Video Introduction

- Welcome to Jeremy's IT Lab. This is a free, complete course for the CCNA.
- If you like these videos, please subscribe to follow along with the series.
- Please like and leave a comment, and share the video to help spread this free series of Lectures. Thanks for your help.

SNMP and the CCNA Exam

- This video will cover SNMP, the Simple Network Management Protocol.
- SNMP is mentioned in exam topic 4.4, which says you must be able to explain the function of SNMP in network operations.
- You don't need to know the detailed workings of SNMP, how to set up an SNMP server, how to configure SNMP, etc.
- Basically, you just need to know its role and purpose in network operations.

What Will Be Covered in This Lecture

- **SNMP overview**: its purpose, how it works, etc.
- **Different versions of SNMP**: there have actually been many different versions developed over the years, however you only really need to know 3 of them.
- **The different messages SNMP uses** to fulfill its purpose.
- **Some very basic SNMP configurations**: although the exam topics don't list SNMP configuration as a requirement, it's a good idea to learn some very basic commands which will then be tried out in the next lab video.
- Watch until the end of the video for a bonus practice question from Boson Software's ExSim for CCNA, the best practice exams for the CCNA.

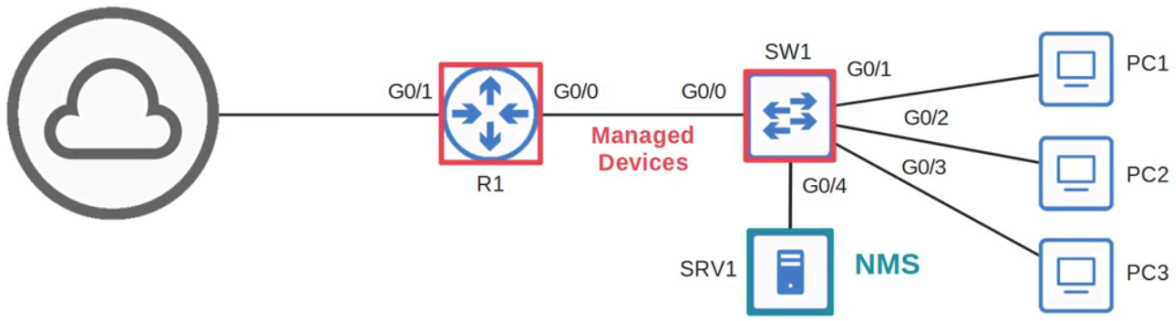
SNMP Overview

- SNMP is an **industry-standard framework and protocol**, originally released in **1988**.
- Most people think of SNMP as a single protocol, but actually it fits into a larger framework of network management, sometimes called the **SNMP framework**.
- **RFCs (Requests For Comments)** are how the **IETF (Internet Engineering Task Force)** defines standards for the Internet.
- The three RFCs that make up **SNMP version 1**:
  - **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
- There have been many more RFCs since then defining other versions of SNMP, a few of which will be introduced later in this video.
- *Note: You don't have to memorize these RFCs — the professor is just giving a little history.*
- Don't let the "simple" in the name fool you:
  - SNMPv1 was relatively simple compared to later versions
  - The current version, **SNMPv3**, is actually fairly complicated
- For the CCNA or even the CCNP, you don't need to know all the details — but you do need to understand the **purpose and basics** of SNMP.
- SNMP can be used to:
  - Monitor the status of devices
  - Make configuration changes
  - Etc.

- **Two main types of devices in SNMP:**
  - **Managed devices** — the devices being managed using SNMP
    - Example: network devices like routers and switches
    - We can use SNMP to monitor the status of the routers and switches in our networks
  - **Network Management Station (NMS)** — you might also hear *Network Management System* instead of *Station*; it's the same thing
    - The device, or devices, managing the managed devices
    - This is the SNMP "server," although typically we use the term **NMS** instead of SNMP server

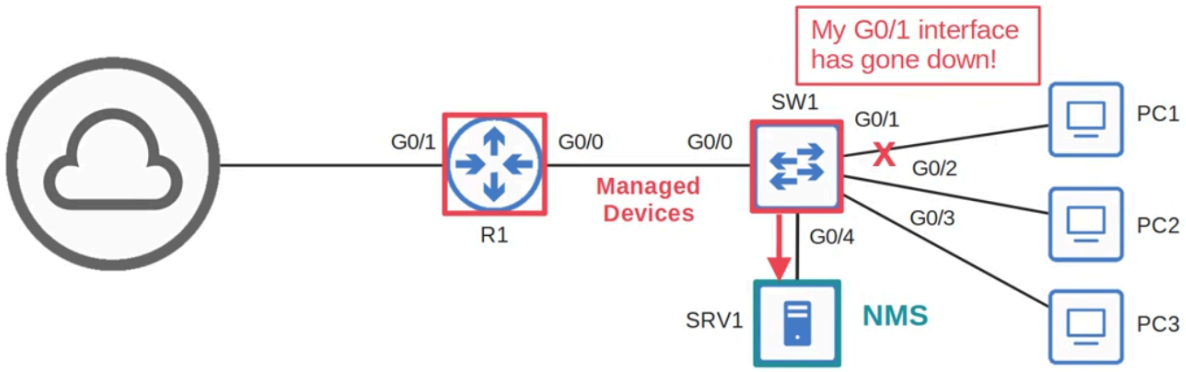
---

How SNMP Works — Three Main Operations



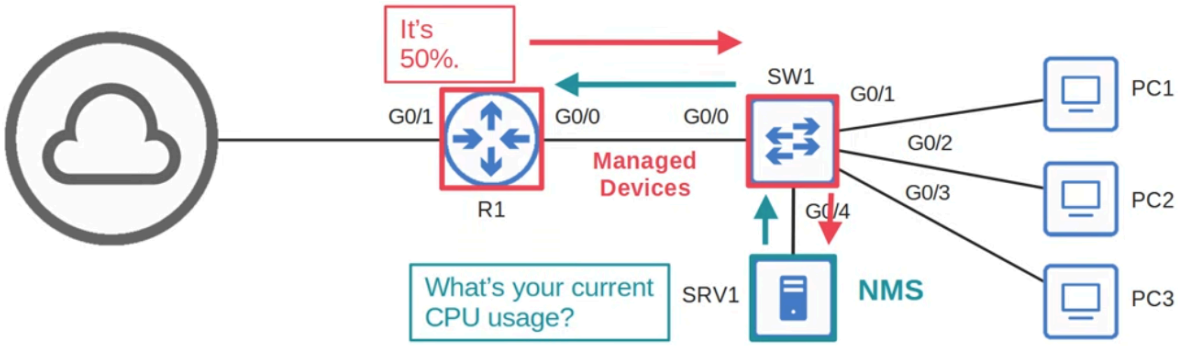
- In this network, **SRV1** is the **NMS** (Network Management Station or System).
- We're using SNMP to manage **R1** and **SW1**, so they are the **managed devices**.
- There are **three main operations** used in SNMP — three main ways SNMP can be used to help manage a network.

