System Security Command Reference for Cisco NCS 6000 Series Routers

First Published: 2013-09-19
Last Modified: 2018-12-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface ix
Changes to This Document ix
Communications, Services, and Additional Information x

CHAPTER 1

Authentication, Authorization, and Accounting Commands 1
aaa accounting 2
aaa accounting system default 4
aaa accounting update 5
aaa authentication (XR-VM) 6
aaa authorization (XR-VM) 8
show nacm (XR-VM) 10
aaa default-taskgroup 13
aaa group server radius 14
aaa group server tacacs+ 15
aaa password-policy 16
accounting (line) 19
authorization (line) 20
deadtime (server-group configuration) 21
description (AAA) 22
group (AAA) 23
inherit taskgroup 25
inherit usergroup 26
key (TACACS+) 27
login authentication 28
password (AAA) 29
radius-server dead-criteria time 31
usergroup 77
username 78
users group 82
vrf (RADIUS) 83
vrf (TACACS+) 84

CHAPTER 2

IPSec Commands 87
clear crypto ipsec sa 87
description (IPSec profile) 88
show crypto ipsec sa 89
show crypto ipsec summary 92
show crypto ipsec transform-set 93

CHAPTER 3

Keychain Management Commands 95
accept-lifetime 95
accept-tolerance 96
key (key chain) 97
key chain (key chain) 98
key-string (keychain) 100
send-lifetime 101
show key chain 102

CHAPTER 4

Lawful Intercept Commands 105
lawful-intercept disable 105
overlap-tap enable 106

CHAPTER 5

Management Plane Protection Commands 107
address ipv4 (MPP) 107
allow 108
control-plane 110
inband 111
interface (MPP) 112
management-plane 113
out-of-band 114
show mgmt-plane 115
vrf (MPP) 117

CHAPTER 6
Public Key Infrastructure Commands 119
  clear crypto ca certificates 120
  clear crypto ca crl 121
  crl optional (trustpoint) 122
  crypto ca authenticate 123
  crypto ca cancel-enroll 124
  crypto ca enroll 125
  crypto ca import 126
  crypto ca trustpoint 127
  crypto ca trustpool import url 129
  crypto ca trustpool policy 130
  crypto key generate dsa 131
  crypto key generate ecdsa 132
  crypto key generate rsa 133
  crypto key import authentication rsa 134
  crypto key zeroize dsa 135
  crypto key zeroize ecdsa 136
  crypto key zeroize rsa 136
  description (trustpoint) 138
  enrollment retry count 138
  enrollment retry period 140
  enrollment terminal 141
  enrollment url 142
  ip-address (trustpoint) 143
  query url 145
  rsakeypair 146
  serial-number (trustpoint) 147
  sftp-password (trustpoint) 148
  sftp-username (trustpoint) 149
  subject-name (trustpoint) 150
  show crypto ca certificates 151
show crypto ca crls 153
show crypto ca trustpool policy 154
show crypto key mypubkey dsa 155
show crypto key mypubkey ecdsa 156
show crypto key mypubkey rsa 156

CHAPTER 7

Secure Shell Commands 159

clear ssh 160
clear netconf-yang agent session 161
netconf-yang agent ssh 162
sftp 163
sftp (Interactive Mode) 166
show netconf-yang clients 168
show netconf-yang statistics 169
show ssh 171
show ssh history 173
show ssh history details 174
show ssh session details 175
ssh 177
ssh client knownhost 178
ssh client source-interface 179
ssh client vrf 180
ssh server 181
ssh server rekey-time 183
ssh server rekey-volume 184
show ssh rekey 184
ssh server logging 185
ssh server rate-limit 186
ssh server session-limit 187
ssh server v2 188
ssh server netconf port 189
ssh server netconf 190
show tech-support ssh 191
ssh timeout 193
CHAPTER 8

Secure Socket Layer Protocol Commands  195

show ssl  195
Preface

This guide describes the commands used to display and configure system security on Cisco IOS XR software. For System Security configuration information and examples, refer to the System Security Configuration Guide for Cisco NCS 6000 Series Routers and System Security Command Reference for Cisco NCS 6000 Series Routers.

The preface contains the following sections:

- Changes to This Document, on page ix
- Communications, Services, and Additional Information, on page x

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Table 1: Changes to This Document

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2013</td>
<td>Initial release of this document.</td>
</tr>
<tr>
<td>August 2014</td>
<td>Republished for Release 5.2.1.</td>
</tr>
<tr>
<td>January 2015</td>
<td>Republished for Release 5.2.3.</td>
</tr>
<tr>
<td>August 2016</td>
<td>Republished for Release 6.1.2.</td>
</tr>
<tr>
<td>July 2017</td>
<td>Republished for Release 6.2.2.</td>
</tr>
<tr>
<td>September 2017</td>
<td>Republished for Release 6.3.1.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.3.2.</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.4.1.</td>
</tr>
</tbody>
</table>
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
CHAPTER 1

Authentication, Authorization, and Accounting Commands

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

For detailed information about AAA concepts, configuration tasks, and examples, see the:

- aaa accounting, on page 2
- aaa accounting system default, on page 4
- aaa accounting update, on page 5
- aaa authentication (XR-VM), on page 6
- aaa authorization (XR-VM), on page 8
- show nacm (XR-VM), on page 10
- aaa default-taskgroup, on page 13
- aaa group server radius, on page 14
- aaa group server tacacs+, on page 15
- aaa password-policy, on page 16
- accounting (line), on page 19
- authorization (line), on page 20
- deadtime (server-group configuration), on page 21
- description (AAA), on page 22
- group (AAA), on page 23
- inherit taskgroup, on page 25
- inherit usergroup, on page 26
- key (TACACS+), on page 27
- login authentication, on page 28
- password (AAA), on page 29
- radius-server dead-criteria time, on page 31
- radius-server dead-criteria tries, on page 32
- radius-server deadtime(BNG), on page 33
- radius-server key(BNG), on page 34
- radius-server retransmit(BNG), on page 35
- radius-server timeout(BNG), on page 35
- radius source-interface(BNG), on page 36
- secret, on page 37
aaa accounting

To create a method list for accounting, use the `aaa accounting` command. To remove a list name from the system, use the `no` form of this command.

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commands</td>
<td>Enables accounting for XR EXEC shell commands.</td>
</tr>
<tr>
<td>exec</td>
<td>Enables accounting of a XR EXEC session.</td>
</tr>
</tbody>
</table>

**aaa accounting**
Enables accounting for all network-related service requests, such as Internet Key Exchange (IKE) and Point-to-Point Protocol (PPP).

Sets accounting lists for subscribers.

Enables accounting for all system-related events.

Sets the authorization list for XR EXEC.

**Command Default**
AAA accounting is disabled.

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>The mobile keyword was added.</td>
</tr>
</tbody>
</table>

**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, 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.

This command cannot be used with TACACS or extended TACACS.

**Note**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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:

```bash
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. To disable system accounting, use the `no` form of this command.

```bash
aaa accounting system default {start-stop} {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.
- **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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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+

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication (XR-VM), on page 6</td>
<td>Creates a method list for authentication.</td>
</tr>
<tr>
<td>aaa authorization (XR-VM), on page 8</td>
<td>Creates a method list for authorization.</td>
</tr>
</tbody>
</table>

### aaa accounting update

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

```text
aaa accounting update {periodic minutes}
no aaa accounting update
```

**Syntax Description**

- **periodic** *(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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to send periodic interim accounting records to the RADIUS server at 30-minute intervals:
aaa authentication (XR-VM)

To create a method list for authentication, use the `aaa authentication` command. 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
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

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+
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting</code>, on page 2</td>
<td>Creates a method list for accounting.</td>
</tr>
<tr>
<td><code>aaa authorization (XR-VM)</code>, on page 8</td>
<td>Creates a method list for authorization.</td>
</tr>
<tr>
<td><code>aaa group server radius</code>, on page 14</td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><code>aaa group server tacacs+</code>, on page 15</td>
<td>Groups different TACACS+ server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><code>login authentication</code>, on page 28</td>
<td>Enables AAA authentication for logins.</td>
</tr>
</tbody>
</table>
aaa authorization (XR-VM)

To create a method list for authorization, use the `aaa authorization` command. 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|group {tacacs+|radius group-name}}
```

```
no aaa authorization {commands|eventmanager|exec|network |subscriber|nacm} {default list-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>commands</code></td>
<td>Configures authorization for all XR EXEC shell commands.</td>
</tr>
<tr>
<td><code>eventmanager</code></td>
<td>Applies an authorization method for authorizing an event manager (fault manager).</td>
</tr>
<tr>
<td><code>exec</code></td>
<td>Configures authorization for an interactive (XR EXEC) session.</td>
</tr>
<tr>
<td><code>network</code></td>
<td>Configures authorization for network services, such as PPP or Internet Key Exchange (IKE).</td>
</tr>
<tr>
<td><code>subscriber</code></td>
<td>Sets the authorization lists for the subscriber.</td>
</tr>
<tr>
<td><code>nacm</code></td>
<td>Enables the nacm functionality.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.</td>
</tr>
<tr>
<td><code>list-name</code></td>
<td>Character string used to name the list of authorization methods.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Uses no authorization. If you specify <code>none</code>, no subsequent authorization methods is attempted. However, the task ID authorization is always required and cannot be disabled.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Uses local authorization. This method of authorization is not available for command authorization.</td>
</tr>
<tr>
<td><code>group tacacs+</code></td>
<td>Uses the list of all configured TACACS+ servers for authorization.</td>
</tr>
<tr>
<td><code>group radius</code></td>
<td>Uses the list of all configured RADIUS servers for authorization. This method of authorization is not available for command authorization.</td>
</tr>
<tr>
<td><code>group group-name</code></td>
<td>Uses a named subset of TACACS+ or RADIUS servers for authorization as defined by the <code>aaa group server tacacs+</code> or <code>aaa group server radius</code> command.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

XR Config
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa authorization commands listname1 group tacacs+
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting, on page 2</td>
<td>Creates a method list for accounting.</td>
</tr>
</tbody>
</table>

show nacm (XR-VM)

To display information about NETCONF Access Control information such as users, groups, rule-lists and traces, use the `show nacm` command. To disable authorization for a function, use the `no` form of this command.

```
show nacm
{summary | [users [<user-name>]] | [groups [<group-name>]] | [rule-list [<rule-list-name>] | [rule [<rule-name>]]] | [trace]}
no show nacm
{summary | [user-name] | [groups <group-name>] | [rule-list <rule-list-name> | [rule <rule-name>]] | [trace]}
```

Syntax Description

<table>
<thead>
<tr>
<th>Summary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays NACM summary information.</td>
</tr>
<tr>
<td>Users</td>
<td>Displays list of users in NACM database.</td>
</tr>
<tr>
<td>user-name</td>
<td>Displays info for a given user-name.</td>
</tr>
<tr>
<td>groups</td>
<td>Displays list of groups in the NACM database.</td>
</tr>
<tr>
<td>group-name</td>
<td>Displays information for a given group name.</td>
</tr>
<tr>
<td>rule-list</td>
<td>Displays list of rule-lists in the NACM database.</td>
</tr>
<tr>
<td>rule-list-name</td>
<td>Displays info for given rule-list-name.</td>
</tr>
<tr>
<td>rule</td>
<td>Displays list of rules under the rule-list in the NACM database.</td>
</tr>
<tr>
<td>rule-name</td>
<td>Displays info for given rule-name under rule-name in the NACM database.</td>
</tr>
</tbody>
</table>
trace tacacs+

Displays NACM process traces.

Command Default
None

Command Modes
XR Config

Command History
Release 6.4.1 This command was introduced.

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

Task ID

Task ID Operations ID

nacm read

Examples
The following example shows how to use the show nacm command:

```
RP/0/RP0/CPU0:xr-nacm #show nacm summary
NACM SUMMARY
--------------------------------------------------------------------------------
Enable Nacm : False
Enable External Groups : True
Number of Groups : 2
Number of Users : 2
Number of Rules : 2
Number of Rulelist : 2
Default Read : permit
Default Write : permit
Default Exec : permit
Denied Operations : 0
Denied Data Writes : 0
Denied Notifications : 0
--------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm users
USERS LIST:
--------------------------------------------------------------------------------
lab, admin,
--------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm users lab
USER NAME: lab
--------------------------------------------------------------------------------
Groups List For User:
root-lr, root-system,
--------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
```

RP/0/RP0/CPU0:xr-nacm#show nacm groups
GROUPS LIST:
--------------------------------------------------------------------------------
root-system, root-lr,
--------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm groups root-system

GROUP NAME: root-system

-----------------------------------------------------------------------------------------------
Users List:
admin, lab,
Rules List:
rule-list-1, rule-list-2,
-----------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list

RULELISTS:
-----------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Rulelist Index</th>
<th>Rulelist Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule-list-2</td>
<td>rule-list-2</td>
</tr>
<tr>
<td>rule-list-1</td>
<td>rule-list-1</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1
RULELIST NAME: rule-list-1

<table>
<thead>
<tr>
<th>Rule Index</th>
<th>Rule Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule1</td>
<td>rule1</td>
</tr>
<tr>
<td>rule2</td>
<td>rule2</td>
</tr>
</tbody>
</table>

Group List
root-system, root-lr,

-----------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1 rule
RULELIST NAME: rule-list-1

Rule Info:
Name: rule1
Index: rule1
Value: edit-config
ModuleName: *
Action: permit
RuleType: Rpc
Comment:
AccessOperations: All
HitCount: 0

-----------------------------------------------------------------------------------------------
Rule Info:
Name: rule2
Index: rule2
Value: /nacm/rule-list
ModuleName: ietf-netconf-acm
Action: deny
RuleType: Data
Comment:
AccessOperations: Read,
HitCount: 0

-----------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1 rule rule2,rule2
RULELIST NAME: rule-list-1

Rule Info:
Name: rule2
Index: rule2

-----------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:xr-nacm#
RP/0/RP0/CPU0:xr-nacm#show nacm rule-list rule-list-1,rule-list-1 rule rule2,rule2
RULELIST NAME: rule-list-1

Rule Info:
Name: rule2
Index: rule2
aaa default-taskgroup

To specify a task group for both remote TACACS+ authentication and RADIUS authentication, use the `aaa default-taskgroup` command. 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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

To group different RADIUS server hosts into distinct lists, use the `aaa group server radius` command. 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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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 swichover 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.
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.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius source-interface(BNG), on page 36</code></td>
<td>Forces RADIUS to use the IP address of a specified interface or subinterface for all outgoing RADIUS packets.</td>
</tr>
<tr>
<td><code>server (RADIUS), on page 39</code></td>
<td>Associates a RADIUS server with a defined server group.</td>
</tr>
<tr>
<td><code>server-private (RADIUS), on page 41</code></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
<tr>
<td><code>vrf (RADIUS), on page 83</code></td>
<td>Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.</td>
</tr>
</tbody>
</table>

### aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists, use the `aaa group server tacacs+` command. 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

**Command History**

- **Release 5.0.0** 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.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting, on page 2</td>
<td>Creates a method list for accounting.</td>
</tr>
<tr>
<td>aaa authentication (XR-VM), on page 6</td>
<td>Creates a method list for authentication.</td>
</tr>
<tr>
<td>aaa authorization (XR-VM), on page 8</td>
<td>Creates a method list for authorization.</td>
</tr>
<tr>
<td>server (TACACS+), on page 40</td>
<td>Specifies the host name or IP address of an external TACACS+ server.</td>
</tr>
<tr>
<td>tacacs-server host, on page 66</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

**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 {min-length min-length|max-length max-length|special-char special-char|upper-case upper-case|lower-case lower-case|numeric numeric|lifetime {years|months|days|hours|minutes|seconds} lifetime|min-char-change min-char-change|authen-max-attempts authen-max-attempts|lockout-time {days|hours|minutes|seconds} lockout-time}

no aaa password-policy policy-name {min-length min-length|max-length max-length|special-char special-char|upper-case upper-case|lower-case lower-case|numeric numeric|lifetime {years|months|days|hours|minutes|seconds} lifetime|min-char-change min-char-change|authen-max-attempts authen-max-attempts|lockout-time {days|hours|minutes|seconds} lockout-time}

**Syntax Description**

- **policy-name**
  - Specifies the name of the password, in characters.
- **min-length**
  - Specifies the minimum length of the password, in integer.
- **max-length**
  - Specifies the maximum length of the password, in integer.
- **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.
- **lower-case**
  - Specifies the number of lower case alphabets allowed in the password policy, in integer.
- **numeric**
  - Specifies the number of numerals allowed in the password policy, in integer.
- **lifetime**
  - Specifies the maximum lifetime for the password, the value of which is specified in integer, as years, months, days, hours, minutes or seconds.
- **min-char-change**
  - Specifies the number of character change required between subsequent passwords, in integer.
- **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.
- **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.

**Command Default** None

**Command Modes** XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 6000 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 FIPS Mode** chapter in the *System Security Configuration Guide for Cisco NCS 6000 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.

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

<table>
<thead>
<tr>
<th>Command Variables</th>
<th>Default Value</th>
<th>Maximum Value</th>
<th>Minimum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy-name</strong></td>
<td>None</td>
<td>253</td>
<td>1</td>
</tr>
<tr>
<td><strong>max-length</strong></td>
<td>253</td>
<td>253</td>
<td>2</td>
</tr>
<tr>
<td><strong>min-length</strong></td>
<td>2</td>
<td>253</td>
<td>2</td>
</tr>
<tr>
<td><strong>special-char</strong></td>
<td>0</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td><strong>upper-case</strong></td>
<td>0</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td><strong>lower-case</strong></td>
<td>0</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td><strong>numeric</strong></td>
<td>0</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td><strong>For lifetime:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>years</strong></td>
<td>0</td>
<td>99</td>
<td>1</td>
</tr>
<tr>
<td><strong>months</strong></td>
<td>0</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td><strong>days</strong></td>
<td>0</td>
<td>30</td>
<td>1</td>
</tr>
<tr>
<td><strong>hours</strong></td>
<td>0</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td><strong>minutes</strong></td>
<td>0</td>
<td>59</td>
<td>1</td>
</tr>
<tr>
<td><strong>seconds</strong></td>
<td>0</td>
<td>59</td>
<td>1</td>
</tr>
<tr>
<td><strong>min-char-change</strong></td>
<td>4</td>
<td>253</td>
<td>0</td>
</tr>
<tr>
<td><strong>authen-max-attempts</strong></td>
<td>0</td>
<td>24</td>
<td>1</td>
</tr>
<tr>
<td><strong>For lockout-time:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>days</strong></td>
<td>0</td>
<td>255</td>
<td>1</td>
</tr>
<tr>
<td><strong>hours</strong></td>
<td>0</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td><strong>minutes</strong></td>
<td>0</td>
<td>59</td>
<td>1</td>
</tr>
<tr>
<td><strong>seconds</strong></td>
<td>0</td>
<td>59</td>
<td>1</td>
</tr>
</tbody>
</table>
This example shows how to define a AAA password security policy:

```bash
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa password-policy, on page 50</td>
<td>Displays the details of AAA password policy.</td>
</tr>
<tr>
<td>username, on page 78</td>
<td></td>
</tr>
</tbody>
</table>

### 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 shell commands.
- **exec**: Enables accounting of XR EXEC 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa accounting</strong>, on page</td>
<td>Creates a method list for accounting.</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

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 (EXEC)( XR EXEC) 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 5.0.0  This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authorization (XR-VM), on page 8</code></td>
<td>Creates a method list for authorization.</td>
</tr>
</tbody>
</table>

```
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
```

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
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 5.0.0 This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>taskgroup</code>, on page 74</td>
<td>Accesses task group configuration mode and configures a task group by associating it with a set of task IDs.</td>
</tr>
<tr>
<td><code>usergroup</code>, on page 77</td>
<td>Accesses user group configuration mode and configures a user group by associating it with a set of task groups.</td>
</tr>
</tbody>
</table>

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

Syntax Description

- `root-lr` Adds the user to the predefined root-lr group. Only users with root-lr authority may use this option.
Add the user to the predefined network administrators group.

Add the user to the predefined system administrators group.

Add the user to the predefined operator group.

Add the user to the predefined Cisco support personnel group.

**Note** Starting from IOS XR 4.3.1 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.

Add the user to the predefined service administrators group.

Add the user to a named user group that has already been defined with the `usergroup` command.

### Command Modes

Username configuration

### Command History

**Release** Modification

Release 5.0.0 This command was introduced.

### Usage Guidelines

Use the `group` command in username configuration mode. To access username configuration mode, use the `username`, on page 78 command in XR Config mode.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password (AAA), on page 29</td>
<td>Creates a login password for a user.</td>
</tr>
<tr>
<td>usergroup, on page 77</td>
<td>Configures a user group and associates it with a set of task groups.</td>
</tr>
<tr>
<td>username, on page 78</td>
<td>Accesses username configuration mode, configures a new user with a username, and establishes a password and permissions for that user.</td>
</tr>
</tbody>
</table>
**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
---           ------------------
5.0.0         This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 5.0.0  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-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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description (AAA), on page 22</td>
<td>Creates a description of a task group in task group configuration mode, or creates a description of a user group in user group configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>taskgroup, on page 74</td>
<td>Configures a task group to be associated with a set of task IDs.</td>
</tr>
<tr>
<td>usergroup, on page 77</td>
<td>Configures a user group to be associated with a set of task groups.</td>
</tr>
</tbody>
</table>

**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|7 encrypted-key auth-key}
no key {0 clear-text-key|7 encrypted-key auth-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**

TACACS host configuration

**Command History**

Release 5.0.0 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.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 5.0.0** 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**
```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```
password (AAA)

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
```

```
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

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

When an XR EXEC process 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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group (AAA), on page 23</td>
<td>Adds a user to a group.</td>
</tr>
<tr>
<td>usergroup, on page 77</td>
<td>Accesses user group configuration mode and configures a user group, associating it with a set of task groups.</td>
</tr>
<tr>
<td>username, on page 78</td>
<td>Accesses username configuration mode and configures a new user with a username, establishing a password and granting permissions for that user.</td>
</tr>
<tr>
<td>line</td>
<td>Enters line template configuration mode for the specified line template. For more information, see the Cisco IOS XR System Management Command Reference.</td>
</tr>
</tbody>
</table>
**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 to 120 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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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. 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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server dead-criteria time, on page 31</code></td>
<td>Defines the length 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.</td>
</tr>
<tr>
<td><code>radius-server deadtime(BNG), on page 33</code></td>
<td>Defines the length of time, in minutes, for a RADIUS server to remain marked dead.</td>
</tr>
<tr>
<td><code>show radius dead-criteria, on page 56</code></td>
<td>Displays information for the dead-server detection criteria.</td>
</tr>
</tbody>
</table>

`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 XR Config mode. To set deadtime to 0, use the `no` form of this command.

```
radius-server deadtime minutes
```

**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. The default value is 0.

**Command Default**

Dead time is set to 0.

