Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Cisco 910 Industrial Routers (hereafter referred to as the router).

- Understanding SNMP, page 1
- Configuring SNMP, page 3
- Displaying SNMP Status, page 10

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the router. To configure SNMP on the router, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager’s requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

These sections contain this conceptual information:

- SNMP Versions, page 1
- SNMP Agent Functions, page 3
- SNMP Community Strings, page 3
- SNMP Notifications, page 3

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.
SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:

- Message integrity—ensuring that a packet was not tampered with in transit
- Authentication—determining that the message is from a valid source
- Encryption—mixing the contents of a package to prevent it from being read by an unauthorized source.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent’s MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Table 14 identifies the characteristics of the different combinations of security models and levels.

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv2C</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authNoPriv</td>
<td>Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authPriv</td>
<td>Data Encryption Standard (DES) or Advanced Encryption Standard (AES)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms:</td>
</tr>
<tr>
<td></td>
<td>(requires the cryptographic software image)</td>
<td></td>
<td></td>
<td>- DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 3DES 168-bit encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- AES 128-bit, 192-bit, or 256-bit encryption</td>
</tr>
</tbody>
</table>

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.
SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.

- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the router, the community string definitions on the NMS must match at least one of the three community string definitions on the router.

A community string can have one of these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access

- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

SNMP Notifications

SNMP allows the router to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword *traps* refers to either traps or informs, or both. Use the `snmp-server host` command to specify whether to send SNMP notifications as traps or informs.

SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be re-sent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be re-sent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the router is a concern and notification is not required, use traps.

Configuring SNMP

- Default SNMP Configuration, page 4
- Configuring Community Strings, page 4
- Configuring SNMP Groups and Users, page 5
Default SNMP Configuration

Table 15 shows the default SNMP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP agent</td>
<td>Enabled.</td>
</tr>
<tr>
<td>SNMP trap receiver</td>
<td>None configured.</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>Enabled.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>If no version keyword is present, the default is Version 1.</td>
</tr>
<tr>
<td>SNMPv3 authentication</td>
<td>If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.</td>
</tr>
<tr>
<td>SNMP notification type</td>
<td>If no type is specified, all notifications are sent.</td>
</tr>
</tbody>
</table>

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. Optionally, you can specify one or more of these characteristics associated with the string:

- **A MIB view**, which defines the subset of all MIB objects accessible to the given community
- **Read and write or read-only permission** for the MIB objects accessible to the community
Beginning in privileged EXEC mode, follow these steps to configure a community string on the router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2. snmp-server community string [view view-name] [ro | rw] | Configure the community string.  
- For string, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length.  
- (Optional) For view, specify the view record accessible to the community.  
- (Optional) Specify either read-only (ro) if you want authorized management stations to retrieve MIB objects, or specify read-write (rw) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. |
| 3. snmp-server view view-name oid-tree {included | excluded} | Create or update an SNMP view entry.  
- For view-name, specify the name of the view.  
- For oid-tree, specify MIB view family name with:  
  - OID. For example, .1.3.6.1.  
  - Object name. For example, .internet.  
- Specify either included if MIB family name is included in the view, or excluded if MIB family name is excluded from the view. |
| 4. exit | Return to privileged EXEC mode. |
| 5. show running-config | Verify your entries. |
| 6. copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To remove a specific community string, use the no snmp-server community string global configuration command.

This example shows how to assign the string public to SNMP, to allow read-only access:

Router(config)# snmp-server community public ro

Configuring SNMP Groups and Users

You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the router:
### Configuring SNMP

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>2.</td>
<td><code>snmp-server group</code>&lt;br&gt;groupname {v1 / v2c</td>
</tr>
<tr>
<td>3.</td>
<td><code>snmp-server user</code>&lt;br&gt;username&lt;br&gt;groupname {v1 / v2c</td>
</tr>
</tbody>
</table>

- **Command Purpose**

  1. `configure terminal`
     - Enter global configuration mode.

  2. `snmp-server group`<br>groupname {v1 / v2c | v3<br>[auth | noauth | priv]} [read readview] [write writeview]<br>
     - Configure a new SNMP group on the remote device.
     - For `groupname`, specify the name of the group.
     - Specify a security model:
       - `v1` is the least secure of the possible security models.
       - `v2c` is the second least secure model. It allows transmission of informs and integers twice the normal width.
       - `v3`, the most secure, requires you to select an authentication level:
         - `auth`—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.
         - `noauth`—Enables the noAuthNoPriv security level. This is the default if no keyword is specified.
         - `priv`—Enables Data Encryption Standard (DES) packet encryption (also called `privacy`).
     - (Optional) Enter `read readview` with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent. Default read view is `v1default`.
     - (Optional) Enter `write writeview` with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent. Default write view is `none`.