Operation 1: Managed Devices Notify the NMS of Events



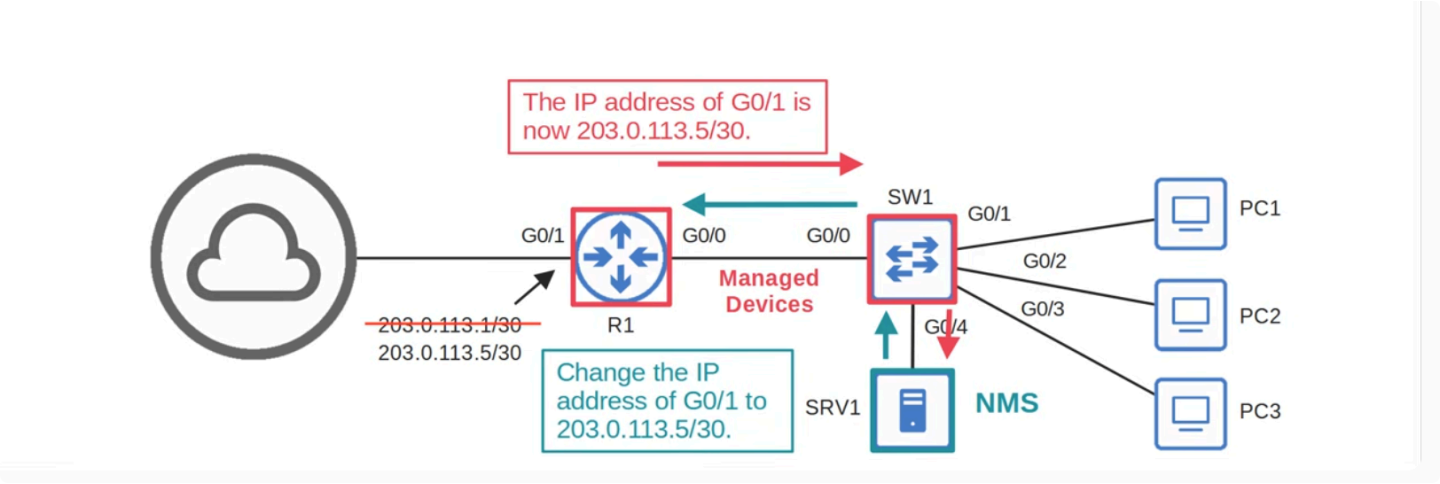
- Managed devices can notify the NMS of events.
- Example: Perhaps SW1's G0/1 interface had a hardware failure and its status changed to DOWN. It can send an SNMP message to the NMS, SRV1, telling it that the G0/1 interface has gone down.
- The actual SNMP software on the server, or the NMS, might be configured to notify the network administrator to inform them of this event.

Operation 2: NMS Asks Managed Devices for Information



- The NMS can also ask the managed devices for information about their status.
- Example: Perhaps the NMS, SRV1, asks R1 what its current CPU usage is. You want to make sure your network devices aren't being overloaded and working too hard.
- R1 will then reply to the NMS, for example telling SRV1 that its CPU usage is at 50%.

Operation 3: NMS Tells Managed Devices to Change Configuration

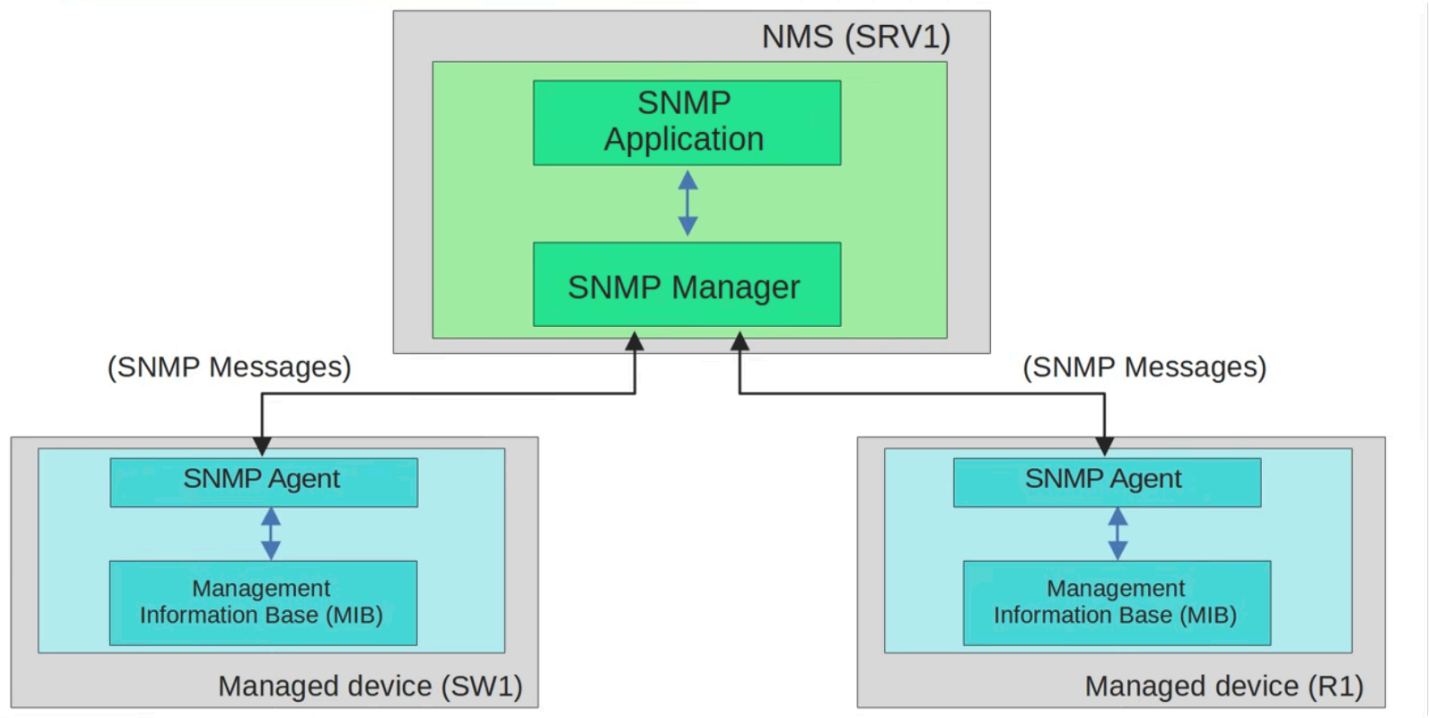


- The NMS tells the managed devices to change aspects of their configuration.
- Example: Let's say the IP address of R1's G0/1 interface is 203.0.113.1/30. The NMS can tell R1 to change that IP address to 203.0.113.5/30. R1 will change the IP address and tell the NMS that it did so.

