detailed statistics for the RADIUS authentication server and port, use the **show radius authentication** command in the XR EXEC mode.

show radius authentication

Syntax Description

This command has no keywords or arguments.

Command Default

If no RADIUS servers are configured on the router, the output is empty. If the default values are for the counter (for example, request and pending), the values are all zero because the RADIUS server was just defined and not used yet.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius authentication** command:

```
RP/0/RP0/CPU0:router# show radius authentication

Server: 12.26.25.61, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.26.49.12, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.38.28.18, port: 21099
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 3: show radius authentication Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.

show radius dead-criteria

To obtain information about the dead server detection criteria, use the **show radius dead-criteria** command in the XR EXEC mode.

show radius dead-criteria host *ip-addr* [**auth-port** *auth-port*] [**acct-port** *acct-port*]

Syntax Description

host *ip-addr*	Specifies the name or IP address of the configured RADIUS server.
auth-port *auth-port*	(Optional) Specifies the authentication port for the RADIUS server. The default value is 1645.
acct-port *acct-port*	(Optional) Specifies the accounting port for the RADIUS server. The default value is 1646.

Command Default

The default values for time and tries are not fixed to a single value; therefore, they are calculated and fall within a range of 10 to 60 seconds for time and 10 to 100 for tries.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read

Examples

The following sample output is for the **show radius dead-criteria** command:

```
RP/0/RP0/CPU0:router# show radius dead-criteria host 12.26.49.12 auth-port 11000 acct-port
 11001

Server: 12.26.49.12/11000/11001
Dead criteria time: 10 sec (computed) tries: 10 (computed)
```

This table describes the significant fields shown in the display.

Table 4: show radius dead-criteria Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.
Timeout	Number of seconds the router waits for a server host to reply before timing out.

Field	Description
Retransmits	Number of times Cisco IOS XR software searches the list of RADIUS server hosts before giving up.

show radius server-groups

To display information about the RADIUS server groups that are configured in the system, use the **show radius server-groups** command in the XR EXEC mode.

show radius server-groups [*group-name* [**detail**]]

Syntax Description

group-name	(Optional) Name of the server group. The properties are displayed.
detail	(Optional) Displays properties for all the server groups.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show radius server-groups** command to display information about each configured RADIUS server group, including the group name, numbers of servers in the group, and a list of servers in the named server group. A global list of all configured RADIUS servers, along with authentication and accounting port numbers, is also displayed.

Task ID

Task ID	Operations
aaa	read

Examples

The inherited global message is displayed if no group level deadtime is defined for this group; otherwise, the group level deadtime value is displayed and this message is omitted. The following sample output is for the **show radius server-groups** command:

```
RP/0/RP0/CPU0:router# show radius server-groups

Global list of servers
  Contains 2 server(s)
    Server 10.1.1.1/1645/1646
    Server 10.2.2.2/1645/1646

Server group 'radgrp1' has 2 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 2 server(s)
    Server 10.1.1.1/1645/1646
    Server 10.2.2.2/1645/1646

Server group 'radgrp-priv' has 1 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
    Server 10.3.3.3/1645/1646 [private]
```

The following sample output shows the properties for all the server groups in group “radgrp1:”

```
RP/0/RP0/CPU0:router# show radius server-groups radgrp1 detail

Server group 'radgrp1' has 2 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 2 server(s)
      Server 10.1.1.1/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
      Server 10.2.2.2/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

The following sample output shows the properties for all the server groups in detail in the group “raddgrp-priv:”

```
RP/0/RP0/CPU0:router# show radius server-groups radgrp-priv detail

Server group 'radgrp-priv' has 1 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 1 server(s)
      Server 10.3.3.3/1645/1646 [private]
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

This table describes the significant fields shown in the display.

Table 5: show radius server-groups Field Descriptions

Field	Description
Server	Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.

show tacacs

To display information about the TACACS+ servers that are configured in the system, use the **show tacacs** command in the XR EXEC mode.

show tacacs

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show tacacs** command to display statistics for each configured TACACS+ server.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs** command:

```
RP/0/RP0/CPU0:router# show tacacs

For IPv4 IP addresses:
Server:10.1.1.1/21212 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

Server:10.2.2.2/21232 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

For IPv6 IP addresses:
Server: 10.2.3.5/49  family = AF_INET opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false
```

This table describes the significant fields shown in the display.

Table 6: show tacacs Field Descriptions

Field	Description
Server	Server IP address.
opens	Number of socket opens to the external server.

Field	Description
closes	Number of socket closes to the external server.
aborts	Number of tacacs requests that have been terminated midway.
errors	Number of error replies from the external server.
packets in	Number of TCP packets that have been received from the external server.
packets out	Number of TCP packets that have been sent to the external server.

show tacacs server-groups

To display information about the TACACS+ server groups that are configured in the system, use the **show tacacs server-groups** command in the XR EXEC mode.

show tacacs server-groups

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show tacacs server-groups** command to display information about each configured TACACS+ server group, including the group name, numbers of servers in the group, and a list of servers in the named server group. A global list of all configured TACACS+ servers is also displayed.

Task ID

Task ID	Operations
aaa	read

Examples

The following is sample output from the **show tacacs server-groups** command:

