CNP Assignment -2

Group 5

Topic SNMP

Simple Network Management Protocol (SNMP)

Subject - Computer Network Protocols ICT 2255
Date - 11/4/23

Names -	Daksh Dadhania	210911072
	Ojas Parashar	210911076
	Ayushi Jain	210911086
	PVS Prashanth	210911084

1. Write the steps to generate and capture the specified protocol packets using wireshark.

Ans: Following are the steps to be followed to produce SNMP Protocols on iReasoning SNMP Simulator:

Pre requisite: Download and install Wireshark on your computer.

1. Open wireshark and click on the interface you want to capture SNMP packets on.
2. Click on the "Capture" button to start capturing network traffic.
3. In the "Filter" field type "snmp" to filter for SNMP protocols.
4. Launch iReasoning SNMP Simulator.
5. Create a new simulation by selecting "File" > "New" > "Simulation".
6. Add a device to the simulation by selecting "Device" > "New Device".
7. Configure the device's SNMP properties such as version, community string, port.
8. Add SNMP objects to the device by selecting "Device" → "Add Object".
9. Set the values of the SNMP objects as needed.

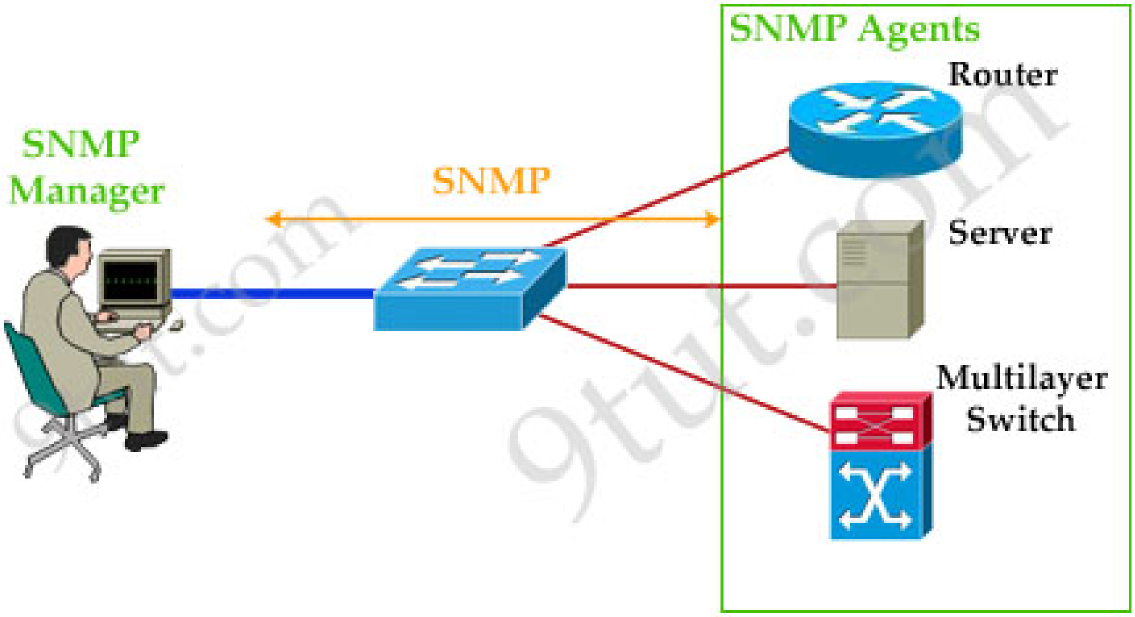
10. Start the simulation by selecting "Simulation" > "Start".

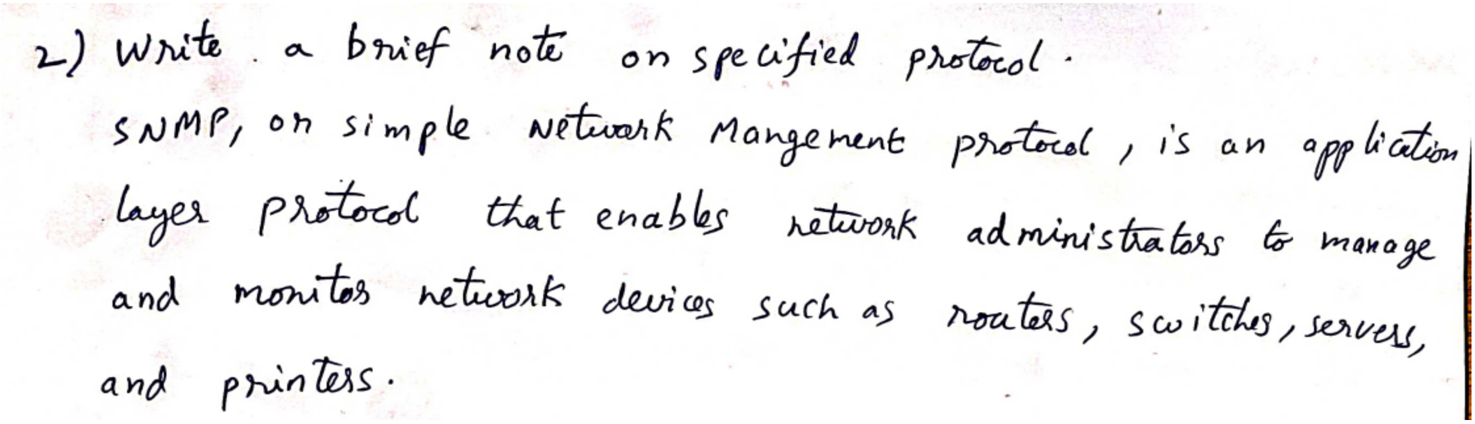
11. To generate SNMP packets, you can use iReasoning SNMP Simulator's built in SNMP client to send SNMP requests or traps. To do this, select "Tools" > "SNMP client" and configure the client's SNMP properties such as SNMP vertion, community string and SNMP port.

