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 the Cisco ASR 9000 Series Router Software configuration module in the System Security Configuration Guide for Cisco ASR 9000 Series Routers.

- clear ssh, on page 2
- clear netconf-yang agent session, on page 4
- netconf-yang agent ssh , on page 5
- sftp, on page 6
- sftp (Interactive Mode), on page 9
- show netconf-yang clients, on page 12
- show netconf-yang statistics, on page 13
- show ssh, on page 15
- show ssh session details, on page 18
- ssh, on page 20
- ssh client knownhost, on page 22
- ssh client source-interface, on page 24
- ssh client vrf, on page 26
- ssh server, on page 27
- ssh server rekey-time, on page 29
- ssh server rekey-volume, on page 30
- show ssh rekey, on page 31
- ssh server logging, on page 33
- ssh server rate-limit, on page 34
- ssh server session-limit, on page 36
- ssh server v2, on page 37
- ssh server netconf port, on page 38
- ssh server netconf , on page 40
- ssh timeout, on page 42
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**

- `session-id` Session ID number of an incoming connection as displayed in the `show ssh` command output. Range is from 0 to 1024.
- `outgoing session-id` Specifies the session ID number of an outgoing connection as displayed in the `show ssh` command output. Range is from 1 to 10.

**Command Default**

None

**Command Modes**

EXEC

**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>

**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</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/RSP0/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

```

RP/0/RSP0/CPU0:router# clear ssh 0

```
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/RSP0/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/RSP0/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>type</th>
<th>ver</th>
</tr>
</thead>
</table>

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/RSP0/CPU0:router# clear ssh 0

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssh, on page 15</td>
<td>Displays the incoming and outgoing connections to the router.</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**

EXEC mode

**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**

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/RSP0/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/RSP0/CPU0:router (config) # netconf-yang agent ssh
```
To start the secure FTP (SFTP) client, use the `sftp` command.

```
sftp [username @ host : remote-filenam e] source-filenamel dest-filenamel [source-interface type interface-path-id] [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>username</strong></td>
<td>(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.</td>
</tr>
<tr>
<td><strong>hostname:remote-filenam e</strong></td>
<td>(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.</td>
</tr>
<tr>
<td><strong>source-filenam e</strong></td>
<td>SFTP source, including the path.</td>
</tr>
<tr>
<td><strong>dest-filenam e</strong></td>
<td>SFTP destination, including the path.</td>
</tr>
<tr>
<td><strong>source-interface</strong></td>
<td>(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>Specifies the name of the VRF associated with the source interface.</td>
</tr>
</tbody>
</table>

**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**

EXEC

**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>

**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.

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.

<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`:

```plaintext
RP/0/RSP0/CPU0:router#sftp abc@ena-view1:ssh.diff disk0
```

In the following example, user `abc` is uploading multiple files from `disk0:/sam_*` to `/users/abc/` on a remote SFTP server called `ena-view1`:

```plaintext
RP/0/RSP0/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:

```plaintext
RP/0/RSP0/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
```

```plaintext
RP/0/RSP0/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:

```plaintext
RP/0/RSP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:
/disk0a:/V6copy
    Transferred 308413 Bytes
```
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/RSP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile
Connecting to 2.2.2.2...
Password:
disk0:/sampfile
   Transferred 986 Bytes
986 bytes copied in 0 sec (493000)bytes/sec
RP/0/RSP0/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/RSP0/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/RSP0/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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>(Optional) Name of the user performing the file transfer. The at symbol (@) following the username is required.</td>
</tr>
<tr>
<td><code>hostname:remote-filenam e</code></td>
<td>(Optional) Name of the Secure Shell File Transfer Protocol (SFTP) server. The colon (:) following the hostname is required.</td>
</tr>
<tr>
<td><code>source-interface</code></td>
<td>(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>Specifies the name of the VRF associated with the source interface.</td>
</tr>
</tbody>
</table>

**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**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</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
The following commands are not supported:

- lcd, lls, lpwd, lumask, lmkdir
- ln, symlink
- chgrp, chown
- !, !command
- ?
- mget, mput

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/RSP0/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:/frmRouterdownoad
/auto/tftp-server1-users5/admin/frmRouter
Transferred 1578 Bytes
1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againstServer
/disk0:/frmRouterdownoad
Transferred 1578 Bytes
1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```
In the following example, user `abc` is downloading and uploading a file from/to an external SFTP server using an IPv4 address:

```
RP/0/RSP0/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:/frmRouterdownload
/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownload againoServer
/disk0:/frmRouterdownload
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure Shell Commands</strong></td>
<td>ssh client source-interface, on page 24</td>
<td>Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td></td>
<td>ssh client vrf, on page 26</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.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

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 clients` command:

```
RP/0/RSP0/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 1: 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.

