JEREMY'S IT LAB

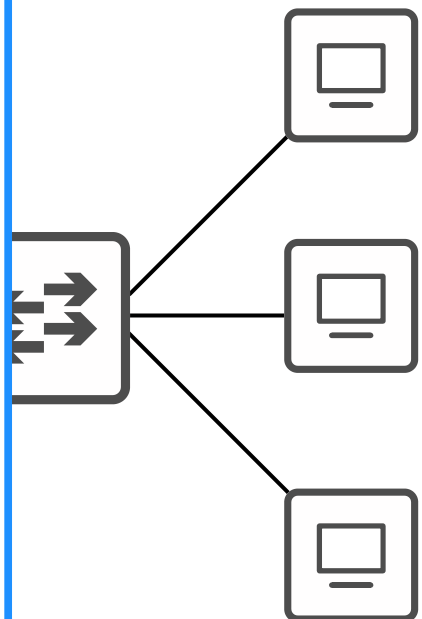
CCNA Day 40

Simple Network Management Protocol

1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%

4.1 Configure and verify inside source NAT using static and pools
4.2 Configure and verify NTP operating in a client and server mode
4.3 Explain the role of DHCP and DNS within the network
4.4 Explain the function of SNMP in network operations
4.5 Describe the use of syslog features including facilities and levels
4.6 Configure and verify DHCP client and relay
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping
4.8 Configure network devices for remote access using SSH
4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%



Things we'll cover

- SNMP overview
- SNMP versions
- SNMP messages
- SNMP configuration (basic)

Simple Network Management Protocol

- SNMP is an industry-standard framework and protocol that was originally released in 1988.

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

SNMPv1

- Don't let the 'Simple' in the name fool you!

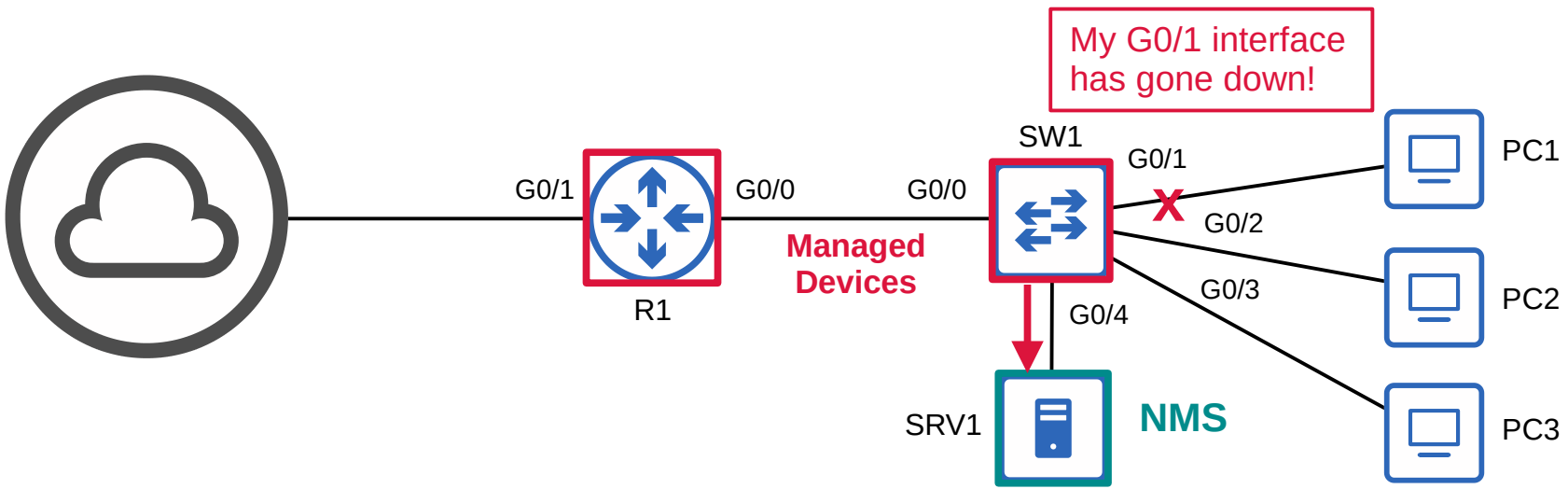
- SNMP can be used to monitor the status of devices, make configuration changes, etc.

- There are two main types of devices in SNMP:
  1) Managed Devices
  → These are the devices being managed using SNMP.
  → For example, network devices like routers and switches.

  2) Network Management Station (NMS)
  → The device/devices managing the managed devices.
  → This is the SNMP 'server'.