**Command Modes**

XR Config mode

**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.

**Examples**

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

```
RP/0//CPU0:router# configure
RP/0//CPU0:router(config)# radius-server deadtime 5
```
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 XR Config mode. To disable the key, use the `no` form of this command.

```
radius-server key {0 clear-text-key|7 encrypted-key clear-text-key}
```

**Syntax Description**

- `0 clear-text-key` Specifies an unencrypted (cleartext) shared key.
- `7 encrypted-key` Specifies a encrypted shared key.
- `clear-text-key` Specifies an unencrypted (cleartext) shared key.

**Command Default**
The authentication and encryption key is disabled.

**Command Modes**
XR Config mode

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set the cleartext key to “samplekey”

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

The following example shows how to set the encrypted shared key to “anykey”

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key (RADIUS)</td>
<td>Specifies the authentication and encryption key that is used between the router and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td>server-private (RADIUS), on page 41</td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>
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 XR Config mode. To disable retransmission, use the `no` form of this command.

```
radius-server retransmit retries
```

**Syntax Description**

- `retries` Maximum number of retransmission attempts. The range is from 1 to 100. Default is 3.

**Command Default**

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

**Command Modes**

XR Config mode

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key(BNG)</code></td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td><code>retransmit (RADIUS)</code></td>
<td>Specifies the number of times a RADIUS request is resent to a server if the server is not responding or is responding slowly.</td>
</tr>
<tr>
<td><code>server-private (RADIUS)</code></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>

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 XR Config mode. To restore the default, use the `no` form of this command.

```
radius-server timeout seconds
```
**Syntax Description**

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

**Command Default**

5 seconds

**Command Modes**

XR Config mode

**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.

**Examples**

The following example shows how to change the interval timer to 10 seconds:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key(BNG), on page 34</code></td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
<tr>
<td><code>server-private (RADIUS), on page 41</code></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
<tr>
<td><code>timeout (RADIUS)</code></td>
<td>Specifies the number of seconds the router waits for the RADIUS server to reply before retransmitting.</td>
</tr>
</tbody>
</table>

---

**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 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-name [vrf vrf-id]
```

**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

**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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key(BNG), on page 34</code></td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
</tbody>
</table>

**secret**

To configure an MD5-encrypted secret to be associated with an encrypted username, use the `secret` command in username configuration mode or line template configuration mode. To remove the secure secret, use the `no` form of this command.

```
secret {0|5} secret-login
no secret {0|5} secret-login
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(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.</td>
</tr>
<tr>
<td>5</td>
<td>Specifies that an encrypted MD5 password (secret) follows.</td>
</tr>
</tbody>
</table>
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.

Command Default
No password is specified.

Command Modes
Username configuration
Line template configuration

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 5.0.0   | This command was introduced.

Usage Guidelines
Cisco IOS XR software allows you to configure 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).

You can specify 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 be encrypted.

When an XR EXEC 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. If the “username name secret 5” line appears in the command output, enhanced password security is enabled.

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
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples
The following example shows how to establish the clear-text secret “lab” for the user `user2`:

```
RP/0/CPU0:router# configure
RP/0/CPU0:router(config)# username user2
RP/0/CPU0:router(config-un)# secret 0 lab
RP/0/CPU0:router(config-un)# commit
```
RP//CPU0:router(config-un)# show running-config
Building configuration...
username user2
    secret 5 $1$DTmd$q7C6f9zje7Cc7XzmU2FrX1
end

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group (AAA), on page 23</td>
<td>Adds a user to a group.</td>
</tr>
<tr>
<td>password (AAA), on page 29</td>
<td>Creates a login password for a user.</td>
</tr>
<tr>
<td>usergroup, on page 77</td>
<td>Accesses user group configuration mode and configures a user group, associating it with a set of task groups.</td>
</tr>
<tr>
<td>username, on page 78</td>
<td>Accesses username configuration mode and configures a new user with a username, establishing a password and granting permissions for that user.</td>
</tr>
</tbody>
</table>

**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]
o 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa group server radius</code>, on page 14</td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><code>deadtime (server-group configuration)</code>, on page 21</td>
<td>Configures the deadtime value at the RADIUS server group level.</td>
</tr>
<tr>
<td><code>server-private (RADIUS)</code>, on page 41</td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>

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}
```
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]
no server-private ip-address [auth-port port-number] [acct-port port-number]
```

**Syntax Description**

- `ip-address`  IP address of the RADIUS server host.

**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)# aa group server tacac+ tac1
RP/0/RP0/CPU0:router(config-sg-tacac+)# server 192.168.60.15
```
**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.

---

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

---

**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 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)#
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server tacacs+, on page 15</td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
</tbody>
</table>
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 {hostname ip-address} [port port-number] [timeout seconds] [key string]
no server-private {hostname ip-address}
```

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Character string used to name the server host.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the TACACS+ server host. Both IPv4 and IPv6 addresses are supported.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.</td>
</tr>
<tr>
<td>port-number</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td>(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 <code>tacacs-server timeout</code> command for only this server. The range is from 1 to 1000. The default is 5.</td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>key</td>
<td>(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 <code>tacacs-server key</code> command. If no key string is specified, the global value is used.</td>
</tr>
<tr>
<td>string</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.0</td>
<td>IPv6 support was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server tacacs+, on page 15</td>
<td>Groups different TACACS+ server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td>tacacs-server key, on page 68</td>
<td>Sets the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon.</td>
</tr>
<tr>
<td>tacacs-server timeout, on page 69</td>
<td>Sets the interval for which a router waits for a server host to reply before timing out.</td>
</tr>
<tr>
<td>key (TACACS+), on page 27</td>
<td>Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>timeout (TACACS+), on page 75</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>vrf (TACACS+), on page 84</strong></td>
<td>Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA TACACS+ server group.</td>
</tr>
</tbody>
</table>

---

**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.

```
show aaa {ikegroup ikegroup-name|login sync |usergroup [usergroup-name]|trace|userdb [username]|task|taskgroup }
```

**Syntax Description**

- **ikegroup** Displays details for local IKE groups.
- **ikegroup-name** (Optional) IKE group whose details are to be displayed.
- **locald** Displays local data for subsystem.
- **login** Displays data for login subsystem.
- **sync** Syncs data with the subsystem.
- **usergroup** Displays details for all user groups.
- **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** Show task information.
- **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
show aaa (XR-VM)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the show aaa command to list details for all IKE groups, user groups, local users, 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.

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
```
<table>
<thead>
<tr>
<th>Task: atm</th>
<th>READ</th>
<th>WRITE</th>
<th>EXECUTE</th>
<th>DEBUG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task: basic-services</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: bfd</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: bgp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: boot</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: bundle</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: cdp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: cef</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: cgn</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: config-mgmt</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: config-services</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: crypto</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: diag</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: drivers</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: dwdm</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: eem</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: eigrp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ethernet-services</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ext-access</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: fabric</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: fault-mgr</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: filesystem</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: firewall</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: fr</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: hdlc</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: host-services</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: hsrp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: interface</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: inventory</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ip-services</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ipv4</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ipv6</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: isis</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: l2vpn</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: li</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: logging</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: lpts</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: monitor</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: mpls-ldp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: mpls-static</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: mpls-te</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: multicast</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: netflow</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: network</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ospf</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ouni</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: pkg-mgmt</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: pos-dpt</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: ppp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: qos</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: rib</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: rip</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: route-map</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: route-policy</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: sbc</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: snmp</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: sonet-sdh</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: static</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: syslog</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: system</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: transport</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
<tr>
<td>Task: tty-access</td>
<td>READ</td>
<td>WRITE</td>
<td>EXECUTE</td>
<td>DEBUG</td>
</tr>
</tbody>
</table>
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
diag : READ
Task: ext-access : READ EXECUTE
Task: logging : READ

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
bclid
bfd
bgp
boot
bundle
cdp
cef
cisco-support
config-mgmt
config-services
crypto
diag
disallowed
drivers
eigrp
ext-access
fabric
fault-mgr
filesystem
firewall
fr
hdlc
host-services
hsrp
interface
inventory
ip-services
ipv4
ipv6
isis
logging
ipts
monitor
mpls-ldp
mpls-static
mpls-te
multicast
```

Authentication, Authorization, and Accounting Commands
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**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

System Admin EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
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
terminal'
2014-11-03.13:37:03 UTC cisco 57 0/RP0 CLI 'config terminal'
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 ***
2014-11-03.13:37:12 UTC cisco 57 0/RP0 CLI done
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 6.2.1**  This command was introduced.
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.

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
```
show radius

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

Command Modes
XR EXEC

Command History
Release 6.1.2  This command was updated to display IPv6 address details.

Release 5.0.0  This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

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

**Output for IPV4 server**

```
RP/0/RP0/CPU0:router# show radius
Global dead time: 0 minute(s)
Number of Servers: 1
Server: 2.3.4.5/2000/2001 is UP
  Address family: IPv6
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
```

**Output for IPV6 server**

```
RP/0/RP0/CPU0:router# show radius
Global dead time: 0 minute(s)
Number of Servers: 1
Server: 2001:b::2/2000/2001 is UP
  Address family: IPv6
  Total Deadtime: 0s Last Deadtime: 0s
  Timeout: 5 sec, Retransmit limit: 3
  Quarantined: No
```

This table describes the significant fields shown in the display.
Table 2: show radius Field Descriptions

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf (RADIUS), on page 83</td>
<td>Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.</td>
</tr>
<tr>
<td>radius-server retransmit(BNG), on page 35</td>
<td>Specifies how many times Cisco IOS XR software searches the list of RADIUS server hosts before giving up.</td>
</tr>
<tr>
<td>radius-server timeout(BNG), on page 35</td>
<td>Sets the interval for which a router waits for a server host to reply.</td>
</tr>
</tbody>
</table>

show radius accounting

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

```bash
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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>
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 3: `show radius accounting` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa accounting</code>, on page 2</td>
<td>Creates a method list for accounting.</td>
</tr>
<tr>
<td><code>aaa authentication (XR-VM)</code>, on page 6</td>
<td>Creates a method list for authentication.</td>
</tr>
<tr>
<td><code>show radius authentication</code>, on page 54</td>
<td>Obtains information and detailed statistics for the RADIUS authentication server and port.</td>
</tr>
</tbody>
</table>

**show radius authentication**

To obtain information and detailed statistics for the RADIUS authentication server and port, use the `show radius authentication` command.

```
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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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 4: show radius authentication Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address/UDP destination port for authentication requests; UDP destination port for accounting requests.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting, on page 2</td>
<td>Creates a method list for accounting.</td>
</tr>
</tbody>
</table>
show radius dead-criteria

To obtain information about the dead server detection criteria, use the `show radius dead-criteria` command.

```
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `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 5: show radius dead-criteria Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Number of seconds the router waits for a server host to reply before timing out.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>Number of times Cisco IOS XR software searches the list of RADIUS server hosts before giving up.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-server dead-criteria time, on page 31</td>
<td>Forces one or both of the criteria that is used to mark a RADIUS server as dead.</td>
</tr>
<tr>
<td>radius-server deadtime(BNG), on page 33</td>
<td>Defines the length of time in minutes for a RADIUS server to remain marked dead.</td>
</tr>
</tbody>
</table>

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.

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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.
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 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp1' has 2 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 2 server(s)
    Server 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp-priv' has 1 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
    Server 3.3.3.3/1645/1646 [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 1.1.1.1/1645/1646
      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 2.2.2.2/1645/1646
      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 3.3.3.3/1645/1646 [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 6: show radius server-groups Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address/UDP destination port for authentication requests/UDP destination port for accounting requests.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf (RADIUS), on page 83</td>
<td>Configures the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an AAA RADIUS server group.</td>
</tr>
</tbody>
</table>

**show tacacs**

To display information about the TACACS+ servers that are configured in the system, use the `show tacacs` command.

```
show tacacs
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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

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

For IPv4 IP addresses:
Server:1.1.1.1/21212 opens=0 closes=0 aborts=0 errors=0
   packets in=0 packets out=0
   status=up single-connect=false
Server:2.2.2.2/21232 opens=0 closes=0 aborts=0 errors=0
   packets in=0 packets out=0
   status=up single-connect=false

For IPv6 IP addresses:
Server: 1.2.3.5/49 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address.</td>
</tr>
<tr>
<td>opens</td>
<td>Number of socket opens to the external server.</td>
</tr>
<tr>
<td>closes</td>
<td>Number of socket closes to the external server.</td>
</tr>
<tr>
<td>aborts</td>
<td>Number of tacacs requests that have been aborted midway.</td>
</tr>
<tr>
<td>errors</td>
<td>Number of error replies from the external server.</td>
</tr>
<tr>
<td>packets in</td>
<td>Number of TCP packets that have been received from the external server.</td>
</tr>
<tr>
<td>packets out</td>
<td>Number of TCP packets that have been sent to the external server.</td>
</tr>
</tbody>
</table>
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.

Syntax Description
This command has no keywords or arguments.

Command Default
None

Command Modes
XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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 12.26.25.61/23456
  Server 12.26.49.12/12345
  Server 12.26.49.12/9000
  Server 12.26.25.61/23432
  Server 5.5.5.5/23456
  Server 1.1.1.1/49
Server group 'tac100' has 1 servers
  Server 12.26.49.12
```

This table describes the significant fields shown in the display.
Table 8: show tacacs server-groups Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server IP address.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

show user

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

**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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>—</td>
</tr>
</tbody>
</table>
Examples

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

```
RP/0/RP0/CPU0# show user authentication
local
```

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

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

```
Task: aaa : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: config- : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: mpls- : READ WRITE EXECUTE DEBUG
Task: mpls- : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : READ WRITE EXECUTE DEBUG
Task: : 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
```
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**

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>System Admin EXEC mode</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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
```
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

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

System Admin EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read</td>
</tr>
</tbody>
</table>

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
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 5.0.0  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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host, on page 66</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

**tacacs-server host**

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

```
tacacs-server host host-name [port port-number] [timeout seconds] [key [{0|7}] auth-key] [single-connection]
no tacacs-server host host-name [port port-number]
```
Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-name</td>
<td>Host or domain name or IP address of the TACACS+ server.</td>
</tr>
<tr>
<td>port port-number</td>
<td>(Optional) Specifies a server port number. This option overrides the default, which is port 49. Valid port numbers range from 1 to 65535.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>(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 <code>tacacs-server timeout</code> command for this server only. The valid timeout range is from 1 to 1000 seconds. Default is 5.</td>
</tr>
<tr>
<td>key [0</td>
<td>7] auth-key</td>
</tr>
<tr>
<td>single-connection</td>
<td>(Optional) Multiplexes all TACACS+ requests to this server over a single TCP connection. By default, a separate connection is used for each session.</td>
</tr>
</tbody>
</table>

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.

Command Modes

XR Config

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key (TACACS+), on page 27</td>
<td>Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.</td>
</tr>
<tr>
<td>single-connection, on page 65</td>
<td>Multiplexes all TACACS+ requests to this server over a single TCP connection.</td>
</tr>
<tr>
<td>tacacs-server key, on page 68</td>
<td>Globally sets the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon.</td>
</tr>
<tr>
<td>tacacs-server timeout, on page 69</td>
<td>Globally sets the interval that the router waits for a server host to reply.</td>
</tr>
<tr>
<td>timeout (TACACS+), on page 75</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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. 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.
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key (TACACS+), on page 27</td>
<td>Specifies an authentication and encryption key shared between the AAA server and the TACACS+ server.</td>
</tr>
<tr>
<td>tacacs-server host, on page 66</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

**tacacs-server timeout**

To set the interval that the server waits for a server host to reply, use the `tacacs-server timeout` command. 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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host, on page 66</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

**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 global configuration mode.

```
tacacs-server ipv4 dscp dscp-value
```

Syntax Description

<table>
<thead>
<tr>
<th>ipv4</th>
<th>Specifies the dscp bit for the IPv4 packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp</td>
<td>Sets the DSCP in the IP header.</td>
</tr>
</tbody>
</table>
**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

Global Configuration mode

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
### Tacacs Source-Interface

To specify the source IP address of a selected interface for all outgoing TACACS+ packets, use the `tacacs source-interface` command. 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]
nolcacs 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.
- `vrf` Specifies the name of the assigned VRF.
- `vrf-id`

**Note**

Use the `show interfaces` command in EXEC 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.

**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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### 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 GigabitEthernet 0/0/0/29 vrf abc
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server tacacs+, on page 15</td>
<td>Groups different server hosts into distinct lists and distinct methods.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>Enables read-only privileges for the named task ID.</td>
</tr>
<tr>
<td>write</td>
<td>Enables write privileges for the named task ID. The term “write” implies read also.</td>
</tr>
<tr>
<td>execute</td>
<td>Enables execute privileges for the named task ID.</td>
</tr>
<tr>
<td>debug</td>
<td>Enables debug privileges for the named task ID.</td>
</tr>
<tr>
<td>taskid-name</td>
<td>Name of the task ID.</td>
</tr>
</tbody>
</table>

### Command Default

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

### Command Modes

Task group configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskgroup, on page 74</td>
<td>Configures a task group to be associated with a set of task IDs.</td>
</tr>
</tbody>
</table>

**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. 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.
**Task Group Permissions**

(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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description (AAA), on page 22</td>
<td>Creates a task group description in task configuration mode.</td>
</tr>
<tr>
<td>task, on page 73</td>
<td>Adds a task ID to a task group.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs-server host, on page 66</td>
<td>Specifies a TACACS+ host.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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 the line console. After the timeout value has expired, the user is prompted again. The retry is allowed three times.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login authentication, on page 28</td>
<td>Enables AAA authentication for logging in.</td>
</tr>
</tbody>
</table>

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. 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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 26** 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 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.

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>description (AAA), on page 22</strong></td>
<td>Creates a description of a task group during configuration.</td>
</tr>
<tr>
<td><strong>inherit usergroup, on page 26</strong></td>
<td>Enables a user group to derive permissions from another user group.</td>
</tr>
<tr>
<td><strong>taskgroup, on page 74</strong></td>
<td>Configures a task group to be associated with a set of task IDs.</td>
</tr>
</tbody>
</table>

### 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. To delete a user from the database, use the **no** form of this command.