```
RP/0/RP0/CPU0:router# show tacacs server-groups

Global list of servers
  Server 192.168.25.61/23456
  Server 192.168.49.12/12345
  Server 192.168.49.12/9000
  Server 192.168.25.61/23432
  Server 10.5.5.5/23456
  Server 10.1.1.1/49
Server group 'tac100' has 1 servers
Server 192.168.49.12
```

This table describes the significant fields shown in the display.

Table 7: show tacacs server-groups Field Descriptions

Field	Description
Server	Server IP address.

show user

To display all user groups and task IDs associated with the currently logged-in user, use the **show user** command in the XR EXEC mode.

show user [**all** | **authentication** | **group** | **tasks**]

Syntax Description

all	(Optional) Displays all user groups and task IDs for the currently logged-in user.
authentication	(Optional) Displays authentication method parameters for the currently logged-in user.
group	(Optional) Displays the user groups associated with the currently logged-in user.
tasks	(Optional) Displays task IDs associated with the currently logged-in user. The **tasks** keyword indicates which task is reserved in the sample output.

Command Default

When the **show user** command is used without any option, it displays the ID of the user who is logged in currently.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show user** command to display all user groups and task IDs associated with the currently logged-in user.

Task ID

Task ID	Operations
none	—

Examples

The following sample output displays the authentication method parameters from the **show user** command:

```
RP/0/RP0/CPU0:router# show user authentication method

local
```

The following sample output displays the groups from the **show user** command:

```
RP/0/RP0/CPU0:router# show user group

root-system
```

The following sample output displays all the information for the groups and tasks from the **show user** command:

```
RP/0/RP0/CPU0:router# show user all
Username: lab
Groups: root-system
Authenticated using method local
User lab has the following Task ID(s):

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:               root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:             route-map  : READ    WRITE    EXECUTE    DEBUG
Task:          route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                   sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:             sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:                static  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

The following sample output displays the tasks and indicates which tasks are reserved from the **show user** command:

```
RP/0/RP0/CPU0:router# show user tasks

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:         root-system   : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           route-map   : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy   : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc   : READ    WRITE    EXECUTE    DEBUG
Task:                snmp   : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh   : READ    WRITE    EXECUTE    DEBUG
Task:              static   : READ    WRITE    EXECUTE    DEBUG
Task:              sysmgr   : READ    WRITE    EXECUTE    DEBUG
Task:              system   : READ    WRITE    EXECUTE    DEBUG
Task:           transport   : READ    WRITE    EXECUTE    DEBUG
Task:         tty-access    : READ    WRITE    EXECUTE    DEBUG
Task:              tunnel   : READ    WRITE    EXECUTE    DEBUG
Task:           universal   : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                vlan   : READ    WRITE    EXECUTE    DEBUG
Task:                vrrp   : READ    WRITE    EXECUTE    DEBUG
```

show aaa user-group

To display user group information for AAA sub-system, use the **show aaa user-group** command in the System Admin EXEC mode. You must have a group aaa-r or root-system on System Admin VM.

show aaa user-group

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

System Admin EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read

This is the sample output of the **show aaa user-group** command:

```
sysadmin-vm:0_RP0#show aaa user-group
Mon Nov  3  13:39:33.380 UTC

User group : root-system
sysadmin-vm:0_RP0#
```

show tech-support aaa

To collect AAA debug and trace files from System Admin VM, use the **show tech-support aaa** command in the System Admin EXEC mode.

show tech-support aaa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

System Admin EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read

This is the sample output of the **show tech-support aaa** command:

```
sysadmin-vm:0_RP0#show tech-support aaa
Mon Nov  3  13:39:33.380 UTC

Fri Oct  24 07:22:15.740 UTC ++ Show tech start time: 2014-Oct-24.072216.UTC ++
Waiting for gathering to complete /opt/cisco/calvados/script/show_tech_aaa: line 27: rse:
command not found .
Compressing show tech output
Show tech output available at /misc/disk1//showtech-aaa-admin-2014-Nov-04.082457.UTC.tgz
Please collect show tech-support ctrace in addition to any sysadmin show-tech-support
collection
++ Show tech end time: 2014-Nov-04.UTC ++
sysadmin-vm:0_RP0#
```

single-connection

To multiplex all TACACS+ requests to this server over a single TCP connection, use the **single-connection** command in TACACS host configuration mode. To disable the single TCP connection for all new sessions that use a separate connection, use the **no** form of this command.

single-connection
no single-connection

Syntax Description

This command has no keywords or arguments.

Command Default

By default, a separate connection is used for each session.

