

Chapter 26

Configure SNMP

To configure SNMP, you include statements at the [edit snmp] hierarchy level of the configuration.

```
snmp {
  description description;
  location location;
  contact contact;
  interface [ interface-names ];
  community community-name {
    authorization authorization;
    clients {
      default restrict;
      address <restrict>;
    }
  }
  trap-group group-name {
    categories category;
    targets {
      address;
    }
    version version;
  }
  traceoptions {
    file <files number> <size size>;
    flag flag <disable>;
  }
}
```

By default, SNMP is disabled.

This section describes the minimum required configuration and discusses the following tasks for configuring SNMP:

Minimum SNMP Configuration on page 284

Enable SNMP on page 284

Configure the System Contact on page 284

Configure the System Location on page 285

Configure the System Description on page 285

Configure the SNMP Community String on page 286

Configure SNMP Trap Groups on page 287

Configure the Interfaces on which SNMP Requests Can Be Accepted on page 288

Trace SNMP Traffic on page 288

Minimum SNMP Configuration

All SNMP configuration statements are optional.

Enable SNMP

To enable SNMP on the router, include the following statement in the configuration:

```
[edit]
snmp;
```

Configure the System Contact

You can specify an administrative contact for each system being managed by SNMP. This name is placed into the MIB II sysContact object. To configure a contact name, include the contact statement at the [edit snmp] hierarchy level:

```
[edit snmp]
contact contact;
```

If the name contains spaces, enclose it in quotation marks (" ").

Example: Configure the System Contact

Define the system contact:

```
[edit]
snmp {
  contact "Junipero Berry, (650) 555-1234";
}
```

Configure the System Location

You can specify the location of each system being managed by SNMP. This string is placed into the MIB II sysLocation object. To configure a system location, include the location statement at the [edit snmp] hierarchy level:

```
[edit snmp]
location location;
```

If the location contains spaces, enclose it in quotation marks (" ").

Example: Configure the System Location

Specify where the system is located:

```
[edit]
snmp {
  location "Row 11, Rack C";
}
```

Configure the System Description

You can specify a description for each system being managed by SNMP. This string is placed into the MIB II sysDescription object. To configure a description, include the description statement at the [edit snmp] hierarchy level:

```
[edit snmp]
description description;
```

If the description contains spaces, enclose it in quotation marks (" ").

Example: Configure the System Description

Specify the system description:

```
[edit]
snmp {
  description "M40 router with 8 FPCs";
}
```

Configure the SNMP Community String

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string, include the community statement at the [edit snmp] hierarchy level:

```
[edit snmp]
community name {
  authorization authorization;
  clients {
    default restrict;
    address <restrict>;
  }
}
```

If the community name contains spaces, enclose it in quotation marks (" ").

The default authorization level for a community is read-only. You can change this to read-write; however, the JUNOS SNMP implementation currently does not support Set requests.

You can specify the members of the community in the clients statement. For the *address*, you must specify an address, not a host name. Community members are SNMP clients that are allowed to access the local router. If you do not specify any addresses, all SNMP clients have access to the router. Include the default restrict option to deny access to all SNMP clients for which access is not explicitly granted. We recommend that you always include the default restrict option to limit SNMP client access to the local router.

Examples: Configure the SNMP Community String

Grant read-only access to all clients. With this configuration, the system responds to SNMP Get, GetNext, and GetBulk commands that contain the community string public.

```
[edit]
snmp {
  community public {
    authorization read-only;
  }
}
```

Grant read-write access to all clients. With this configuration, the system responds to SNMP SetRequest commands that contain the community string private. (The JUNOS SNMP implementation currently does not support Set requests.)

```
[edit]
snmp {
  community private {
    authorization read-write;
  }
}
```

Allow read-only access to clients with IP addresses in the range 172.16.0.0/16, and deny access to systems in the range of 172.16.3/24:

```
[edit]
snmp {
  community field-service {
    authorization read-only;
    clients {
      default restrict;      # Restrict access to all SNMP clients not explicitly
                            # listed on the following lines.
      172.16.0.0/16;        # Allow access by all clients in 172.16/16 except
      172.16.3/24 restrict; # 172.16.3/24
    }
  }
}
```

Configure SNMP Trap Groups

You can create and name a group of one or more types of SNMP traps and then define which systems receive the group of SNMP traps. To create an SNMP trap group, include the trap-group statement at the [edit snmp] hierarchy level:

```
[edit snmp]
trap-group group-name {
  categories category;
  targets {
    address;
  }
  version version;
}
```

The trap group name can be any string of your choice and is used in SNMP display output. Each trap group you define must have a name and one or more targets, which are the systems that receive the SNMP traps. Specify the targets by address, not by host name.

Specify the types of traps the trap group can receive in the categories statement. For information about the traps that the JUNOS software supports, see “SNMP Traps Supported by the JUNOS Software” on page 262.

Specify the SNMP version level in the version statement.

Example: Configure SNMP Trap Groups

Set up a trap notification list named urgent-dispatcher for link and startup traps. This list is used to identify the network management hosts (192.168.10.22 and 172.17.1.2) to which traps generated by the local router should be sent. The name specified for a trap group is used as the SNMP community string when the agent sends traps to the listed targets.

```
[edit]
snmp {
  trap-group "urgent-dispatcher" {
    version v2;
    categories link startup;
    targets {
      192.168.10.22;
      172.17.1.2;
    }
  }
}
```


routing-socket—Trace routing socket calls.

subagent—Trace subagent restarts.

timer—Trace internal timer events.

varbind-error—Trace variable binding errors.

Examples: Trace SNMP Traffic

Trace information about SNMP packets:

```
[edit]
snmp {
  traceoptions {
    file size 10k files 5;
    flag pdu;
    flag protocol-timeouts;
    flag varbind-error;
  }
}
```

