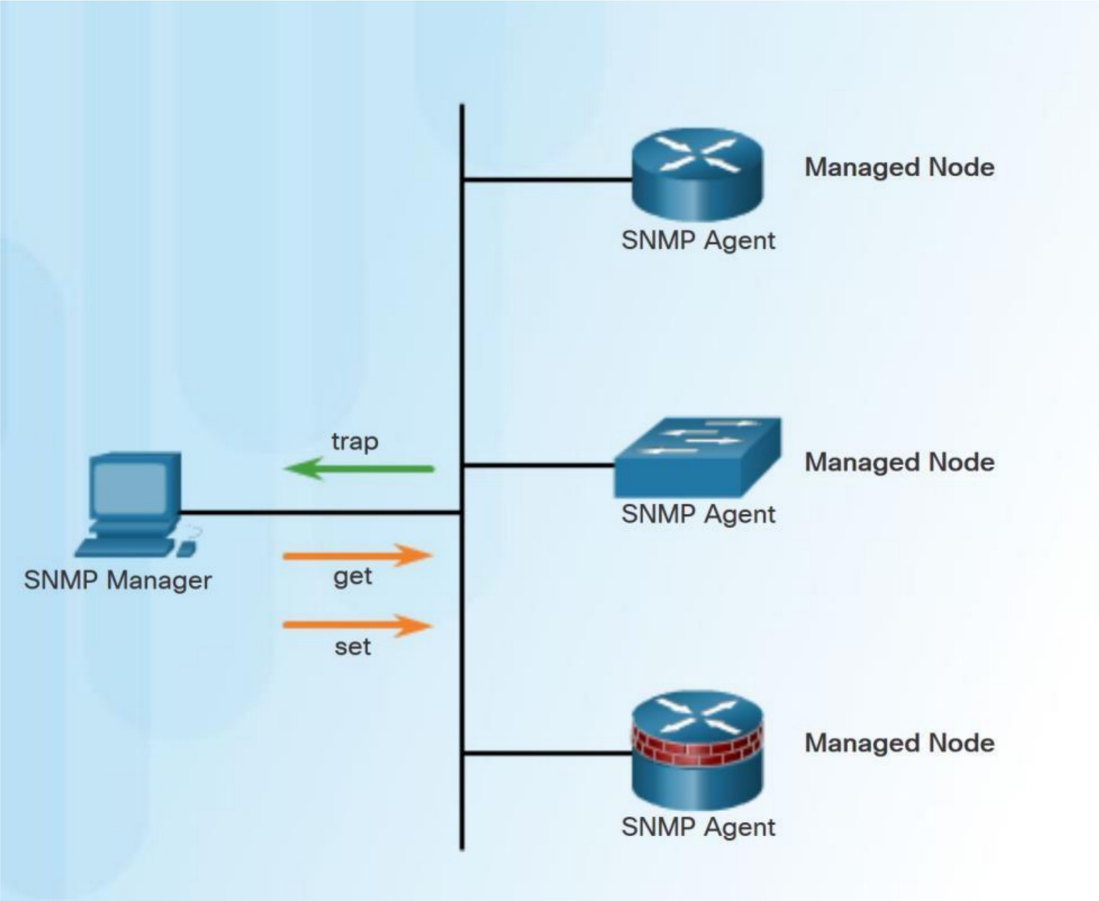
SNMP

SNMP Operation

Introduction to SNMP

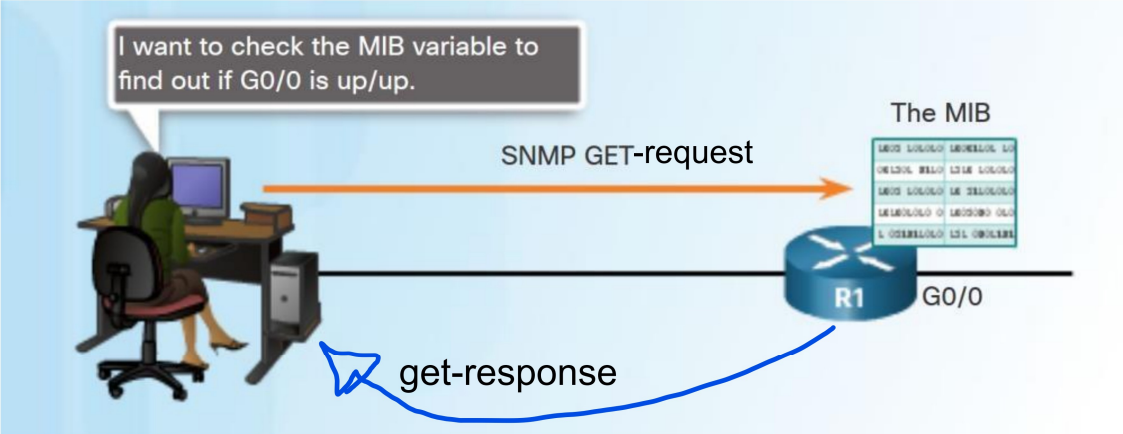
- Simple Network Management Protocol (SNMP) enables network administrators to monitor and manage network nodes.
- The SNMP system consists of three elements:
  - **SNMP manager-** collects information from an SNMP agent using the "get" action. Changes configurations on an agent using the "set" action.
  - **SNMP agents** (managed node)
  - **Management Information Base (MIB)-** stores data and operational statistics about the managed device. (in SNMP agent side)



SNMP Operation

- SNMP agents that reside on managed devices collect and store information about the device.
- This information is stored by the agent locally in the MIB.
- SNMP manager then uses the SNMP agent to access information within the MIB.
- SNMP agent responds to SNMP manager requests as follows:
  - **Get an MIB variable** - The SNMP agent performs this n response to a GetRequest-PDU from the network manager.
  - **Set an MIB variable** - The SNMP agent performs this in response to a SetRequest-PDU from the network manager.

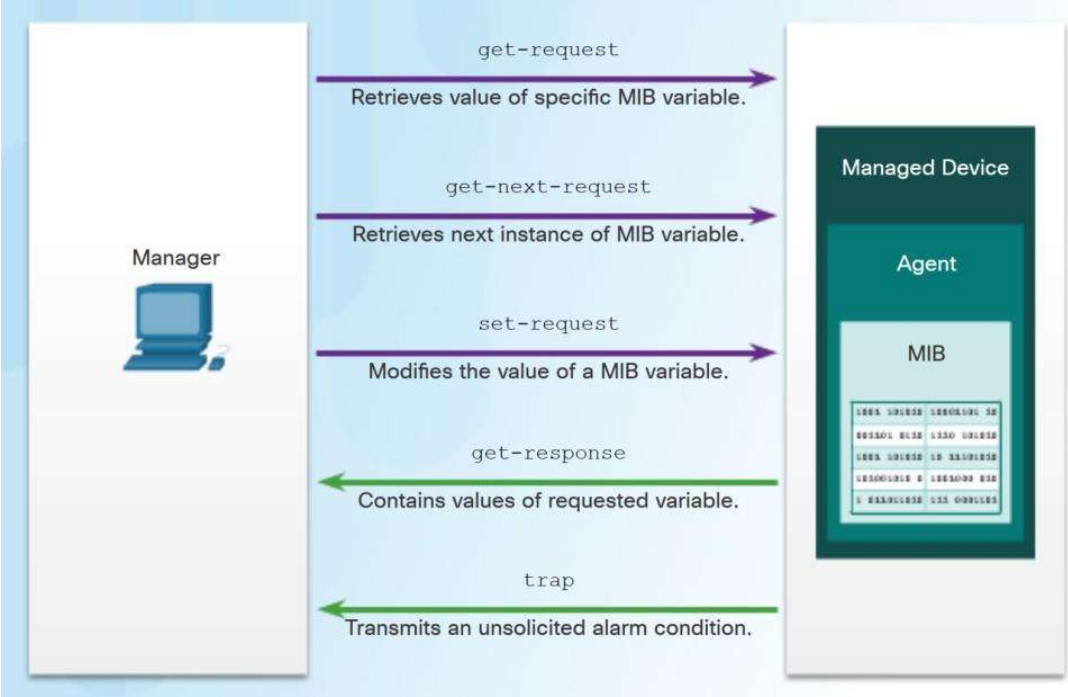
Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.



PDU:-Data unit carry the discussion between SNMP manager and SNMP agent

SNMP Operation

SNMP Agent Traps



- An Network Management System (NMS) periodically polls the SNMP agents using the get request.
- Using this process, SNMP can collect information to monitor traffic loads and to verify device configurations of managed devices.
- SNMP agents to generate and send traps to inform the NMS immediately of certain events.
  - Traps are unsolicited messages alerting the SNMP manager to a condition or event such as improper user authentication or link status.