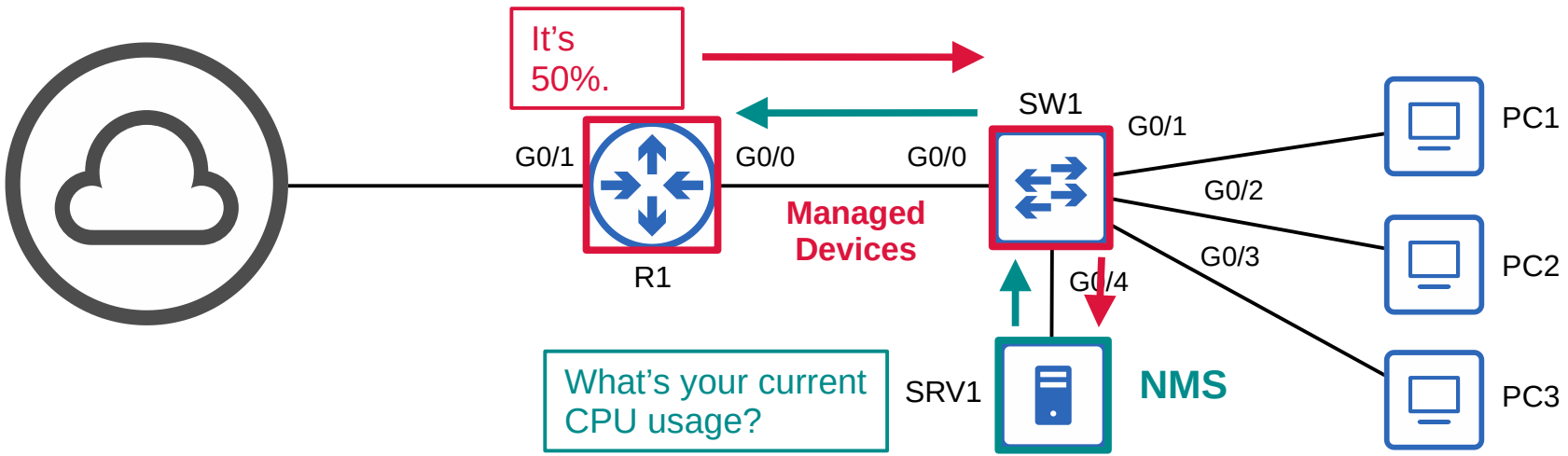
SNMP Operations

- There are three main operations used in SNMP.
  1) Managed devices can notify the NMS of events.



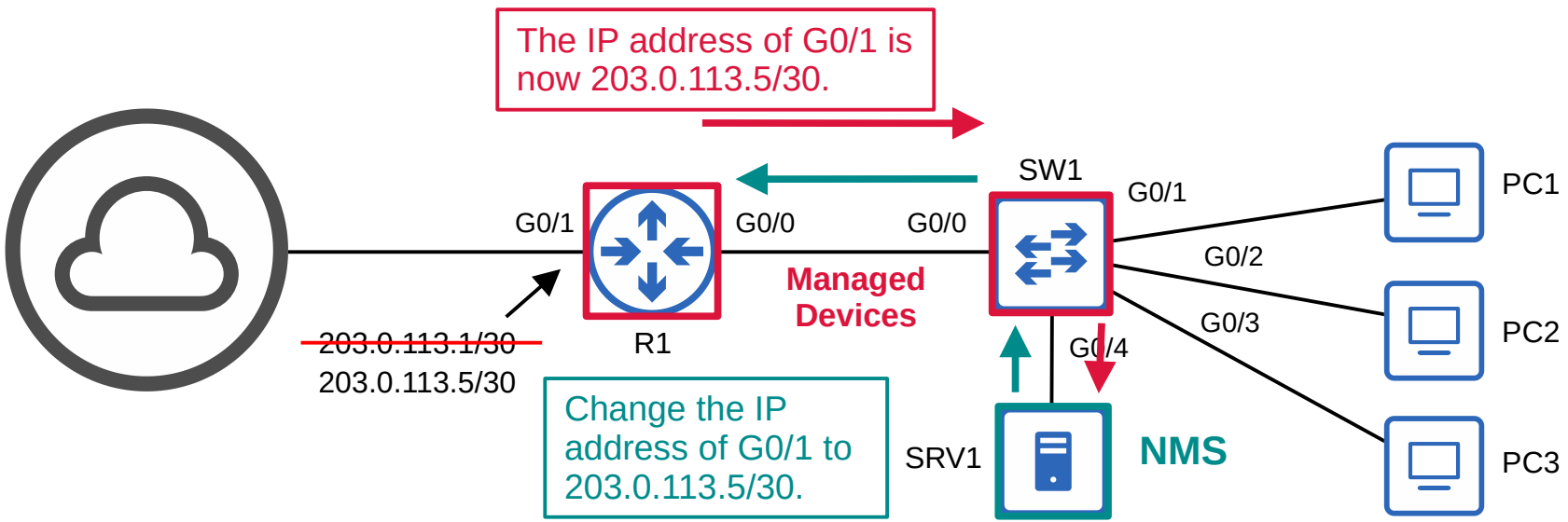
SNMP Operations

- 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.

