Monday, July 28, 2025 5:03 PM

SNMP (Simple Network Management Protocol)

SNMP OVERVIEW

- SNMP is an INDUSTRY-STANDARD FRAMEWORK and PROTOCOL that was originally released in 1988

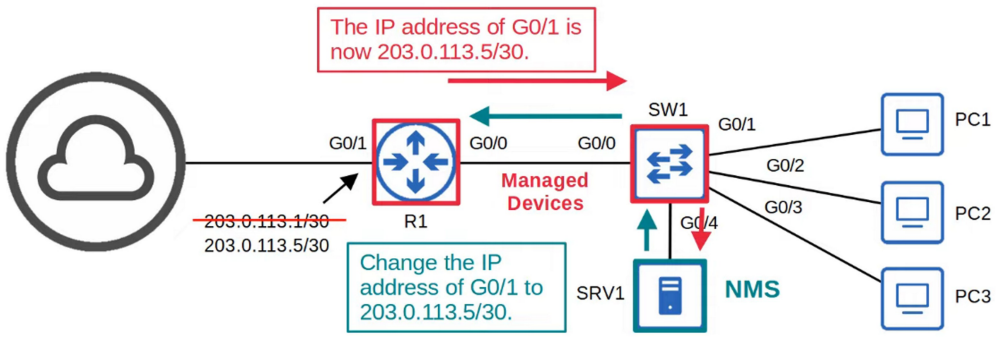
These RFCs make up SNMPv1 (Do not need to memorize)

RFC 1065 - Structure and identification of management information for TCP/IP based internets
RFC 1066 - Management information base for network management of TCP/IP based internets
RFC 1067 - A simple network management protocol

- Don't let the 'Simple' in the name fool you !
- SNMP can be used to monitor the STATUS of DEVICES, make CONFIGURATION CHANGES, etc.
- There are TWO MAIN TYPES of DEVICES in SNMP:
  - MANAGED DEVICES
    - These are the DEVICES being managed using SNMP
      - Ex: ROUTERS, SWITCHES
  - NETWORK MANAGEMENT STATION (NMS)
    - The DEVICE / DEVICES managing the MANAGED DEVICES
    - THIS is the SNMP 'SERVER'

SMNP OPERATIONS

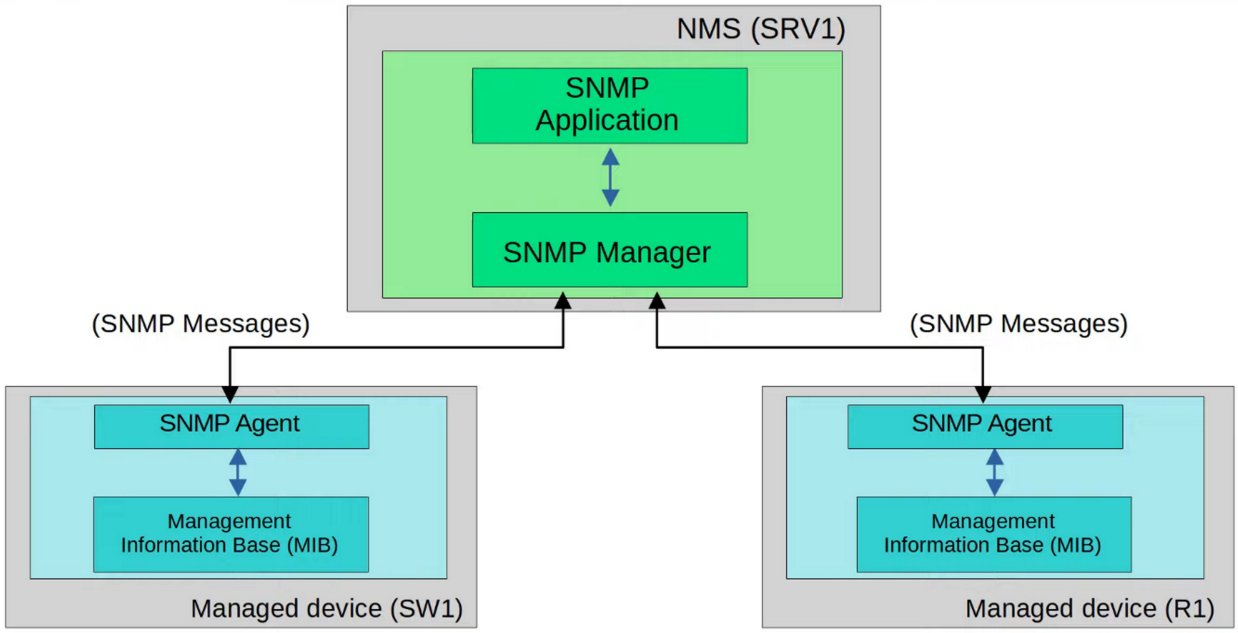
- There are three main operations used in SNMP.
  1) Managed devices can notify the NMS of events.
  2) The NMS can ask the managed devices for information about their current status.
  3) The NMS can tell the managed devices to change aspects of their configuration.