SNMP Operation

SNMP Versions

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. • 3DES 168-bit encryption. • AES 128-bit, 192-bit, or 256-bit encryption.

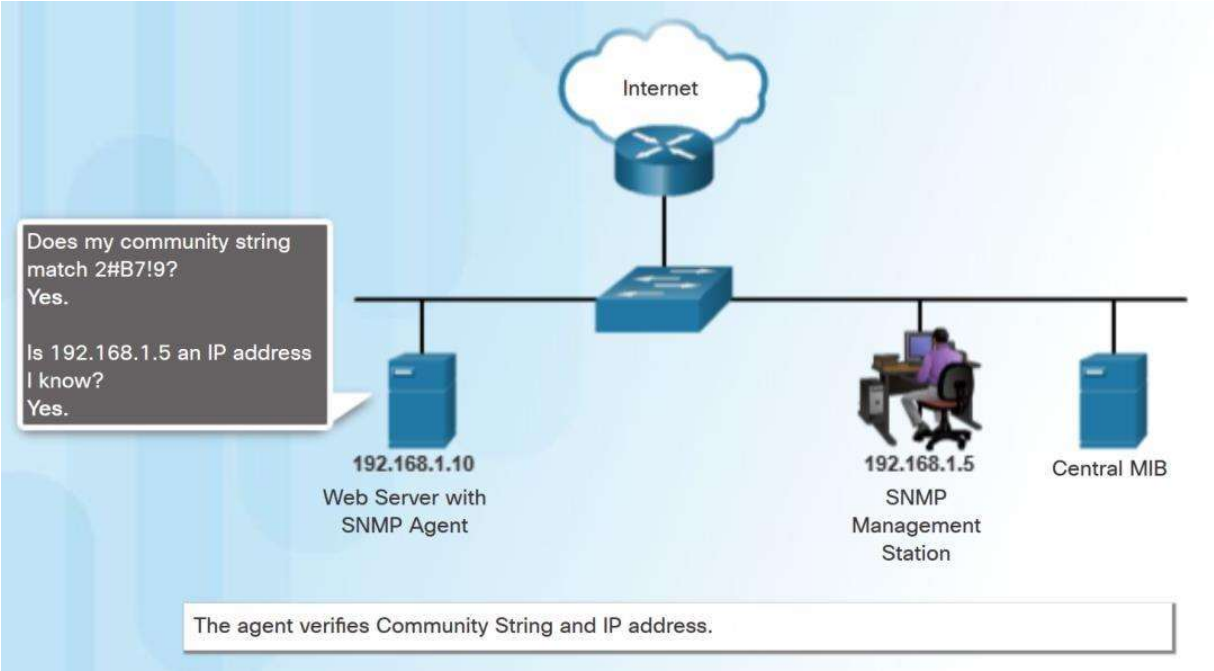
- All versions use SNMP managers, agents, and MIBs, this course focuses on versions 2c and 3.
- A network administrator must configure the SNMP agent to use the SNMP version supported by the management station.

SNMP Operation

Community Strings

SNMPv1 and SNMPv2c use community strings that control access to the MIB.