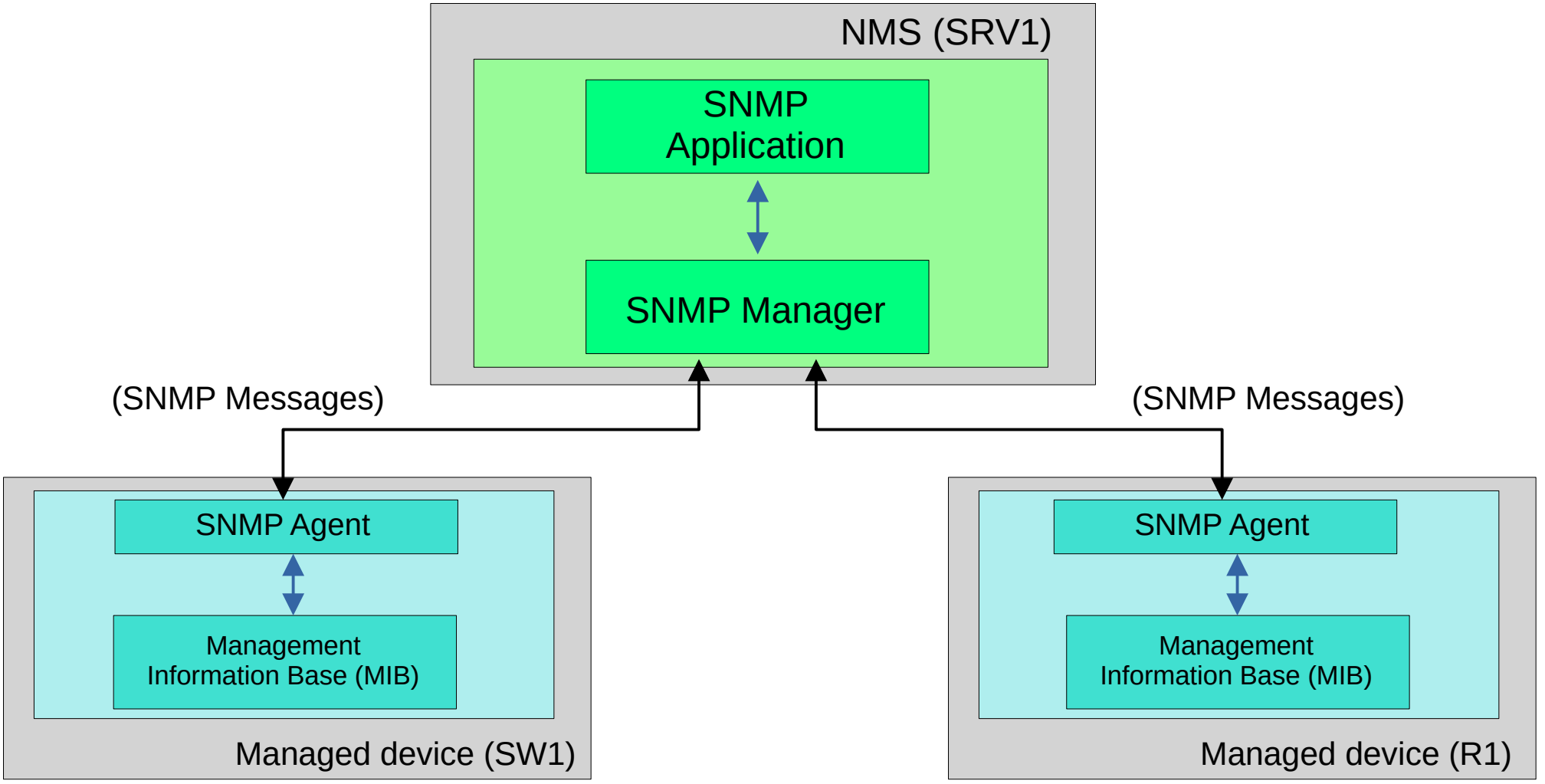


SNMP Operations

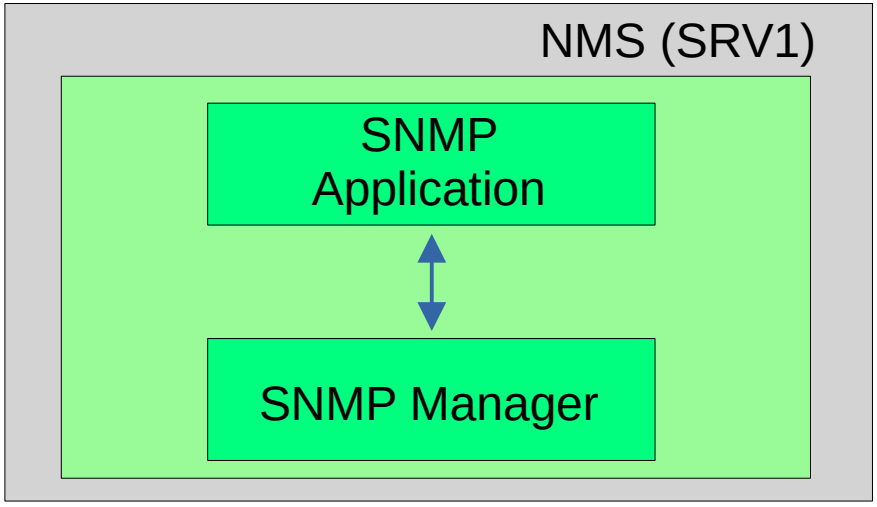
- There are three main operations used in SNMP.
  1) Managed devices can notify the NMS of events.
  2) The NMS can ask the managed devices for information about their current status.
  3) The NMS can tell the managed devices to change aspects of their configuration.