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **single-connection** command allows the TACACS+ server to handle a greater number of TACACS operations than would be possible if multiple TCP connections were used to send requests to a server.

The TACACS+ server that is being used must support single-connection mode for this to be effective; otherwise, the connection between the network access server and the TACACS+ server locks up or you can receive unauthentic errors.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to configure a single TCP connection to be made with the TACACS+ server (IP address 209.165.200.226) and all authentication, authorization, accounting requests to use this TCP connection. This works only if the TACACS+ server is also configured in single-connection mode. To configure the TACACS+ server in single connection mode, refer to the respective server manual.

```
RP/0/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)# single-connection
```

single-connection-idle-timeout

To set the idle timeout value for the single TCP connection to the TACACS+ server, use the **single-connection-idle-timeout** command in *tacacs-server host* configuration mode. To remove the configuration or to disable the idle timeout for the single connection, use the **no** form of this command.

single-connection-idle-timeout *time-in-seconds*

Syntax Description

time-in-seconds	Specifies the single connection timeout value, in seconds. The range is: • 500 to 7200 (prior to Cisco IOS XR Software Release 7.3.2/Release 7.4.1) • 5 to 7200 (from Cisco IOS XR Software Release 7.3.2/Release 7.4.1, and later)

Command Default

Single connection idle timeout is not set, by default.

Command Modes

tacacs-server host

Command History

Release	Modification
Release 7.3.2 Release 7.4.1	This command was modified to change the timeout range.
Release 6.6.3	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to set an idle timeout value of 60 seconds for the single TCP connections to the TACACS+ server:

```
RP/0/RP0/CPU0:router(config)#tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)#single-connection-idle-timeout 60
RP/0/RP0/CPU0:router(config-tacacs-host)#commit
```

Related Commands

Command	Description
single-connection, on page 96	Multiplexes all TACACS+ requests to the server over a single TCP connection.

tacacs-server host

To specify a TACACS+ host server, use the **tacacs-server host** command in XR Config mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host *host-name* [**holddown-time** *time*] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] **auth-key**] [**single-connection**]
[**single-connection-idle-timeout** *time-in-seconds*]
no tacacs-server host *host-name* [*port port-number*]

Syntax Description

host-name	Host or domain name or IP address of the TACACS+ server.
holddown-time *time*	Specifies a duration, in seconds, for which an unresponsive TACACS+ server is to be marked as DOWN. The range is from 0 to 1200. Zero indicates that the hold-down timer feature is disabled.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.
timeout *seconds*	(Optional) Specifies a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server. This option overrides the global timeout value set with the **tacacs-server timeout** command for this server only. The valid timeout range is from 1 to 1000 seconds. Default is 5. Note: You can use this parameter only in the config-tacacs-host sub-mode.
key [**0** | **7**] *auth-key*	(Optional) Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server. The TACACS+ packets are encrypted using this key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the **tacacs-server key**command for this server only. (Optional) Entering **0** specifies that an unencrypted (clear-text) key follows. (Optional) Entering **7** specifies that an encrypted key follows. The *auth-key* argument specifies the unencrypted key between the AAA server and the TACACS+ server. Note: You can use this parameter only in the config-tacacs-host sub-mode.
single-connection	(Optional) Multiplexes all TACACS+ requests to this server over a single TCP connection. By default, a separate connection is used for each session. Note: You can use this parameter only in the config-tacacs-host sub-mode.

single-connection-idle-timeout *time-in-seconds*	(Optional) Specifies the single connection idle timeout value, in seconds. The range is: • 500 to 7200 (prior to Cisco IOS XR Software Release 7.3.2/Release 7.4.1) • 5 to 7200 (from Cisco IOS XR Software Release 7.3.2/Release 7.4.1, and later)

Command Default

No TACACS+ host is specified.

The *port-name* argument, if not specified, defaults to the standard port 49.

The *seconds* argument, if not specified, defaults to 5 seconds.

Single connection idle timeout is not set, by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.4.1	This command was modified to include **holddown-time** option.
Release 7.3.2 Release 7.4.1	This command was modified to change the range for **single-connection-idle-timeout**.
Release 6.6.3	This command was modified to include **single-connection-idle-timeout** option.
Release 6.0	This command was introduced.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. Cisco IOS XR software searches for hosts in the order in which you specify them.