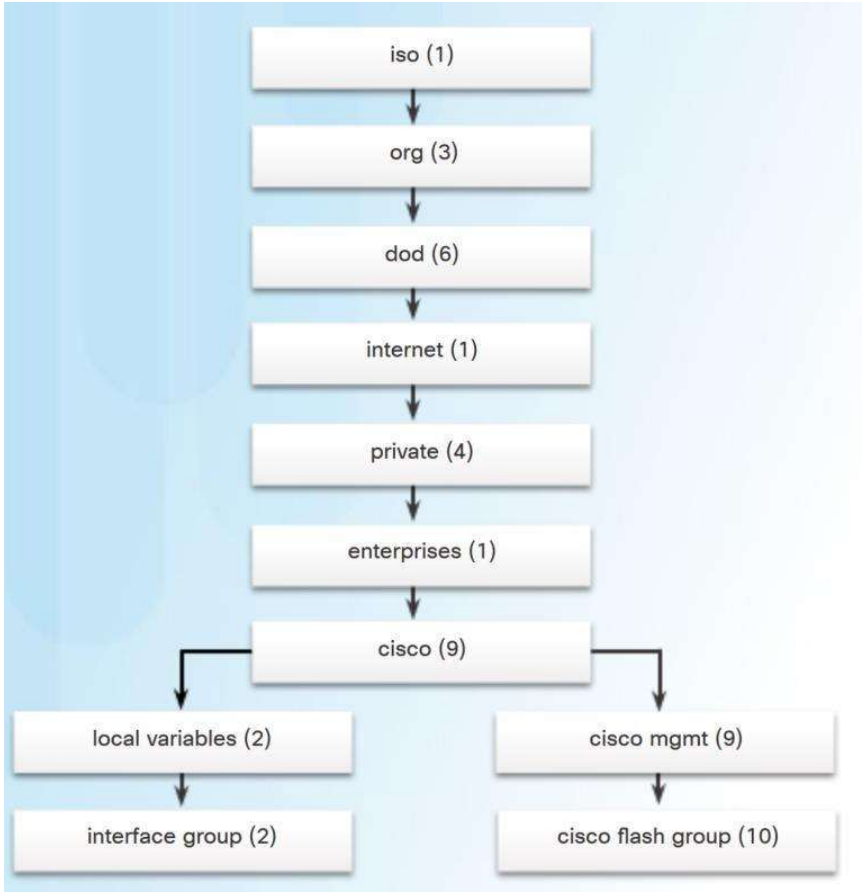
- Two types of community strings:
  - **Read-only (ro)** - Provides access to the MIB variables, but no changes can be made. (get)
  - **Read-write (rw)** - Provides read and write access to all objects in the MIB. (get & set)



SNMP Operation

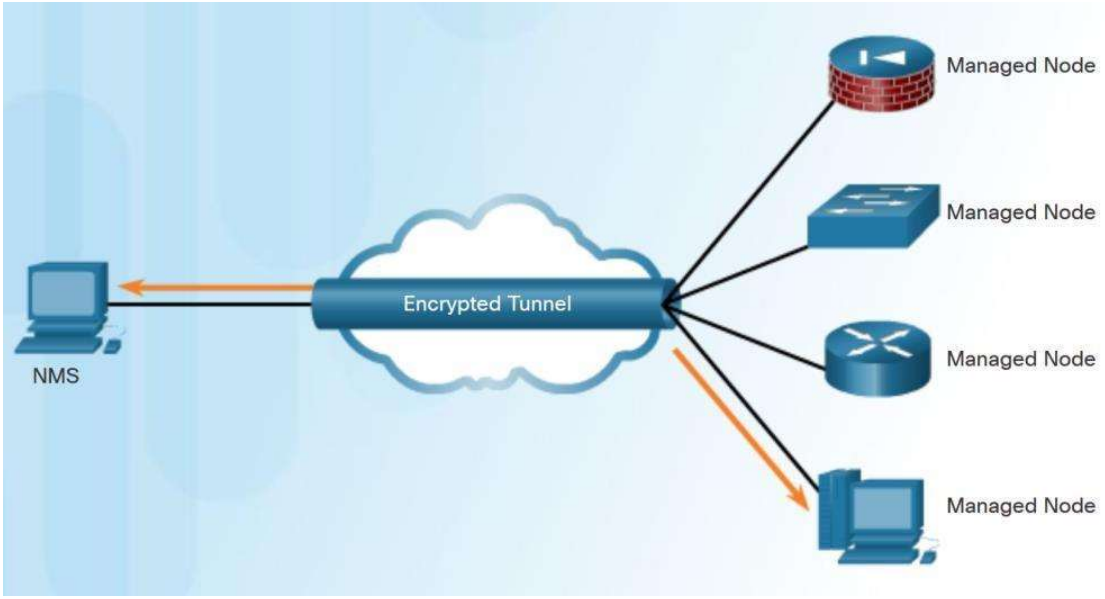
Management Information Base Object ID

- The MIB defines each variable as an object ID (OID).
  - OIDs uniquely identify managed objects.
  - OIDs are organized based on RFC standards into a hierarchy or tree.
- Most devices implement RFC defined common public variables.
  - Vendors such as Cisco can define private branches on the tree to accommodate their own variables.
- CPU is one of the key resources, it should be measured continuously.
  - An SNMP graphing tool can periodically poll SNMP agents, and graph the values.
  - The data is retrieved via the snmpget utility.