Summary of the Three Main SNMP Operations

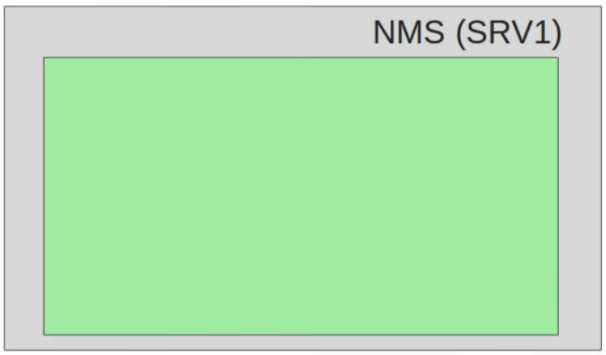
- The managed devices can **notify the NMS of events**
- The NMS can **ask managed devices for information** about their current status
- The NMS can also **tell the managed devices to change their configuration**

Main Components of SNMP

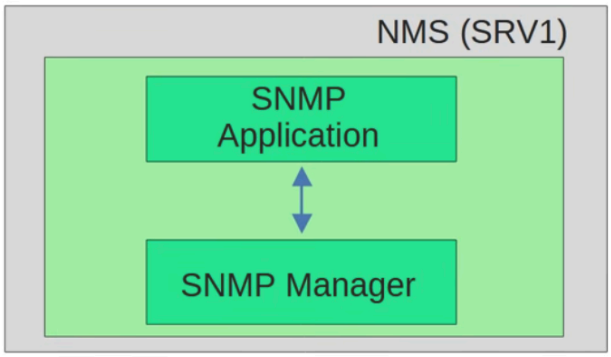


- Up top there is the **NMS** from the previous network diagram, **SRV1**.
- On the bottom, the two **managed devices**, **SW1** and **R1**.
- Let me break this diagram down step by step.

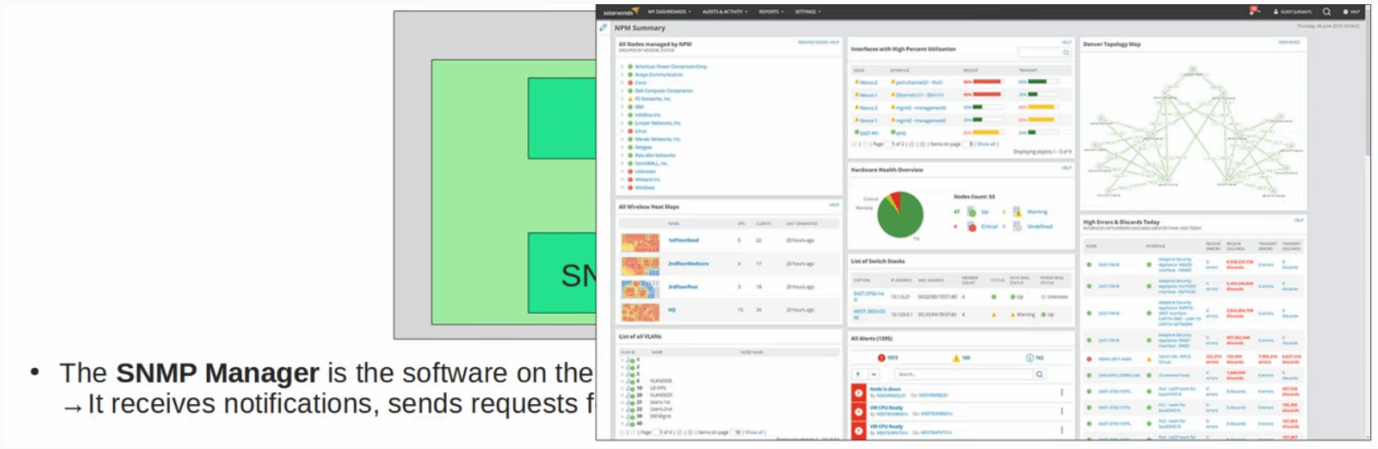
Components of the NMS



- This green section represents the **SNMP software** on the NMS.
- The NMS probably isn't a machine dedicated to SNMP — it could just be the network admin's PC which is running SNMP software.



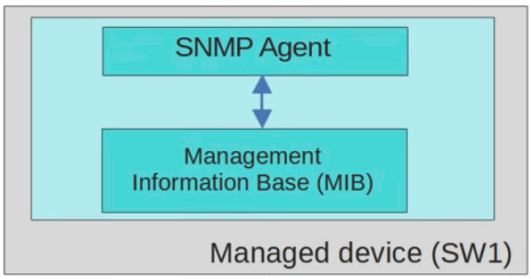
- **SNMP Manager**:
  - The SNMP software on the NMS that interacts with the managed devices.
  - It receives notifications, sends requests for information, sends configuration changes, etc.
- **SNMP Application**:

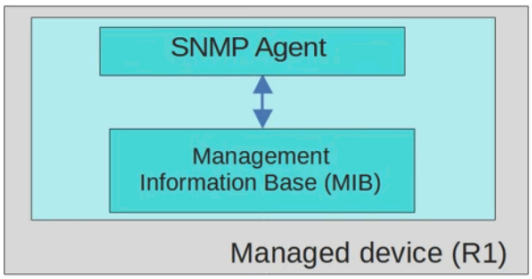


  - The application that provides an interface for the network admin to interact with.
  - It displays alerts, statistics, charts, etc.
  - Example: Here's what an SNMP Application might look like. There are plenty of free and commercial SNMP applications available. This screenshot is from SolarWinds.

Components of the Managed Devices

- This blue area represents the **SNMP entity** on the managed devices (SW1 and R1 from the example before).
- These devices are a router and a switch, so of course SNMP is just a part of what's running on these devices.

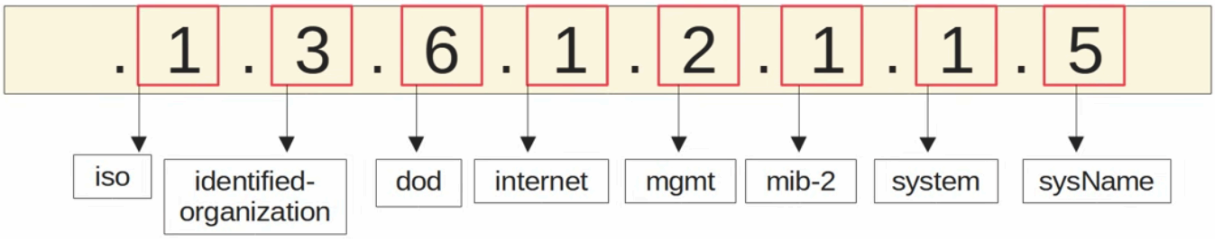




- **SNMP Agent**:
  - The SNMP software running on the managed devices that interacts with the SNMP Manager on the NMS.
  - It sends notifications to and receives messages from the NMS.
- **MIB (Management Information Base)**:
  - The structure that contains the variables that are managed by SNMP.
  - Each of these variables is identified with an **Object ID (OID)**.
  - Example: Some examples of variables stored in the MIB are the status of each interface on the device, the traffic throughput, CPU usage, device temperature, etc. Each of these will have their own OID to identify them.
- So, that's the basic structure of SNMP. Then, the SNMP messages exchanged between the agent and manager make SNMP work.