```plaintext
username user-name [ { password { 0 | 7 } password-policy policy-name | secret { 0 | 5 } password|group usergroup-name }]
no username user-name [ { password { 0 | 7 } password-policy policy-name | secret { 0 | 5 } password|group usergroup-name }]
```
<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>user-name</strong></td>
<td><strong>Name of the user. The user-name argument can be only one word. Spaces and quotation marks are not allowed.</strong>&lt;br&gt;The allowed range for a user-defined username is 2-253 characters.</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td><strong>(Optional) Enables a password to be created for the named user.</strong></td>
</tr>
<tr>
<td><strong>0</strong></td>
<td><strong>(Optional) Specifies that an unencrypted (clear-text) password follows. The password will be encrypted for storage in the configuration using a Cisco proprietary encryption algorithm.</strong></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>(Optional) Specifies that an encrypted password follows.</strong></td>
</tr>
<tr>
<td><strong>password</strong></td>
<td><strong>(Optional) 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.</strong>&lt;br&gt;Can be up to 253 characters in length.</td>
</tr>
<tr>
<td><strong>password-policy</strong></td>
<td><strong>(Optional) Applies a particular password policy to the user.</strong></td>
</tr>
<tr>
<td><strong>policy-name</strong></td>
<td><strong>Specifies the name of the password policy.</strong>&lt;br&gt;This policy name has to be configured prior to applying this policy to the user.</td>
</tr>
<tr>
<td><strong>secret</strong></td>
<td><strong>(Optional) Enables an MD5-secured password to be created for the named user.</strong></td>
</tr>
<tr>
<td><strong>0</strong></td>
<td><strong>(Optional) Specifies that an unencrypted (clear-text) password follows. The password will be encrypted for storage in the configuration using an MD5 encryption algorithm.</strong></td>
</tr>
<tr>
<td>Command Default</td>
<td>No usernames are defined in the system.</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Command Modes</td>
<td>XR Config</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong>  <strong>Modification</strong></td>
</tr>
<tr>
<td></td>
<td>Release 5.0.0  This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>Release 6.2.1  Added support for <code>password-policy</code>, as part of AAA password security for FIPS compliance.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

**Note**

A user is never allowed to have cisco-support privileges as the only group.

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.

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 6 command.

**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.

For more details on defining a password policy, refer `aaa password-policy` command. The AAA password security policy feature works as such for Cisco IOS XR platforms. Whereas, it is supported only on XR VM, for Cisco IOS XR 64 bit platforms and Cisco NCS 6000 Series Routers.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>(Optional) Specifies that an encrypted password follows.</td>
</tr>
<tr>
<td>group</td>
<td>(Optional) Enables a named user to be associated with a user group.</td>
</tr>
<tr>
<td>usergroup-name</td>
<td>(Optional) Name of a user group as defined with the <code>usergroup</code> command.</td>
</tr>
</tbody>
</table>
## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

## Examples

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

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

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

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

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

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

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

```plaintext
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# username user1 password-policy test-policy password abc
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication (XR-VM), on page 6</td>
<td>Defines a method list for authentication.</td>
</tr>
<tr>
<td>group (AAA), on page 23</td>
<td>Adds a user to a group.</td>
</tr>
</tbody>
</table>
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.

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.
- **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.
- **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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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
5.0.0      This command was introduced.
4.1.0      This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server tacacs+, on page 15</td>
<td>Groups different TACACS+ server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td>server (TACACS+), on page 40</td>
<td>Specifies the source IP address of a selected interface for all outgoing TACACS+ packets.</td>
</tr>
<tr>
<td>server-private (TACACS+), on page 43</td>
<td>Configures the IP address of the private TACACS+ server for the group server.</td>
</tr>
</tbody>
</table>
CHAPTER 2

IPSec Commands

This module describes the IPSec commands.

The following IPSec commands are available only if the <platform>-k9sec.pie is installed.

- clear crypto ipsec sa, on page 87
- description (IPSec profile), on page 88
- show crypto ipsec sa, on page 89
- show crypto ipsec summary, on page 92
- show crypto ipsec transform-set, on page 93

**clear crypto ipsec sa**

To delete specific security associations (SAs), or all SAs in the IP Security (IPSec) security associations database (SADB), use the **clear crypto ipsec sa** command.

```
clear crypto ipsec sa {sa-id|all|counters |{sa-id|all}|interface tunnel-ipsec}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Identifier for the SA. IPSec supports from 1 to 64,500 sessions.</th>
<th>sa-id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes all IPSec SAs in the IPSec SADB.</td>
<td>all</td>
</tr>
<tr>
<td>Clears the counters in the IPSec SADB.</td>
<td>counters</td>
</tr>
<tr>
<td>Clears the interfaces in the IPSec SADB.</td>
<td>interface</td>
</tr>
<tr>
<td>The range of tunnel-ipsec is &lt;0-4294967295&gt;.</td>
<td>tunnel-ipsec</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release 5.0.0</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>
**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SAs are established to secure data flows in IPSec. Use the `clear crypto ipsec sa` command to delete active IPSec sessions or force IPSec to reestablish new SAs. Usually, the establishment of SAs is negotiated between peers through Internet Key Exchange (IKE) on behalf of IPSec.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to remove the SA with ID 100 from the SADB:

```
RP/0/RP0/CPU0:router# clear crypto ipsec sa 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ipsec sa, on page 89</td>
<td>Displays the settings used by current SAs.</td>
</tr>
</tbody>
</table>

**description (IPSec profile)**

To create a description of an IPSec profile, use the `description` command in profile configuration mode. To delete a profile description, use the `no` form of this command.

```
description string
no description
```

**Syntax Description**

- `string` Character string describing the IPSec profile.

**Command Default**

None

**Command Modes**

Crypto IPSec profile

**Command History**

- **Release**  5.0.0  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `description` command inside the profile configuration submode to create a description for an IPSec profile.
show crypto ipsec sa

To display security association (SA) information based on the rack/slot/module location, use the `show crypto ipsec sa` command.

```
show crypto ipsec sa [ { sa-id | peer ip-address | profile profile-name | detail | count | fvrf fvrf-name | ivrf ivrf-name | location node-id } ]
```

### Syntax Description

- **sa-id** (Optional) Identifier for the SA. The range is from 1 to 64500.
- **peer ip-address** (Optional) IP address used on the remote (PC) side. Invalid IP addresses are not accepted.
- **profile profile-name** (Optional) Specifies the alphanumeric name for a security profile. The character range is from 1 to 64. Profile names cannot be duplicated.
- **detail** (Optional) Provides additional dynamic SA information.
- **count** (Optional) Provides SA count.
- **fvrf fvrf-name** (Optional) Specifies that all existing SAs for front door virtual routing and forwarding (FVRF) is the same as the fvrf-name.
- **ivrf ivrf-name** (Optional) Specifies that all existing SAs for inside virtual routing and forwarding (IVRF) is the same as the ivrf-name.
- **location node-id** (Optional) Specifies that the SAs are configured on a specified location.

### Command Modes

XR EXEC

### Command History

**Release** | **Modification**
--- | ---
5.0.0 | This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
If no optional argument or keyword is used, all SAs are displayed within a flow. Within a flow, the SAs are listed by protocol (Encapsulating Security Payload [ESP] or Authentication Header [AH]) and direction (inbound or outbound).

The `detail` keyword provides additional information only for SAs that are configured in a software crypto engine. The SAs are configured by using `tunnel-ipsec` and `transport`.

### Examples

The following sample output is from the `show crypto ipsec sa` command:

```plaintext
RP/0/RP0/CPU0:router# show crypto ipsec sa

SSA id: 510
Node id: 0/1/0
SA Type: MANUAL
type: service-ipsec22
profile : p7
local ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.255/512/0)
remote ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.0/512/0)
local crypto endpt: 0.0.0.0, remote crypto endpt: 0.0.0.0, vrf default

#pkts tx :0 #pkts rx :0
#bytes tx :0 #bytes rx :0
#pkts encrypt :0 #pkts decrypt :0
#pkts digest :0 #pkts verify :0
#pkts encrpt fail:0 #pkts decrpt fail:0
#pkts digest fail:0 #pkts verify fail:0
#pkts replay fail:0
#pkts tx errors :0 #pkts rx errors :0

outbound esp sas:
spi: 0x322(802)
transform: esp-3des-md5
in use settings = Tunnel
sa agreed lifetime: 3600s, 4194303kb
sa timing: remaining key lifetime: 3142303931sec/0kb
sa DPD: disable, mode none, timeout 0s
sa idle timeout: disable, 0s
sa anti-replay (HW accel): enable, window 64

inbound esp sas:
spi: 0x322(802)
transform: esp-3des-md5
in use settings = Tunnel
sa agreed lifetime: 3600s, 4194303kb
sa timing: remaining key lifetime: 3142303931sec/0kb
sa DPD: disable, mode none, timeout 0s
sa idle timeout: disable, 0s
sa anti-replay (HW accel): enable, window 64
```

This table describes the significant fields shown in the display.
Table 9: show crypto ipsec sa Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA id</td>
<td>Identifier for the SA.</td>
</tr>
<tr>
<td>interface</td>
<td>Identifier for the interface.</td>
</tr>
<tr>
<td>profile</td>
<td>String of alphanumeric characters that specify the name of a security profile.</td>
</tr>
<tr>
<td>local ident</td>
<td>IP address, mask, protocol, and port of the local peer.</td>
</tr>
<tr>
<td>remote ident</td>
<td>IP address, mask, protocol and port of the remote peer.</td>
</tr>
<tr>
<td>outbound esp sas</td>
<td>Outbound ESP SAs.</td>
</tr>
<tr>
<td>inbound esp sas</td>
<td>Inbound ESP SAs.</td>
</tr>
<tr>
<td>transform</td>
<td>The transform being used in the SA.</td>
</tr>
<tr>
<td>sa lifetime</td>
<td>The lifetime value used in the SA.</td>
</tr>
</tbody>
</table>

The following sample output is from the `show crypto ipsec sa` command for the `profile` keyword for a profile named pn1:

```
RP/0/RP0/CPU0:router# show crypto ipsec sa profile pn1
SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
  spi: 0x8b0e950f (2323988687)
  transform: esp-3des-sha
  in use settings = Tunnel
  sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
  spi: 0x2777997c (662149500)
  transform: esp-3des-sha
  in use settings = Tunnel
  sa lifetime: 3600s, 4194303kb
```

The following sample output is from the `show crypto ipsec sa` command for the `peer` keyword:

```
RP/0/RP0/CPU0:router# show crypto ipsec sa peer 172.19.72.120
SA id: 2
interface: tunnel0
profile: pn1
```
show crypto ipsec summary

To display IP Security (IPSec) summary information, use the show crypto ipsec summary command.

**show crypto ipsec summary**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the show crypto ipsec summary command:

```
RP/0/RP0/CPU0:router# show crypto ipsec summary
# * Attached to a transform indicates a bundle
```
Active IPSec Sessions: 1

<table>
<thead>
<tr>
<th>SA Interface</th>
<th>Local Peer/Port</th>
<th>Remote Peer/Port</th>
<th>FVRF</th>
<th>Profile</th>
<th>Transform</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>502 -ipsec100</td>
<td>70.70.70.2/500</td>
<td>60.60.60.2/500</td>
<td>default</td>
<td>ipsec1</td>
<td>esp-3des</td>
<td>esp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3600/10000000</td>
<td></td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

### Table 10: show crypto ipsec summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA</td>
<td>Identifier for the security association.</td>
</tr>
<tr>
<td>Node</td>
<td>Identifier for the node.</td>
</tr>
<tr>
<td>Local Peer</td>
<td>IP address of the local peer.</td>
</tr>
<tr>
<td>Remote Peer</td>
<td>IP address of the remote peer.</td>
</tr>
<tr>
<td>FVRF</td>
<td>The front door virtual routing and forwarding (FVRF) of the SA. If the FVRF</td>
</tr>
<tr>
<td></td>
<td>is global, the output shows f_vrf as an empty field.</td>
</tr>
<tr>
<td>Mode</td>
<td>Profile mode type.</td>
</tr>
<tr>
<td>Profile</td>
<td>Crypto profile in use.</td>
</tr>
<tr>
<td>Transform</td>
<td>Transform in use.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Lifetime value, displayed in seconds followed by kilobytes.</td>
</tr>
</tbody>
</table>

**show crypto ipsec transform-set**

To display the configured transform sets, use the `show crypto ipsec transform-set` command.

```
show crypto ipsec transform-set [transform-set-name]
```

**Syntax Description**

- `transform-set-name` (Optional) IPSec transform set with the specified value for the `transform-set-name` argument are displayed.

**Command Default**

No default values. The default behavior is to print all the available transform-sets.

**Command Modes**

XR EXEC

**Command History**

Release 5.0.0  This command was introduced.
**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If no transform is specified, all transforms are displayed.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the `show crypto ipsec transform-set` command:

```
RP/0/RP0/CPU0:router# show crypto ipsec transform-set
Transform set combined-des-sha: {esp-des esp-sha-hmac}
Transform set tsfm2: {esp-md5-hmac esp-3des }
  Mode: Transport
Transform set tsfm1: {esp-md5-hmac esp-3des }
  Mode: Tunnel
Transform set ts1: {esp-des }
  Mode: Tunnel
```
CHAPTER 3

Keychain Management Commands

This module describes the commands used to configure keychain management.

For detailed information about keychain management concepts, configuration tasks, and examples, see the Implementing Keychain Management on configuration module in the System Security Configuration Guide for Cisco NCS 6000 Series Routers.

- accept-lifetime, on page 95
- accept-tolerance, on page 96
- key (key chain), on page 97
- key chain (key chain), on page 98
- key-string (keychain), on page 100
- send-lifetime, on page 101
- show key chain, on page 102

accept-lifetime

To set the time period during which the authentication key on a keychain is received as valid, use the accept-lifetime command in key configuration mode. To revert to the default value, use the no form of this command.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-time</td>
<td>Start time, in \textit{hh:mm:ss day month year} format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month is from 1 to 31. The range for the years is from 1993 to 2035.</td>
</tr>
<tr>
<td>duration duration value</td>
<td>(Optional) Determines the lifetime of the key in seconds. The range is from 1-2147483646.</td>
</tr>
<tr>
<td>infinite</td>
<td>(Optional) Specifies that the key never expires after it becomes valid.</td>
</tr>
<tr>
<td>end-time</td>
<td>(Optional) Time, in \textit{hh:mm:ss day month year} format, after which the key expires. The range is from 0:0:0 to 23:59:59.</td>
</tr>
</tbody>
</table>
accept-tolerance

To specify the tolerance or acceptance limit, in seconds, for an accept key that is used by a peer, use the **accept-tolerance** command in keychain configuration mode. To disable this feature, use the **no** form of this command.

```
accept-tolerance [{value|infinite}]
no accept-tolerance [{value|infinite}]
```

**Syntax Description**

- **value** (Optional) Tolerance range, in seconds. The range is from 1 to 8640000.
**Keychain Management Commands**

**key (key chain)**

To create or modify a keychain key, use the `key` command in keychain-key configuration mode. To disable this feature, use the `no` form of this command.

```plaintext
key  key-id
no  key  key-id
```

**infinite** (Optional) Specifies that the tolerance specification is infinite. The accept key never expires. The tolerance limit of infinite indicates that an accept key is always acceptable and validated when used by a peer.

**Command Default**
The default value is 0, which is no tolerance.

**Command Modes**
Keychain configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you do not configure the `accept-tolerance` command, the tolerance value is set to zero.

Even though the key is outside the active lifetime, the key is deemed acceptable as long as it is within the tolerance limit (for example, either prior to the start of the lifetime, or after the end of the lifetime).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to use the `accept-tolerance` command:

```plaintext
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime, on page 95</td>
<td>Accepts the valid key.</td>
</tr>
<tr>
<td>key chain (key chain), on page 98</td>
<td>Creates or modifies a keychain.</td>
</tr>
<tr>
<td>show key chain, on page 102</td>
<td>Displays the keychain.</td>
</tr>
</tbody>
</table>
key chain (key chain)

To create or modify a keychain, use the `key chain` command. To disable this feature, use the `no` form of this command.

```
key chain  key-chain-name
```
no key chain key-chain-name

**Syntax Description**

*key-chain-name* Specifies the name of the keychain. The maximum number of characters is 48.

**Command Default**

No default behavior or values

**Command Modes**

XR Config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure a keychain for Border Gateway Protocol (BGP) as a neighbor, session group, or neighbor group. BGP can use the keychain to implement a hitless key rollover for authentication.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the name of the keychain isis-keys is for the `key chain` command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime, on page 95</td>
<td>Accepts the valid key.</td>
</tr>
<tr>
<td>accept-tolerance, on page 96</td>
<td>Configures a tolerance value to accept keys for the keychain.</td>
</tr>
<tr>
<td>key (key chain), on page 97</td>
<td>Creates or modifies a keychain key.</td>
</tr>
<tr>
<td>key-string (keychain), on page 100</td>
<td>Specifies the text for the key string.</td>
</tr>
<tr>
<td>send-lifetime, on page 101</td>
<td>Sends the valid key.</td>
</tr>
<tr>
<td>show key chain, on page 102</td>
<td>Displays the keychain.</td>
</tr>
</tbody>
</table>
key-string (keychain)

To specify the text string for the key, use the **key-string** command in keychain-key configuration mode. To disable this feature, use the **no** form of this command.

```
key-string  [{clear|password}]  key-string-text
no  key-string  [{clear|password}]  key-string-text
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>clear</th>
<th>Specifies the key string in clear-text form.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>password</td>
<td>Specifies the key in encrypted form.</td>
</tr>
<tr>
<td>key-string-text</td>
<td></td>
<td>Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Plain-text key strings—Minimum of 1 character and a maximum of 32.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encrypted key strings—Minimum of 4 characters and no maximum.</td>
</tr>
</tbody>
</table>

**Command Default**
The default value is clear.

**Command Modes**
Keychain-key configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimals.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

- **1234abcd**
- **or**
- **50aefd**
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to use the `keystring` command:

```
RP/0/RP0/CPU0:router:# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aeFD
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime, on page 95</td>
<td>Accepts the valid key.</td>
</tr>
<tr>
<td>key (key chain), on page 97</td>
<td>Creates or modifies a keychain key.</td>
</tr>
<tr>
<td>key chain (key chain), on page 98</td>
<td>Creates or modifies a keychain.</td>
</tr>
<tr>
<td>send-lifetime, on page 101</td>
<td>Sends the valid key.</td>
</tr>
<tr>
<td>show key chain, on page 102</td>
<td>Displays the keychain.</td>
</tr>
</tbody>
</table>

### send-lifetime

To send the valid key and to authenticate information from the local host to the peer, use the `send-lifetime` command in keychain-key configuration mode. To disable this feature, use the `no` form of this command.

```
send-lifetime start-time [{duration duration value|infinite|end-time}]
no send-lifetime start-time [{duration duration value|infinite|end-time}]
```

### Syntax Description

- **start-time**
  
  Start time, in `hh:mm:ss day month year` format, in which the key becomes valid. The range is from 0:0:0 to 23:59:59. The range for the number of days of the month to start is from 1 to 31. The range for the years is from 1993 to 2035.

- **duration**
  
  Duration value (Optional) Determines the lifetime of the key in seconds.

- **infinite**
  
  (Optional) Specifies that the key never expires once it becomes valid.

- **end-time**
  
  (Optional) Time, in `hh:mm:ss day month year` format, after which the key expires. The range is from 0:0:0 to 23:59:59

### Command Default

No default behavior or values.
Command Modes

Keychain-key configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to use the `send-lifetime` command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime, on page 95</td>
<td>Accepts the valid key.</td>
</tr>
<tr>
<td>key (key chain), on page 97</td>
<td>Creates or modifies a keychain key.</td>
</tr>
<tr>
<td>key chain (key chain), on page 98</td>
<td>Creates or modifies a keychain.</td>
</tr>
<tr>
<td>key-string (keychain), on page 100</td>
<td>Specifies the text for the key string.</td>
</tr>
</tbody>
</table>

show key chain

To display the keychain, use the `show key chain` command.

