Implementing the Network Configuration Protocol

This module provides details of the Network Configuration Protocol. For relevant commands, see *Cisco IOS XR System Security Command Reference for the Cisco CRS Router*.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.0</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 5.3.1</td>
<td>Support extended for more Yang models.</td>
</tr>
<tr>
<td>Release 6.0</td>
<td>Support extended for the Netconf subsystem configuration to be vrf aware. The configuration of the netconf port is no longer sufficient to start the Netconf subsystem support. At least one vrf needs to be configured. The configuration of the port is now optional.</td>
</tr>
</tbody>
</table>

- The Network Configuration Protocol, page 1
- Netconf and Yang, page 3
- Supported Yang Models, page 4
- Denial of Services Defence for Netconf-Yang, page 4
- Enabling NETCONF over SSH, page 5
- Additional Reference, page 7

The Network Configuration Protocol

The Network Configuration Protocol (Netconf) provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. Yang is a data modeling language used with Netconf.
Netconf uses a simple RPC-based (Remote Procedure Call) mechanism to facilitate communication between a client and a server. The client can be a script or application typically running as part of a network manager. The server is typically a network device.

The configuration of features need not be done the traditional way (using CLIs), the client application (controller) reads the Yang model and communicates with the Netconf server (IOS XR) accordingly.

Netconf Sessions and Operations

A Netconf session is the logical connection between a network configuration application and a network device. A device should be capable of supporting multiple sessions and atleast one Netconf session.

Characteristics of a netconf session:

- Netconf is connection-oriented - SSH or TLS can be the underlying transport.
- The netconf client establishes session with the server.
- Netconf sessions are established with the hello message. Features and capabilities are announced.
- Sessions can be terminated using the close or kill messages.

Basic Netconf operations:

- Get configuration <get-config>
- Get all information <get>
- Edit configuration <edit-config>
- Copy configuration <copy-config>
- Delete configuration <delete-config>
- <lock>, <unlock>
- <kill-session>
- <close-session>
- Commit configuration <commit>

The Yang data model

Each feature has a defined Yang Model which is synthesized from the schemas. A model is published in a tree format and includes:

- Top level nodes and their subtrees
- Subtrees that augment nodes in other yang models

Example: The aaa Yang model

```
module: Cisco-IOS-XR-aaa-lib-cfg
  +--rw aaa
    +--rw accountings
      | +--rw accounting* [type listname]
      |   +--rw type xr:Cisco-ios-xr-string
      |   +--rw listname xr:Cisco-ios-xr-string
      |   +--rw rp-failover? Aaa-accounting-rp-failover
```
Advantages of using the Yang model are:

- Yang supports programmatic interfaces.
- Yang supports simplified network management applications.
- Yang supports interoperability that provides a standard way to model management data.

### Netconf and Yang

The workflow displayed here, will help the user to understand how Netconf-Yang can configure and control the network with minimal user intervention. The required components:

- Cisco Router (ASR9000 series or CRS) with Netconf capability
- Netconf Client Application with connection to the router

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Device / component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco router (ASR 9000 or CRS router)</td>
<td>Login/ access the router.</td>
</tr>
</tbody>
</table>
| 2      | Cisco router      | Prerequisites for enabling Netconf.  
|        |                   |   • k9sec pie must be installed.  
|        |                   |   • Crypto keys must be generated. |
| 3      | Cisco router      | Enable Netconf agent. Use the `netconf-yang agent ssh` and `ssh server netconf` command. The port can be selected. By default, it is set as 830. |
| 4      | Cisco router      | Yang models are a part of the software image. The models can be retrieved from the router , using the `<get-schema>` operation. |
Supported Yang Models

The Yang models can be downloaded from a prescribed location (ftp server) or can also be retrieved directly from the router using the get-schema operation.

For a feature, separate Yang models are available for configuring the feature and to get operational statistics (show commands). The -cfg.yang suffix denotes configuration and -oper*.yang is for operational data statistics. In some cases, -oper is followed by -sub, indicating that a submodule(s) is available.

For a list of supported Yang models, see https://github.com/YangModels/yang/tree/master/vendor/cisco/xr

Denial of Services Defence for Netconf-Yang

In case of a DoS (Denial of Service) attack on Netconf, wherein, Netconf receives numerous requests in a short span of time, the router may become irresponsive if Netconf consumes most of the bandwidth or CPU processing time. This can be prevented, by limiting the traffic directed at the Netconf agent. This is achieved using the netconf-yang agent rate-limit and netconf-yang agent session commands.

If rate-limit is set, the Netconf processor measures the incoming traffic from the SSH server. If the incoming traffic exceeds the set rate-limit, the packets are dropped.