For details on TACACS+ hold-down timer, see the **holddown-time** command.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to specify a TACACS+ host with the IP address 209.165.200.226:

```
RP/0/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)#
```

The following example shows that the default values from the **tacacs-server host** command are displayed from the **show run** command:

```
RP/0/RP0/CPU0:router# show run

Building configuration...
!! Last configuration change at 13:51:56 UTC Mon Nov 14 2005 by lab
!
tacacs-server host 209.165.200.226 port 49
 timeout 5
!
```

The following example shows how to specify that the router consult the TACACS+ server host named host1 on port number 51. The timeout value for requests on this connection is 30 seconds; the encryption key is a_secret.

```
RP/0/RP0/CPU0:router(config)# tacacs-server host host1 port 51
RP/0/RP0/CPU0:router(config-tacacs-host)# timeout 30
RP/0/RP0/CPU0:router(config-tacacs-host)# key a_secret
```

Related Commands

Command	Description
holddown-time (TACACS+), on page 32	Specifies a duration for which an unresponsive TACACS+ server is to be marked as down.
key (TACACS+), on page 36	
single-connection, on page 96	
single-connection-idle-timeout, on page 97	Sets the idle timeout value for the single TCP connection to the TACACS+ server.
timeout (TACACS+), on page 111	

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon, use the **tacacs-server key** command in XR Config mode. To disable the key, use the **no** form of this command.

tacacs-server key {**0** *clear-text-key* | **7** *encrypted-keyauth-key*}
no tacacs-server key {**0** *clear-text-key* | **7** *encrypted-keyauth-key*}

Syntax Description

0 *clear-text-key*	Specifies an unencrypted (cleartext) shared key.
7 *encrypted-key*	Specifies an encrypted shared key.
auth-key	Specifies the unencrypted key between the AAA server and the TACACS+ server.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The key name entered must match the key used on the TACACS+ daemon. The key name applies to all servers that have no individual keys specified. All leading spaces are ignored; spaces within and after the key are not. 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.

The key name is valid only when the following guidelines are followed:

- The *clear-text-key* argument must be followed by the **0** keyword.
- The *encrypted-key* argument must be followed by the **7** keyword.

The TACACS server key is used only if no key is configured for an individual TACACS server. Keys configured for an individual TACACS server always override this global key configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example sets the authentication and encryption key to key1:

```
RP/0/RP0/CPU0:router(config)# tacacs-server key key1
```

tacacs-server timeout

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** command in XR Config mode. To restore the default, use the **no** form of this command.

tacacs-server timeout *seconds*
no tacacs-server timeout *seconds*

Syntax Description

seconds	Integer that specifies the timeout interval (in seconds) from 1 to 1000.

Command Default

5 seconds

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The TACACS+ server timeout is used only if no timeout is configured for an individual TACACS+ server. Timeout intervals configured for an individual TACACS+ server always override this global timeout configuration.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the interval timer being changed to 10 seconds:

```
RP/0/RP0/CPU0:router(config)# tacacs-server timeout 10
```

tacacs-server ipv4

To set the Differentiated Services Code Point (DSCP), which is represented by the first six bits in the Type of Service (ToS) byte of the IP header, use the **tacacs-server ipv4** command in XR Config mode.

tacacs-server ipv4 dscp *dscp-value*

Syntax Description

ipv4	Specifies the dscp bit for the IPv4 packets.
dscp	Sets the DSCP in the IP header.
dscp-value	Specifies the options for setting the value of DSCP. The available options are: • <0-63> Differentiated services codepoint value • af11 Match packets with AF11 dscp (001010) • af12 Match packets with AF12 dscp (001100) • af13 Match packets with AF13 dscp (001110) • af21 Match packets with AF21 dscp (010010) • af22 Match packets with AF22 dscp (010100) • af23 Match packets with AF23 dscp (010110) • af31 Match packets with AF31 dscp (011010) • af32 Match packets with AF32 dscp (011100) • af33 Match packets with AF33 dscp (011110) • af41 Match packets with AF41 dscp (100010) • af42 Match packets with AF42 dscp (100100) • af43 Match packets with AF43 dscp (100110) • cs1 Match packets with CS1(precedence 1) dscp (001000) • cs2 Match packets with CS2(precedence 2) dscp (010000) • cs3 Match packets with CS3(precedence 3) dscp (011000) • cs4 Match packets with CS4(precedence 4) dscp (100000) • cs5 Match packets with CS5(precedence 5) dscp (101000) • cs6 Match packets with CS6(precedence 6) dscp (110000) • cs7 Match packets with CS7(precedence 7) dscp (111000) • default Match packets with default dscp (000000) • ef Match packets with EF dscp (101110)

Command Default None

Command Modes XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
aaa	read, write

Examples The following example sets the DSCP value to Assured Forwarding (AF)11:

```
RP/0/RP0/CPU0:router(config)# tacacs-server ipv4 dscp af11
```

tacacs source-interface

To specify the source IP address of a selected interface for all outgoing TACACS+ packets, use the **tacacs source-interface** command in XR Config mode. To disable use of the specified interface IP address, use the **no** form of this command.

tacacs source-interface *type path-id* [**vrf** *vrf-id*]
no tacacs source-interface *type path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in XR Config mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
vrf *vrf-id*	Specifies the name of the assigned VRF.