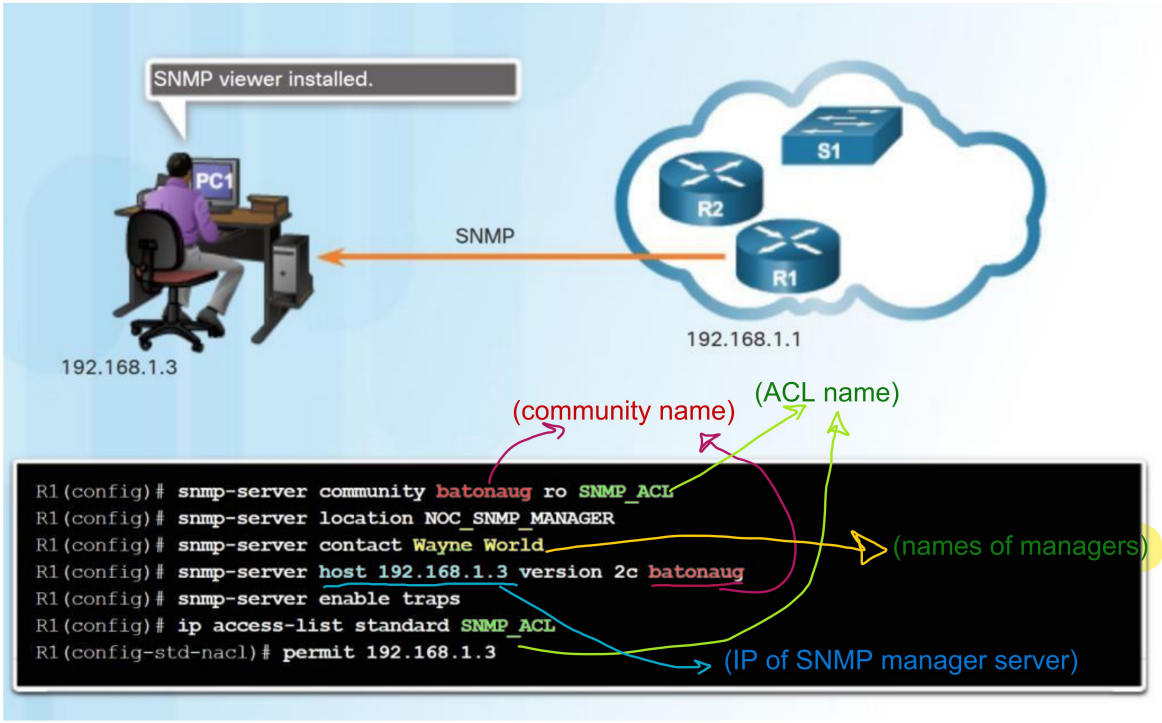
SNMP Operation

SNMPv3



- SNMPv3 authenticates and encrypts packets over the network to provide secure access to devices.
- SNMPv3 provides three security features:
  - **Message integrity and authentication** - Transmissions from the SNMP manager to agents (managed nodes) can be authenticated.
  - **Encryption** - SNMPv3 messages may be encrypted to ensure privacy.
  - **Access control** - Restricts SNMP managers to certain actions on specific portions of data.

Steps for Configuring SNMP



- Basic steps to configuring SNMP:
  1. Configure the community string and access level using **snmp-server community** *string* **ro | rw** command.
  2. (Optional) Document the location of the device using the **snmp-server location** *text* command.
  3. (Optional) Document the system contact using the **snmp-server contact** *text* command.
  4. (Optional)Use an ACL to restrict SNMP access to NMS hosts (SNMP managers). Reference the ACL using **snmp-server community** *string access-list-number-or-name.*