**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>5.3.0</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>config-services</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `show netconf-yang statistics` command:

```
RP/0/RSP0:router (config) # sh netconf-yang statistics
Summary statistics

  # requests| total time| min time per request| max
  time per request| avg time per request|
  other       | 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  close-session| 4         | 0h 0m 0s 3ms| 0h 0m 0s 0ms|
  kill-session| 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  get-schema   | 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  get-config   | 1         | 0h 0m 0s 1ms| 0h 0m 0s 1ms|
  edit-config  | 3         | 0h 0m 0s 2ms| 0h 0m 0s 0ms|
  commit       | 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  cancel-commit| 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  lock         | 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  unlock       | 0         | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
  discard-changes| 0    | 0h 0m 0s 0ms| 0h 0m 0s 0ms|
```
<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>
<tr>
<td>Total time</td>
<td>Total processing time of all requests of a given type</td>
</tr>
<tr>
<td>Min time per request</td>
<td>Minimum processing time for a request of a given type</td>
</tr>
<tr>
<td>Max time per request</td>
<td>Maximum processing time for a request of a given type</td>
</tr>
<tr>
<td>Avg time per request</td>
<td>Average processing time for a request type</td>
</tr>
</tbody>
</table>
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

EXEC

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 5.3.2</td>
<td>The command output was enhanced to reflect multichannel and subsystem support for ssh.</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

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

Examples

This is sample output from the `show ssh` command when SSH is enabled:

```
RP/0/RSP0/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/RSP0/CPU0:router# show ssh
SSH version : Cisco-2.0
```
This table describes significant fields shown in the display.

<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, Scp, Sftp-Subsystem, or Netconf-Subsystem)</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. For more information, see the System Management Command Reference for Cisco ASR 9000 Series Routers</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show ssh session details, on page 18</td>
<td>Displays the details for all the incoming and outgoing SSHv2 connections, to the router.</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.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</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.

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.

**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 ssh session details` command to display the details for all the incoming and outgoing SSHv2 connections:

```
RP/0/RSP0/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-sha1  hmac-sha1
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 4: 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>
</tbody>
</table>
### Field | Description
--- | ---
key-exchange | Key exchange algorithm chosen by both peers to authenticate each other.
pubkey | Public key algorithm chosen for key exchange.
incipher | Encryption cipher chosen for the Rx traffic.
outcipher | Encryption cipher chosen for the Tx traffic.
inmac | Authentication (message digest) algorithm chosen for the Rx traffic.
outmac | Authentication (message digest) algorithm chosen for the Tx traffic.

### 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 15</td>
<td>Displays all the incoming and outgoing connections to the router.</td>
</tr>
</tbody>
</table>
To start the Secure Shell (SSH) client connection and enable an outbound connection to an SSH server, use the `ssh` command.

```plaintext
ssh [vrf vrf-name] {ipv4-address|ipv6-address|hostname} [username user-id] [cipher aes {128-ctr|192-ctr|256-ctr|128-gcm|256-gcm}] [source-interface type interface-path-id] [command command-name]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4-address</code></td>
<td>IPv4 address in A:B:C:D format.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>IPv6 address in X:X::X format.</td>
</tr>
<tr>
<td><code>hostname</code></td>
<td>Hostname of the remote node. If the hostname has both IPv4 and IPv6 addresses, the IPv6 address is used.</td>
</tr>
<tr>
<td><code>username</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>cipher aes</code></td>
<td>SSHv2 supports only AES (protocol supports only ciphers greater than or equal to 128 bits)</td>
</tr>
<tr>
<td><code>source interface</code></td>
<td>(Optional) Specifies the source IP address of a selected interface for all outgoing SSH connections.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>command</code></td>
<td>(Optional) Specifies a remote command. Adding this keyword prompts the SSHv2 server to parse and execute the <code>ssh</code> command in non-interactive mode instead of initiating the interactive session.</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>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.1</td>
<td>Support for the <code>command</code> keyword was added.</td>
</tr>
<tr>
<td>Release 6.2.1</td>
<td>Cipher suite SSHv2 supports only AES (protocol supports only ciphers greater than or equal to 128 bits)</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 the `source-interface` keyword is specified in the `ssh` command, the `ssh` interface takes precedence over the interface specified in the `ssh client source-interface` 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/RSP0/CPU0:router# ssh remote-host 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 15</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:** Complete path of the filename (for example, slot0:/server_pubkey). The colon (`:`) and slash (`/`) are required.

### Command Default

None

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.7.2   | 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 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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/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/RSP0/CPU0:host1# exit
RP/0/RSP0/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.

**Command Default**

No source interface is used.

**Command Modes**

Global configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</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.

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.

**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 IP address of the Management Ethernet interface for all outgoing SSH connections:
configure
ssh client source-interface MgmtEth 0/RSP0/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

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.8.0</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 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 22 or `ssh client source-interface`, on page 24.

### 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 the SSH client being configured to start with the specified VRF:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client vrf green
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ssh client dscp &lt;value from 0 - 63&gt;</code></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**

- **vrf vrf-name**: Specifies the name of the VRF to be used by the SSH server. The maximum VRF length is 32 characters.
  - **Note**: If no VRF is specified, the default VRF is assumed.