```
show key chain key-chain-name
```

Syntax Description

`key-chain-name` Names of the keys in the specified keychain. The maximum number of characters is 32.

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

XR EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

When a secure key storage becomes available, it is desirable for keychain management to alternatively prompt you for a master password and display the key label after decryption. The following example displays only the encrypted key label for the **show key chain** command:

```
RP/0/RP0/CPU0:router# show key chain isis-keys
Key-chain: isis-keys/ -
accept-tolerance -- infinite
Key 8 -- text "8"
cryptographic-algorithm -- MD5
Send lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime, on page 95</td>
<td>Accepts the valid key.</td>
</tr>
<tr>
<td>accept-tolerance, on page 96</td>
<td>Configures a tolerance value to accept keys for the keychain.</td>
</tr>
<tr>
<td>key (key chain), on page 97</td>
<td>Creates or modifies a keychain key.</td>
</tr>
<tr>
<td>key chain (key chain), on page 98</td>
<td>Creates or modifies a keychain.</td>
</tr>
<tr>
<td>key-string (keychain), on page 100</td>
<td>Specifies the text for the key string.</td>
</tr>
<tr>
<td>send-lifetime, on page 101</td>
<td>Sends the valid key.</td>
</tr>
</tbody>
</table>
show key chain
Lawful Intercept Commands

This module describes the Cisco IOS XR software commands used to configure lawful intercept (LI).

For detailed information about keychain management concepts, configuration tasks, and examples, see the Implementing Lawful Intercept in the Configuration Module.

- lawful-intercept disable, on page 105
- overlap-tap enable, on page 106

lawful-intercept disable

To disable the Lawful Intercept (LI) feature, use the lawful-intercept disable command. To re-enable the LI feature, use the no form of this command.

lawful-intercept disable
no lawful-intercept disable

Syntax Description
This command has no keywords or arguments.

Command Default
LI feature is enabled by default only if the LI package is installed.

Command Modes
XR Config

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you disable lawful intercept, all Mediation Devices and associated TAPs are deleted.

To enable this command, you must install and activate the.
**overlaps-tap enable**

To configure traffic interception separately for two inter-communicating intercepted hosts, use the `overlap-tap enable` command in XR Config mode. To revert to the default configuration, use the `no` form of this command.

```
overlap-tap enable
no overlap-tap enable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

For two inter-communicating hosts where both the hosts are separately intercepted, only the ingress traffic on the ASR 9000 router related to one of the hosts is intercepted.

**Command Modes**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use `overlap-tap enable` command, you must have lawful intercept configured by installing and activating `asr9k-li-px.pie`.

**Example**

The following example shows how to configure interception of both the ingress and egress traffic on the ASR 9000 router related to two inter-communicating hosts.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# overlap-tap enable
```
Management Plane Protection Commands

This module describes the commands used to configure management plane protection (MPP).

For detailed information about keychain management concepts, configuration tasks, and examples, see the Implementing Management Plane Protection on module in the System Security Configuration Guide for Cisco NCS 6000 Series Routers.

- address ipv4 (MPP), on page 107
- allow, on page 108
- control-plane, on page 110
- inband, on page 111
- interface (MPP), on page 112
- management-plane, on page 113
- out-of-band, on page 114
- show mgmt-plane, on page 115
- vrf (MPP), on page 117

address ipv4 (MPP)

To configure the peer IPv4 address in which management traffic is allowed on the interface, use the address ipv4 command in interface peer configuration mode. To remove the IP address that was previously configured on this interface, use the no form of this command.

**Syntax Description**

```
peer-ip-address
```

Peer IPv4 address in which management traffic is allowed on the interface. This address can effectively be the source address of the management traffic that is coming in on the configured interface.

```
peer ip-address/length
```

Prefix of the peer IPv4

- IPv4—A.B.C.D/length

**Command Default**

If no specific peer is configured, all peers are allowed.

**Command Modes**

Interface peer configuration
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure the peer address for management traffic:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RP0/CPU0:router(config-mpp-inbandoutband-all)# allow all peer
RP/0/RP0/CPU0:router(config-telnettftp-peer)# address ipv4 10.1.0.0/16
```

allow

To configure an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols, use the `allow` command in management plane protection inband interface configuration mode or management plane protection out-of-band interface configuration. To disallow a protocol on an interface, use the `no` form of this command.

```
allow {protocol|all} [peer]
no allow {protocol|all} [peer]
```

Syntax Description

- **protocol**: Interface configured to allow peer-filtering for the following specified protocol’s traffic:
  - HTTP(S)
  - SNMP (also versions)
  - Secure Shell (v1 and v2)
  - TFTP
  - Telnet
  - XML

- **all**: Configures the interface to allow peer-filtering for all the management traffic that is specified in the list of protocols.

- **peer** (Optional): Configures the peer address on the interface. Peer refers to the neighboring router interface in which traffic might arrive to the main router.

Command Default

By default, no management protocol is allowed on any interface except the management interfaces.

Command Modes

Management plane protection inband interface configuration
Management Plane Protection Commands

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you permit or allow a specific protocol to an interface, traffic is allowed only for that protocol, and all other management traffic is dropped.

After you configure the interface as inband or out-of-band, the specified protocol's traffic, or all protocol traffic, is allowed on the interface. Interfaces that are not configured as inband or out-of-band interfaces, drop the protocol traffic.

The IOS XR XML API provides a programmatic interface to the router for use by external management applications. This interface provides a mechanism for router configuration and monitoring utilizing XML formatted request and response streams. As one of the management services, XML should be capable of applying MPP. To secure XML MPP data, XML keyword has been added to the command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure all management protocols for all inband interfaces:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# control-plane
RP/0/RP0/CPU0:router (config-ctrl)# management-plane
RP/0/RP0/CPU0:router (config-mpp)# inband
RP/0/RP0/CPU0:router (config-mpp-inband)# interface all
RP/0/RP0/CPU0:router (config-mpp-inband-all)# allow all
```

The following example shows how to configure peer interface for the TFTP protocol for out-of-band interfaces:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# control-plane
RP/0/RP0/CPU0:router (config-ctrl)# management-plane
RP/0/RP0/CPU0:router (config-mpp)# out-of-band
RP/0/RP0/CPU0:router (config-mpp-outband)# interface GigabitEthernet 0/1/1/2
RP/0/RP0/CPU0:router (config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RP0/CPU0:router (config-tftp-peer)#
```

The following example shows how to configure MPP support on an XML peer in-band interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# control-plane
RP/0/RP0/CPU0:router (config-ctrl)# management-plane
RP/0/RP0/CPU0:router (config-ctrl-mpp)# inband interface all allow xml peer address ipv4 172.10.10.1
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control-plane, on page 110</td>
<td>Configures the control plane.</td>
</tr>
<tr>
<td>inband, on page 111</td>
<td>Configures an inband interface or protocol.</td>
</tr>
<tr>
<td>interface (MPP), on page 112</td>
<td>Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.</td>
</tr>
<tr>
<td>management-plane, on page 113</td>
<td>Configures management plane protection to allow and disallow protocols.</td>
</tr>
<tr>
<td>out-of-band, on page 114</td>
<td>Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.</td>
</tr>
<tr>
<td>show mgmt-plane, on page 115</td>
<td>Displays the management plane.</td>
</tr>
</tbody>
</table>

**control-plane**

To enter the control plane configuration mode, use the `control-plane` command. To disable all the configurations under control plane mode, use the `no` form of this command.

```
control-plane
no control-plane
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR Config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `control-plane` command to enter control plane configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter control plane configuration mode using the `control-plane` command:
### inband

To configure an inband interface and to enter management plane protection inband configuration mode, use the `inband` command in management plane protection configuration mode. To disable all configurations under inband configuration mode, use the `no` form of this command.

```
inband
no inband
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

Management plane protection configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `inband` command to enter management plane protection inband configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter management plane protection inband configuration mode using the `inband` command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)#
```
**interface (MPP)**

To configure a specific interface or all interfaces as an inband or out-of-band interface, use the `interface` command in management plane protection inband configuration mode or management plane protection out-of-band configuration mode. To disable all the configurations under an interface mode, use the `no` form of this command.

```
interface {type interface-path-id|all}
no interface {type interface-path-id|all}
```

### Syntax Description

- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Virtual interface instance. Number range varies depending on interface type.

**Note** Use the `show interfaces` command in EXEC 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.

```
all Configures all interfaces to allow for management traffic.
```

### Command Default

None

### Command Modes

Management plane protection out-of-band configuration

### Command History

**Release** Modification

Release 5.0.0 This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `interface` command to enter management plane protection inband interface configuration mode or management plane protection out-of-band interface configuration mode.
For the *instance* argument, you cannot configure Management Ethernet interfaces as inband interfaces.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure all inband interfaces for MPP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# inband
RP/0/RP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RP0/CPU0:router(config-mpp-inband-all)#
```

The following example shows how to configure all out-of-band interfaces for MPP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)# interface all
RP/0/RP0/CPU0:router(config-mpp-outband-all)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow, on page 108</td>
<td>Configures an interface as an inband or out-of-band interface to allow all peer addresses for a specified protocol or all protocols.</td>
</tr>
<tr>
<td>control-plane, on page 110</td>
<td>Configures the control plane.</td>
</tr>
<tr>
<td>inband, on page 111</td>
<td>Configures an inband interface or protocol.</td>
</tr>
<tr>
<td>management-plane, on page 113</td>
<td>Configures management plane protection to allow and disallow protocols.</td>
</tr>
<tr>
<td>out-of-band, on page 114</td>
<td>Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.</td>
</tr>
<tr>
<td>show mgmt-plane, on page 115</td>
<td>Displays the management plane.</td>
</tr>
</tbody>
</table>

---

**management-plane**

To configure management plane protection to allow and disallow protocols, use the `management-plane` command in control plane configuration mode. To disable all configurations under management-plane mode, use the `no` form of this command.

```
management-plane  no management-plane
```
Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Control plane configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the management-plane command to enter the management plane protection configuration mode.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enter management plane protection configuration mode using the management-plane command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
```

out-of-band

To configure out-of-band interfaces or protocols and to enter management plane protection out-of-band configuration mode, use the out-of-band command in management plane protection configuration mode. To disable all configurations under management plane protection out-of-band configuration mode, use the no form of this command.

```
out-of-band
no out-of-band
```

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Management plane protection out-of-band configuration
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `out-of-band` command to enter management plane protection out-of-band configuration mode.

*Out-of-band* refers to an interface that allows only management protocol traffic to be forwarded or processed. An *out-of-band management interface* is defined by the network operator to specifically receive network management traffic. The advantage is that forwarding (or customer) traffic cannot interfere with the management of the router.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to enter management plane protection out-of-band configuration mode using the `out-of-band` command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)#
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control-plane, on page 110</td>
<td>Configures the control plane.</td>
</tr>
<tr>
<td>inband, on page 111</td>
<td>Configures an inband interface or protocol.</td>
</tr>
<tr>
<td>interface (MPP), on page 112</td>
<td>Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.</td>
</tr>
<tr>
<td>management-plane, on page 113</td>
<td>Configures management plane protection to allow and disallow protocols.</td>
</tr>
<tr>
<td>show mgmt-plane, on page 115</td>
<td>Displays the management plane.</td>
</tr>
<tr>
<td>vrf (MPP), on page 117</td>
<td>Configures a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface.</td>
</tr>
</tbody>
</table>

**show mgmt-plane**

To display information about the management plane such as type of interface and protocols enabled on the interface, use the `show mgmt-plane` command.
show mgmt-plane [{inband|out-of-band}] [{interface type interface-path-id|vrf}]

Syntax Description

inband  (Optional) Displays the inband management interface configurations that are the interfaces that process management packets as well as data-forwarding packets. An inband management interface is also called a shared management interface.

out-of-band  (Optional) Displays the out-of-band interface configurations. Out-of-band interfaces are defined by the network operator to specifically receive network management traffic.

interface  (Optional) Displays all the protocols that are allowed in the specified interface.

type  Interface type. For more information, use the question mark (?) online help function.

interface-path-id  Interface instance. Number range varies depending on interface type.

Note  Use the show interfaces command 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  (Optional) Displays the Virtual Private Network (VPN) routing and forwarding reference of an out-of-band interface.

Command Default  None

Command Modes  XR EXEC

Command History

Release 5.0.0  This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The vrf keyword is valid only for out-of-band VRF configurations.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following sample output displays all the interfaces that are configured as inband or out-of-band interfaces under MPP:

RP/0/RP0/CPU0:router# show mgmt-plane

Management Plane Protection

inband interfaces
------------------------
interface - GigabitEthernet0_1_1_0
  ssh configured -
    All peers allowed
telnet configured -
  peer v4 allowed - 10.1.0.0/16
  all configured -
    All peers allowed
interface - GigabitEthernet0_1_1_0
telnet configured -
  peer v4 allowed - 10.1.0.0/16
interface - all
  all configured -
    All peers allowed

outband interfaces
----------------------
interface - GigabitEthernet0_1_1_0
tftp configured -
  peer v6 allowed - 33::33

The following sample output displays the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface:

RP/0/RP0/CPU0:router# show mgmt-plane out-of-band vrf
Management Plane Protection -
  out-of-band VRF - my_out_of_band

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf (MPP)</td>
<td>management-plane, on page 113</td>
<td>Configures management plane protection to allow and disallow protocols.</td>
</tr>
</tbody>
</table>

vrf (MPP)

To configure a Virtual Private Network (VPN) routing and forwarding (VRF) reference of an out-of-band interface, use the vrf command in management plane protection out-of-band configuration mode. To remove the VRF definition before the VRF name is used, 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 VRF concept must be used to configure interfaces as out-of-band. If no VRF is configured during an out-of-band configuration, the interface goes into a default VRF.

**Command Modes**

Management plane protection out-of-band configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the VRF reference is not configured, the default name MPP_OUTBAND_VRF is used.

If there is an out-of-band configuration that is referring to a VRF and the VRF is deleted, all the MPP bindings are removed.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>system read</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure the VRF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# vrf my_out_of_band
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# exit
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# commit
RP/0/RP0/CPU0:router(config-vrf-af)# end
RP/0/RP0/CPU0:router#
```

The following example shows how to configure the VRF definition for MPP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# control-plane
RP/0/RP0/CPU0:router(config-ctrl)# management-plane
RP/0/RP0/CPU0:router(config-mpp)# out-of-band
RP/0/RP0/CPU0:router(config-mpp-outband)# vrf my_out_of_band
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control-plane, on page 110</td>
<td>Configures the control plane.</td>
</tr>
<tr>
<td>interface (MPP), on page 112</td>
<td>Configures a specific inband or out-of-band interface or all inband or out-of-band interfaces.</td>
</tr>
<tr>
<td>management-plane, on page 113</td>
<td>Configures management plane protection to allow and disallow protocols.</td>
</tr>
<tr>
<td>out-of-band, on page 114</td>
<td>Configures out-of-band interfaces or protocols and enters management plane protection out-of-band configuration mode.</td>
</tr>
<tr>
<td>show mgmt-plane, on page 115</td>
<td>Displays the management plane.</td>
</tr>
</tbody>
</table>
Public Key Infrastructure Commands

This module describes the commands used to configure Public Key Infrastructure (PKI).

For detailed information about PKI concepts, configuration tasks, and examples, see the Implementing Certification Authority Interoperability on module in the System Security Configuration Guide for Cisco NCS 6000 Series Routers.

- clear crypto ca certificates, on page 120
- clear crypto ca crl, on page 121
- crl optional (trustpoint), on page 122
- crypto ca authenticate, on page 123
- crypto ca cancel-enroll, on page 124
- crypto ca enroll, on page 125
- crypto ca import, on page 126
- crypto ca trustpoint, on page 127
- crypto ca trustpool import url, on page 129
- crypto ca trustpool policy, on page 130
- crypto key generate dsa, on page 131
- crypto key generate ecdsa, on page 132
- crypto key generate rsa, on page 133
- crypto key import authentication rsa, on page 134
- crypto key zeroize dsa, on page 135
- crypto key zeroize ecdsa, on page 136
- crypto key zeroize rsa, on page 136
- description (trustpoint), on page 138
- enrollment retry count, on page 138
- enrollment retry period, on page 140
- enrollment terminal, on page 141
- enrollment url, on page 142
- ip-address (trustpoint), on page 143
- query url, on page 145
- rsakeypair, on page 146
- serial-number (trustpoint), on page 147
- sftp-password (trustpoint), on page 148
- sftp-username (trustpoint), on page 149
- subject-name (trustpoint), on page 150
clear crypto ca certificates

To clear certificates associated with trustpoints that no longer exist in the configuration file, use the clear crypto ca certificates command.

```
clear crypto ca certificates trustpoint
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustpoint</td>
<td>Trustpoint name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

Release 5.0.0  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the router is loaded with a new configuration file and certificates in the new configuration file do not have their corresponding trustpoint configuration, use the clear crypto ca certificates command to clear the certificates associated with trustpoints that no longer exist in the configuration file.

The clear crypto ca certificates command deletes both certification authority (CA) and router certificates from the system.

**Examples**

The following example shows how to clear the certificates associated with trustpoints that no longer exist in the configuration file:

```
RP/0/RP0/CPU0:router# clear crypto ca certificates tp_1
```
clear crypto ca crl

To clear all the Certificate Revocation Lists (CRLs) stored on the router, use the `clear crypto ca crl` command.

```
clear crypto ca crl
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `clear crypto ca crl` command to clear all CRLs stored on the router. As a result, the router goes through the certification authorities (CAs) to download new CRLs for incoming certificate validation requests.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear all CRLs stored on the router:

```
RP/0/RP0/CPU0:router# show crypto ca crls
CRL Entry
-----------------------------------------------
Issuer : cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
Last Update : [UTC] Wed Jun 5 02:40:04 2002
Next Update : [UTC] Wed Jun 5 03:00:04 2002
CRL Distribution Point :
ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

RP/0/RP0/CPU0:router# clear crypto ca crl
RP/0/RP0/CPU0:router# show crypto ca crls
RP/0/RP0/CPU0:router#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ca crls, on page 153</td>
<td>Displays the information about CRLs on the router.</td>
</tr>
</tbody>
</table>
crl optional (trustpoint)

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the `crl optional` command in trustpoint configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the `no` form of this command.

```
crl optional
no crl optional
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The router must have and check the appropriate CRL before accepting the certificate of another IP security peer.

**Command Modes**

Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When your router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. If the certificate appears on the CRL, your router cannot accept the certificate and will not authenticate the peer. To instruct the router not to download the CRL and treat the certificate as not revoked, use the `crl optional` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RP0/CPU0:router(config-trustp)# crl optional
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpoint, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td>enrollment retry count, on page 138</td>
<td>Specifies how many times a router resends a certificate request.</td>
</tr>
<tr>
<td>enrollment retry period, on page 140</td>
<td>Specifies the wait period between certificate request retries.</td>
</tr>
<tr>
<td>enrollment url, on page 142</td>
<td>Specifies the URL of the CA.</td>
</tr>
</tbody>
</table>

crypto ca authenticate

To authenticate the certification authority (CA) by getting the certificate for the CA, use the `crypto ca authenticate` command.

```
crypto ca authenticate ca-name
```

**Syntax Description**

- `ca-name`  Name of the CA Server.

**Command Default**
None

**Command Modes**
XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `crypto ca authenticate` command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the CA certificate, which contains the public key for the CA. For self-signed root CA, because the CA signs its own certificate, you should manually authenticate the CA public key by contacting the CA administrator when you use this command. The certificate fingerprint matching is done out-of-band (for example, phone call, and so forth).

Authenticating a second-level CA requires prior authentication of the root CA.

After the `crypto ca authenticate` command is issued and the CA does not respond by the specified timeout period, you must obtain terminal control again to re-enter the command.
The CA sends the certificate, and the router prompts the administrator to verify the certificate by checking the certificate fingerprint (a unique identifier). The CA administrator can also display the CA certificate fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the display matches the fingerprint displayed by the CA administrator, you should accept the certificate as valid.

The following example shows that the router requests the CA certificate:

```
RP/0/RP0/CPU0:router# crypto ca authenticate msiox
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Subject:  
    Name: CA2
    CN= CA2
  Issued By :
    cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
    http://10.56.8.236/CertEnroll/CA2.crl
  Certificate has the following attributes:
    Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

Do you accept this certificate? [yes/no]: yes
```

```
RP/0/RP0/CPU0:router# Apr 10 00:28:52.324 : cepki[335]: %SECURITY-CEPKI-6-INFO : certificate database updated
Do you accept this certificate? [yes/no] yes
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpoint, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td>show crypto ca certificates, on page 151</td>
<td>Displays information about your certificate and the certificate of the CA.</td>
</tr>
</tbody>
</table>

### crypto ca cancel-enroll

To cancel a current enrollment request, use the `crypto ca cancel-enroll` command.

```
crypto ca cancel-enroll ca-name
```

**Syntax Description**

- `ca-name`  
  Name of the certification authority (CA).