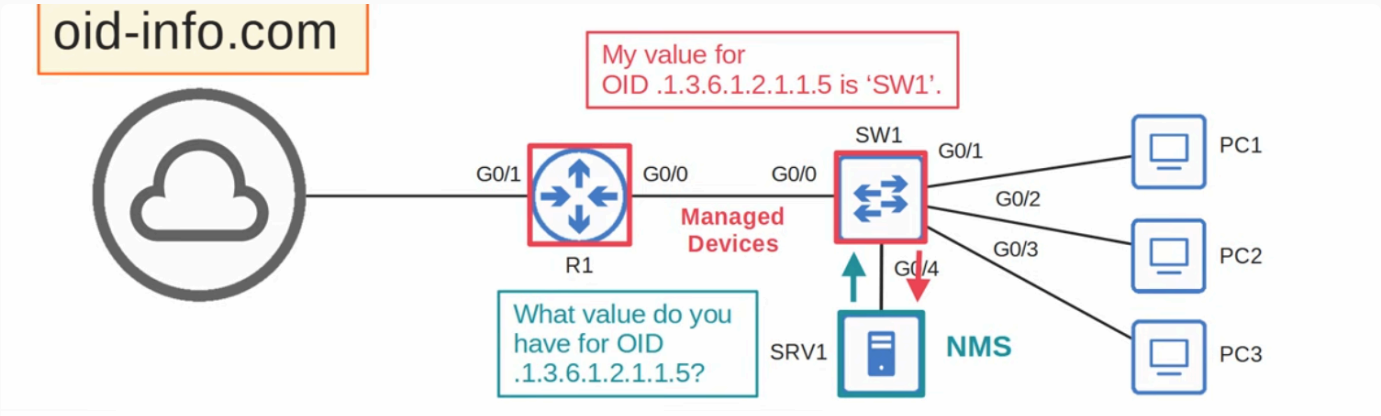
Object IDs (OIDs) and the MIB

- Before moving on to introduce the different SNMP versions, the professor briefly introduces **Object IDs (OIDs)**, which are organized in the **Management Information Base (MIB)**.
- SNMP Object IDs are organized in a **hierarchical structure**.
- Example: Here's an example of an OID, and here's how it breaks down:



  - `iso`
  - `identified-organization`
  - `dod`
  - `internet`
  - `mgmt`
  - `mib-2`
  - `system`
  - `sysName`

- So, this OID is used to identify the **system name**, the **host name**, of the managed device.



  - Example: Here's that same network again. The NMS asks one of the managed devices, SW1, what value do you have for this OID? SW1 then replies, telling the NMS its host name.
- There are **countless different OIDs**.
- If you want to explore some different OIDs you can take a look around oid-info.com.
  - Note: That's how the professor got the OID information for the system name OID used as an example here.

SNMP Versions

- Many versions of SNMP have been proposed and developed, however only **three major versions** have achieved widespread use.

SNMPv1

- This is the **original version** of SNMP.

SNMPv2c

- There are multiple versions of SNMPv2, but **v2c** is the most widely used.
- Version 2 added another message type which allows the NMS to retrieve **large amounts of information** from a managed device using a **single request**, making it much more efficient — there is less unnecessary network traffic.

- The **'c'** in the name refers to the **'community strings'**:
  - Community strings are passwords that were used in SNMPv1, removed from SNMPv2, and then added back for this version, SNMPv2c.
  - When we take a look at SNMP configuration the professor will use version 2c to demonstrate, so you'll see how these community strings work.
  - Basically they're just passwords.

SNMPv3

- The next major version and the **best version so far** is SNMPv3.
- It is a much more **secure** version of SNMP that supports **strong encryption** and **authentication**.
- The professor will talk more about those terms in the security section of this course, but basically it means that SNMPv3 makes sure that **only the intended devices can read the SNMP messages** — they can't be intercepted and read by an attacker.

SNMP Message Types

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*

- In this chart, the professor lists the **four message classes**:
  - **Read**
  - **Write**
  - **Notification**
  - **Response**
- A description is given for each class, along with the actual SNMP messages in each class.

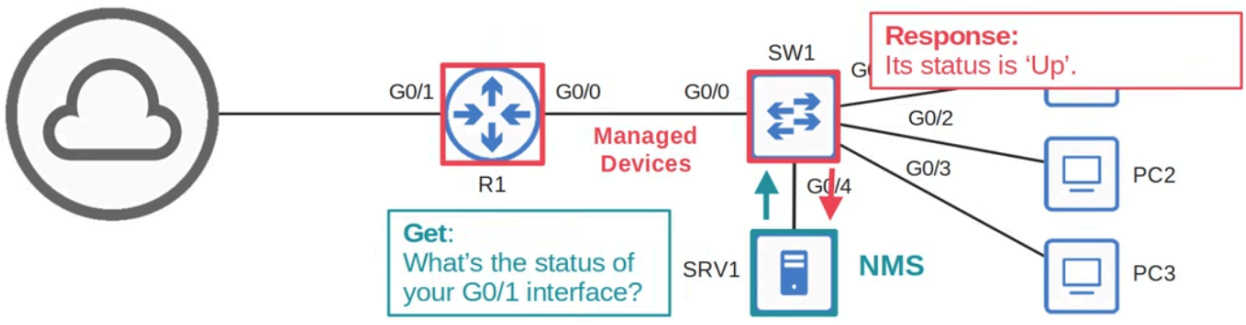
Read Message Class

- These messages are sent by the **NMS** to **read information** from the managed devices.
- Example: The professor already showed a few examples before, like when SRV1 asked SW1 what its host name is.
- There are **three messages** in this class:
  - **Get**
  - **GetNext**
  - **GetBulk**

SNMP Message Types — Read Messages (Continued)

- The professor notes this is more depth than necessary for the CCNA, so he gives a quick outline of these messages.

Get



- A request sent from the **manager to the agent** (the NMS to the managed device) to retrieve the value of a variable, an OID, or multiple variables.
- The agent will send a **'Response' message** with the current value of each variable.
- Example: Our NMS here might ask SW1, what's the status of your G0/1 interface? And SW1 responds with an SNMP 'response' message.