SNMP Components



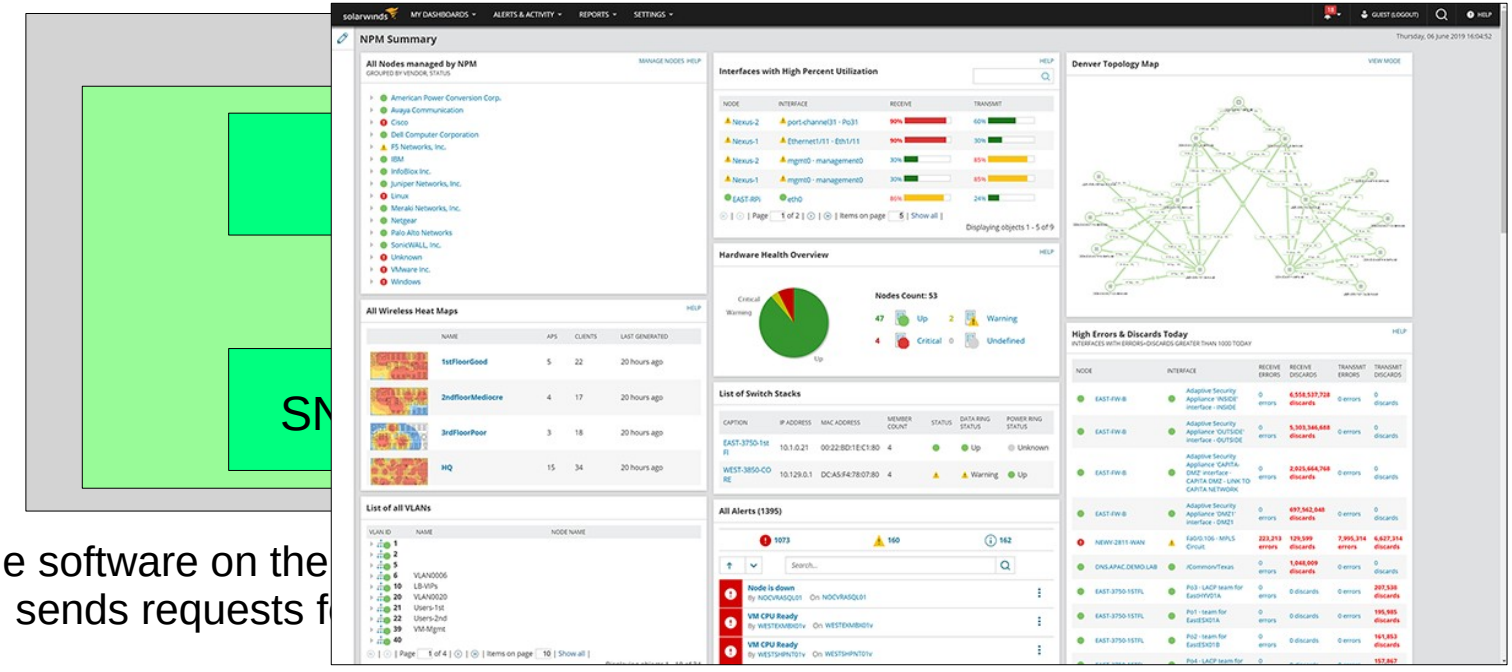
SNMP Components



- 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.

SNMP Components



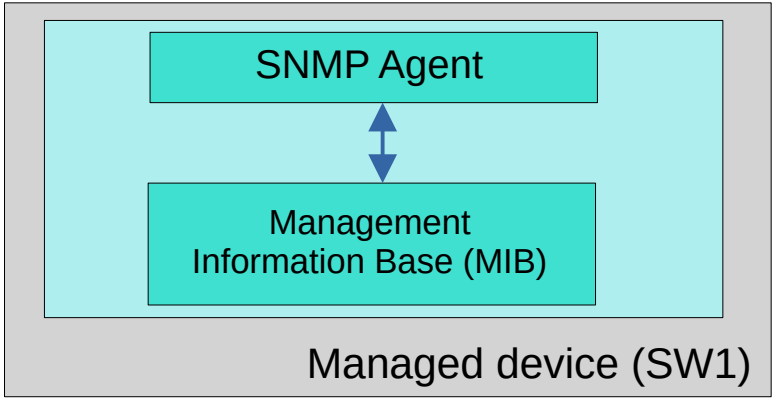
- The **SNMP Manager** is the software on the
  → It receives notifications, sends requests f

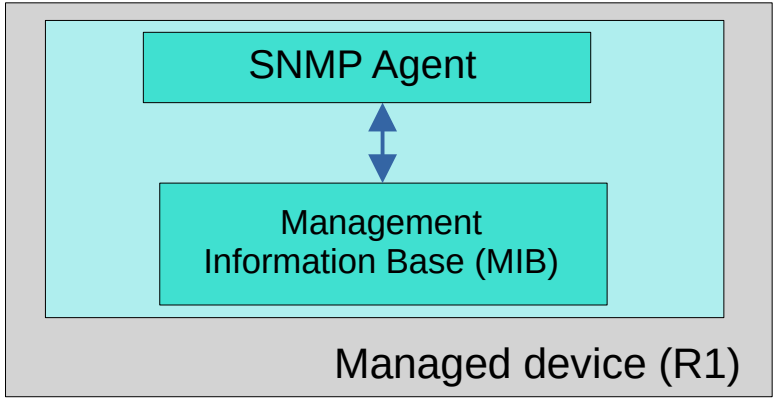
- The **SNMP Application** provides an interface for the network admin to interact with.
  → Displays alerts, statistics, charts, etc.