**Command Default**  
None

**Command Modes**  
XR EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 5.0.0 | This command was introduced.  

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto ca enroll` command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the `rsakeypair, on page 146` command in trustpoint configuration mode. If no `rsakeypair, on page 146` command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. Use the `crypto ca cancel-enroll` command to cancel a current enrollment request.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to cancel a current enrollment request from a CA named `myca`:

```
RP/0/RP0/CPU0:router# crypto ca cancel-enroll myca
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ca enroll, on page 125</code></td>
<td>Obtains a router certificate from the CA.</td>
</tr>
<tr>
<td><code>rsakeypair, on page 146</code></td>
<td>Specifies a named RSA key pair for a trustpoint.</td>
</tr>
</tbody>
</table>

**crypto ca enroll**

To obtain a router certificate from the certification authority (CA), use the `crypto ca enroll` command.

```
crypto ca enroll ca-name
```

Syntax Description

- `ca-name` Name of the CA Server.

Command Default

None

Command Modes

XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 5.0.0 | This command was introduced.  

System Security Command Reference for Cisco NCS 6000 Series Routers
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto ca enroll` command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the `rsakeypair`, on page 146 command in trustpoint configuration mode. If no `rsakeypair`, on page 146 command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. (Enrolling and obtaining certificates are two separate events, but they both occur when the `crypto ca enroll` command is issued.) When using manual enrollment, these two operations occur separately.

The router needs a signed certificate from the CA for each of the RSA key pairs on the router; if you previously generated general-purpose keys, this command obtains the one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special-usage keys, this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for your keys, you are unable to configure this command; instead, you are prompted to remove the existing certificate first. (You can remove existing certificates by removing the trustpoint configuration with the `no crypto ca trustpoint` command.)

The `crypto ca enroll` command is not saved in the router configuration.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

### Examples

The following sample output is from the `crypto ca enroll` command:

```
RP/0/RP0/CPU0:router# crypto ca enroll msiox
% Start certificate enrollment...
% Create a challenge password. You will need to verbally provide this password to the
% CA Administrator in order to revoke your certificate.
% For security reasons you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7
RP/0/RP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ca trustpoint</code>, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td><code>rsakeypair</code>, on page 146</td>
<td>Specifies a named RSA key pair for a trustpoint.</td>
</tr>
</tbody>
</table>

### crypto ca import

To import a certification authority (CA) certificate manually through TFTP, SFTP, or cut and paste it at the terminal, use the `crypto ca import` command.
**crypto ca import** name certificate

**Syntax Description**

| name | Name of the certification authority (CA). This name is the same name used when the CA was declared with the **crypto ca trustpoint**, on page 127 command. |
| certificate |  |

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to import a CA certificate through cut-and-paste. In this example, the certificate is myca.

```
RP/0/RP0/CPU0:router# crypto ca import myca certificate
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpoint, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td>show crypto ca certificates, on page 151</td>
<td>Displays information about your certificate and the certification authority (CA) certificate.</td>
</tr>
</tbody>
</table>

---

**crypto ca trustpoint**

To configure a trusted point with a selected name, use the **crypto ca trustpoint** command. To unconfigure a trusted point, use the **no** form of this command.

```
crypto ca trustpoint ca-name
no crypto ca trustpoint ca-name
```

**Syntax Description**

| ca-name | Name of the CA. |
**Command Default**
None

**Command Modes**
XR Config

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto ca trustpoint` command to declare a CA.

This command allows you to configure a trusted point with a selected name so that your router can verify certificates issued to peers. Your router need not enroll with the CA that issued the certificates to the peers.

The `crypto ca trustpoint` command enters trustpoint configuration mode, in which you can specify characteristics for the CA with the following commands:

- `crl optional (trustpoint), on page 122` command—The certificates of other peers are accepted without trying to obtain the appropriate CRL.
- `enrollment retry count, on page 138` command—The number of certificate request retries your router sends before giving up. Optional.
- `enrollment retry period, on page 140` command—(Optional)—The time the router waits between sending certificate request retries.
- `enrollment url, on page 142` command—(Optional)—The URL of the CA.
- `ip-address (trustpoint), on page 143`command—A dotted IP address that is included as an unstructured address in the certificate request.
- `query url, on page 145`command—The directory server URL in which the Certificate Revocation List (CRL) is published. Only a string that begins with “ldap://” is accepted. Required only if your CA supports Lightweight Directory Access Protocol (LDAP).
- `rsakeypair, on page 146`command—The named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint.
- `serial-number (trustpoint), on page 147`command—Router serial number in the certificate request.
- `sftp-password (trustpoint), on page 148`command—FTP secure password.
- `sftp-username (trustpoint), on page 149`command—FTP secure username.
- `subject-name (trustpoint), on page 150`command—Subject name in the certificate request.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to use the `crypto ca trustpoint` command to create a trustpoint:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RP0/CPU0:router(config-trustp)# sftp-password xxxxxx
RP/0/RP0/CPU0:router(config-trustp)# sftp-username tmordeko
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crl optional (trustpoint), on page 122</td>
<td>Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.</td>
</tr>
<tr>
<td>enrollment retry count, on page 138</td>
<td>Specifies how many times a router resends a certificate request.</td>
</tr>
<tr>
<td>enrollment retry period, on page 140</td>
<td>Specifies the wait period between certificate request retries.</td>
</tr>
<tr>
<td>enrollment url, on page 142</td>
<td>Specifies the URL of the CA.</td>
</tr>
<tr>
<td>query url, on page 145</td>
<td>Specifies the LDAP URL of the CRL distribution point.</td>
</tr>
<tr>
<td>rsakeypair, on page 146</td>
<td>Specifies a named RSA key pair for this trustpoint.</td>
</tr>
<tr>
<td>sftp-password (trustpoint), on page 148</td>
<td>Secures the FTP password.</td>
</tr>
<tr>
<td>sftp-username (trustpoint), on page 149</td>
<td>Secures the FTP username.</td>
</tr>
</tbody>
</table>

**crypto ca trustpool import url**

To manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated, use the `crypto ca trustpool import url` command.

```
crypto ca trustpool import url {cleanURL}
```

**Syntax Description**

`clean` (Optional) Manually remove all downloaded certificate authority (CA) certificates.

`URL` Specify the URL from which the CA trust pool certificate bundle must be downloaded. This manually imports (downloads) the CA certificate bundle into the CA trust pool to update or replace the existing CA certificate bundle.

**Command Default**

The CA trust pool feature is enabled. The router uses the built-in CA certificate bundle in the CA trust pool which is updated automatically from Cisco.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
The CA trust pool feature is enabled by default and uses the built-in CA certificate bundle in the trust pool, which receives automatic updates from Cisco. Use the `crypto ca trustpool import url` command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

### Example
This example shows how to run the command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

```
RP/0/RSP0/CPU0:IMC0#crypto ca trustpool import url
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show crypto ca trustpool policy</td>
<td>Display the CA trust pool certificates of the router in a verbose format.</td>
</tr>
<tr>
<td>crypto ca trustpool policy</td>
<td>Configure CA trust pool policy parameters.</td>
</tr>
</tbody>
</table>

---

**crypto ca trustpool policy**

To configure certificate authority (CA) trust pool policy, use the `crypto ca trustpool policy` command.

```
crypto ca trustpool policy {cabundle url url|crl optional|description line}
```

### Syntax Description

- **cabundle url**: Configures the URL from which the CA trust pool bundle is downloaded.
- **crl optional**: To specify the certificate revocation list (CRL) query for the CA trust pool, use the `crl` command in ca-trustpool configuration mode. By default, the router enforces a check of the revocation status of the certificate by querying the certificate revocation list (CRL). Setting this to optional disables revocation checking when the trust pool policy is in use.

- **description line**: Indicates the description for the trust pool policy.

### Command Default

The default CA trust pool policy is used.

### Command Modes

XR Config

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `crypto ca trustpool policy` command enters ca-trustpool configuration mode, where commands can be accessed to configure certificate authority (CA) trustpool policy parameters.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>READ,</td>
<td>WRITE</td>
</tr>
</tbody>
</table>

Example

This example shows you how to disable certificate revocation checks when the trust pool policy is in use.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:IMC0(config)#crypto ca trustpool policy
RP/0/RSP0/CPU0:IMC0(config-trustpool)#crl optional
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpool import url, on page 129</td>
<td>Allows you to manually update certificates in the trust pool.</td>
</tr>
<tr>
<td>show crypto ca trustpool policy, on page 154</td>
<td>Displays the CA trust pool certificates of the router in a verbose format.</td>
</tr>
</tbody>
</table>

**crypto key generate dsa**

To generate Digital Signature Algorithm (DSA) key pairs, use the `crypto key generate dsa` command.

```
crypto key generate dsa
```

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto key generate dsa` command to generate DSA key pairs for your router.
DSA keys are generated in pairs—one public DSA key and one private DSA key.

If your router already has DSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys.

To remove the DSA key generated, use the `crypto key zeroize dsa` command.

### Task ID

| Task ID | Operations
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to generate a 512-bit DSA key:

```
RP/0/RP0/CPU0:router# crypto key generate dsa
The name for the keys will be: the_default
  Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
  How many bits in the modulus [1024]: 512
  Generating DSA keys...
  Done w/ crypto generate keypair
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto key zeroize dsa</code>, on page 135</td>
<td>Deletes a DSA key pair from your router.</td>
</tr>
<tr>
<td><code>show crypto key mypubkey dsa</code>, on page 155</td>
<td>Displays the DSA public keys for your router.</td>
</tr>
</tbody>
</table>

## crypto key generate ecdsa

To generate an Elliptic Curve Digital Signature Algorithm (ECDSA) key pair, use the `crypto key generate ecdsa` command.

```
crypto key generate ecdsa [ nistp256 | nistp384 | nistp521 ]
```

### Syntax Description

- **nistp256**: Generates an ECDSA key of curve type nistp256, with key size 256 bits.
- **nistp384**: Generates an ECDSA key of curve type nistp384, with key size 384 bits.
- **nistp521**: Generates an ECDSA key of curve type nistp521, with key size 521 bits.

### Command Default

None

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To remove an ECDSA key, use the `crypto key zeroize ecdsa` command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

Example

The following example shows how to generate an ECDSA key pair:

```
RP/0/RP0/CPU0:router# crypto key generate ecdsa nistp384
Wed Mar 28 12:53:57.355 UTC
% You already have keys defined for the_default
Do you really want to replace them? [yes/no]: yes
Generating ECDSA keys ...
Done w/ crypto generate ECDSA keypair [OK]
```

crypto key generate rsa

To generate a Rivest, Shamir, and Adelman (RSA) key pair, use the `crypto key generate rsa` command.

`crypto key generate rsa` 

Syntax Description

- `usage-keys` (Optional) Generates separate RSA key pairs for signing and encryption.
- `general-keys` (Optional) Generates a general-purpose RSA key pair for signing and encryption.
- `keypair-label` (Optional) RSA key pair label that names the RSA key pairs.

Command Default

RSA key pairs do not exist. If the `usage-keys` keyword is not used, general-purpose keys are generated. If no RSA label is specified, the key is generated as the default RSA key.

Command Modes

XR EXEC

Command History

- **Release** 5.0.0  This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto key generate rsa` command to generate RSA key pairs for your router.

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys. The keys generated by this command are saved in the secure NVRAM (which is not displayed to the user or backed up to another device).
To remove an RSA key, use the `crypto key zeroize rsa` command.

### Examples

The following example shows how to generate an RSA key pair:

```
RP/0/RP0/CPU0:router# crypto key generate rsa
The name for the keys will be: the_default
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[1024]: <return>
RP/0/RP0/CPU0:router#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key zeroize rsa, on page 136</td>
<td>Deletes the RSA key pair for your router.</td>
</tr>
<tr>
<td>show crypto key mypubkey rsa, on page 156</td>
<td>Displays the RSA public keys for your router.</td>
</tr>
</tbody>
</table>

---

### crypto key import authentication rsa

To import a public key using the Rivest, Shamir, and Adelman (RSA) method, use the `crypto key import authentication rsa` command.

```
crypto key import authentication rsa path
```

**Syntax Description**

- `path` (Optional) This denotes the path to the RSA public key file.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

1. Use ssh-keygen generation mechanism to generate keys using either a LINUX or UNIX client. This creates two keys: one public and one private.
2. Remove the comment and other header tag from the keys, except the base64 encoded text.

3. Decode the base64 encoded text, and use the for authentication.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays how to import a public key:

```
RP/0/RP0/CPU0:k2# crypto key import authentication rsa
```

crypto key zeroize dsa

To delete the Digital Signature Algorithm (DSA) key pair from your router, use the `crypto key zeroize dsa` command.

crypto key zeroize dsa

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto key zeroize dsa` command to delete the DSA key pair that was previously generated by your router.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to delete DSA keys from your router:

```
RP/0/RP0/CPU0:router# crypto key zeroize dsa
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```
Related Commands | Command | Description
--- | --- | ---
| crypto key generate dsa, on page 131 | Generates DSA key pairs. |
| show crypto key mypubkey dsa, on page 155 | Displays the DSA public keys for your router. |

---

**crypto key zeroize ecdsa**

To delete the Elliptic Curve Digital Signature Algorithm (ECDSA) key pair from your router, use the `crypto key zeroize ecdsa` command.

`crypto key zeroize ecdsa [ nistp256 | nistp384 | nistp521 ]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nistp256</td>
<td>Deletes an ECDSA key of curve type nistp256, with key size 256 bits.</td>
</tr>
<tr>
<td>nistp384</td>
<td>Deletes an ECDSA key of curve type nistp384, with key size 384 bits.</td>
</tr>
<tr>
<td>nistp521</td>
<td>Deletes an ECDSA key of curve type nistp521, with key size 521 bits.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to delete ECDSA keys from your router:

```
RP/0/RP0/CPU0:router# crypto key zeroize ecdsa nistp384
% Keys to be removed are named the_default
Do you really want to remove these keys ?? [yes/no]: yes
```

**crypto key zeroize rsa**

To delete all Rivest, Shamir, and Adelman (RSA) keys from the router, use the `crypto key zeroize rsa` command.
**crypto key zeroize rsa**

**Syntax Description**

`keypair-label` (Optional) Names the RSA key pair to be removed.

**Command Default**

If the key pair label is not specified, the default RSA key pair is removed.

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `crypto key zeroize rsa` command to delete all RSA keys that were previously generated by the router. After issuing this command, you must perform two additional tasks:

- Ask the certification authority (CA) administrator to revoke the certificates for the router at the CA; you must supply the challenge password you created when you originally obtained the router certificates with the `crypto ca enroll, on page 125` command CA.
- Manually remove the certificates from the configuration using the `clear crypto ca certificates` command.

**Examples**

The following example shows how to delete the general-purpose RSA key pair that was previously generated:

```
RP/0/*CPU0:router# crypto key zeroize rsa key1
% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto ca certificates, on page 120</td>
<td>Clears certificates associated with trustpoints that no longer exist in the configuration file.</td>
</tr>
<tr>
<td>crypto ca enroll, on page 125</td>
<td>Obtains a router certificate from the CA.</td>
</tr>
<tr>
<td>crypto key generate rsa, on page 133</td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td>show crypto key mypubkey rsa, on page 156</td>
<td>Displays the RSA public keys for your router.</td>
</tr>
</tbody>
</table>
description (trustpoint)

To create a description of a trustpoint, use the `description` command in trustpoint configuration mode. To delete a trustpoint description, use the `no` form of this command.

```
description string
no description
```

**Syntax Description**

- `string`  Character string describing the trustpoint.

**Command Default**

The default description is blank.

**Command Modes**

Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `description` command in the trustpoint configuration mode to create a description for a trustpoint.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to create a trustpoint description:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# description this is the primary trustpoint
```

enrollment retry count

To specify the number of times a router resends a certificate request to a certification authority (CA), use the `enrollment retry count` command in trustpoint configuration mode. To reset the retry count to the default, use the `no` form of this command.

```
enrollment retry count number
no enrollment retry count number
```
**Syntax Description**

```
number  Number of times the router resends a certificate request when the router does not receive a certificate from the previous request. The range is from 1 to 100.
```

**Command Default**

If no retry count is specified, the default value is 10.

**Command Modes**

Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

To reset the retry count to the default of 10, use the **no** form of this command. Setting the retry count to 0 indicates an infinite number of retries. The router sends the CA certificate requests until a valid certificate is received (there is no limit to the number of retries).

**Examples**

The following example shows how to declare a CA, change the retry period to 10 minutes, and change the retry count to 60 retries. The router resends the certificate request every 10 minutes until receipt of the certificate or approximately 10 hours pass since the original request was sent, whichever occurs first (10 minutes x 60 tries = 600 minutes = 10 hours).

```bash
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry count 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crt optional (trustpoint), on page 122</code></td>
<td>Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.</td>
</tr>
<tr>
<td><code>crypto ca trustpoint, on page 127</code></td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td><code>enrollment retry period, on page 140</code></td>
<td>Specifies the wait period between certificate request retries.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>enrollment url, on page 142</td>
<td>Specifies the certification authority (CA) location by naming the CA URL.</td>
</tr>
</tbody>
</table>

**enrollment retry period**

To specify the wait period between certificate request retries, use the `enrollment retry period` command in trustpoint configuration mode. To reset the retry period to the default of 1 minute, use the `no` form of this command.

```
enrollment retry period minutes
no enrollment retry period minutes
```

**Syntax Description**

`minutes` Period (in minutes) between certificate requests issued to a certification authority (CA) from the router. The range is from 1 to 60 minutes.

**Command Default**

`minutes: 1`

**Command Modes**

Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

The router sends the CA another certificate request every minute until a valid certificate is received. (By default, the router sends ten requests, but you can change the number of permitted retries with the `enrollment retry count` command.)

**Examples**

The following example shows how to declare a CA and change the retry period to 5 minutes:

```
RP/0/CPU0:router# configure
```
enrollment terminal

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

```
enrollment terminal
no enrollment terminal
```

### Syntax Description
This command has no keywords or arguments.

### Command Default
None

### Command Modes
Trustpoint configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can manually cut and paste certificate requests and certificates when you do not have a network connection between the router and certification authority (CA). When the enrollment terminal command is enabled, the router displays the certificate request on the console terminal, which allows you to enter the issued certificate on the terminal.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples
The following example shows how to manually specify certificate enrollment through cut-and-paste. In this example, the CA trustpoint is myca.

RP/0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/CPU0:router(config-trustp)# enrollment retry period 5
enrollment url

To specify the certification authority (CA) location by naming the CA URL, use the `enrollment url` command in trustpoint configuration mode. To remove the CA URL from the configuration, use the `no` form of this command.

```
enrollment url CA-URL
no enrollment url CA-URL
```

**Syntax Description**

- **CA-URL**
  - URL of the CA server. The URL string must start with `http://CA_name`, where `CA_name` is the host Domain Name System (DNS) name or IP address of the CA (for example, `http://ca-server`).
  - If the CA cgi-bin script location is not `/cgi-bin/pkiclient.exe` at the CA (the default CA cgi-bin script location), you must also include the nonstandard script location in the URL, in the form of `http://CA-name/script-location`, where `script-location` is the full path to the CA scripts.

**Command Default**

None

**Command Modes**

Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 5.0.0    | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `enrollment url` command to specify the CA URL. This command is required when you declare a CA with the `crypto ca trustpoint` command. The URL must include the CA script location if the CA scripts are not loaded into the default cgi-bin script location. The CA administrator should be able to tell you where the CA scripts are located.

This table lists the available enrollment methods.