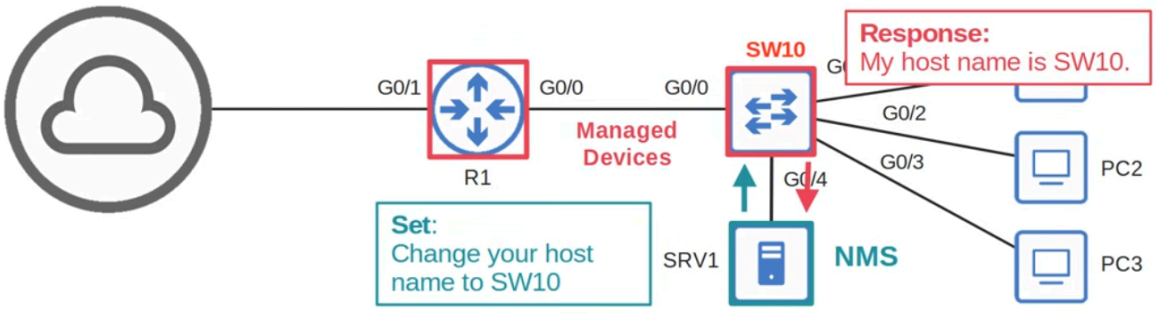
GetNext

- Sent from the **manager to the agent** to **discover the available variables** in the MIB.
- Basically, it says 'tell me the next OID', so it can be used to discover what other OIDs are available.

GetBulk

- A more efficient version of **GetNext**, introduced in **SNMPv2**.
- *Note: If you know the purpose of the basic Get message, you'll be fine for the CCNA.*

SNMP Message Types — Write Messages



Set

- There is only **one kind** of 'write' message, which is **Set**.
- These are sent by the **NMS** to **change information** on the managed devices — to change the value of a specific variable, such as changing an IP address.
- The Set message is a request from the **manager to the agent** to change the value of one or more variables.
- Then the agent will send a **Response message** with the new values.

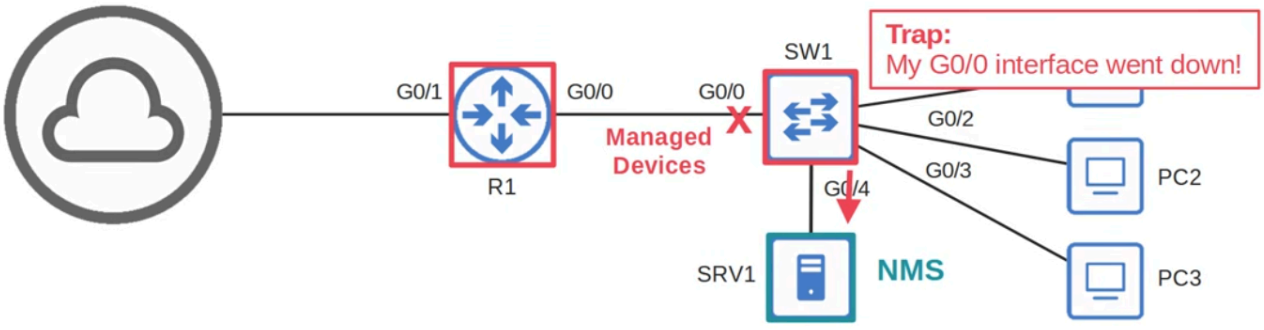
- Example: The professor already showed an example of an SNMP Set message when SRV1 made R1 change the IP address of its G0/1 interface, but he demonstrates again.
- Example: SRV1 can send a Set message to SW1, requesting that it change its host name to SW10. SW1 will then change its host name, and send a Response message with its new host name.

SNMP Message Types — Notification Messages

- These are messages sent by the **managed devices** to **alert the NMS** of a particular event, for example when an interface goes down.
- There are **two different messages** in this class:
  - **Trap**
  - **Inform**

Trap

- A notification sent from the **agent to the manager** — so the managed device to the NMS.
- The manager does **not** send a Response message to acknowledge that it received the Trap, so these messages are **unreliable**.
- Also, SNMP uses **UDP**, so there are no TCP retransmissions.
- Unless there's some problem in the network, the Trap will reach the NMS no problem, but since there is no reliability mechanism built-in, they are called **unreliable messages**.



- Example: SW1's G0/0 interface went down, so it sends a Trap message to the NMS, SRV1. That's it — no response is sent to SW1. This Trap will probably appear as an alert in the SNMP application on SRV1, and perhaps it will send an email notification to the network admin, or something like that.

Inform

- Like a Trap message, but it is **acknowledged with a Response message**.
- Even though this message is sent with **UDP**, not TCP, there is **reliability built into the message itself**.
- Example: If SW1 sends an Inform to SRV1, SRV1 will send a Response to tell SW1 that the Inform was received.
- This message type was originally used for **communications between managers**, for networks with multiple SNMP managers.
- However, later updates to the protocol allow **agents to send Inform messages to managers**, too.
- So, those are the SNMP **Trap** and **Inform** messages.

SNMP Message Types — Response 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

Response

- There is **one message** in this class, **Response**.
- These are messages sent in **Response to a previous message or request**.
- Examples: Get messages, Set messages, and Inform messages.
- The professor just showed some examples of Response messages, so that's enough for now.

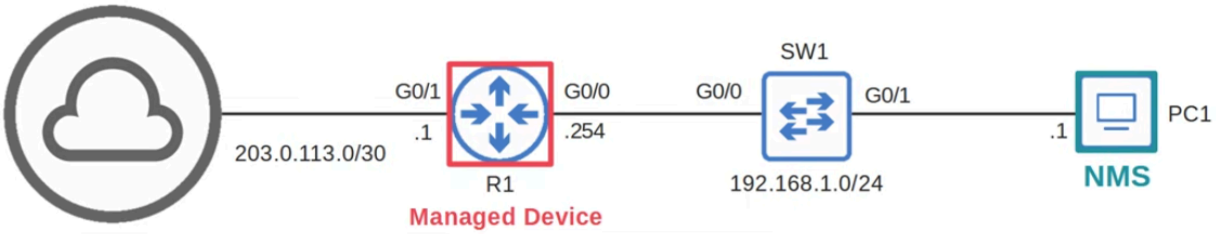
SNMP Port Numbers

- The professor mentioned these port numbers in the Day 30 video on TCP and UDP.
- **SNMP Agents** listen for messages on **UDP port 161**.
- **SNMP Managers** listen for messages on **UDP port 162**.
- *Note: Make sure you remember those port numbers.*
- The information just covered is more than enough for the CCNA.