If session-limit is set, the Netconf processor checks for the number of open sessions. If the number of current sessions is greater than or equal to, the set limit, no new sessions are opened.
Session idle-timeout and absolute-timeout also prevent DoS attacks. The Netconf processor closes the sessions, even without user input or intervention, as soon as the timeout session is greater than or equal to the set time limit.

The relevant commands are discussed in detail, in the *Cisco IOS XR System Security Command Reference for the Cisco CRS Router*

## Enabling NETCONF over SSH

This task enables NETCONF over SSH. SSH is currently the only supported transport method.

If the client supports, Netconf over ssh can utilize the multi-channeling capabilities of IOS XR ssh server. For additional details about Multi-channeling in SSH, see *Implementing Secure Shell in System Security Configuration Guide*.

### Prerequisites:

- k9sec pie must be installed, otherwise the port configuration for the netconf ssh server cannot be completed. (The Netconf subsystem for SSH, as well as, SSH cannot be configured without the k9sec pie.)
- Crypto keys must be generated prior to this configuration.
- The Netconf-YANG feature is packaged in the mgbl pie, which must be installed before enabling the Netconf-YANG agent.

### SUMMARY STEPS

1. configure
2. netconf-yang agent ssh
3. ssh server netconf [vrf vrf-name[ipv4 access-listipv4 access list name][ipv6 access-list ipv6 access list name]]
4. ssh server netconf port port-number

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>netconf-yang agent ssh</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RP0/CPU0:router (config) # netconf agent ssh</td>
</tr>
<tr>
<td></td>
<td>Enables NETCONF agent over SSH connection. After NETCONF is enabled, the Yang model in the controller, can configure the relevant models.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Yang models can be retrieved from the router via NETCONF &lt;get-schema&gt; operation.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ssh server netconf [vrf vrf-name[ipv4 access-listipv4 access list name][ipv6 access-list ipv6 access list name]]</td>
</tr>
<tr>
<td></td>
<td>Brings up the netconf subsystem support with SSH server using a specified VRF of up to 32 characters. If no VRF is specified, the default VRF is used. To stop the SSH server from receiving any further connections for the specified VRF, use the no form of this command.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>RP/0/RP0/CPU0:router (config) # ssh server netconf vrf netconfvrf ipv4 access-list InternetFilter</td>
<td>Note: The netconf subsystem support with SSH server can be configured for use with multiple VRFs.</td>
</tr>
</tbody>
</table>

**Step 4**

```bash
ssh server netconf port port-number
```

**Example:**

```bash
RP/0/RP0/CPU0:router (config) # ssh server netconf port 830
```

Configures a port for the netconf ssh server. This command is optional. If no port is specified, port 830 is used by default.

**Note:** 830 is the IANA-assigned TCP port for NETCONF over SSH, but it can be changed using this command.

---

**What to Do Next**

The `show netconf-yang statistics` command and `show netconf-yang clients` command can be used to verify the configuration details of the netconf agent.

The `clear netconf-yang agent session` command clears the specified Netconf session (on the Netconf server side).

---

**Examples: Netconf over SSH**

This section illustrates some examples relevant to Netconf:

**Enabling netconf-yang for ssh transport and netconf subsystem for default vrf with default port (830)**

```bash
config
netconf-yang agent ssh
ssh server netconf vrf default
! 
```

**Enabling netconf-yang for ssh transport and netconf subsystem for vrf green and vrf red with netconf port (831)**

```bash
config
netconf-yang agent ssh
! 
ssh server netconf vrf green
ssh server netconf vrf red
ssh server netconf port 831
! 
```

---

**Show command outputs**

<table>
<thead>
<tr>
<th>Command outputs</th>
</tr>
</thead>
</table>

```
show netconf-yang statistics
Summary statistics | requests| total time| min time per request| max
| time per request| avg time per request| time per request| time per request| time per request| time per request|
| other 0| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms|
| close-session 0| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms|
| kill-session 0| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms|
| get-schema 0| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms|
| get 0| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms| 0h 0m 0s 0ms|
```
### Additional Reference

#### Table 1: Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netconf-Yang</td>
<td>For related commands, see <em>Cisco IOS XR System Security Command Reference for the Cisco CRS Router</em></td>
</tr>
</tbody>
</table>

#### Table 2: Standards

<table>
<thead>
<tr>
<th>Component</th>
<th>RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>YANG</td>
<td>6020</td>
</tr>
<tr>
<td>NETCONF</td>
<td>6241</td>
</tr>
<tr>
<td>NETCONF over SSH</td>
<td>6242</td>
</tr>
</tbody>
</table>
Implementing the Network Configuration Protocol

Additional Reference