SNMP Components

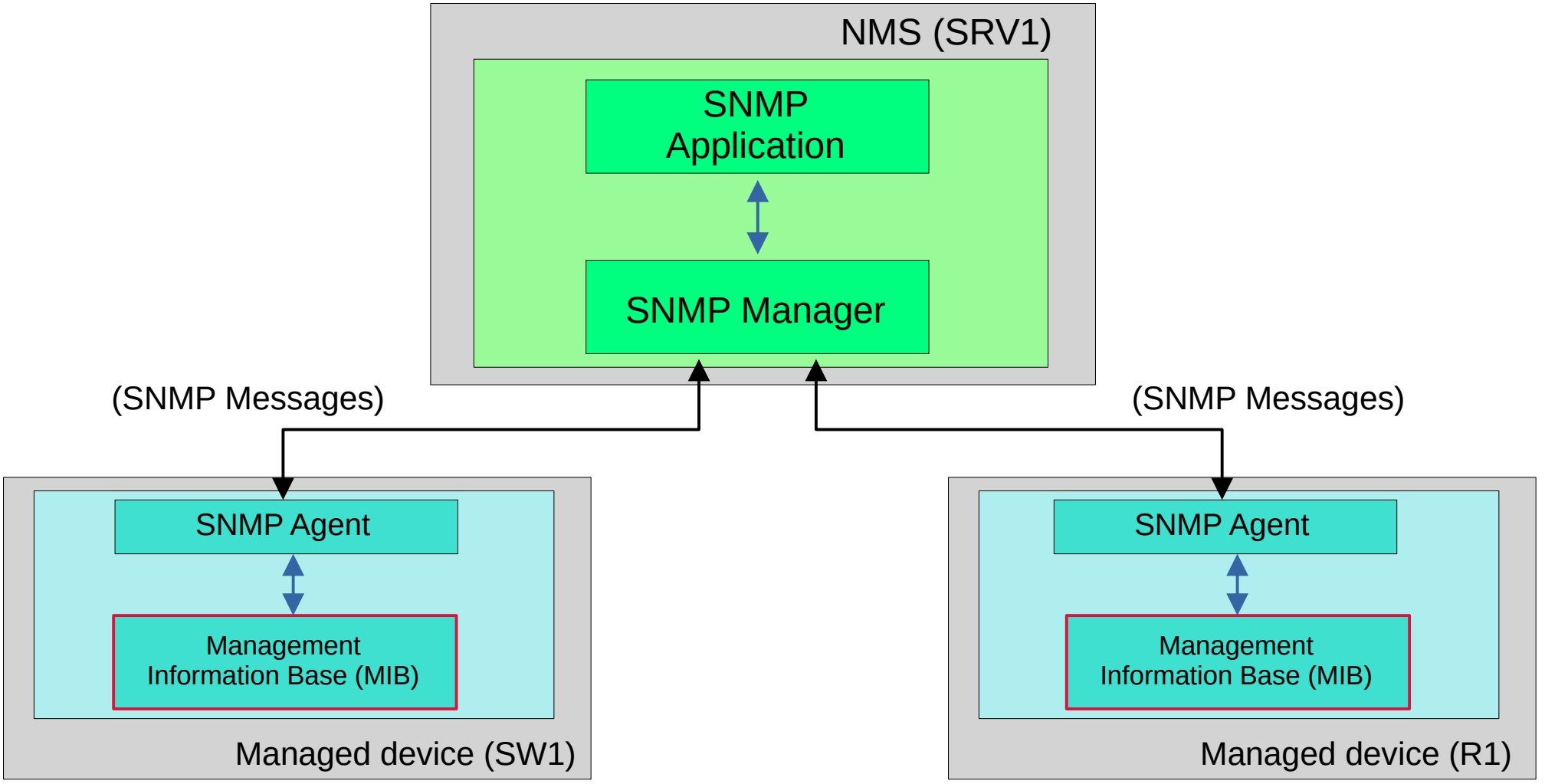
- The **SNMP Agent** is the SNMP software running on the managed devices that interacts with the SNMP Manager on the NMS.
  → It sends notifications to/receives messages from the NMS.

- 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.