Basic SNMP 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



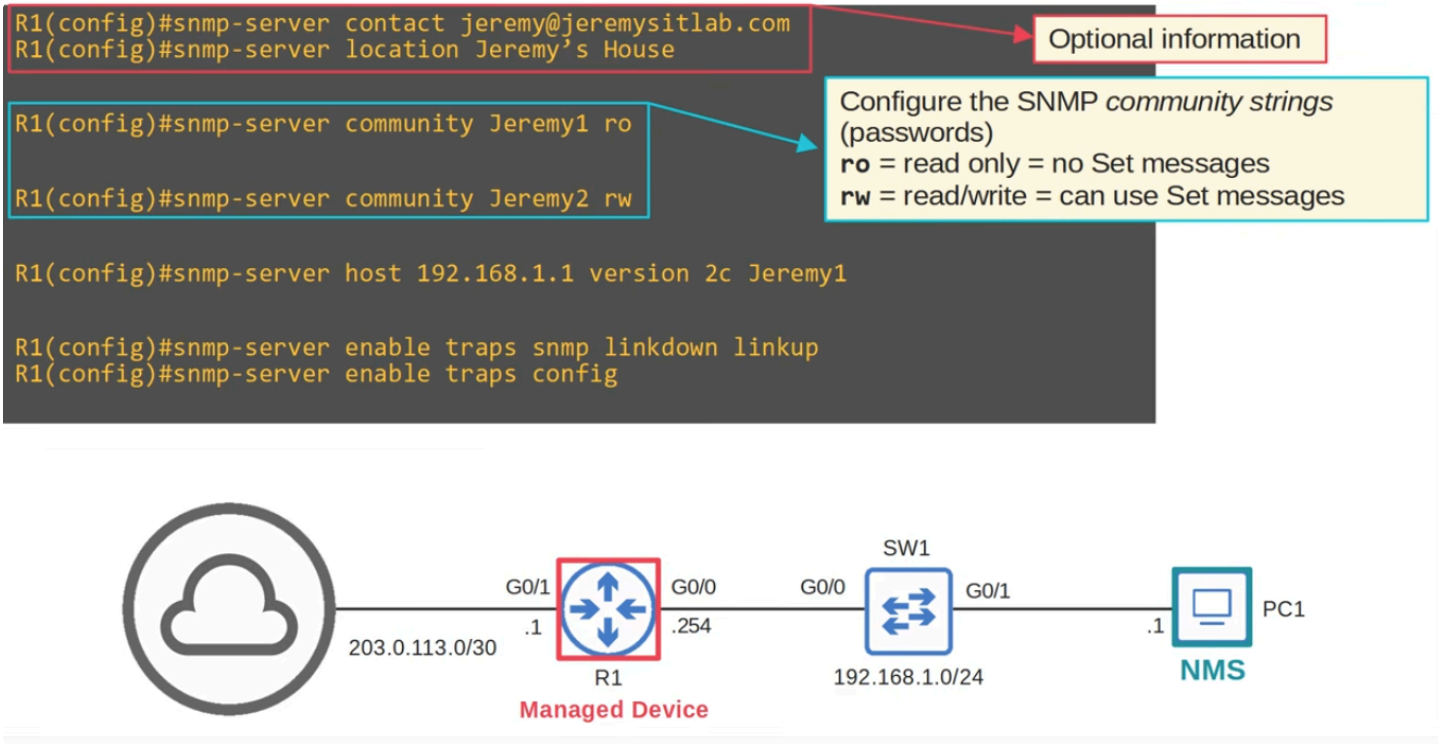
- The professor demonstrates some basic SNMP configuration.

- As said before, SNMP configuration isn't mentioned in the exam topics list, but getting a bit of hands-on practice is always helpful.
- Setting up the NMS will **not** be covered — that's definitely out-of-scope for the CCNA.
- This demonstration covers how to set up the **SNMP agent** on a Cisco router.
- In this network:
  - **R1** is the managed device
  - **PC1** is the NMS, running an SNMP application

Optional Information

- First, the professor configured some optional information on R1, giving some contact information and the location of the device.
- This is **optional** information — you don't need to configure this.

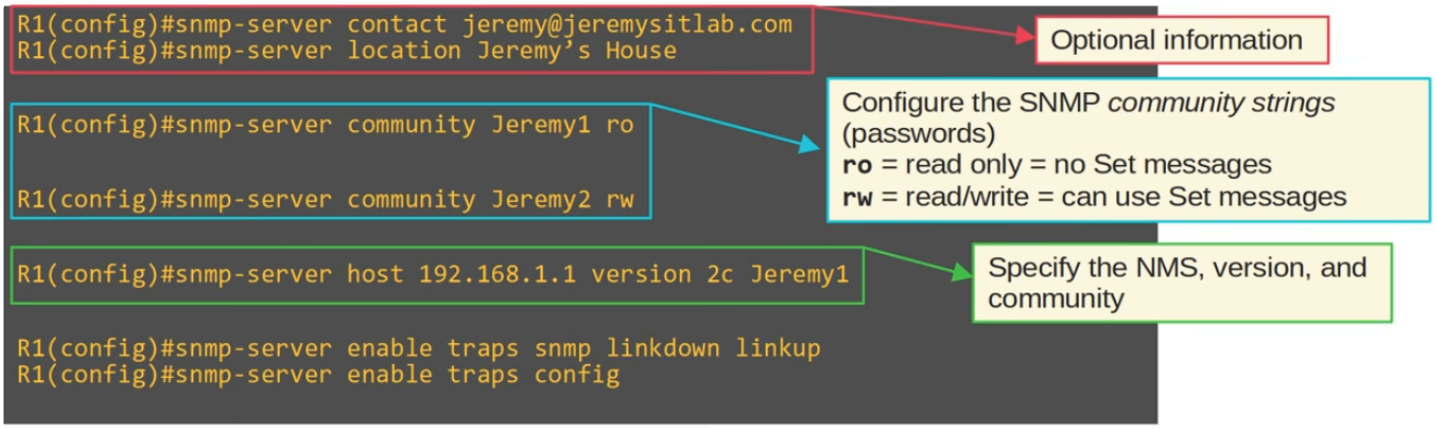
Community Strings

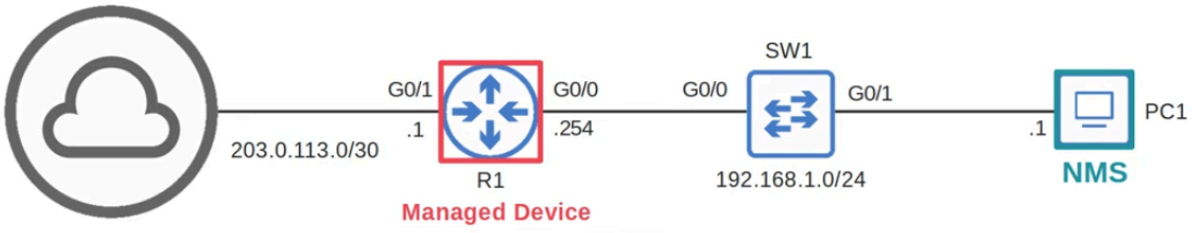


- The professor configured **two community strings**.
- As mentioned before, community strings are basically SNMP passwords.