SMNP COMPONENTS

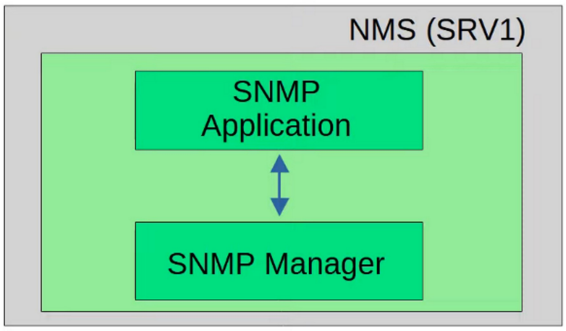
OVERVIEW

SNMP Components



NMS

SNMP Components



- The **SNMP Manager** is the software on the NMS that interacts with the managed devices.
  → It receives notifications, sends requests for information, sends configuration changes, etc.

- The **SNMP Application** provides an interface for the network admin to interact with.
  → Displays alerts, statistics, charts, etc.

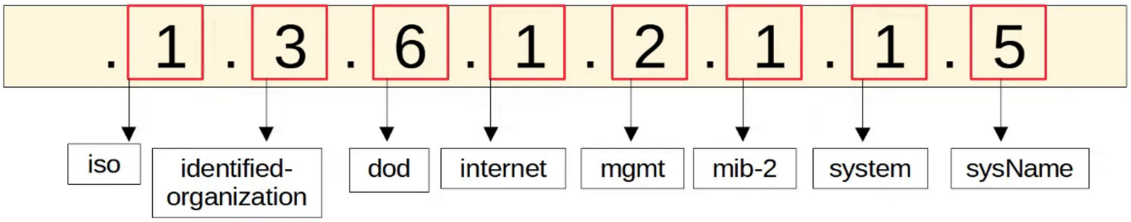
MANAGED DEVICES

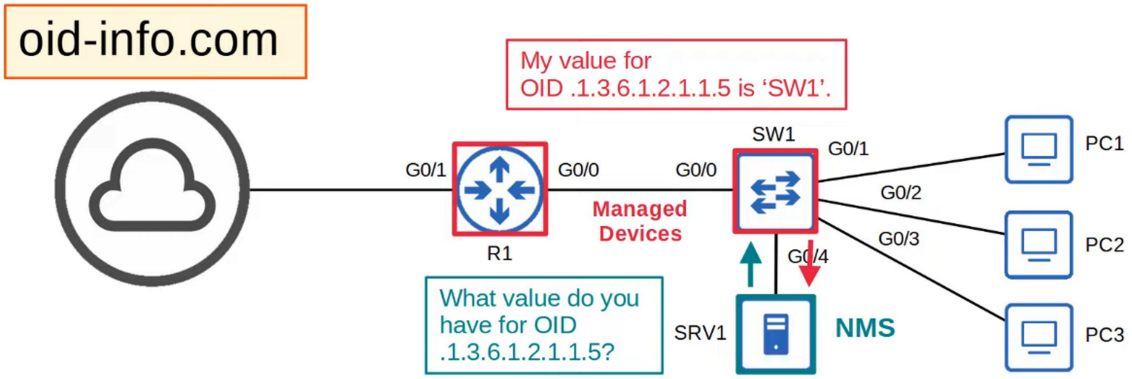
SNMP Components

- The **SNMP Agent** is the SNMP software running on the managed devices that interacts with the SNMP Manager on the NMS.
  → It sends notifications to/receives messages from the NMS.
- The **Management Information Base (MIB)** is the structure that contains the variables that are managed by SNMP.
  → Each variable is identified with an Object ID (OID)
  → Example variables: Interface status, traffic throughput, CPU usage, temperature, etc.

SNMP OIDs

- SNMP Object IDs are ORGANIZED in a HIERARCHICAL STRUCTURE





SNMP VERSIONS

- Many versions of SNMP have been proposed/developed, however, only three major versions have achieved wide-spread use:
- SNMPv1
  - The ORIGINAL version of SNMP
- SNMPv2c
  - Allows the NMS to retrieve LARGE AMOUNTS of information in a SINGLE REQUEST, so it is

more efficient
    - ‘c’ refers to the ‘community strings’ used as PASSWORDS in SNMPv1, removed from SNMPv2, and then added BACK for SNMPv2
- SNMPv3
    - A much more SECURE version of SNMP that supports STRONG ENCRYPTION and AUTHENTICATION.
        - 💡 WHENEVER POSSIBLE, this version should be used!