Command Default

If a specific source interface is not configured, or the interface is down or does not have an IP address configured, the system selects an IP address.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **tacacs source-interface** command to set the IP address of the specified interface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

When the specified interface does not have an IP address or is in a *down* state, TACACS+ behaves as if no source interface configuration is used.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the IP address of the specified interface for all outgoing TACACS+ packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tacacs source-interface HundredGigabitEthernet 0/0/0/29 vrf
abc
```

task

To add a task ID to a task group, use the **task** command in task group configuration mode. To remove a task ID from a task group, use the **no** form of this command.

task {**read** | **write** | **execute** | **debug**} *taskid-name*
no task {**read** | **write** | **execute** | **debug**} *taskid-name*

Syntax Description

read	Enables read-only privileges for the named task ID.
write	Enables write privileges for the named task ID. The term "write" implies read also.
execute	Enables execute privileges for the named task ID.
debug	Enables debug privileges for the named task ID.
taskid-name	Name of the task ID.

Command Default

No task IDs are assigned to a newly created task group.

Command Modes

Task group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **task** command in task group configuration mode. To access task group configuration mode, use the **taskgroup** command in global configuration mode.

Task IDs are the base of command authorization. Only users who have the required permissions can execute a particular command on the router. To execute a command, the user must be part of a user group that consists of task group(s) that includes required task IDs and privileges. Cisco IOS XR software supports multiple task IDs. For example, **aaa**, **config-services**, **crypto**, **system**, and so on. To see the list of task IDs available for the user, use the **show user tasks** command.

Likewise, all commands are associated with one or more task IDs, and their corresponding operations (such as **read**, **write**, **execute**, and **debug**) that denote the permissions required to execute those commands. You can use the **describe** command to know the task ID and permissions that are required to execute a particular command.

For example, the following output shows that the user needs **aaa** task ID with **read** and **write** permission to execute the **show run aaa** command. So, users can execute this command if they belong to a user group associated with a task group that includes this **aaa** task ID having read and write privileges.

```
Router# describe show run aaa
The command is defined in aaa_cmds.parser

User needs ALL of the following taskids:

    aaa (READ WRITE) ----------->

It will take the following actions:
```

```
Wed Mar 16 07:58:01.451 UTC
  Spawn the process:
    nvgen "-c" "-q" "gl/aaa/"
Router#
```

Root users (users in **root-lr** or **root-system** user group) have all task IDs, and hence will be able to execute all commands. Also, certain commands might not require any task ID as such to execute it. So, all users will have permission to execute such commands. If you do not have the required permission to execute a command, the command authorization fails. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

A few other examples that describe the commands to list the task ID:

```
Router#describe show interfaces
The command is defined in show_interface.parser

show_interface.parser
User needs ALL of the following taskids:

   interface (READ)---------->

It will take the following actions:
Thu Mar 17 06:42:08.264 UTC
  Spawn the process:
    show_interface "-a"
Router#


Router(config)#describe ssh server
The command is defined in ssh.parser

ssh.parser
User needs ALL of the following taskids:

   crypto (READ WRITE) ---------->

It will take the following actions:
  Create/Set the configuration item:
       Path: gl/crypto/ssh/server/sshd/vrf/default
       Value: packed[ 0x1 <string> <string> ]
Router(config)#
```

For more details, see *Configuring AAA Services* chapter in the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to enable execute privileges for the config-services task ID and associate that task ID with the task group named taskgroup1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup taskgroup1
RP/0/RP0/CPU0:router(config-tg)# task execute config-services
```

taskgroup

To configure a task group to be associated with a set of task IDs, and to enter task group configuration mode, use the **taskgroup** command in XR Config mode. To delete a task group, use the **no** form of this command.

taskgroup *taskgroup-name* [**description** *string* | **task** {**read** | **write** | **execute** | **debug**} *taskid-name* | **inherit taskgroup** *taskgroup-name*]
no taskgroup *taskgroup-name*

Syntax Description

taskgroup-name	Name of a particular task group.
description	(Optional) Enables you to create a description for the named task group.
string	(Optional) Character string used for the task group description.
task	(Optional) Specifies that a task ID is to be associated with the named task group.
read	(Optional) Specifies that the named task ID permits read access only.
write	(Optional) Specifies that the named task ID permits read and write access only.
execute	(Optional) Specifies that the named task ID permits execute access.
debug	(Optional) Specifies that the named task ID permits debug access only.
taskid-name	(Optional) Name of a task: the task ID.
inherit taskgroup	(Optional) Copies permissions from the named task group.
taskgroup-name	(Optional) Name of the task group from which permissions are to be inherited.

Command Default

Five predefined user groups are available by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Task groups are configured with a set of task IDs for each action type. Deleting a task group that is still referenced in the system results in a warning and rejection of the deletion. For more details on task IDs, see the Usage Guidelines section of the **task** command.

You can use the **show user group** command in XR Config mode to know the group(s) that the current user is part of. Similarly, you can use the **show user all** to know the group or task information (such as username, groups, authentication method, task IDs, and so on) of the current user.