- The community string **Jeremy1** was specified as **RO**, which means **read only**:
  - An NMS using this password can only read information from R1.
  - It can't use Set to make any changes to R1.
- The community string **Jeremy2** was specified as **RW**, which means **read/write**:
  - An NMS using this password will be able to both read, using Get messages, and write, using Set messages.
- *Note: There are actually default community strings:*
  - **'public'** for RO
  - **'private'** for RW
  - If you don't specify community strings, these will be used.
  - Of course, it's best to configure the community strings and not use the defaults, as they are less secure.

NMS Address Configuration

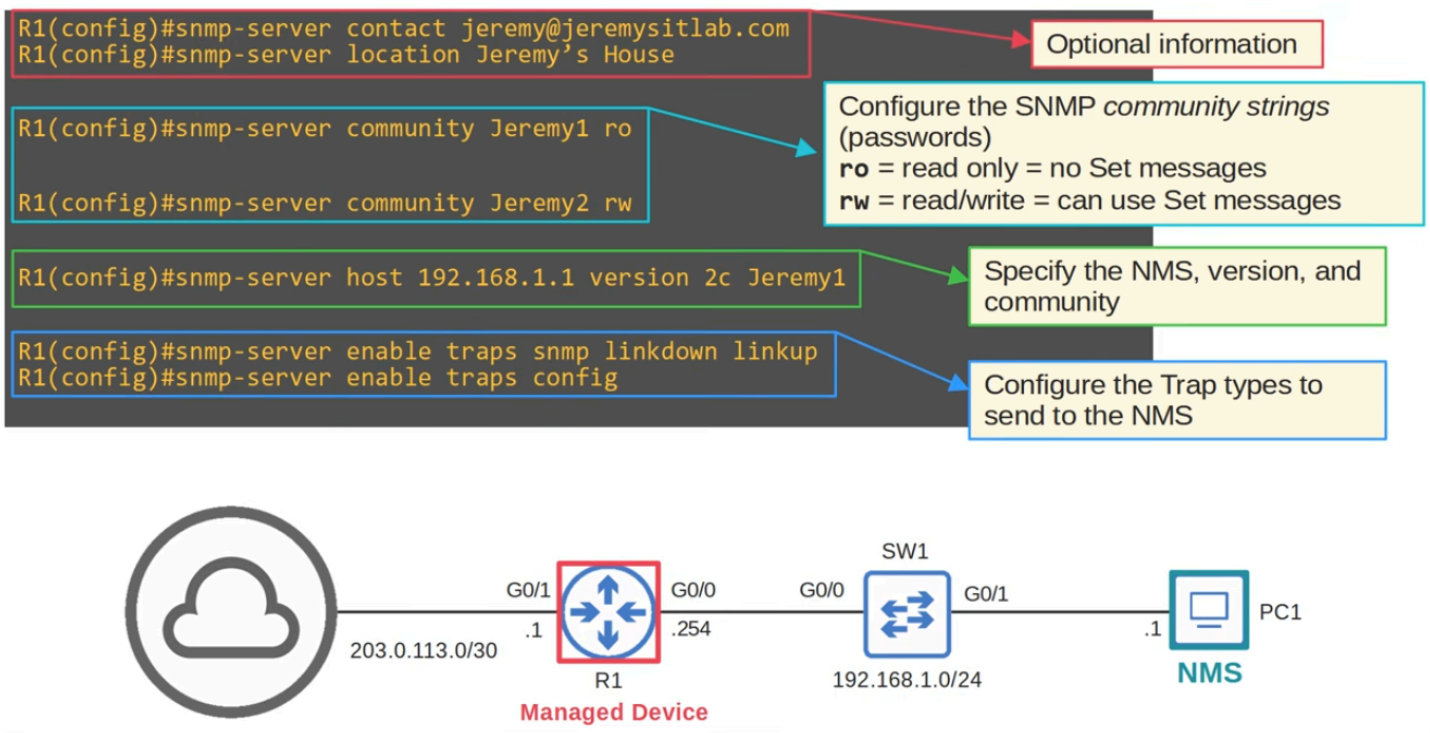




- The professor specified the address of the NMS, **PC1 at 192.168.1.1**.

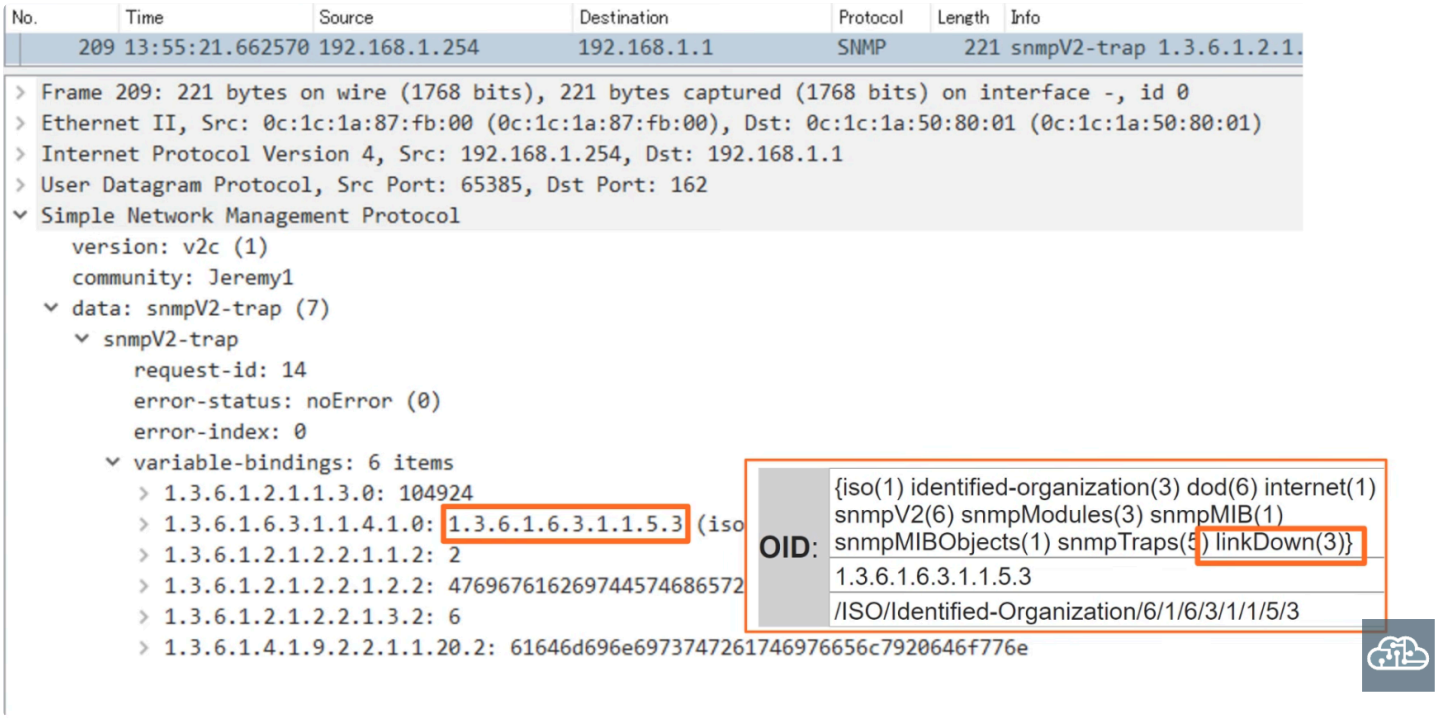
- In this command, he also specified the version and which community string to use with this server.
- He configured **Jeremy1**, so PC1 will be able to read information from R1, but it won't be able to use Set messages to make changes to R1.
- So, the read/write community string **Jeremy2** isn't being used in this configuration.