SNMP MESSAGES

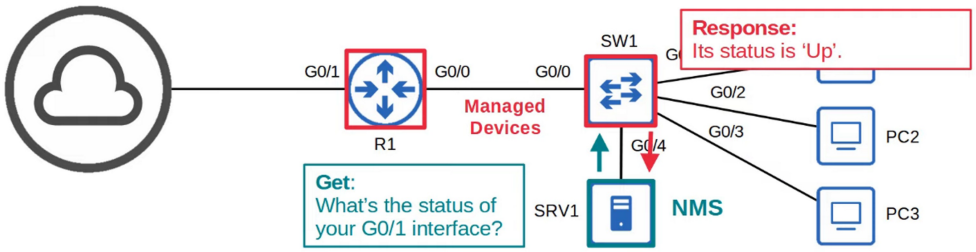
SNMP Messages

Message Class	Description	Messages
Read	Messages sent by the **NMS** to read information from the **managed devices**. (ie. What’s your current CPU usage %?)	*Get* *GetNext* *GetBulk*
Write	Messages sent by the **NMS** to change information on the **managed devices.** (ie. change an IP address)	*Set*
Notification	Messages sent by the **managed devices** to alert the **NMS** of a particular event. (ie. interface going down)	*Trap* *Inform*
Response	Messages sent in response to a previous message/request.	*Response*

1. SNMP READ

SNMP ‘Read’ Messages

- **Get**
  →A request sent from the manager to the agent to retrieve the value of a variable (OID), or multiple variables. The agent will send a *Response* message with the current value of each variable.
- **GetNext**
  →A request sent from the manager to the agent to discover the available variables in the MIB.
- **GetBulk**
  →A more efficient version of the **GetNext** message (introduced in SNMPv2).



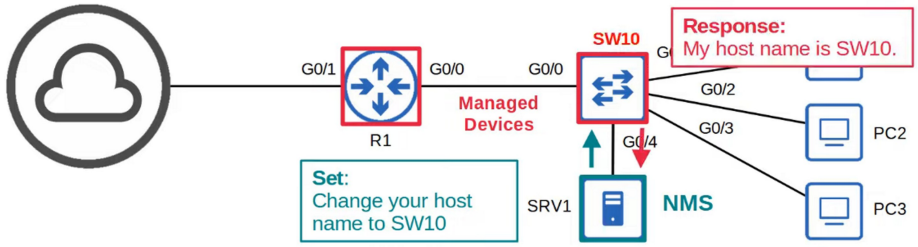
2. SMNP WRITE

SNMP ‘Write’ Messages

- **Set**

SNMP 'Write' Messages

- **Set**
  →A request sent from the manager to the agent to change the value of one or more variables. The agent will send a *Response* message with the new values.

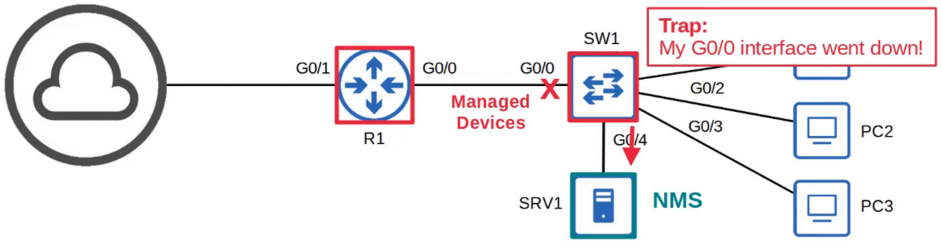


3. SNMP NOTIFICATION

SNMP 'Notification' Messages

- **Trap**
  →A notification sent from the agent to the manager. The manager does not send a Response message to acknowledge that it received the Trap, so these messages are 'unreliable'.

- **Inform**
  →A notification message that is acknowledged with a Response message.
  →Originally used for communications between managers, but later updates allow agents to send Inform messages to managers, too.