From global configuration mode, you can display all the configured task groups. However, you cannot display all the configured task groups in taskgroup configuration mode.

Entering the **taskgroup** command with no keywords or arguments enters task group configuration mode, in which you can use the **description**, **inherit**, **show**, and **task** commands.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example assigns read bgp permission to the task group named alpha:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup alpha
RP/0/RP0/CPU0:router(config-tg)# task read bgp
```

timeout (TACACS+)

To specify a timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server, use the **timeout** (TACACS+) command in TACACS host configuration mode. To disable this command and return to the default timeout value of 5 seconds, use the **no** form of this command.

timeout *seconds*
no timeout *seconds*

Syntax Description

seconds	Timeout value (in seconds). The range is from 1 to 1000. If no timeout is specified, the global value is used.

Command Default

seconds: 5

Command Modes

TACACS host configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The **timeout** (TACACS+) command overrides the global timeout value set with the **tacacs-server timeout** command for this server only.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to set the number of seconds for the timeout value:

```
RP/0/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)# timeout 500
```

timeout login response

To set the interval that the server waits for a reply to a login, use the **timeout login response** command in line template configuration mode. To restore the default, use the **no** form of this command.

timeout login response *seconds*
no timeout login response *seconds*

Syntax Description

seconds	Integer that specifies the timeout interval (in seconds) from 0 to 300.

Command Default

seconds: 30

Command Modes

Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **timeout login response** command in line template configuration mode to set the timeout value. This timeout value applies to all terminal lines to which the entered line template is applied. This timeout value cannot be applied to line console. After the timeout value has expired, the user is prompted again. The retry is allowed three times.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to change the interval timer to 20 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template alpha
RP/0/RP0/CPU0:router(config-line)# timeout login response 20
```

usergroup

To configure a user group and associate it with a set of task groups, and to enter user group configuration mode, use the **usergroup** command in XR Config mode. To delete a user group, or to delete a task-group association with the specified user group, use the **no** form of this command.

usergroup *usergroup-name*
no usergroup *usergroup-name*

Syntax Description

usergroup-name	Name of the user group. The *usergroup-name* argument can be only one word. Spaces and quotation marks are not allowed.

Command Default

Five predefined user groups are available by default.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

User groups are configured with the command parameters for a set of users, such as task groups. You can remove specific user groups by using the **no** form of the **usergroup** command. You can remove the user group itself by using the **no** form of the command without giving any parameters. Deleting a user group that is still referenced in the system results in a warning and a rejection of the deletion.

Use the inherit usergroup, on page 35 command to copy permissions from other user groups. The user group is inherited by the parent group and forms a union of all task IDs specified in those groups. Circular inclusions are detected and rejected. User groups cannot inherit properties from predefined groups, such as root-system and owner-sdr.