12. Once you have generated or captured SNMP packets, you can view the details of each packet in WireShark by clicking on the packet in packet List.

13. You can also use "Statistics" menu in wireshark to view various statistics about the captured packets, such as packet count, byte count and protocol distribution.

⇒ To save the captured packets for later analysis, you can use the "File" menu in Wireshark to save the captured packets in various formats, such as pcap, pcapng or CSV.





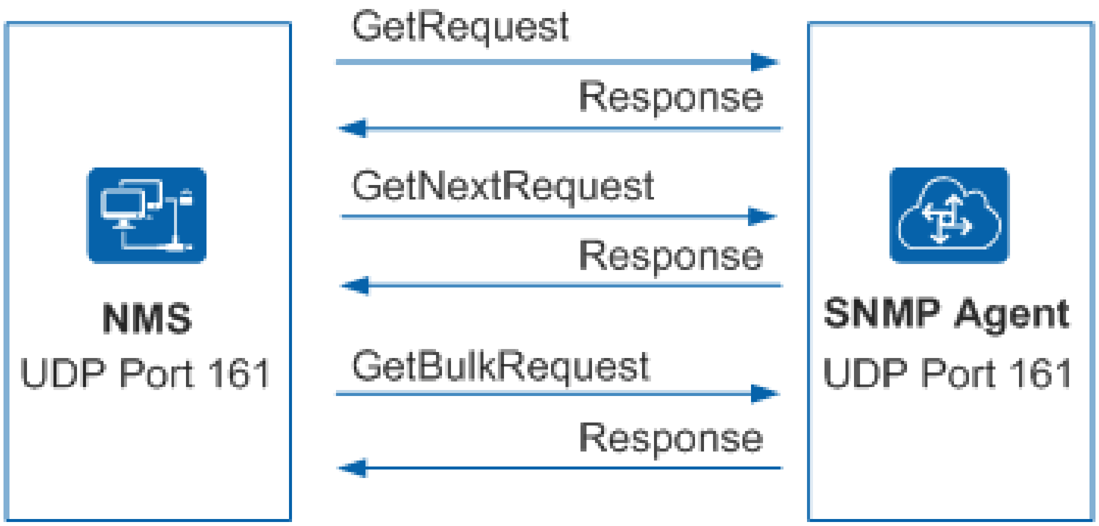
2) Write a brief note on specified protocol.

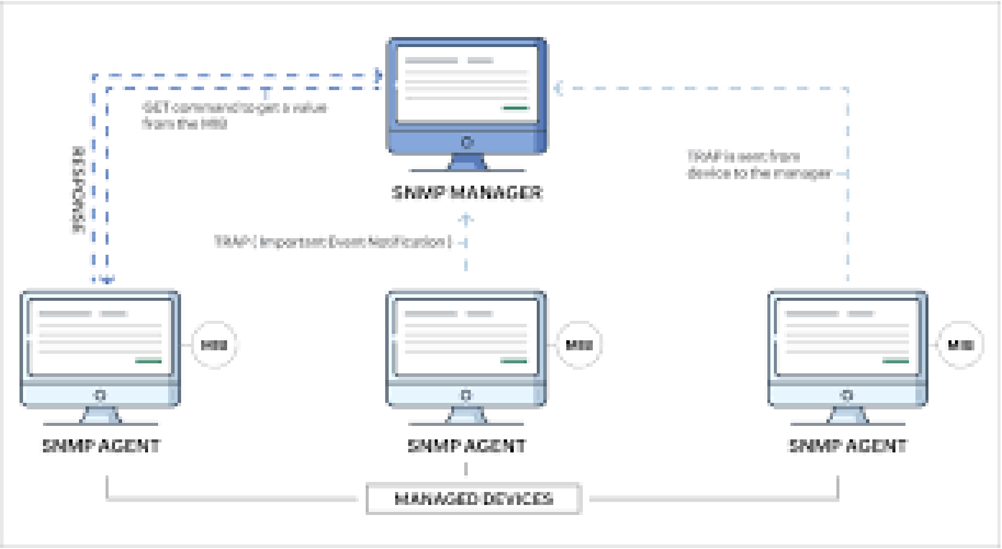
SNMP, or simple Network Mangement protocol, is an application layer protocol that enables network administrators to manage and monitor network devices such as routers, switches, servers, and printers.