SNMP AGENT listens for MESSAGES on UDP Port 161

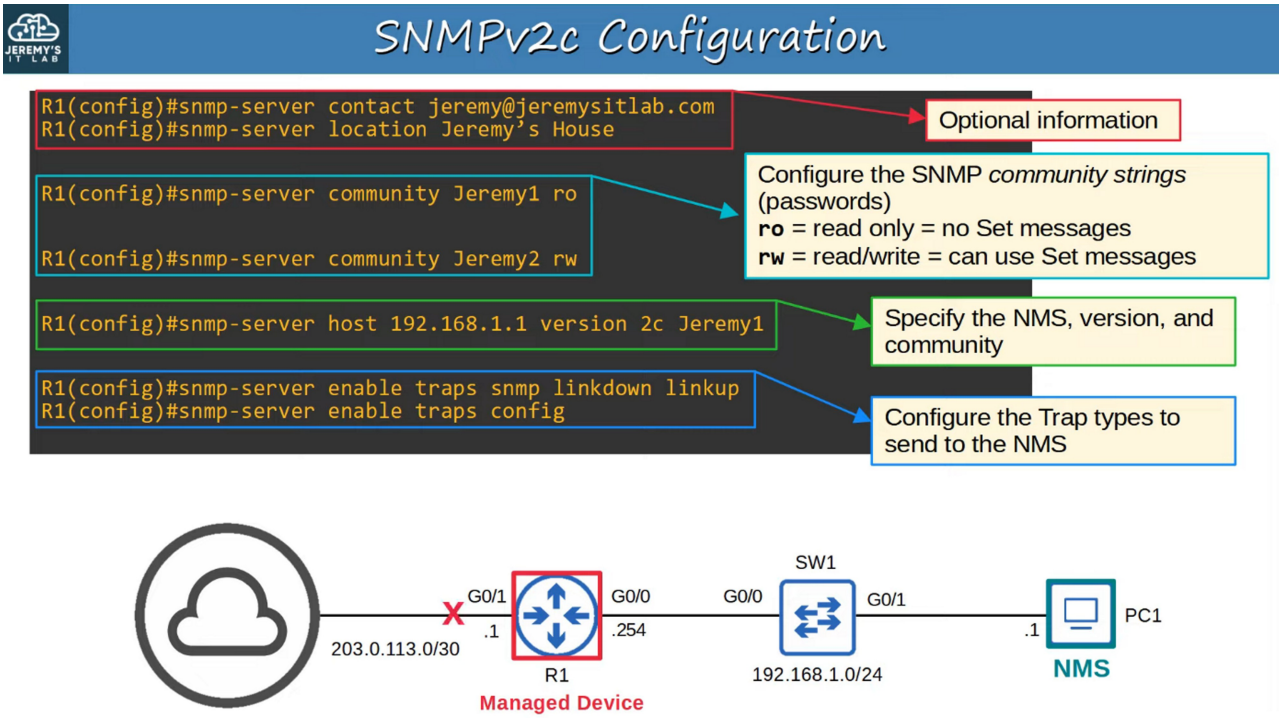
SNMP MANAGER listens for MESSAGES on UDP Port 162

SNMP Agents (managed devices) listen for messages on UDP port 161, and SNMP Managers listen for messages on UDP port 162.

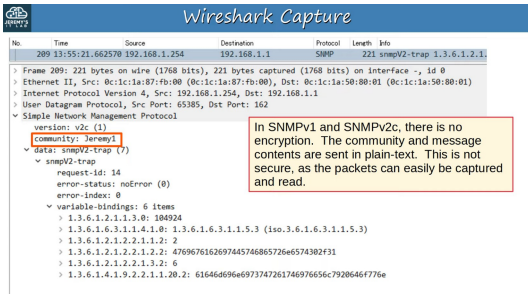
Trap and **Inform** are both messages sent from an SNMP Agent to an SNMP Manager, so they are sent to UDP port 162.

Get and **Set**, on the other hand, are sent from a Manager to an Agent, so they are sent to UDP port 161.

SNMPv2c CONFIGURATION (Basic)



WHAT HAPPENS WITH R1's G0/1 INTERFACE GOES DOWN?



NOTE:

UDP message sent to Destination Port 162 (SNMP Manager)

"version" is set to v2c

community is "Jeremy1" (Read Only - no Set messages)

snmpV2-trap : trap message sent due to interface G0/1 going down

variable-bindings : contains the OID sent to identify the issue.

SNMP SUMMARY

- SNMP helps MANAGE DEVICES over a NETWORK
- MANAGED DEVICES are the devices being managed using SNMP (such as ROUTERS, SWITCHES, FIREWALLS)
- NETWORK MANAGEMENT STATIONS (NMS) are the SNMP “servers” that manage the devices
  - NMS receives notifications from Managed Devices
  - NMS changes settings on Managed Devices
  - NMS checks status of Managed Devices
- Variables, such as Interface Status, Temperature, Traffic Load, Hostname, etc are STORED in the MANAGMENT INFORMATION BASE (MIB) and identified using Object IDs (OIDs)

Main SNMP versions : SNMPv1, SNMPv2c, SNMPv3

SNMP MESSAGES :
* Get / GetNext / GetBulk
* Set
* Trap
* Inform
* Response