From global configuration mode, you can display all the configured user groups. However, you cannot display all the configured user groups in usergroup configuration mode.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to add permissions from the user group beta to the user group alpha:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# usergroup alpha
RP/0/RP0/CPU0:router(config-ug)# inherit usergroup beta
```

username

To configure a new user with a username, establish a password, associate a password policy with the user, grant permissions for the user, and to enter username configuration mode, use the **username** command in XR Config mode or Admin Configuration modeSystem Admin Config mode. To delete a user from the database, use the **no** form of this command.

username *name* [**group** *name* | **policy** *name* | [**password-policy** *name*] { **password** | **masked-password** } [*type*] *password* | { **secret** | **masked-secret** } [*type* | **0** [**enc-type** *type*] *secret*]]
no username *name* [**group** *name* | **policy** | **password** | **masked-password** | **secret** | **masked-secret** | **password-policy** *name* [**masked-password** [*type*] *password*]]

Syntax Description

name	Name of the user. The *name* argument can be only one word. Spaces and quotation marks are not allowed. The allowed range for a user-defined username is 2-253 characters.
group *name*	Enables a user to be associated with a user group, as defined with the **usergroup** command.
policy *name*	Configures a password policy that is common to user password and secret.
password-policy *name*	(Optional) Specifies the password policy for cleartext and Type 7 password authentication.
password	Enables a password to be created for the specified user.
masked-password	Enables a password to be created for the specified user. When you key in the password, it is not visible on the screen.

type password	Specifies the password type and the password to be keyed in. Enter 0 or 7 for the *type* argument. 0 specifies a cleartext password, and 7 specifies a Type 7 encrypted password. If Type 7 encryption is enabled with the **password** keyword, the password is not visible to the user. The password can be up to 253 characters in length. (Optional) *type* argument
secret	Enables a secret to be created for the specified user.
masked-secret	Enables a secret to be created for the specified user. When you key in the secret, it is not visible on the screen.
type secret	Specifies the secret type and the secret to be keyed in. Enter 0, or enter 5, 8, 9, or 10, for the *type* argument. Details: • 0 specifies a cleartext secret that will be encrypted for use. • 5 specifies a Type 5 password that uses MD5 hashing algorithm. • 8 specifies a Type 8 password that uses SHA256 hashing algorithm. • 9 specifies a Type 9 password that uses scrypthashing algorithm. • 10 specifies a Type 10 password that uses SHA512 hashing algorithm. (Optional) *type* argument.

0 enc-type *type secret*	Specifies that you enter a cleartext secret to be encrypted by a specified encryption method. • 0 specifies that you should enter a cleartext secret. • **enc-type** specifies that you enter 5, 8, 9, or 10, for the *type* argument. • Enter the cleartext secret for the *secret* argument. (Optional) **enc-type** *type* keyword-argument combination.

Command Default

No usernames are defined in the system.

Command Modes

XR Config mode

Admin Configuration modeSystem Admin Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.
Release 7.0.1	Added the support for Type 8 (SHA256), Type 9 (scrypt) and Type 10 (SHA512) for **secret** configuration.
Release 7.2.1	Added the support for **policy** option to configure policy common to user password and secret.
Release 7.3.1	Password Masking feature options (**masked-password** and **masked-secret**) were added. When you key in a password or secret, it is not displayed on the screen

Usage Guidelines

Note

- A user is never allowed to have cisco-support privileges as the only group.
- From Release 7.0.1 and later, Type 10 (SHA512) is applied as the default type for the **secret** configuration. Prior to this, Type 5 (MD5) was the default one.

Use the **username** command to identify the user and enter username configuration mode. Password and user group assignments can be made from either XR Config mode or username configuration submode. Permissions (task IDs) are assigned by associating the user with one or more defined user groups.

From XR Config mode, you can display all the configured usernames. You can display configured usernames in configuration mode by router(config): **do show run username**.

Each user is identified by a username that is unique across the administrative domain. Each user should be made a member of at least one user group. Deleting a user group may orphan the users associated with that group. The AAA server authenticates orphaned users, but most commands are not authorized.

The **username** command is associated with a particular user for local login authentication by default. Alternatively, a user and password can be configured in the database of the TACACS+ server for TACACS+ login authentication. For more information, see the description of the aaa authentication (XR-VM), on page 9 command.

The predefined group root-system may be specified only by root-system users while administration is configured.

Note To enable the local networking device to respond to remote Challenge Handshake Authentication Protocol (CHAP) challenges, one **username** command entry must be the same as the hostname entry that has already been assigned to the other networking device.

The following are password masking guidelines for various command forms:

- **username** *name* **password** *type password*

  username *name* **masked-password** *type password*

  Enter 0 or 7 for the *type* argument. *0* specifies a cleartext password, and *7* specifies a Type 7 encrypted password.

- **secret** *type secret*

  masked-secret *type secret*

  Enter 0, or enter 5, 8, 9, or 10, for the *type* argument. 0 specifies a cleartext secret, and 5, 8, 9, and 10 specify a Type 5, Type 8, Type 9, and Type 10 secret, respectively.

- **secret 0 enc-type** *type secret*

  masked-secret 0 enc-type *type secret*

  Enter 5, 8, 9, or 10, for the *type* argument.

- **masked-password** *type password*

  masked-secret *type secret*

  After specifying the password encryption type, press **Enter** or **return** on your keyboard. The password/secret option appears in the next line. Example:

```
Router(config)# masked-secret 10

Enter secret:
Re-enter secret:
```

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows the commands available after executing the **username** command:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# ?
```

clear	Clear the uncommitted configuration
commit	Commit the configuration changes to running
describe	Describe a command without taking real actions
do	Run an exec command
exit	Exit from this submode
group	User group in which this user will be a member of
no	Negate a command or set its defaults
password	Specify the password for the user
policy	Specify the policy common to password and secret for the user
pwd	Commands used to reach current submode
root	Exit to the XR Config mode
secret	Specify the secure password for the user
show	Show contents of configuration

```
RP/0/RP0/CPU0:router(config-un)#
```

The following example shows how to establish the clear-text password *password1* for the user name *user1*:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# password 0 password1
```

This example shows how to apply a password policy for the user secret:

```
Router#configure
Router(config)#username user1
Router(config-un)#policy test-policy1
Router(config-un)#secret 10
$6$dmwuW0Ajicf98W0.$y/vzynWF1/OcGxwBwHs79VAy5ZZLhoHd7TicR4mOo8IIVriYCGAKW0A.wlJvTPO7IbZry.DxHrE3SN2BBzBJe0
Router(config-un)#commit
```

The following example shows how to configure a Type 8 (SHA256) password for the user, *user8*. You can also see the examples and usage of the secret, on page 58 command.

You can specify Type as '8' under the **secret** keyword, to explicitly configure Type 8 password.