Configuring SNMP

Verifying SNMP Configuration

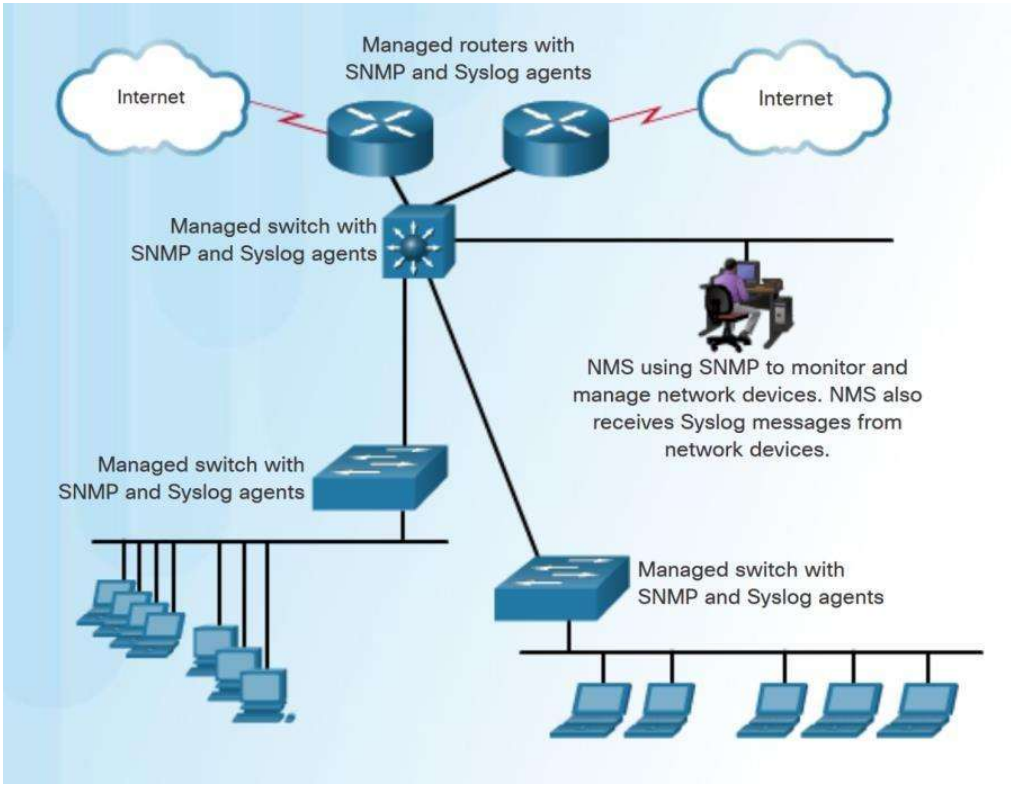
```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    19 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
    Logging to 192.168.1.3.162, 0/10, 19 sent, 0 dropped.
```

- Kiwi Syslog Server is one of several solutions that display SNMP output.
- The SNMP traps are sent to the SNMP manager and displayed on the syslog server.
- To verify the SNMP configuration use the **show snmp** command.
- Use the **show snmp community** command to show SNMP community string and ACL information.

```
R1# show snmp community

Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only             active


Community name: batonaug
Community Index: cisco7
Community SecurityName: batonaug
storage-type: nonvolatile           active      access-list: SNMP_ACL


Community name: batonaug@1
Community Index: cisco8
Community SecurityName: batonaug@1
storage-type: nonvolatile           active      access-list: SNMP_ACL
```

SNMP Best Practices

- SNMP can create security vulnerabilities.
- For SNMPv1 and SNMPv2c - community strings should be strong and changed frequently.
- ACLs should be used to prevent SNMP messages from going beyond the required devices and to limit access to monitored devices.
- SNMPv3 is recommended because it provides security authentication and encryption.
  - The **snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} command creates a new SNMP group on the device.
  - The **snmp-server user** *username groupname* command is used to add a new user to the group.



Steps for Configuring SNMPv3

- Steps to configure SNMPv3:
  1. Configure a standard ACL that will permit access for authorized SNMP managers.
  2. Configure an SNMP view to identify which OIDs the SNMB manager will be able to read.
  3. Configure the SNMP group and features including name, version, type of authentication and encryption, associates view to the group, read or write, filter with ACL.
  4. Configure a user with features including username, associates with group, version, authentication type, encryption type and password.

Step 1: Configure an ACL to permit access to the protected management network.

```
Router(config)# ip access-list standard acl-name
Router(config-std-nacl)# permit source_net
```

Step 2: Configure an SNMP view.

```
Router(config)# snmp-server view view-name oid-tree
```

Step 3: Configure an SNMP group.

```
Router(config)# snmp-server group group-name v3 priv read view-name access [acl-
number | acl-name]
```

Step 4: Configure a user as a member of the SNMP group.

```
Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-
password priv {des | 3des | aes {128 | 192 | 256}} privpassword
```

SNMPv3 Configuration

- The example configures a standard ACL named PERMIT-ADMIN. It is configured to permit only the 192.168.1.0/24 network. All hosts attached to this network will be allowed to access the SNMP agent running on R1.
- An SNMP view is named SNMP-RO and is configured to include the entire ISO tree from the MIB.