Trap Configuration



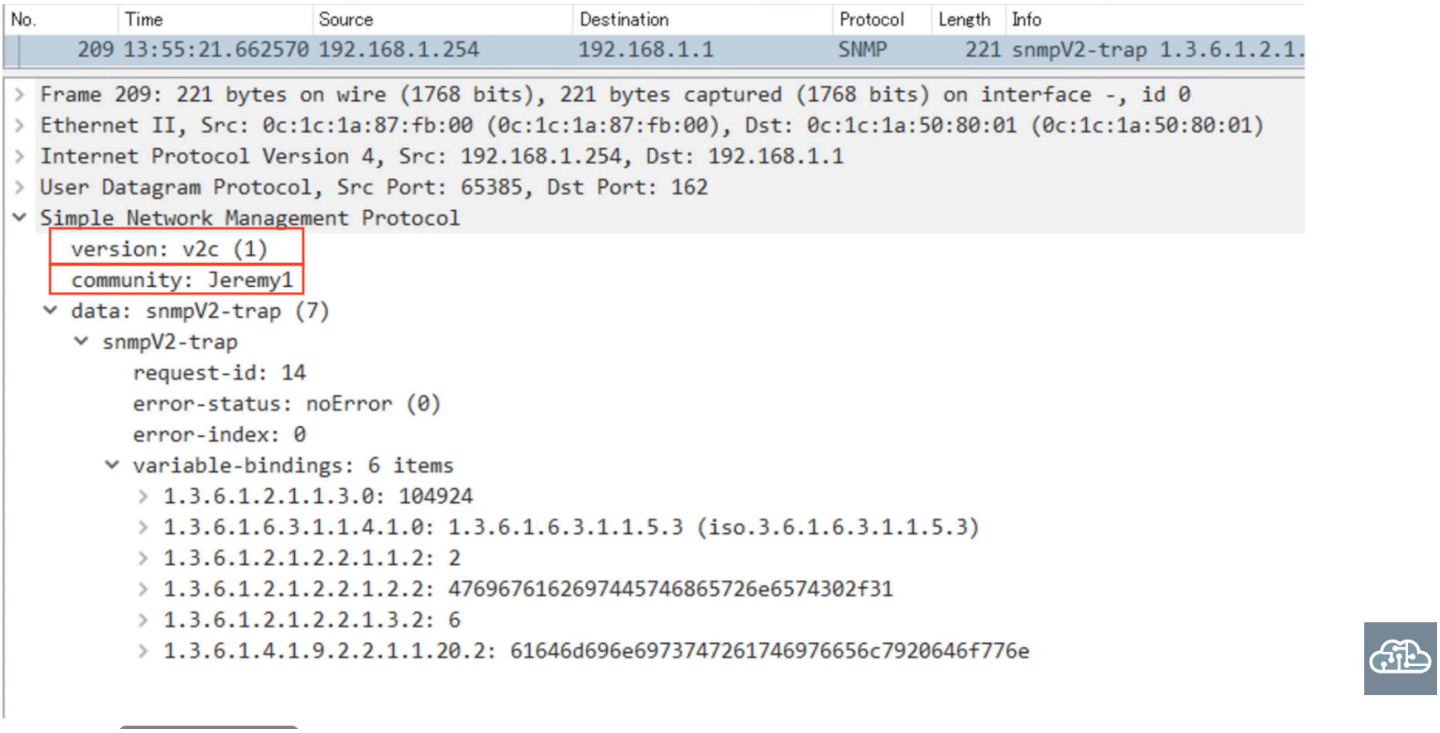
- The professor configured what kinds of traps to send to the NMS.
- He specified **LINKDOWN** and **LINKUP** messages, so if an interface goes up or down, Traps will be sent.
- He also specified **config traps**, so for example if configuration changes are made, Traps will be sent.
- So, that's a simple **SNMPv2c configuration**.

Wireshark Capture of the SNMP Trap



- The professor shows a Wireshark capture of the **Trap** that was sent from **R1** to the **NMS, PC1**.
- If you look at the bottom, you'll see **numerous OIDs** included in this Trap.
- He looked up this OID using [oid-info.com](), and it is a **linkDown Trap**, notifying the NMS that R1's interface went down.

Other Fields of the SNMP Message



- You can see the **version of 2c** that he configured.
- And here's the **community, Jeremy1** — the RO community string he configured.
- *Note: This community string, this password, is displayed in **plain text**. 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.*
- So, as mentioned before, **SNMPv3 is the preferred option**.
- However, SNMPv3 configuration is also more complicated, so for this simple demonstration he selected **version 2c**.

Summary of SNMP

- SNMP helps manage devices over a network.
- There are **two main components** of SNMP:
  - **Managed devices** — the devices being managed using SNMP, such as network devices, for example routers, switches, and firewalls.
  - **Network Management Stations (NMS)** — the SNMP servers that manage the devices.

- The NMS:
  - Receives notifications from managed devices
  - Can change the settings on managed devices
  - Can also check on the status of managed devices
- Variables such as interface status, temperature, traffic load, host name, etc., are stored in the **MIB** of the managed devices, and each variable is identified using an **Object ID (OID)**.
- There are **three main SNMP versions**: version 1, version 2c, and version 3.
- **Version 3 is preferred** because it is more secure than the previous versions, providing encryption and authentication of SNMP messages.
- The SNMP messages covered: **Get, GetNext, GetBulk, Set, Trap, Inform, and Response**.
- That should be more than enough information about SNMP for the CCNA.
- Remember, the exam topics state you need to know the **function of SNMP in network operations**.
- There's a lot more that can be learned about SNMP, of course, but the professor leaves it here.
- As always, make sure to watch until the end of the quiz for a bonus practice question from Boson Software's ExSim, the best practice exams for the CCNA.