  3. `snmp-server user`<br>username<br>groupname {v1 / v2c | v3<br>[auth {md5 | sha<br>auth-password}] | [priv {des | aes } priv-password] | Add a new user for an SNMP group.
     - The `username` is the name of the user on the host that connects to the agent.
     - The `groupname` is the name of the group to which the user is associated.
     - Enter the SNMP version number (`v1`, `v2c`, or `v3`). If you enter `v3`, you have an additional option:
       - `auth`—An authentication level setting session that can be either the HMAC-MD5-96 (`md5`) or the HMAC-SHA-96 (`sha`) authentication level and requires a password string `auth-password` (not to exceed 64 characters).
     - If you enter `v3`, you can also configure a private (`priv`) encryption algorithm and password string `priv-password` (not less than 8 alphanumeric characters and not to exceed 64 characters).
       - `priv` specifies the User-based Security Model (USM).
       - `des` specifies the use of the 56-bit DES algorithm.
       - `aes` specifies the use of the AES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.
Configuring SNMP

This example shows how to configure an snmp group with the name *grp1*:

```
Router(config) # snmp-server group grp1 v3 priv read view1 write view1
```

This example shows how to configure an snmp user *user1*:

```
Router(config) # snmp-server user user1 grp1 v3 auth md5 12345678 priv des 12345678
```

Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the router generates when certain events occur. The following notification types are supported on the router:

- snmp authentication
- snmp linkdown
- snmp linkup

By default, no trap manager is defined, and no traps are sent.

You can enable any or all of these traps and configure a trap manager to receive them. To enable the sending of SNMP inform notifications, use the `snmp-server enable traps` global configuration command combined with the `snmp-server host host-addr informs` global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure the router to send traps or informs to a host:

**Command** | **Purpose**
--- | ---
4. | Exit Return to privileged EXEC mode.
5. | `show running-config` Verify your entries.
6. | `copy running-config startup-config` (Optional) Save your entries in the configuration file.

This example shows how to configure an snmp group with the name *grp1*:

```
Router(config) # snmp-server group grp1 v3 priv read view1 write view1
```

This example shows how to configure an snmp user *user1*:

```
Router(config) # snmp-server user user1 grp1 v3 auth md5 12345678 priv des 12345678
```

**Command** | **Purpose**
--- | ---
1. | `configure terminal` Enter global configuration mode.
2. | `snmp-server user username groupname {v1 / v2c | v3 [auth {md5 | sha} auth-password] [priv {des | aes} priv-password]}` Configure an SNMP user.
3. | `snmp-server group groupname {v1 / v2c | v3 [auth | noauth | priv] [read readview] [write writeview]}` Configure an SNMP group.

Note: To display SNMPv3 information about auth | noauth | priv mode configuration, you must enter the `show snmp user` privileged EXEC command.

(Optional) Save your entries in the configuration file.
### Configuring SNMP

The `snmp-server host` command specifies which hosts receive the notifications. The `snmp-server enable trap` command globally enables the mechanism for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an `snmp-server host informs` command for the host and globally enable informs by using the `snmp-server enable traps` command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. <strong>snmp-server host</strong> `host-addr [informs</td>
<td>traps] [version {1 / 2c</td>
</tr>
<tr>
<td></td>
<td>- For <code>host-addr</code>, specify the name or Internet address of the host (the targeted recipient).</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Enter <code>informs</code> to send SNMP informs to the host.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Enter <code>traps</code> (the default) to send SNMP traps to the host.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Specify the SNMP version (1, 2c, or 3). Default is version 1. SNMPv1 does not support informs.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For Version 3, select authentication level <code>auth</code>, <code>noauth</code>, or <code>priv</code>.</td>
</tr>
<tr>
<td><strong>Note:</strong> The <code>priv</code> keyword is available only when the cryptographic software image is installed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- For <code>community-string</code>, when version 1 or version 2c is specified, enter the password-like community string sent with the notification operation. When version 3 is specified, enter the SNMPv3 username.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>port</code>, specify the UDP port of the notification host. Default is port 162.</td>
</tr>
<tr>
<td>5. <strong>snmp-server inform</strong> <code>[retries retries] [timeout timeout]</code></td>
<td>(Optional) Specify SNMP inform request options.</td>
</tr>
<tr>
<td></td>
<td>- For <code>retries</code>, specify the retry count for informs. Default is 3. Valid range is from 0 to 100.</td>
</tr>
<tr>
<td></td>
<td>- For <code>timeout</code>, specify the timeout for informs in seconds. Default is 15 seconds. Valid range is from 0 to 4294967 seconds.</td>
</tr>
<tr>
<td>6. <strong>snmp-server enable traps</strong> <code>[notification-types]</code></td>
<td>Enable the router to send traps or informs and specify the type of notifications to be sent. The following notification types are supported on the router:</td>
</tr>
<tr>
<td></td>
<td>- snmp authentication</td>
</tr>
<tr>
<td></td>
<td>- snmp linkdown</td>
</tr>
<tr>
<td></td>
<td>- snmp linkup</td>
</tr>
<tr>
<td></td>
<td>By default, all supported notification types are enabled.</td>
</tr>
<tr>
<td>7. <strong>exit</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8. <strong>show running-config</strong></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Note:</strong> To display SNMPv3 information about `auth</td>
<td>noauth</td>
</tr>
<tr>
<td>9. <strong>copy running-config startup-config</strong></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove the specified host from receiving traps, use the no snmp-server host host global configuration command. The no snmp-server host command with no keywords disables traps, but not informs, to the host. To disable informs, use the no snmp-server host informs global configuration command. To disable a specific trap type, use the no snmp-server enable traps notification-types global configuration command.