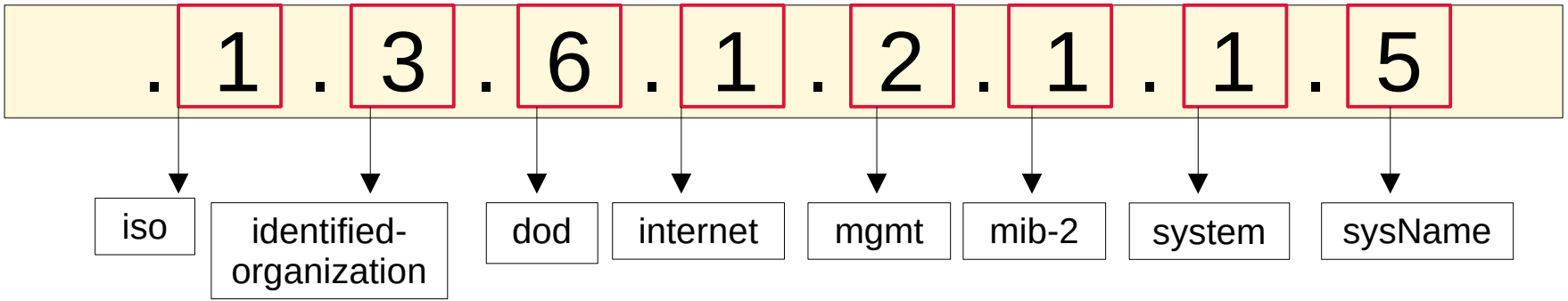


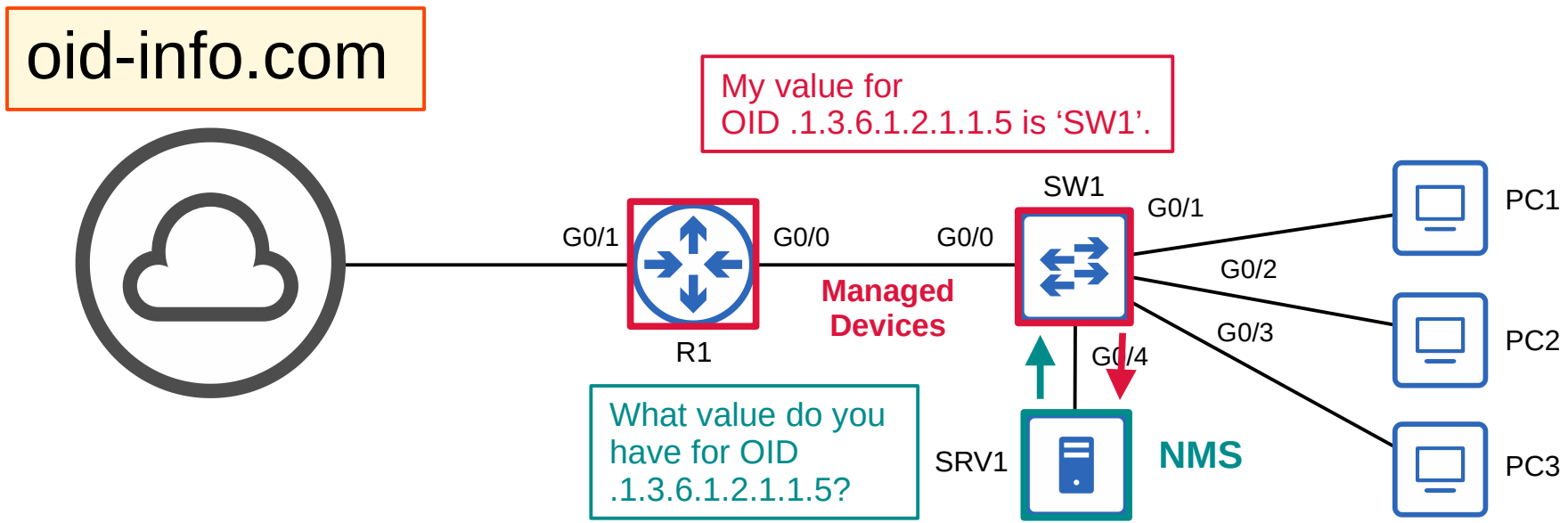
SNMP Components



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 SNMPv2c.

- **SNMPv3**
  → A much more secure version of SNMP that supports strong **encryption** and **authentication**. Whenever possible, this version should be used!

SNMP Messages

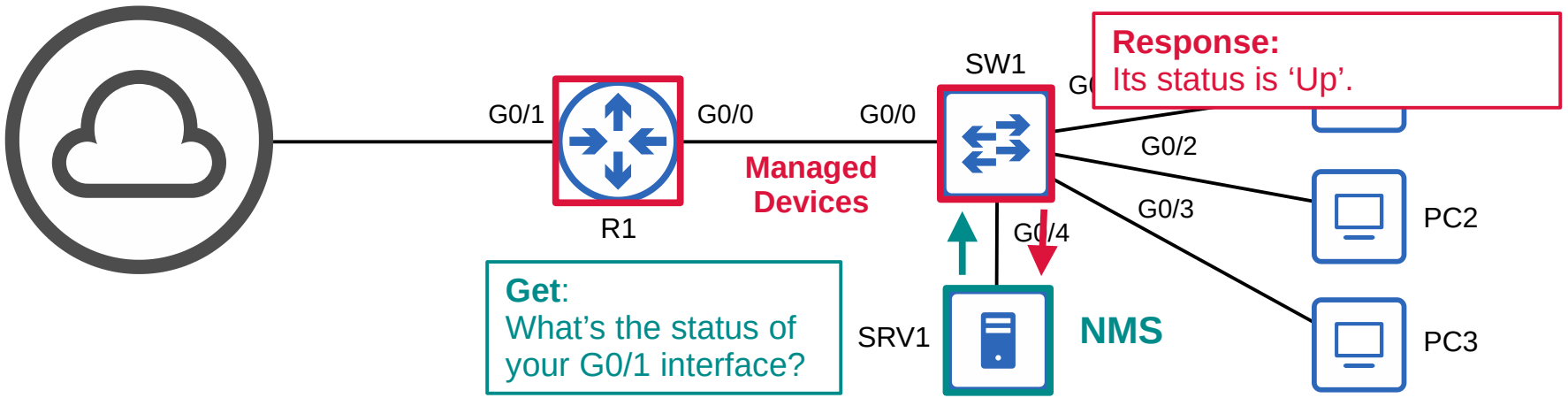
Message Class	Description	Messages
Read	Messages sent by the **NMS** to read information from the **managed devices**. (ie. What's your current CPU usage %?)	*Get* *GetNext* *GetBulk*
Write	Messages sent by the **NMS** to change information on the **managed devices.** (ie. change an IP address)	*Set*
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*

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).