<table>
<thead>
<tr>
<th>Enrollment Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP</td>
<td>Enroll through SFTP: file system</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ca trustpoint</code>, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
</tbody>
</table>
### Enrollment Method

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP</td>
<td>Enroll through TFTP: filesystem</td>
</tr>
</tbody>
</table>

1. If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file specification is optional.)

TFTP enrollment sends the enrollment request and retrieves the certificate of the CA and the certificate of the router. If the file specification is included in the URL, the router appends an extension to the file specification.

To change the CA URL, repeat the `enrollment url` command to overwrite the previous URL.

### Examples

The following example shows the absolute minimum configuration required to declare a CA:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#
crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)#
enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crl optional</code> (trustpoint)</td>
<td>Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.</td>
</tr>
<tr>
<td><code>crypto ca trustpoint</code></td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td><code>ip-address</code> (trustpoint)</td>
<td>Specifies a dotted IP address that is included as an unstructured address in the certificate request.</td>
</tr>
</tbody>
</table>

### `ip-address` (trustpoint)

To specify a dotted IP address that is included as an unstructured address in the certificate request, use the `ip-address` command in trustpoint configuration mode. To restore the default behavior, use the `no` form of this command.

```
ip-address {ip-address|none}
no ip-address {ip-address|none}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Dotted IP address that is included in the certificate request.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that an IP address is not included in the certificate request.</td>
</tr>
</tbody>
</table>
You are prompted for the IP address during certificate enrollment.

Trustpoint configuration

Release 5.0.0  This command was introduced.

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
RP/0/RP0/CPU0:router(config-trustp)# ip-address none
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crl optional</code> (trustpoint), on page 122</td>
<td>Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.</td>
</tr>
<tr>
<td><code>crypto ca trustpoint</code>, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td><code>enrollment url</code>, on page 142</td>
<td>Specifies the certification authority (CA) location by naming the CA URL.</td>
</tr>
<tr>
<td><code>serial-number</code> (trustpoint), on page 147</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
</tbody>
</table>
query url

To specify Lightweight Directory Access Protocol (LDAP) protocol support, use the `query url` command in trustpoint configuration mode. To remove the query URL from the configuration, use the `no` form of this command.

`query url LDAP-URL`
`no query url LDAP-URL`

**Syntax Description**

`LDAP-URL` URL of the LDAP server (for example, ldap://another-server).

This URL must be in the form of ldap://server-name where server-name is the host Domain Name System (DNS) name or IP address of the LDAP server.

**Command Default**
The URL provided in the router certificate’s CRLDistributionPoint extension is used.

**Command Modes**
Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDAP is a query protocol used when the router retrieves the Certificate Revocation List (CRL). The certification authority (CA) administrator should be able to tell you whether the CA supports LDAP; if the CA supports LDAP, the CA administrator can tell you the LDAP location where certificates and certificate revocation lists should be retrieved.

To change the query URL, repeat the `query url` command to overwrite the previous URL.

**Examples**
The following example shows the configuration required to declare a CA when the CA supports LDAP:

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

To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the `rsakeypair` command in trustpoint configuration mode. To reset the RSA key pair to the default, use the `no` form of this command.

```
rsakeypair  keypair-label
no rsakeypair  keypair-label
```

### Syntax Description
- **keypair-label**  RSA key pair label that names the RSA key pairs.

### Command Default
If the RSA key pair is not specified, the default RSA key is used for this trustpoint.

### Command Modes
- Trustpoint configuration

### Command History
- **Release 5.0.0**  This command was introduced.

### Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `rsakeypair` command to specify a named RSA key pair generated using the `crypto key generate rsa` command for this trustpoint.

### Task ID
- **Task ID**
  - `crypto`  read, write

### Examples
The following example shows how to specify the named RSA key pair `key1` for the trustpoint `myca`:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# rsakeypair key1
```
serial-number (trustpoint)

To specify whether the router serial number should be included in the certificate request, use the `<command>` command in trustpoint configuration mode. To restore the default behavior, use the `no` form of this command.

```
serial-number [none]
no serial-number
```

**Syntax Description**
- `none` (Optional) Specifies that a serial number is not included in the certificate request.

**Command Default**
You are prompted for the serial number during certificate enrollment.

**Command Modes**
Trustpoint configuration

**Command History**
- **Release** 5.0.0  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before you can use the `serial-number` command, you must enable the `crypto ca trustpoint` command, which declares the certification authority (CA) that your router should use and enters trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the `none` keyword to specify that a serial number should not be included in the certificate request.

**Examples**
The following example shows how to omit a serial number from the root certificate request:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RP0/CPU0:router(config-trustp)# ip-address none
RP/0/RP0/CPU0:router(config-trustp)# serial-number none
RP/0/RP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems, C=US
```
sftp-password (trustpoint)

To secure the FTP password, use the `sftp-password` command in trustpoint configuration mode. To disable this feature, use the `no` form of this command.

```
sftp-password {clear text|clear text|password encrypted string}
no sftp-password {clear text|clear text|password encrypted string}
```

**Syntax Description**

- `clear text` Clear text password and is encrypted only for display purposes.
- `password encrypted string` Enters the password in an encrypted form.

**Command Default**
The `clear text` argument is the default behavior.

**Command Modes**
Trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Passwords are stored in encrypted form and not as plain text. The command-line interface (CLI) contains the provisioning (for example, clear and encrypted) to specify the password input.

The username and password are required as part of the SFTP protocol. If you specify the URL that begins with the prefix (`sftp://`), you must configure the parameters for the `sftp-password` command under the trustpoint. Otherwise, the certificate from the SFTP server, which is used for manual certificate enrollment, cannot be retrieved.
Examples

The following example shows how to secure the FTP password in an encrypted form:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint msi0x
RP/0/RP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

sftp-username (trustpoint)

To secure the FTP username, use the **sftp-username** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

```
sftp-username username
no sftp-username username
```

**Syntax Description**

- `username`: Name of the user.

**Command Default**

None

**Command Modes**

Trustpoint configuration

**Command History**

- **Release** 5.0.0  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **sftp-username** command is used only if the URL has (sftp://) in the prefix. If (sftp://) is not specified in the prefix, the manual certificate enrollment using SFTP fails.
subject-name (trustpoint)

To specify the subject name in the certificate request, use the subject-name command in trustpoint configuration mode. To clear any subject name from the configuration, use the no form of this command.

```
snmp-server共同体 PRIV
```

Syntax Description

- **x.500-name** (Optional) Specifies the subject name used in the certificate request.

Command Default

If the `x.500-name` argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, is used.

Command Modes

Trustpoint configuration

Command History

```
Modification  Release
This command was introduced.  5.0.0
```

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before you can use the `subject-name` command, you must enable the `crypto ca trustpoint` command, which declares the certification authority (CA) that your router should use and enters trustpoint configuration mode.

The `subject-name` command is an attribute that can be set for automatic enrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.
The following example shows how to specify the subject name for the frog certificate:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crl optional (trustpoint), on page 122</td>
<td>Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.</td>
</tr>
<tr>
<td>crypto ca trustpoint, on page 127</td>
<td>Configures a trusted point with a selected name.</td>
</tr>
<tr>
<td>enrollment url, on page 142</td>
<td>Specifies the certification authority (CA) location by naming the CA URL.</td>
</tr>
<tr>
<td>ip-address (trustpoint), on page 143</td>
<td>Specifies a dotted IP address that is included as an unstructured address in the certificate request.</td>
</tr>
<tr>
<td>serial-number (trustpoint), on page 147</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
</tbody>
</table>

### show crypto ca certificates

To display information about your certificate and the certification authority (CA) certificate, use the `show crypto ca certificates` command.

```
show crypto ca certificates
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show crypto ca certificates` command to display information about the following certificates:

- Your certificate, if you have requested one from the CA (see the `crypto ca enroll` command).
- CA certificate, if you have received the certificate (see the `crypto ca authenticate` command).

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following sample output is from the `show crypto ca certificates` command:

```
RP/0/RP0/CPU0:router# show crypto ca certificates
Trustpoint : msiox

--- CA certificate ---
Subject:
    Name: CA2
    CN= CA2
Issued By : cn=CA2
Validity Start : 07:51:51 UTC Wed Jul 06 2005
Validity End : 08:00:43 UTC Tue Jul 06 2010
CRL Distribution Point
    http://10.56.8.236/CertEnroll/CA2.crl

--- Router certificate ---
Status : Available
Key usage : Signature
Serial Number : 38:6B:C6:B8:00:04:00:00:01:45
Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
Issued By : cn=CA2
Validity Start : 08:30:03 UTC Mon Apr 10 2006
Validity End : 08:40:03 UTC Tue Apr 10 2007
CRL Distribution Point
    http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX

--- Router certificate ---
Status : Available
Key usage : Encryption
Serial Number : 38:6D:2B:A7:00:04:00:00:01:46
Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
Issued By : cn=CA2
Validity Start : 08:31:34 UTC Mon Apr 10 2006
Validity End : 08:41:34 UTC Tue Apr 10 2007
CRL Distribution Point
```
show crypto ca crls

To display information about the local cache Certificate Revocation List (CRL), use the show crypto ca crls command.

show crypto ca crls

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following sample output is from the show crypto ca crls command:

RP/0//CPU0:router# show crypto ca crls
CRL Entry
-------------------------------------------------------------------------------
Issuer : cn=xyz-w2k-root,ou=HFR,o=Cisco System,l=San Jose,st=CA,c=US
Last Update : [UTC] Thu Jan 10 01:01:14 2002
CRL Distribution Point :
http://xyz-w2k.cisco.com/CertEnroll/xyz-w2k-root.crl
show crypto ca trustpool policy

To display the CA trust pool certificates of the router in a verbose format use the `show crypto ca trustpool policy` command.

**show crypto ca trustpool policy**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the command to display the CA trust pool certificates of the router in a verbose format.

**Example**

This example shows you how to run the command to view details of your CA certificate trust pool policy.

```
RP/0/RSP0/CPU0:IMC0#show crypto ca trustpool policy

Trustpool Policy

Trustpool CA certificates will expire [UTC] Thu Sep 30 14:01:15 2021
CA Bundle Location: http://cisco.com/security/pki/trs/ios.p7b
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto ca crl, on page 121</td>
<td>Clears all the CRLs stored on the router.</td>
</tr>
<tr>
<td>show crypto ca trustpool import url, on page 129</td>
<td>Allows you to manually update certificates in the trust pool.</td>
</tr>
<tr>
<td>show crypto ca trustpool policy, on page 130</td>
<td>Configures CA trust pool policy parameters.</td>
</tr>
</tbody>
</table>
show crypto key mypubkey dsa

To display the Directory System Agent (DSA) public keys for your router, use the `show crypto key mypubkey dsa` command.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 5.0.0   | This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following sample output is from the `show crypto key mypubkey dsa` command:

```
RP/0/RP0/CPU0:router# show crypto key mypubkey dsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 17:33:23 UTC Thu Sep 18 2003
Data :
3081F230 81AA0605 2B0E0302 0C3081A0 02020200 02A0C8 A36B6179 56B8D620
1F77595C 32EF3004 5779F79A 08ABD44 89FB9699 35C04E7E 5491ED4E 120C657C
610576E5 841696B6 094B8E46C 92F56E5 B4921458 70FC4902 1500AB61 5C0D63D3
EB0822B9 F16030C5 AA0B5D1A DFE50240 73F661EA 95F79E77 B413D8C4 9047B4F2
10A1CFB1 14D98857 369BA979 9B5120AD F522BDC7 15B63454 8CB54895 92B6CD9F
7DC27768 FD296844 42024945 5EB6C81A 03430002 4071B49E F80F9E4B AF2B62E7
AA817460 87EF503 C668AD8C D606050B 225CC277 7CA0A974 8072D7D7 2ADDDE42
329FE896 AB016E1 3A414254 6935FDCA 0043BA4F 66
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate dsa, on page 131</td>
<td>Generates DSA key pairs.</td>
</tr>
<tr>
<td>crypto key zeroize dsa, on page 135</td>
<td>Deletes all DSA keys from the router.</td>
</tr>
</tbody>
</table>
show crypto key mypubkey ecdsa

To display the Elliptic Curve Digital Signature Algorithm (ECDSA) public keys for your router, use the `show crypto key mypubkey ecdsa` command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

```
RP/0/RSP0/CPU0:Router# show crypto key mypubkey ecdsa

Key label: the_default
Type : ECDSA General Curve Nistp256
Degree : 256
Created : 19:10:54 IST Mon Aug 21 2017
Data :
04255331 89B3CC40 BCD5A5A3 3BCCE7FF 522BF88D F3CC300D CEC9D7FD 98796ABB
6A69523F E5FAB66 804A05BF ECCDABC6 63F73AE8 E89827DD 18EB106A 7735C34A
```

show crypto key mypubkey rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys for your router, use the `show crypto key mypubkey rsa` command.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
XR EXEC
This command was introduced. Release 5.0.0

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the `show crypto key mypubkey rsa` command:

```
RP/0//CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 07:46:15 UTC Fri Mar 17 2006
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4DL64D F6EB788B 926B1DE0 0383027F BA7BC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4B7A1BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6FF40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Created : 07:46:15 UTC Fri Mar 17 2006
Data :
305C300D 06092A86 486F70A1 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCEBF3DF D1327DBA C130C45 2EEB4981 B1B4822B 1AF14665 178058FB 8F6B6B6B
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF ECBE5822 9B020301 0001
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td>crypto key zeroize rsa</td>
<td>Deletes all RSA keys from the router.</td>
</tr>
</tbody>
</table>
show crypto key mypubkey rsa
Secure Shell Commands

This module describes the Cisco IOS XR software commands used to configure Secure Shell (SSH).

For detailed information about SSH concepts, configuration tasks, and examples, see the Implementing Secure Shell on module in the System Security Configuration Guide for Cisco NCS 6000 Series Routers.

- clear ssh, on page 160
- clear netconf-yang agent session, on page 161
- netconf-yang agent ssh, on page 162
- sftp, on page 163
- sftp (Interactive Mode), on page 166
- show netconf-yang clients, on page 168
- show netconf-yang statistics, on page 169
- show ssh, on page 171
- show ssh history, on page 173
- show ssh history details, on page 174
- show ssh session details, on page 175
- ssh, on page 177
- ssh client knownhost, on page 178
- ssh client source-interface, on page 179
- ssh client vrf, on page 180
- ssh server, on page 181
- ssh server rekey-time, on page 183
- ssh server rekey-volume, on page 184
- show ssh rekey, on page 184
- ssh server logging, on page 185
- ssh server rate-limit, on page 186
- ssh server session-limit, on page 187
- ssh server v2, on page 188
- ssh server netconf port, on page 189
- ssh server netconf, on page 190
- show tech-support ssh, on page 191
- ssh timeout, on page 193
clear ssh

To terminate an incoming or outgoing Secure Shell (SSH) connection, use the clear ssh command.

clear ssh {session-id|outgoing session-id}

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-id</td>
<td>Session ID number of an incoming connection as displayed in the show ssh command output. Range is from 0 to 1024.</td>
</tr>
<tr>
<td>outgoing session-id</td>
<td>Specifies the session ID number of an outgoing connection as displayed in the show ssh command output. Range is from 1 to 10.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

XR EXEC

Command History

Release 5.0.0 This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the clear ssh command to disconnect incoming or outgoing SSH connections. Incoming connections are managed by the SSH server running on the local networking device. Outgoing connections are initiated from the local networking device.

To display the session ID for a connection, use the show ssh command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
</tbody>
</table>

Examples

In the following example, the show ssh command is used to display all incoming and outgoing connections to the router. The clear ssh command is then used to terminate the incoming session with the ID number 0.

RP/0/RP0/CPU0:router# show ssh

SSH version: Cisco-2.0
session  pty location state userid host ver
--------------------------------------------------------------------
Incoming sessions
0 vty0 0/33/1 SESSION_OPEN cisco 172.19.72.182 v2
1 vty1 0/33/1 SESSION_OPEN cisco 172.18.0.5 v2
2 vty2 0/33/1 SESSION_OPEN cisco 172.20.10.3 v1
3 vty3 0/33/1 SESSION_OPEN cisco 3333::50 v2
Outgoing sessions
1 0/33/1 SESSION_OPEN cisco 172.19.72.182 v2
2 0/33/1 SESSION_OPEN cisco 3333::50 v2

RP/0/RP0/CPU0:router# clear ssh 0

The following output is applicable for the **clear ssh** command starting IOS-XR 5.3.2 releases and later.

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0

id chan pty location state userid host ver
authentication connection type
--------------------------------------------------------------------------------------------------------------------------
Incoming sessions
0 1 vty0 0/RSP0/CPU0 SESSION_OPEN lab 12.22.57.75 v2 rsa-pubkey Command-Line-Interface
0 2 vty1 0/RSP0/CPU0 SESSION_OPEN lab 12.22.57.75 v2 rsa-pubkey Command-Line-Interface
0 3 0/RSP0/CPU0 SESSION_OPEN cisco 12.22.57.75 v2 rsa-pubkey Sftp-Subsystem
1 vty7 0/RSP0/CPU0 SESSION_OPEN cisco 12.22.22.57 v1 password Command-Line-Interface
3 1 0/RSP0/CPU0 SESSION_OPEN lab 12.22.57.75 v2 password Netconf-Subsystem
4 1 vty3 0/RSP0/CPU0 SESSION_OPEN lab 192.168.1.55 v2 password Command-Line-Interface

Outgoing sessions
1 0/RSP0/CPU0 SESSION_OPEN lab 192.168.1.51 v2 password
```

RP/0/RP0/CPU0:router# clear ssh 0

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssh, on page 171</td>
<td>Displays the incoming and outgoing connections to the router.</td>
<td></td>
</tr>
</tbody>
</table>

### clear netconf-yang agent session

To clear the specified netconf agent session, use the **clear netconf-yang agent session** in EXEC mode.

```
clear netconf-yang agent session session-id
```

**Syntax Description**
- **session-id** The session-id which needs to be cleared.

**Command Default**
- None

**Command Modes**
- XR EXEC mode
netconf-yang agent ssh

This command was introduced in Release 5.3.0.

Usage Guidelines

No specific guidelines impact the use of this command.

The `show netconf-yang clients` command can be used to get the required session-id(s).