This example shows how to enable the router to send all SNMP notification types:

Router(config)# snmp-server enable traps snmp

This example shows how to configure the host 192.168.1.0 to receive SNMPv2c traps:

Router(config)# snmp-server host 192.168.1.0 traps version 2c public

### Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2. snmp-server contact text</td>
<td>Set the system contact string. For example: snmp-server contact SystemOperator</td>
</tr>
<tr>
<td>3. snmp-server location text</td>
<td>Set the system location string. For example: snmp-server location Building3</td>
</tr>
<tr>
<td>4. exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5. show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6. copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### SNMP Agent Configuration Example

The following example shows how to configure the SNMP agent:

Router# configure terminal
Router(config)# snmp-server community public ro
Router(config)# snmp-server community private rw
Router(config)# snmp-server contact SystemOperator
Router(config)# snmp-server location Building3
Router(config)# snmp-server view view1 .1.3.6.1 included
Router(config)# snmp-server view view1 .1.3.6.1.6.3.15 excluded
Router(config)# snmp-server group grp1 v3 priv read view1 write view1
Router(config)# snmp-server user user1 grp1 v3 auth md5 12345678 priv des 12345678
Router(config)# snmp-server enable traps snmp authentication
Router(config)# snmp-server host 192.168.1.0 traps version 2c public
Router(config)# snmp-server host 192.168.1.1 traps version 3 priv user1
Router(config)# exit
Configuring SNMP

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the `show snmp` privileged EXEC command. You also can use the other privileged EXEC commands in Table 16 to display SNMP information.

### Table 16  Commands for Displaying SNMP Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show snmp</code></td>
<td>Displays SNMP statistics.</td>
</tr>
<tr>
<td><code>show snmp community</code></td>
<td>Displays all SNMP community access strings.</td>
</tr>
<tr>
<td><code>show snmp contact</code></td>
<td>Displays SNMP contact information.</td>
</tr>
<tr>
<td><code>show snmp group</code></td>
<td>Displays SNMP group information.</td>
</tr>
<tr>
<td><code>show snmp host</code></td>
<td>Displays information configured for SNMP notification operation.</td>
</tr>
<tr>
<td><code>show snmp location</code></td>
<td>Displays SNMP location information.</td>
</tr>
<tr>
<td><code>show snmp mib</code></td>
<td>Display a list of the MIB module OIDs registered on the system.</td>
</tr>
<tr>
<td><code>show snmp user</code></td>
<td>Displays information on each SNMP user name in the SNMP users table.</td>
</tr>
<tr>
<td><code>show snmp view</code></td>
<td>Displays the SNMP view configuration.</td>
</tr>
</tbody>
</table>

You can use the following commands in user mode as well to display SNMP status:

- `show snmp`
- `show snmp contact`
- `show snmp location`

This example shows the SNMP server statistics:

```
Router# show snmp
1 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  11 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  15 Get-next PDUs
  0 Set-request PDUs
1 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  25 Response PDUs
  0 Trap PDUs
SNMP global trap: disabled
SNMP informs: disabled

SNMP agent enabled
```
Configuring SNMP

This example shows the SNMP community:

Router# show snmp community
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile  active

Community name: private
Community Index: private
Community SecurityName: private
storage-type: nonvolatile  active

This example shows the SNMP group:

Router# show snmp group

<table>
<thead>
<tr>
<th>groupname: kp_grp</th>
<th>security model: v3 auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>readview: kp_view</td>
<td>writeview: kp_view</td>
</tr>
<tr>
<td>row status: active</td>
<td></td>
</tr>
</tbody>
</table>

This example shows the SNMP host:

Router# show snmp host

Notification host: 172.18.60.61 udp-port: 162  type: inform
user: public  security model: v2c

Notification host: 172.18.60.61 udp-port: 150  type: trap
user: kpuser  security model: v3 priv

This example shows the SNMP user:

Router# show snmp user

User name: kp_user
Engine ID: 800000090300006440F0D281
storage-type: nonvolatile  active
Authentication Protocol: None
Privacy Protocol: None
Group-name: kp_grp

This example shows the SNMP views:

Router# show snmp views

vldefault .iso - included permanent active
vldefault .iso.org.dod.internet - included permanent active
vldefault .iso.org.dod.internet.snmpV2.snmpModules.snmpUsmMIB - excluded permanent active
vldefault .iso.org.dod.internet.snmpV2.snmpModules.snmpVacmMIB - excluded permanent active
view1 .1.3.6 - included permanent active