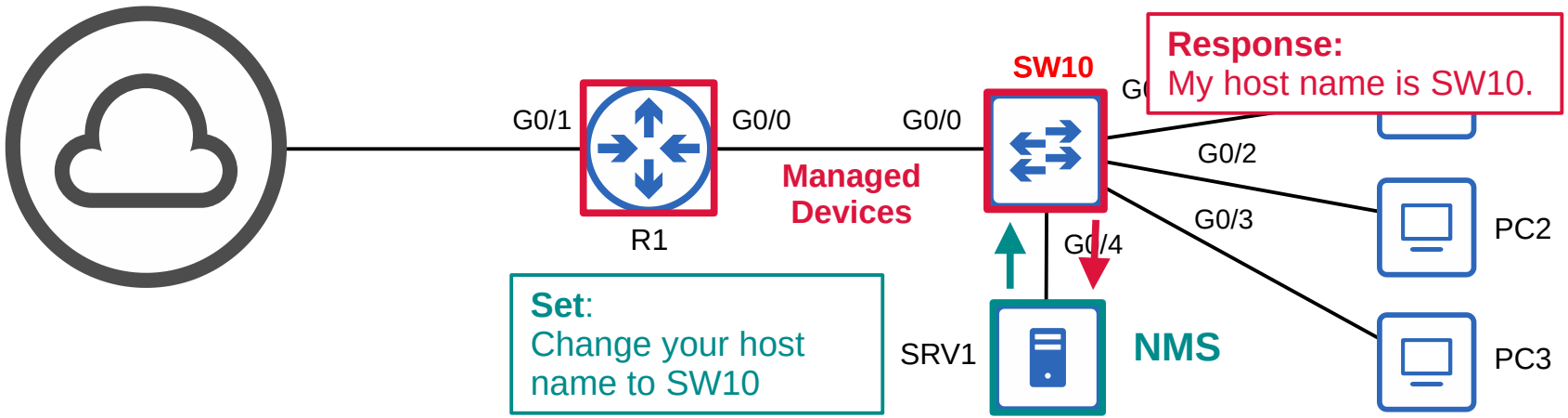


SNMP Messages

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*

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.



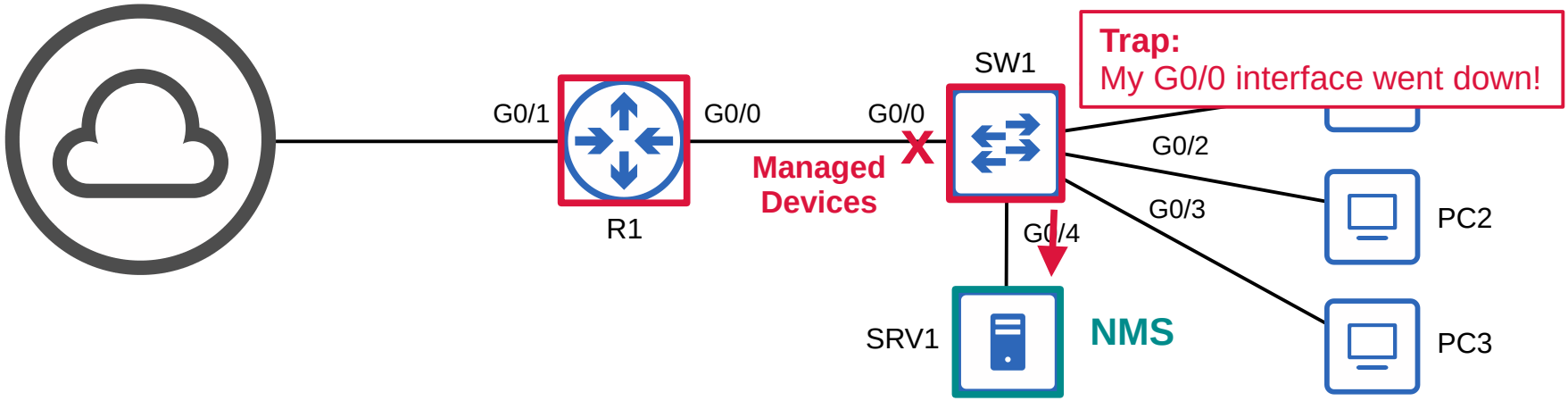
SNMP Messages

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*

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 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*

SNMP Agent = UDP 161
SNMP Manager = UDP 162

SNMPv2c Configuration

```
R1(config)#snmp-server contact jeremy@jeremysitlab.com
R1(config)#snmp-server location Jeremy's House

R1(config)#snmp-server community Jeremy1 ro

R1(config)#snmp-server community Jeremy2 rw

R1(config)#snmp-server host 192.168.1.1 version 2c Jeremy1

R1(config)#snmp-server enable traps snmp linkdown linkup
R1(config)#snmp-server enable traps config
```

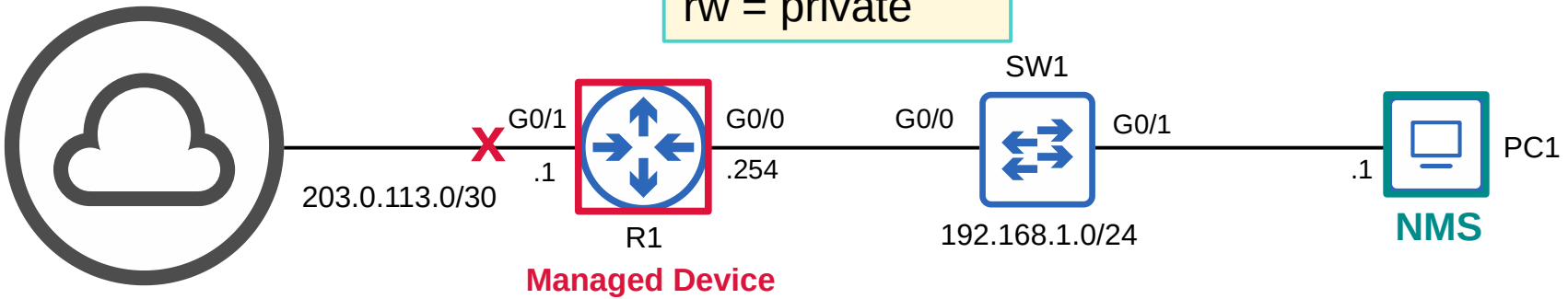
Optional information

Configure the SNMP *community strings* (passwords)
ro = read only = no Set messages
rw = read/write = can use Set messages