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Example

This example shows how to use the `clear netconf-yang agent session` command:

```
RP/0/RP0/CPU0:router (config) # clear netconf-yang agent session 32125
```

netconf-yang agent ssh

To enable netconf agent over SSH (Secure Shell), use the `netconf-yang agent ssh` command in the global configuration mode. To disable netconf, use the `no` form of the command.

```
netconf-yang agent ssh
no netconf-yang agent ssh
```

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global Configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

SSH is currently the supported transport method for Netconf.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read, write</td>
</tr>
</tbody>
</table>
### Example
This example shows how to use the `netconf-yang agent ssh` command:
```
RP/0/RP0/CPU0:router (config) # netconf-yang agent ssh
```

### sftp
To start the secure FTP (SFTP) client, use the `sftp` command.
```
sftp [username @ host : remote-filenam e] source-filenam e dest-filenam e [source-interface type interface-path-id] [vrf vrf-name]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.</td>
</tr>
<tr>
<td>hostname:remotefilenamed</td>
<td>(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (: ) following the hostname is required.</td>
</tr>
<tr>
<td>source-filenamed</td>
<td>SFTP source, including the path.</td>
</tr>
<tr>
<td>dest-filenamed</td>
<td>SFTP destination, including the path.</td>
</tr>
<tr>
<td>source-interface</td>
<td>(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note** Use the `show interfaces` command in EXEC 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-name** Specifies the name of the VRF associated with the source interface.

#### Command Default
If no `username` argument is provided, the login name on the router is used. If no `hostname` argument is provided, the file is considered local.

#### Command Modes
XR EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

SFTP provides for the secure (and authenticated) copying of files between a router and a remote host. Like the `copy` command, the `sftp` command can be invoked only in EXEC mode.

If a username is not provided, the login name on the router is used as the default. If a host name is not provided, the file is considered local.

If the source interface is specified in the `sftp` command, the `sftp` interface takes precedence over the interface specified in the `ssh client source-interface` command.

When the file destination is a local path, all of the source files should be on remote hosts, and vice versa.

When multiple source files exist, the destination should be a preexisting directory. Otherwise, the destination can be either a directory name or destination filename. The file source cannot be a directory name.

If you download files from different remote hosts, that is, the source points to different remote hosts, the SFTP client spawns SSH instances for each host, which may result in multiple prompts for user authentication.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

### Examples

In the following example, user `abc` is downloading the file `ssh.diff` from the SFTP server `ena-view1` to `disk0`:

```
RP/0/RP0/CPU0:router# sftp abc@ena-view1:ssh.diff disk0
```

In the following example, user `abc` is uploading multiple files from disk `0:/sam_*` to `/users/abc/` on a remote SFTP server called `ena-view1`:

```
RP/0/RP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

In the following example, user `admin` is downloading the file `run` from `disk0a:` to `disk0:/V6copy` on a local SFTP server using an IPv6 address:

```
RP/0/RP0/CPU0:router# sftp admin@[2:2:2::2]:disk0a:/run disk0:/V6copy
Connecting to 2:2:2::2...
Password: disk0a:/run
   Transferred 308413 Bytes
   308413 bytes copied in 0 sec (338172)bytes/sec
RP/0/RP0/CPU0:router# dir disk0:/V6copy
Directory of disk0:
    70144 -rwx 308413 Sun Oct 16 23:06:52 2011 V6copy
2102657024 bytes total (1537638400 bytes free)
```
In the following example, user admin is uploading the file v6copy from disk0: to disk0a:/v6back on a local SFTP server using an IPv6 address:

```
RP/0/RP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:
/disk0:/V6copy
   Transferred 308413 Bytes
   308413 bytes copied in 0 sec (421329)bytes/sec
RP/0/RP0/CPU0:router#dir disk0a:/v6back
Directory of disk0a:
  66016 -rwx 308413 Sun Oct 16 23:07:28 2011 v6back
2102788096 bytes total (2098987008 bytes free)
```

In the following example, user admin is downloading the file sampfile from disk0: to disk0a:/sampfile_v4 on a local SFTP server using an IPv4 address:

```
RP/0/RP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile disk0a:/sampfile_v4
Connecting to 2.2.2.2...
Password:
disk0:/sampfile
   Transferred 986 Bytes
   986 bytes copied in 0 sec (493000)bytes/sec
RP/0/RP0/CPU0:router#dir disk0a:/sampfile_v4
Directory of disk0a:
  131520 -rwx 986 Tue Oct 18 05:37:00 2011 sampfile_v4
502710272 bytes total (502001664 bytes free)
```

In the following example, user admin is uploading the file sampfile_v4 from disk0a: to disk0:/sampfile_back on a local SFTP server using an IPv4 address:

```
RP/0/RP0/CPU0:router#sftp disk0a:/sampfile_v4 admin@2.2.2.2:disk0:/sampfile_back
Connecting to 2.2.2.2...
Password:
disk0a:/sampfile_v4
   Transferred 986 Bytes
   986 bytes copied in 0 sec (564000)bytes/sec
RP/0/RP0/CPU0:router#dir disk0:/sampfile_back
Directory of disk0:
  121765 -rwx 986 Tue Oct 18 05:39:00 2011 sampfile_back
524501272 bytes total (512507614 bytes free)
```
### sftp (Interactive Mode)

To enable users to start the secure FTP (SFTP) client, use the `sftp` command.

```
sftp [username @ host : remote-filenam e] [source-interface type interface-path-id] [vrf vrf-name]
```

#### Syntax Description

- **username** (Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.
- **hostname:remote-filenam e** (Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.
- **source-interface** (Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.
- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or virtual interface.
  - **Note** Use the `show interfaces` command in EXEC 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-name** Specifies the name of the VRF associated with the source interface.

#### Command Default

If no `username` argument is provided, the login name on the router is used. If no `hostname` argument is provided, the file is considered local.

#### Command Modes

XR EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
The SFTP client, in the interactive mode, creates a secure SSH channel where the user can enter any supported command. When a user starts the SFTP client in an interactive mode, the SFTP client process creates a secure SSH channel and opens an editor where user can enter any supported command.

More than one request can be sent to the SFTP server to execute the commands. While there is no limit on the number of 'non-acknowledged' or outstanding requests to the server, the server might buffer or queue these requests for convenience. Therefore, there might be a logical sequence to the order of requests.

The following Unix-based commands are supported in the interactive mode:

- `bye`
- `cd <path>`
- `chmod <mode> <path>`
- `exit`
- `get <remote-path> [local-path]`
- `help`
- `ls [-alt] <path>`
- `mkdir <path>`
- `put <local-path> [remote-path]`
- `pwd`
- `quit`
- `rename <old-path> <new-path>`
- `rmdir <path>`
- `rm <path>`

The following commands are not supported:

- `lcd, lls, lpwd, lumask, lmkdir`
- `ln, symlink`
- `chgrp, chown`
- `!, !command`
- `?`
- `mget, mput`

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, user *admin* is downloading and uploading a file from/to an external SFTP server using an IPv6 address:

```
RP/0/RP0/CPU0:router#sftp admin@[2:2:2::2]
Connecting to 2:2:2::2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/admin
sftp> get frmRouter /disk0:/frmRouterdownload
```
In the following example, user *abc* is downloading and uploading a file from/to an external SFTP server using an IPv4 address:

```
RP/0/RP0/CPU0:router#sftp abc@2.2.2.2
Connecting to 2.2.2.2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/abc
sftp> get frmRouter /disk0:/frmRouterdownoad
/auto/tftp-server1-users5/abc/frmRouter
Transferred 1578 Bytes
1578 bytes copied in 0 sec (27684) bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer
/disk0:/frmRouterdownoad
Transferred 1578 Bytes
1578 bytes copied in 0 sec (14747) bytes/sec
sftp>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh client source-interface, on page 179</code></td>
<td>Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td><code>ssh client vrf, on page 180</code></td>
<td>Configures a new VRF for use by the SSH client.</td>
</tr>
</tbody>
</table>

---

**show netconf-yang clients**

To display the client details for netconf-yang, use the `show netconf-yang clients` command in EXEC mode.

**show netconf-yang clients**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

EXEC
This command was introduced.

5.3.0

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

Example

This example shows how to use the `show netconf-yang clients` command:

```
RP/0/RP0/CPU0:router (config) # sh netconf-yang clients
Netconf clients
client session ID| NC version| client connect time| last OP time| last OP type| <lock>
22969| 1.1| 0d 0h 0m 2s| 11:11:24|
close-session| No| |
15389| 1.1| 0d 0h 0m 1s| 11:11:25|
get-config| No| |
```

Table 12: Field descriptions

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client session ID</td>
<td>Assigned session identifier</td>
</tr>
<tr>
<td>NC version</td>
<td>Version of the Netconf client as advertised in the hello message</td>
</tr>
<tr>
<td>Client connection time</td>
<td>Time elapsed since the client was connected</td>
</tr>
<tr>
<td>Last OP time</td>
<td>Last operation time</td>
</tr>
<tr>
<td>Last OP type</td>
<td>Last operation type</td>
</tr>
<tr>
<td>Lock (yes or no)</td>
<td>To check if the session holds a lock on the configuration datastore</td>
</tr>
</tbody>
</table>

**show netconf-yang statistics**

To display the statistical details for netconf-yang, use the `show netconf-yang statistics` command in EXEC mode.

**show netconf-yang statistics**

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None
show netconf-yang statistics

Command Modes

EXEC

Command History

Release | Modification
---|---
Release 5.3.0 | This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

Example

This example shows how to use the `show netconf-yang statistics` command:

```
RP/0/RP0/CPU0:router (config) # sh netconf-yang statistics
Summary statistics

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests</td>
<td>Total number of processed requests of a given type</td>
</tr>
</tbody>
</table>
```

Table 13: Field descriptions
show ssh

To display all incoming and outgoing connections to the router, use the `show ssh` command.

```
show ssh
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

XR EXEC

**Command History**

```
+-----------+-----------+
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
+-----------+-----------+
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show ssh` command to display all incoming and outgoing Secure Shell (SSH) Version 1 (SSHv1) and SSH Version 2 (SSHv2) connections.

**Task ID**

```
Task ID   Operations
ID        ID
crypto    read
```

**Examples**

This is sample output from the `show ssh` command when SSH is enabled:

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

SSH version : Cisco-2.0

id  pty  location  state  userid  host  ver  authentication
-----------------------------------------------
Incoming sessions

Outgoing sessions
1  0/3/CPU0  SESSION_OPEN  lab  12.22.57.  v2  password
2  0/3/CPU0  SESSION_OPEN  lab  12.22.57.75  v2  keyboard-interactive
```
The following output is applicable for the `show ssh` command starting IOS-XR 5.3.2 releases and later.

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0

<table>
<thead>
<tr>
<th>id</th>
<th>chan</th>
<th>pty</th>
<th>location</th>
<th>state</th>
<th>userid</th>
<th>host</th>
<th>ver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Incoming sessions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>vty0</td>
<td>0/RSP0/CPU0</td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>12.22.57.75</td>
<td>v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rsa-pubkey</td>
<td>Command-Line-Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>vty1</td>
<td>0/RSP0/CPU0</td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>12.22.57.75</td>
<td>v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rsa-pubkey</td>
<td>Command-Line-Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>vty3</td>
<td>0/RSP0/CPU0</td>
<td>SESSION_OPEN</td>
<td>cisco</td>
<td>12.22.57.75</td>
<td>v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rsa-pubkey</td>
<td>Sftp-Subsystem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>vty7</td>
<td>0/RSP0/CPU0</td>
<td>SESSION_OPEN</td>
<td>cisco</td>
<td>12.22.22.57</td>
<td>v1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Command-Line-Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>12.22.57.75</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rsa-pubkey</td>
<td>Command-Line-Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>12.22.57.75</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>rsa-pubkey</td>
<td>Netconf-Subsystem</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td></td>
<td></td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>192.168.1.55</td>
<td>password</td>
</tr>
</tbody>
</table>

Outgoing sessions

<table>
<thead>
<tr>
<th>id</th>
<th>chan</th>
<th>pty</th>
<th>location</th>
<th>state</th>
<th>userid</th>
<th>host</th>
<th>ver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SESSION_OPEN</td>
<td>lab</td>
<td>192.168.1.51</td>
<td>v2</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This table describes significant fields shown in the display.

**Table 14: show ssh Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Session identifier for the incoming and outgoing SSH connections.</td>
</tr>
<tr>
<td>chan</td>
<td>Channel identifier for incoming (v2) SSH connections. NULL for SSH v1 sessions.</td>
</tr>
<tr>
<td>pty</td>
<td>pty-id allocated for the incoming session. Null for outgoing SSH connection.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the location of the SSH server for an incoming connection. For an outgoing connection, location specifies from which route processor the SSH session is initiated.</td>
</tr>
<tr>
<td>state</td>
<td>The SSH state that the connection is currently in.</td>
</tr>
<tr>
<td>userid</td>
<td>Authentication, authorization and accounting (AAA) username used to connect to or from the router.</td>
</tr>
<tr>
<td>host</td>
<td>IP address of the remote peer.</td>
</tr>
<tr>
<td>ver</td>
<td>Specifies if the connection type is SSHv1 or SSHv2.</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the type of authentication method chosen by the user.</td>
</tr>
<tr>
<td>connection type</td>
<td>Specifies which application is performed over this connection (Command-Line-Interface, Remote-Command, Sftp, or Netconf-Subsystem).</td>
</tr>
</tbody>
</table>
## show ssh history

To display the last hundred SSH connections that were terminated, use the `show ssh history` command in XR EXEC mode.

```
show ssh history
```

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Examples

The following is sample output from the `show ssh history` command to display the last hundred SSH sessions that were terminated:

```
RP/0/RP0/CPU0:router# show ssh history

SSH version : Cisco-2.0
id           chan   pty   location     userid    host              ver  authentication
connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
1  1       XXXXX  0/RP0/CPU0  root        10.105.227.252  v2  password
Netconf-Subsystem
2  1       XXXXX  0/RP0/CPU0  root        10.105.227.252  v2  password
Netconf-Subsystem
3  1       XXXXX  0/RP0/CPU0  root        10.105.227.252  v2  password
```
show ssh history details

To display the last hundred SSH connections that were terminated, and also the start and end time of the session, use the `show ssh history details` command in XR EXEC mode.

**show ssh history details**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no keywords or arguments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>None</td>
</tr>
<tr>
<td>Command Modes</td>
<td>XR EXEC mode</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 6.4.1 This command was introduced.</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>No specific guidelines impact the use of this command.</td>
</tr>
<tr>
<td>Task ID</td>
<td>crypto read</td>
</tr>
<tr>
<td>Examples</td>
<td>The following is sample output from the <code>show ssh history details</code> command to display the last hundred SSH sessions that were terminated along with the start and end time of the sessions:</td>
</tr>
</tbody>
</table>

```
RP/0/RP0/CPU0:router# show ssh history details
SSH version : Cisco-2.0
id          key-exchange    pubkey     incipher   outcipher   inmac
outmac      start_time     end_time
```

Pty – VTY number used. This is represented as ‘XXXX’ when connection type is SFTP, SCP or Netconf.
Incoming Session
1  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  14-02-18  14:00:39  14-02-18  14:00:41
2  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  14-02-18  16:21:54  14-02-18  16:21:55
3  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
4  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  15-02-18  12:17:44  15-02-18  12:17:46
5  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
6  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  15-02-18  14:44:08  15-02-18  14:44:09
7  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  15-02-18  14:50:15  15-02-18  14:50:16
8  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  
   hmac-sha2-256  15-02-18  14:50:52  15-02-18  14:50:53
9  ecldh-sha2-nistp256  ssh-rsa  aes128-ctr  aes128-ctr  hmac-sha2-256  

This table describes the significant fields shown in the display.

**Table 15: Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session</td>
<td>Session identifier for the incoming and outgoing SSH connections.</td>
</tr>
<tr>
<td>key-exchange</td>
<td>Key exchange algorithm chosen by both peers to authenticate each other.</td>
</tr>
<tr>
<td>pubkey</td>
<td>Public key algorithm chosen for key exchange.</td>
</tr>
<tr>
<td>incipher</td>
<td>Encryption cipher chosen for the receiver traffic.</td>
</tr>
<tr>
<td>outcipher</td>
<td>Encryption cipher chosen for the transmitter traffic.</td>
</tr>
<tr>
<td>inmac</td>
<td>Authentication (message digest) algorithm chosen for the receiver traffic.</td>
</tr>
<tr>
<td>outmac</td>
<td>Authentication (message digest) algorithm chosen for the transmitter traffic.</td>
</tr>
<tr>
<td>start_time</td>
<td>Start time of the session.</td>
</tr>
<tr>
<td>end_time</td>
<td>End time of the session.</td>
</tr>
</tbody>
</table>

**show ssh session details**

To display the details for all incoming and outgoing Secure Shell Version 2 (SSHv2) connections, use the **show ssh session details** command.

**Syntax Description**

This command has no keywords or arguments.
show ssh session details

Command Default
None

Command Modes
XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 5.0.0    | This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show ssh session details` command to display a detailed report of the SSHv2 connections to or from the router, including the cipher chosen for the specific session.

Examples
The following is sample output from the `show ssh session details` command to display the details for all the incoming and outgoing SSHv2 connections:

```
RP/0/RP0/CPU0:router# show ssh session details
id  key-exchange  pubkey  incipher  outcipher  inmac  outmac
---------------------------
Incoming Session
0  diffie-hellman-group14  ssh-rsa  aes128-ctr  aes128-ctr  hmac-shal  hmac-shal
1  ecdh-sha2-nistp521  ssh-rsa  aes256-ctr  aes256-ctr  hmac-sha2-512  hmac-sha2-512
```

This table describes the significant fields shown in the display.

### Table 16: show ssh session details Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session</td>
<td>Session identifier for the incoming and outgoing SSH connections.</td>
</tr>
<tr>
<td>key-exchange</td>
<td>Key exchange algorithm chosen by both peers to authenticate each other.</td>
</tr>
<tr>
<td>pubkey</td>
<td>Public key algorithm chosen for key exchange.</td>
</tr>
<tr>
<td>incipher</td>
<td>Encryption cipher chosen for the Rx traffic.</td>
</tr>
<tr>
<td>outcipher</td>
<td>Encryption cipher chosen for the Tx traffic.</td>
</tr>
<tr>
<td>inmac</td>
<td>Authentication (message digest) algorithm chosen for the Rx traffic.</td>
</tr>
<tr>
<td>outmac</td>
<td>Authentication (message digest) algorithm chosen for the Tx traffic.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sessions</td>
<td>Displays information about open Telnet or rlogin connections.</td>
</tr>
<tr>
<td>show ssh, on page 171</td>
<td>Displays all the incoming and outgoing connections to the router.</td>
</tr>
</tbody>
</table>

## ssh

To start the Secure Shell (SSH) client connection and enable an outbound connection to an SSH server, use the `ssh` command.

### Syntax Description

- **ipv4-address**
  IPv4 address in A:B:C:D format.

- **ipv6-address**
  IPv6 address in X::X::X format.

- **hostname**
  Hostname of the remote node. If the hostname has both IPv4 and IPv6 addresses, the IPv6 address is used.

- **username user-id** (Optional) Specifies the username to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.

- **cipher**

- **source interface** (Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.

- **type**
  Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**
  Physical interface or virtual interface.

  **Note** Use the `show interfaces` command in XR EXEC 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.

- **command** (Optional) Specifies a remote command. Adding this keyword prompts the SSHv2 server to parse and execute the `ssh` command in non-interactive mode instead of initiating the interactive session.

### Command Default

None

### Command Modes

XR EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the ssh command to make an outbound client connection. The SSH client tries to make an SSHv2 connection to the remote peer. If the remote peer supports only the SSHv1 server, it internally spawns an SSHv1 connection to the remote server. The process of the remote peer version detection and spawning the appropriate client connection is transparent to the user.

If is specified in the ssh command, the ssh interface takes precedence over the interface specified in the ssh client source-interface ssh client source-interface, on page 179 command.

Use the command keyword to enable the SSHv2 server to parse and execute the ssh command in non-interactive mode instead of initiating an interactive session.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>execute</td>
</tr>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
</tbody>
</table>

Examples

The following sample output is from the ssh command to enable an outbound SSH client connection:

```
RP/0/RP0/CPU0:router# ssh username userabc
Password: 
Remote-host>
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssh, on page 171</td>
<td>Displays all the incoming and outgoing connections to the router.</td>
</tr>
</tbody>
</table>

**ssh client knownhost**

To authenticate a server public key (pubkey), use the ssh client knownhost command. To disable authentication of a server pubkey, use the no form of this command.

```
ssh client knownhost device:/filename
no ssh client knownhost device:/filename
```

Syntax Description

- **device:/filename** Complete path of the filename (for example, slot0:/server_pubkey). The colon (:) and slash (/) are required.

Command Default

None

Command Modes

XR Config
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The server pubkey is a cryptographic system that uses two keys at the client end—a public key known to everyone and a private, or secret, key known only to the owner of the keys. In the absence of certificates, the server pubkey is transported to the client through an out-of-band secure channel. The client stores this pubkey in its local database and compares this key against the key supplied by the server during the early stage of key negotiation for a session-building handshake. If the key is not matched or no key is found in the local database of the client, users are prompted to either accept or reject the session.

The operative assumption is that the first time the server pubkey is retrieved through an out-of-band secure channel, it is stored in the local database. This process is identical to the current model adapted by Secure Shell (SSH) implementations in the UNIX environment.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the `ssh client knownhost` command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RP0/CPU0:host1# exit
RP/0/RP0/CPU0:router# ssh host1 username user1234
```

**ssh client source-interface**

To specify the source IP address of a selected interface for all outgoing Secure Shell (SSH) connections, use the `ssh client source-interface` command. To disable use of the specified interface IP address, use the `no` form of this command.

```
ssh client source-interface type interface-path-id
no ssh client source-interface type interface-path-id
```

**Syntax Description**

- `type` Interface type. For more information, use the question mark (?) online help function.
interface-path-id  Physical interface or virtual interface.

**Note**  Use the `show interfaces` command 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.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No source interface is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>XR Config</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>Release 5.0.0</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `ssh client source-interface` command to set the IP address of the specified interface for all outgoing SSH connections. If this command is not configured, TCP chooses the source IP address when the socket is connected, based on the outgoing interface used—which in turn is based on the route required to reach the server. This command applies to outbound shell over SSH as well as Secure Shell File Transfer Protocol (SFTP) sessions, which use the ssh client as a transport.