- **ipv4 access-list access list name**: Configures an IPv4 access-list for access restrictions to the ssh server.

- **ipv6 access-list access list name**: Configures an IPv6 access-list for access restrictions to the ssh server.

- **v2**: Forces the SSH server version to be of only version 2.

**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**

Global configuration

**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 3.8.0</td>
<td>The <code>vrf</code> keyword was supported.</td>
</tr>
<tr>
<td>Release 4.0</td>
<td>The ipv4 / ipv6 access-list keywords are supported.</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 37` 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”:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server
```

### Examples

In the following example, the SSH server is configured to use IPv4 ACLs:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh servervrf vrf nameipv4 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. For more information, see the System Management Command Reference for Cisco ASR 9000 Series Routers.</td>
</tr>
<tr>
<td>ssh server v2, on page 37</td>
<td>Forces 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>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rekey-time time in minutes</td>
<td>Specifies the rekey-time interval in minutes. The range is between 30 to 1440 minutes.</td>
</tr>
</tbody>
</table>

Note  If no time interval is specified, the default interval is considered to be 30 minutes.

Command Default
None.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 6.2.1 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:

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rekey-time 450
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  data in megabytes
no ssh server rekey-volume
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>rekey-volume  data in megabytes</td>
<td>Specifies the volume-based rekey threshold in megabytes. The range is between 1024 to 4095 megabytes.</td>
</tr>
<tr>
<td><strong>Note</strong> If no volume threshold is specified, the default size is considered to be 1024 MB.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 6.2.1 This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Examples**

In the following example, the SSH server rekey-volume of 2048 minutes is used:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rekey-volume 2048
```
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.

Command Default

| Command Default | None |

Command Modes

| Command Modes | EXEC |

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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.

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>
<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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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**  
Global configuration

**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.

Only SSHv2 client connections are allowed.

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</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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server logging
```

**Related Commands**  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh server, on page 27</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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rate-limit</code></td>
<td>Number of incoming SSH connection requests allowed per minute. Range is from 1 to 600.</td>
</tr>
</tbody>
</table>

Despite being configured in minute the implementation of rate-limit is per second, per sub-second or per several seconds.

There are two different behaviors for this command depending on whether the configured value is <120 or >=120.

- **If the configured value is <120**, it means 1 session is allowed within (60/configured value) second(s). Below are the examples based on the configured value, which is <120:
  - If you configure 30 sessions per minute it means 1 session every (60/30) = 2 seconds.
  - If you configure 60 sessions per minute it means 1 session every (60/60) = 1 second.
  - If you configure 80 sessions per minute it means 1 session every (60/80) = 0.75 second.

- **If the configured value is >=120**, it means n sessions are allowed within 1 second and it allows for these connections to be simultaneous (at the exact same time). Below are the examples based on the configured value, which is >=120:
  - If you configure 120 sessions per minute it means 2 sessions every 1 second (which can be simultaneous).
  - If you configure 180 sessions per minute it means 3 sessions every 1 second (which can be simultaneous).
  - If you configure 180 sessions per minute it means 3 sessions every 1 second (which can be simultaneous).

In all the above listed cases, if you exceed the allowed configured value the subsequent connection attempts will be refused.

The connection attempts are to the ssh server and not bound per interface or username.

**Command Default**

`rate-limit`: 60 connection requests per minute

**Command Modes**

Global Configuration mode

**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>
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.

<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/RSP0/CPU0:router# configure
RP/0/RSP0/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**

Global configuration

**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>

**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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server session-limit 50
```
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.

```plaintext
ssh server v2
no ssh server v2
```

**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>3.7.2</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.

Only SSHv2 client connections are allowed.

**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 initiate the SSH server version to be only SSHv2:

```plaintext
RP/0/RSP0/CPU0:router(config)# configure
RP/0/RSP0/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 portport number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Port number for the netconf SSH server (default port number is 830).</td>
</tr>
<tr>
<td>port-number</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**
The default port number is 830.

**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</td>
<td>The <code>ssh server netconf</code> command is no longer auto completed to configure the default port. This command is now optional</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.

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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server netconf port 831
```

**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>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>netconf-yang agent ssh</td>
<td>Configures the <strong>ssh netconf-yang backend</strong> for the netconf subsystem (Required to allow the system to service netconf-yang requests). For more information, see the <em>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</em>.</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**

- `vrf name`: Specifies the name of the VRF to be used by the netconf subsystem of the SSH server. The maximum VRF length is 32 characters.
  - **Note**: If no VRF is specified, the default VRF is assumed.

- `IPv4 access list name`: Configures an IPv4 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>5.3.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>The <code>ssh server netconf</code> command is no longer auto completed to configure the default port. The <code>vrf</code> keyword was supported.</td>
</tr>
</tbody>
</table>

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.

**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.

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

**Example**

This example shows how to use the `ssh server netconf vrf vrf name` command:

```plaintext
RP/0/RSP0/CPU0:router (config) # ssh server netconf vrf red
```
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**
- Global configuration

**Command History**
- Release 3.7.2 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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh timeout 60
```