Specify the NMS, version, and community

Configure the Trap types to send to the NMS

Default strings:
ro = public
rw = private



Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
209	13:55:21.662570	192.168.1.254	192.168.1.1	SNMP	221	snmpV2-trap 1.3.6.1.2.1.

```
> Frame 209: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits) on interface -, id 0
> Ethernet II, Src: 0c:1c:1a:87:fb:00 (0c:1c:1a:87:fb:00), Dst: 0c:1c:1a:50:80:01 (0c:1c:1a:50:80:01)
> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 65385, Dst Port: 162
v Simple Network Management Protocol
    version: v2c (1)
    community: Jeremy1
  v data: snmpV2-trap (7)
    v snmpV2-trap
        request-id: 14
        error-status: noError (0)
        error-index: 0
      v variable-bindings: 6 items
        > 1.3.6.1.2.1.1.3.0: 104924
        > 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.3 (iso
        > 1.3.6.1.2.1.2.2.1.1.2: 2
        > 1.3.6.1.2.1.2.2.1.2.2: 476967616269744574686572
        > 1.3.6.1.2.1.2.2.1.3.2: 6
        > 1.3.6.1.4.1.9.2.2.1.1.20.2: 61646d696e697374726174697656c7920646f776e
```

In SNMPv1 and SNMPv2c, there is no encryption. The community and message contents are sent in plain-text. This is not secure, as the packets can easily be captured and read.

OID:	{iso(1) identified-organization(3) dod(6) internet(1) snmpV2(6) snmpModules(3) snmpMIB(1) snmpMIBObjects(1) snmpTraps(5) linkDown(3)}
	1.3.6.1.6.3.1.1.5.3
	/ISO/Identified-Organization/6/1/6/3/1/1/5/3

SNMP Summary

- SNMP helps manage devices over a network.
- **Managed Devices** are the devices being managed using SNMP, such as network devices (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, host name, etc. are stored in the Management Information Base (MIB) and identified using Object IDs (OIDs)
- Main SNMP versions: SNMPv1, SNMPv2c, SNMPv3
- SNMP messages: Get, GetNext, GetBulk, Set, Trap, Inform, Response

Quiz 1

Which of the following SNMP messages are used by the NMS to ‘read’ information from the managed devices? (select all that apply)

a) Set

b) Inform

c) Trap

d) Get

e) Response

f) SetBulk

g) GetNext

Quiz 2

Which of the following SNMP messages are sent to UDP port 162? (Select all that apply)

a) Inform

b) Trap

c) Set

d) Get

Quiz 3

Which of the following SNMP message types was introduced in SNMPv2 and allows mass-retrieval of information from managed devices?

a) Set

b) SetBulk

c) GetNext

d) GetBulk

Quiz 4

Which of the following pieces of software runs on an SNMP NMS?

a) OID

b) Agent

c) Manager

d) Trap

Quiz 5

Which of the following SNMP messages is sent without expecting a Response?

a) Get

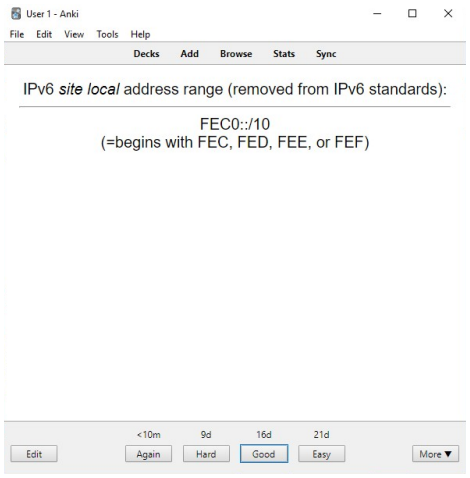
b) Inform

c) Set

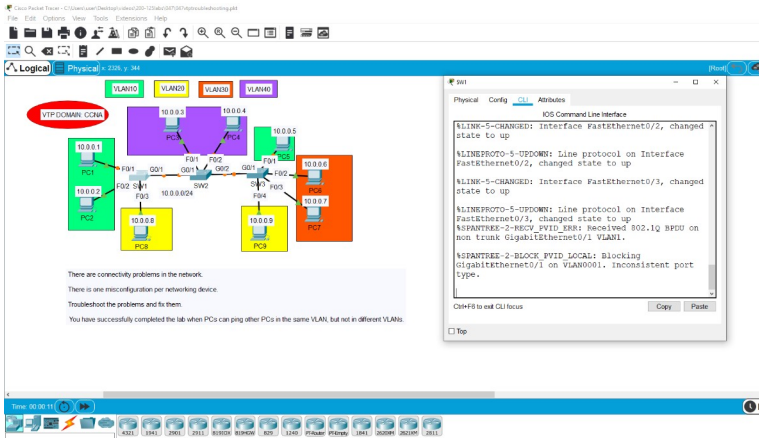
d) Trap

Supplementary Materials

- Review flash cards
  (link in the description)



- Packet Tracer lab



JCNP-Level Channel Members

- H W
- Brandon Byers
- Samil Cañas
- Aaron Kagan
- tech alameda
- Marcel Lord
- Magrathea
- kone fine
- Donald Sabusap
- C Mohd
- Gustavo BR
- Anthony Saab
- Biraj Banker
- Junhong Park
- Benjamin Robbins
- Tshepiso Mokoena
- justin watke
- Prakaash Rajan
- Nasir Chowdhury
- Erlison Santos
- Apogee AOR
- Marko Barbaric
- Daming Li
- jhilmar molina
- Ed Velez
- #VALUE?
- john goff
- funnydart
- velvijaykum
- Channel failed to load
- Mark von kanel
- M Yousif
- Boson Software
- Devin Sukhu
- Lito Castillejo
- Yonatan Makara
- Vance Simmons

*as of February 6th, 2021