The source-interface configuration affects connections only to the remote host in the same address family. The system database (Sysdb) verifies that the interface specified in the command has a corresponding IP address (in the same family) configured.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the IP address of the Management Ethernet interface for all outgoing SSH connections:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client source-interface MgmtEth 0//CPU0/0
```

**ssh client vrf**

To configure a new VRF for use by the SSH client, use the `ssh client vrf` command. To remove the specified VRF, use the `no` form of this command.

```
ssh client vrf vrf-name
```
no ssh client vrf vrf-name

Syntax Description

vrf-name  Specifies the name of the VRF to be used by the SSH client.

Command Default

None

Command Modes

XR Config

Command History

Release 5.0.0  This command was introduced.

Command History

Release 3.8.0  This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An SSH client can have only one VRF.

If a specific VRF is not configured for the SSH client, the default VRF is assumed when applying other SSH client-related commands, such as ssh client knownhost, on page 178 or ssh client source-interface, on page 179.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

Examples

The following example shows the SSH client being configured to start with the specified VRF:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client vrf green

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh client dscp &lt;value from 0 - 63&gt;</td>
<td>SSH Client supports setting DSCP value in the outgoing packets. If not configured, the default DSCP value set in packets is 16 (for both client and server).</td>
</tr>
</tbody>
</table>

ssh server

To bring up the Secure Shell (SSH) server and to configure one or more VRFs for its use, use the ssh server command. To stop the SSH server from receiving any further connections for the specified VRF, use the no
form of this command. Optionally ACLs for IPv4 and IPv6 can be used to restrict access to the server before
the port is opened.

```
ssh server vrf vrf-name [ipv4 access-list ipv4 access list name ] [ipv6 access-list ipv6 access list name ]
```

```
ssh server v2
no ssh server [{vrf vrf-name|v2}]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>Specifies the name of the VRF to be used by the SSH server. The maximum VRF length is 32 characters.</td>
</tr>
<tr>
<td><code>ipv4 access-list access list name</code></td>
<td>Configures an IPv4 access-list for access restrictions to the ssh server.</td>
</tr>
<tr>
<td><code>ipv6 access-list access list name</code></td>
<td>Configures an IPv6 access-list for access restrictions to the ssh server.</td>
</tr>
<tr>
<td><code>v2</code></td>
<td>Forces the SSH server version to be of only version 2.</td>
</tr>
</tbody>
</table>

Command Default

The default SSH server version is 2 (SSHv2), which falls back to 1 (SSHv1) if the incoming SSH client
connection is set to SSHv1.

Command Modes

XR CONFIG

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task
IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An SSH server must be configured at minimum for one VRF. If you delete all configured VRFs, including
the default, the SSH server process stops. If you do not configure a specific VRF for the SSH client when
applying other commands, such as ssh client knownhost or ssh client source-interface, the default VRF is assumed.

The SSH server listens for an incoming client connection on port 22. This server handles both Secure Shell
Version 1 (SSHv1) and SSHv2 incoming client connections for both IPv4 and IPv6 address families. To
accept only Secure Shell Version 2 connections, use the ssh server v2, on page 188 command.

To verify that the SSH server is up and running, use the `show process sshd` command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

In the following example, the SSH server is brought up to receive connections for VRF “green”: 
Examples

In the following example, the SSH server is configured to use IPv4 ACLs:

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh vrf vrf name ipv4 access-list access list name
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes</td>
<td>Displays information about the SSH server.</td>
</tr>
<tr>
<td>ssh server v2, on page 188</td>
<td>Forcesto the SSH server version to be only 2 (SSHv2).</td>
</tr>
<tr>
<td>ssh server dscp &lt;value from 0 - 63&gt;</td>
<td>SSH server supports setting DSCP value in the outgoing packets. If not configured, the default DSCP value set in packets is 16 (for both client and server).</td>
</tr>
</tbody>
</table>

### ssh server rekey-time

To configure rekey of the ssh server key based on time. Use the no form of this command to remove the rekey interval.

```
ssh server rekey-time time in minutes
no ssh server rekey-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>rekey-time time in minutes</th>
<th>Specifies the rekey-time interval in minutes. The range is between 30 to 1440 minutes.</th>
</tr>
</thead>
</table>

**Note**

If no time interval is specified, the default interval is considered to be 30 minutes.

**Command Default**

None.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the SSH server rekey-interval of 450 minutes is used:
ssh server rekey-volume

To configure a volume-based rekey threshold for an SSH session. Use the no form of this command to remove the volume-based rekey threshold.

```
ssh server rekey-volume
no ssh server rekey-volume
```

**Syntax Description**

```
rekey-volume data in megabytes
```

- **Specifies the volume-based rekey threshold in megabytes. The range is between 1024 to 4095 megabytes.**

- **Note** If no volume threshold is specified, the default size is considered to be 1024 MB.

**Command Default**

None.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the SSH server rekey-volume of 2048 minutes is used:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server rekey-time 450
```

show ssh rekey

To display session rekey details such as session id, session rekey count, time to rekey, data to rekey, use the show ssh rekey command.

```
show ssh rekey
```

**Command Default**

None

**Command Modes**

XR EXEC
## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 5.0.0  This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The ssh rekey data is updated ten times between two consecutive rekeys.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following sample output is from the `show ssh rekey` command:

```
# show ssh rekey

id  RekeyCount  TimeToRekey(min)  VolumeToRekey(MB)
-----------------------------------------------
Incoming Session
0    8        59.5            1024.0
```

This table describes the fields shown in the display.

### Table 17: `show ssh rekey` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rekey Count</td>
<td>Number of times the ssh rekey is generated.</td>
</tr>
<tr>
<td>TimeToRekey</td>
<td>Time remaining (in minutes) before the ssh rekey is regenerated based on the value set using the <code>ssh server rekey-time</code> command.</td>
</tr>
<tr>
<td>VolumeToRekey</td>
<td>Volume remaining (in megabytes) before the ssh rekey is regenerated based on the value set using the <code>ssh server rekey-volume</code> command.</td>
</tr>
</tbody>
</table>

## ssh server logging

To enable SSH server logging, use the `ssh server logging` command. To discontinue SSH server logging, use the `no` form of this command.

`ssh server logging`

`no ssh server logging`
### Syntax Description
This command has no keywords or arguments.

### Command Default
None

### Command Modes
XR CONFIG

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Once you configure the logging, the following messages are displayed:

- Warning: The requested term-type is not supported
- SSH v2 connection from %s succeeded (user:%s, cipher:%s, mac:%s, pty:%s)

The warning message appears if you try to connect using an unsupported terminal type. Routers running the Cisco IOS XR software support only the vt100 terminal type.

The second message confirms a successful login.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples
The following example shows the initiation of an SSH server logging:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server logging
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh server, on page 181</code></td>
<td>Initiates the SSH server.</td>
</tr>
</tbody>
</table>

### ssh server rate-limit

To limit the number of incoming Secure Shell (SSH) connection requests allowed per minute, use the `ssh server rate-limit` command. To return to the default value, use the `no` form of this command.

```
ssh server rate-limit rate-limit
no ssh server rate-limit
```
Syntax Description

`rate-limit` Number of incoming SSH connection requests allowed per minute. Range is from 1 to 120. When setting it to 60 attempts per minute, it basically means that we can only allow 1 per second. If you set up 2 sessions at the same time from 2 different consoles, one of them will get rate limited. This is connection attempts to the ssh server, not bound per interface/username or anything like that. So value of 30 means 1 session per 2 seconds and so forth.

Command Default

`rate-limit`: 60 connection requests per minute

Command Modes

XR Config mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `ssh server rate-limit` command to limit the incoming SSH connection requests to the configured rate. Any connection request beyond the rate limit is rejected by the SSH server. Changing the rate limit does not affect established SSH sessions.

If, for example, the `rate-limit` argument is set to 30, then 30 requests are allowed per minute, or more precisely, a two-second interval between connections is enforced.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to set the limit of incoming SSH connection requests to 20 per minute:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server rate-limit 20
```

**ssh server session-limit**

To configure the number of allowable concurrent incoming Secure Shell (SSH) sessions, use the `ssh server session-limit` command. To return to the default value, use the `no` form of this command.

```
ssh server session-limit sessions
```
Syntax Description

sessions Number of incoming SSH sessions allowed across the router. The range is from 1 to 100.

Note Although CLI output option has 1024, you are recommended to configure session-limit not more than 100. High session count may cause resource exhaustion.

Command Default

sessions: 64 per router

Command Modes

XR CONFIG

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 5.0.0 This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `ssh server session-limit` command to configure the limit of allowable concurrent incoming SSH connections. Outgoing connections are not part of the limit.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to set the limit of incoming SSH connections to 50:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server session-limit 50
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show processes</td>
<td>Displays information about the SSH server.</td>
</tr>
</tbody>
</table>

ssh server v2

To force the SSH server version to be only 2 (SSHv2), use the `ssh server v2` command. To bring down an SSH server for SSHv2, use the `no` form of this command.

```
ssh server v2
no ssh server v2
```

Syntax Description

This command has no keywords or arguments.
Command Default

None

Command Modes

XR CONFIG

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only SSHv2 client connections are allowed.

Task ID

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to initiate the SSH server version to be only SSHv2:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)# ssh server v2
```

**ssh server netconf port**

To configure a port for the netconf SSH server, use the `ssh server netconf port` command in the global configuration mode. To return to the default port, use the `no` form of the command.

```
ssh server netconf port  port number
no ssh server netconf port port number
```

Syntax Description

- **port**
  - `port-number`
    - Port number for the netconf SSH server (default port number is 830).

Command Default

The default port number is 830.

Command Modes

XR CONFIG

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Release 6.0 | The `ssh server netconf` command is no longer auto completed to configure the default port. This command is now optional |
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Starting with IOS-XR 6.0.0 it is no longer sufficient to configure a netconf port to enable netconf subsystem support. ssh server netconf needs to be at least configured for one vrf.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

This example shows how to use the ssh server netconf port command with port 831:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh server netconf</td>
<td>Configures the vrf(s), where netconf subsystem requests are to be received.</td>
</tr>
<tr>
<td>netconf-yang agent ssh</td>
<td>Configures the ssh netconf-yang backend for the netconf subsystem (Required to allow the system to service netconf-yang requests).</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference.</td>
</tr>
</tbody>
</table>

**ssh server netconf**

To bring up the netconf subsystem support using a dedicated communication port with the Secure Shell (SSH) server and to configure one or more VRFs for its use, use the **ssh server netconf** command. To stop the SSH server from receiving any further netconf subsystem connections for the specified VRF, use the **no** form of this command.

Optionally ACLs for IPv4 and IPv6 can be used to restrict access to the netconf subsystem of the SSH server before the port is opened.

```
ssh server netconf [ vrf vrf name [ ipv4 access-list access list name ] [ ipv6 access-list access list name ] ]
no ssh server netconf [ vrf vrf name ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>vrf name</strong></th>
<th>Specifies the name of the VRF to be used by the netconf subsystem of the SSH server. The maximum VRF length is 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>If no VRF is specified, the default VRF is assumed.</td>
</tr>
<tr>
<td><strong>IPv4 access list name</strong></td>
<td>Configures an IPv4 access-list for access restrictions to the netconf subsystem of the SSH server.</td>
</tr>
</tbody>
</table>
Configures an IPv6 access-list for access restrictions to the netconf subsystem of the SSH server.

**IPv6 access list name**  Configures an IPv6 access-list for access restrictions to the netconf subsystem of the SSH server.

**Command Default**  If no vrf is specified, the command is auto expanded using the default vrf.

**Command Modes**  Global Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 6.0.0</td>
<td>The <em>ssh server netconf</em> command is no longer auto completed to configure the default port. The vrf keyword was supported. Without parameter the command is now auto expanded to enable the netconf subsystem for vrf default. To start netconf subsystem support at least one vrf needs to be configured.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Netconf subsystem support of the SSH server must be configured at minimum for one VRF. If you delete all configured VRFs, including the default, the SSH server process stops serving the netconf subsystem requests. If you do not configure a specific VRF the default VRF is assumed. The SSH server listens for netconf subsystem connections an incoming client connection on the configured port (using ssh server netconf port) or port 8030 (as the iana assigned default port)

Netconf subsystem support is only available with Secure Shell Version 2 SSHv2 incoming client connections for both IPv4 and IPv6 address families. To verify that the SSH server is up and running, use the show process sshd command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the *ssh server netconf vrf vrf name* command:

```
RP/0/RP0/CPU0:router (config) # ssh server netconf vrf red
```

**show tech-support ssh**

To automatically run show commands that display system information, use the show tech-support command, use the *show tech-support ssh* command in XR EXEC mode.

```
show tech-support ssh
```
Syntax Description
This command has no keywords or arguments.

Command Default
None

Command Modes
XR EXEC mode

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.4.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

Task ID
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples
The following is sample output from the `show tech-support ssh` command:

RP/0/RP0/CPU0:router# show tech-support ssh
++ Show tech start time: 2018-Feb-20.123016.IST ++
Tue Feb 20 12:30:27 IST 2018 Waiting for gathering to complete
............................
Tue Feb 20 12:32:35 IST 2018 Compressing show tech output
Show tech output available at 0/RP0/CPU0:
/harddisk:/showtech/showtech-ssh-2018-Feb-20.123016.IST.tgz
++ Show tech end time: 2018-Feb-20.123236.IST ++
RP/0/RP0/CPU0:turin-secl#

The `show tech-support ssh` command collects the output of these CLI:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging</code></td>
<td>Displays the contents of the logging buffer.</td>
</tr>
<tr>
<td><code>show context location all</code></td>
<td>Displays the contents of the currently running configuration or a subset of that configuration.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays brief information about each interface.</td>
</tr>
<tr>
<td><code>show ssh</code></td>
<td>Displays all incoming and outgoing connections to the router.</td>
</tr>
<tr>
<td><code>show ssh session details</code></td>
<td>Displays the details for all the incoming and outgoing SSHv2 connections, to the router.</td>
</tr>
<tr>
<td><code>show ssh rekey</code></td>
<td>Displays session rekey details such as session id, session rekey count, time to rekey, data to rekey.</td>
</tr>
<tr>
<td><code>show ssh history</code></td>
<td>Displays the last hundred SSH connections that were terminated.</td>
</tr>
</tbody>
</table>
### ssh timeout

To configure the timeout value for authentication, authorization, and accounting (AAA) user authentication, use the `ssh timeout` command. To set the timeout value to the default time, use the `no` form of this command.

```
ssh timeout seconds
no ssh timeout seconds
```

**Syntax Description**

- **seconds**  Time period (in seconds) for user authentication. The range is from 5 to 120.

**Command Default**

- **seconds**: 30

**Command Modes**

- XR CONFIG

**Command History**

- Release 5.0.0  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `ssh timeout` command to configure the timeout value for user authentication to AAA. If the user fails to authenticate itself within the configured time to AAA, the connection is aborted. If no value is configured, the default value of 30 seconds is used.

**Examples**

In the following example, the timeout value for AAA user authentication is set to 60 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh timeout 60
```
CHAPTER 8

Secure Socket Layer Protocol Commands

This module describes the commands used to configure the Secure Socket Layer (SSL) protocol.
For detailed information about SSL concepts, configuration tasks, and examples, see the Implementing Secure Socket Layer on module in the System Security Configuration Guide for Cisco NCS 6000 Series Routers.

• show ssl, on page 195

show ssl

To display active Secure Socket Layer (SSL) sessions, use the show ssl command.

show ssl [process-id]

Syntax Description

| process-id | (Optional) Process ID (PID) of the SSL application. The range is from 1 to 1000000000. |

Command Default

None

Command Modes

XR EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To display a specific process, enter the process ID number. To get a specific process ID number, enter run pidin from the command line or from a shell.

The absence of any argument produces a display that shows all processes that are running SSL.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto</td>
<td>read</td>
</tr>
</tbody>
</table>
The following sample output is from the `show ssl` command:

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

PID  Method  Type    Peer        Port  Cipher-Suite
-----------------------------------------------
1261711  sslv3  Server  172.16.0.5  1296  DES-CBC3-SHA
```

This table describes the fields shown in the display.

**Table 18: show ssl Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process ID of the SSL application.</td>
</tr>
<tr>
<td>Method</td>
<td>Protocol version (sslv2, sslv3, sslv23, or tlsv1).</td>
</tr>
<tr>
<td>Type</td>
<td>SSL client or server.</td>
</tr>
<tr>
<td>Peer</td>
<td>IP address of the SSL peer.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number on which the SSL traffic is sent.</td>
</tr>
<tr>
<td>Cipher-Suite</td>
<td>Exact cipher suite chosen for the SSL traffic. The first portion indicates the encryption, the second portion the hash or integrity method. In the sample display, the encryption is Triple DES and the Integrity (message digest algorithm) is SHA.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>run pidin</td>
<td>Displays the process ID for all processes that are running.</td>
</tr>
</tbody>
</table>
## INDEX

### A
- aaa accounting command 2
- aaa accounting system default command 4
- aaa accounting update command 5
- aaa authentication command 6
- aaa authorization command 8
- aaa default-taskgroup command 13
- aaa group server radius command 14
- aaa group server tacacs+ command 15
- accept-lifetime command 95
- accept-tolerance command 96
- accounting (line) command 19
- address ipv4 (MPP) command 107
- allow command 108
- authorization command 20

### C
- clear crypto ca certificates command 120
- clear crypto ca crl command 121
- clear crypto ipsec sa command 87
- clear ssh command 160
- control-plane command 110
- crl optional (trustpoint) command 122
- crypto ca authenticate command 123
- crypto ca cancel-enroll command 124
- crypto ca enroll command 125
- crypto ca import command 126
- crypto ca trustpoint command 127
- crypto ca trustpool import url command 129
- crypto ca trustpool policy command 130
- crypto key generate dsa command 131
- crypto key generate rsa command 133
- crypto key import authentication rsa command 134
- crypto key zeroize dsa command 135
- crypto key zeroize rsa command 136

### D
- description (AAA) command 22
- description (IPSec profile) command 88
- description (trustpoint) command 138

### E
- enrollment retry count command 138
- enrollment retry period command 140
- enrollment terminal command 141
- enrollment url command 142

### G
- group (AAA) command 23

### I
- inband command 111
- inherit taskgroup command 25
- inherit usergroup command 26
- interface (MPP) command 112
- ip-address (trustpoint) command 143

### K
- key (key chain) command 97
- key (TACACS+) command 27
- key chain (key chain) command 98
- key-string (keychain) command 100

### L
- lawful-intercept disable command 105
- login authentication command 28

### M
- management-plane command 113

### O
- out-of-band command 114

### P
- password (AAA) command 29
INDEX

Q
query url command 145

R
radius-server dead-criteria time command 31
radius-server dead-criteria tries command 32
rsakeypair command 146

S
secret command 37
send-lifetime command 101
serial-number (trustpoint) command 147
server (RADIUS) command 39
server (TACACS+) command 40
server-private (RADIUS) command 41
server-private (TACACS+) command 43
sftp (Interactive Mode) command 166
sftp command 163
sftp-password (trustpoint) command 148
sftp-username (trustpoint) command 149
show aaa accounting command 49
show aaa command 45
show aaa user-group 64
show crypto ca certificates command 151
show crypto ca crls command 153
show crypto ca trustpool policy command 154
show crypto ipsec sa command 89
show crypto ipsec summary command 92
show crypto ipsec transform-set command 93
show crypto key mypubkey dsa command 155
show crypto key mypubkey rsa command 156
show key chain command 102
show mgmt-plane command 115
show nacm 10
show radius accounting command 53
show radius authentication command 54
show radius command 51
show radius dead-criteria command 56
show radius server-groups command 57
show ssh command 171
show ssh session details command 175
show ssl command 184, 195
show tacacs command 59
show tacacs server-groups command 61
show tech-support aaa 65
show user command 62
single-connection command 65
ssh client knownhost command 178
ssh client source-interface command 179
ssh client vrf command 180
ssh command 177
ssh server command 181, 183, 184, 189
ssh server logging command 185
ssh server rate-limit command 186
ssh server session-limit command 187
ssh server v2 command 188
ssh timeout command 193
subject-name (trustpoint) command 150

T
tacacs source-interface command 72
tacacs-server host command 66
tacacs-server ipv4 command 70
tacacs-server key command 68
tacacs-server timeout command 69
task command 73
taskgroup command 74
timeout (TACACS+) command 75
timeout login response command 76

U
usergroup command 77
username command 78
users group command 82

V
vrf (MPP) command 117
vrf (RADIUS) command 83
vrf (TACACS+) command 84