```
Router#configure
Router(config)#username user8 secret 8
$8$ZYKGl1dZIw73Dl$IUWJOqTLoMyExhsNKoL5vMtvCOYguM5ajXf4uGeQj6I
Router(config-un)#commit
```

This example shows how to configure Type 9 password:

```
Router#configure
Router(config)#username user9 secret 9
$9$/rIQL1B3rplRBL$oS2fLWKFYH6B/kApxkkXmIqbPAHpRZkPEoh3WqGbvwQ
Router(config-un)#commit
```

Similarly, this example shows how to configure Type 10 password :

```
Router#configure
Router(config)#username user10 secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
Router(config-un)#commit
```

This example shows how to specify the Type 10 password in System Admin VM:

```
Router#admin
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authentication users user user10 password testpassword
sysadmin-vm:0_RP0(config)# commit
```

Password Masking Examples

The following example shows how to enable password masking for a cleartext password entry:

In this example, for user us3, a cleartext password is entered.

```
Router(config)# username us3 masked-password 0


Enter password:
Re-enter password:

Router(config)#commit
```

In the **show** command output, you can see the encrypted password:

```
Router# show run aaa
..

username us3
 password 7 105A1D0D
```

The encrypted password 105A1D0D is entered in the **Enter password:** and **Re-enter password:** fields, for Type 7 password encryption:

```
Router(config)# username us3 masked-password 7

Enter password:
Re-enter password:
```

```
Router(config)#commit
```

If there is a password mismatch between the two entries, an error message is displayed.

The following example shows how to enable password masking for a AAA password policy:

In this example, for user us6, a cleartext password is entered.

```
Router(config)# aaa password-policy security
Router(config)# username us6 password-policy security masked-password 0

Enter password:
Re-enter password:

Router(config)#commit
```

In the **show** command output, you can see the encrypted password.

```
Router# show run aaa
..

aaa password-policy security
..
username us6
 password-policy security password 7 0835585A
```

The encrypted password 0835585A is entered in the **Enter password:** and **Re-enter password:** fields for Type 7 password encryption.

```
Router(config)# username us6 password-policy test-policy masked-password 7

Enter password:
Re-enter password:


Router(config)#commit
```

users group

To associate a user group and its privileges with a line, use the **users group** command in line template configuration mode. To delete a user group association with a line, use the **no** form of this command.

users group {*usergroup-name* | **cisco-support** | **maintenance** | **netadmin** | **operator** | **provisioning** | **retrieve** | **root-lr** | **serviceadmin** | **sysadmin**}

no users group {*usergroup-name* | **cisco-support** | **maintenance** | **netadmin** | **operator** | **provisioning** | **retrieve** | **root-lr** | **serviceadmin** | **sysadmin**}

Syntax Description

usergroup-name	Name of the user group. The *usergroup-name* argument can be only one word. Spaces and quotation marks are not allowed.
cisco-support	Specifies that users logging in through the line are given Cisco support personnel privileges.
maintenance	Specifies that users logging in through the line are given SCAPA maintenance privileges.
netadmin	Specifies that users logging in through the line are given network administrator privileges.
operator	Specifies that users logging in through the line are given operator privileges.
provisioning	Specifies that users logging in through the line are given SCAPA provisioning privileges.
retrieve	Specifies that users logging in through the line are given SCAPA retrieve privileges.
root-lr	Specifies that users logging in through the line are given root logical router (LR) privileges.
serviceadmin	Specifies that users logging in through the line are given service administrator group privileges.
sysadmin	Specifies that users logging in through the line are given system administrator privileges.

Command Default

None

Command Modes

Line template configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **users group** command to enable a user group and its privileges to be associated with a line, meaning that users logging in through the line are given the privileges of the particular user group.

Task ID

Task ID	Operations
aaa	read, write

Examples

In the following example, if a vty-pool is created with line template *vty*, users logging in through vty are given operator privileges:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa authen login vty-authen line
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# line template vty
RP/0/RP0/CPU0:router(config-line)# users group operator
RP/0/RP0/CPU0:router(config-line)# login authentication
```

vrf (RADIUS)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group, use the **vrf** command in RADIUS server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default VRF is used.

Command Modes

RADIUS server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **vrf** command to specify a VRF for an AAA RADIUS server group and enable dial-up users to use AAA servers in different routing domains.

Task ID

Task ID	Operations
aaa	read, write

Examples

The following example shows how to use the **vrf** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# vrf vrf1
```

vrf (TACACS+)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA TACACS+ server group, use the **vrf** command in TACACS+ server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default VRF is used.

Command Modes

TACACS+ server-group configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **vrf** command to specify a VRF for an AAA TACACS+ server group and enable dial-up users to use AAA servers in different routing domains.

Task ID

Task ID	Operations
aaa	read, write

Examples

This example shows how to use the **vrf** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server 9.27.10.6
RP/0/RP0/CPU0:router(config-sg-tacacs+)# vrf abc
```