It operates using a client-server model, where the SNMP agent runs on the network device being managed, and the SNMP manager runs on the network mangement system. The manager ~~returns~~ communicates with the agent using SNMP messages, which are exchanged over UDP. These messages request information about the device's status, configuration and performance, and can also be used to configure or control the device.

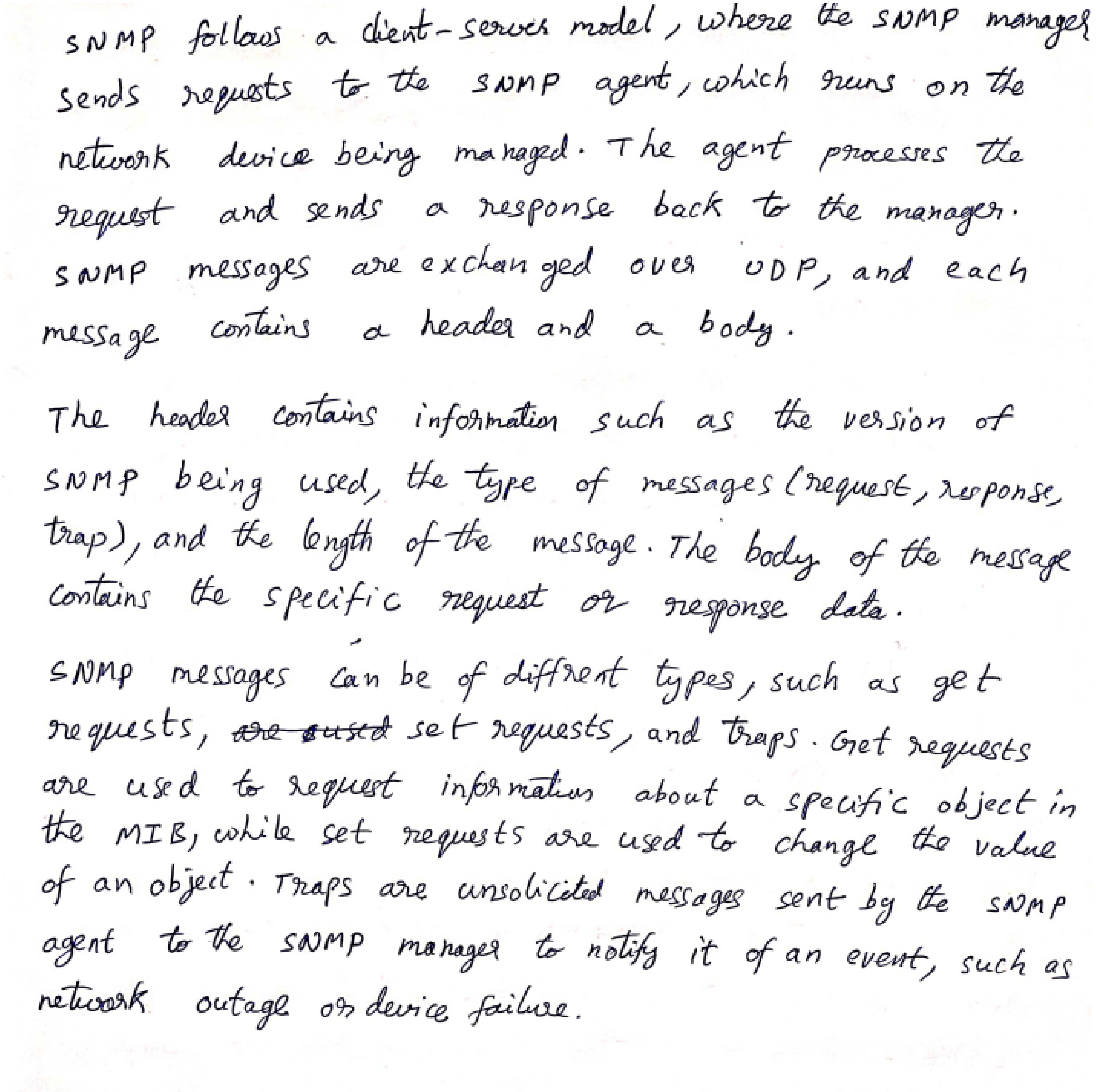
SNMP operates on a hierachical structure of objects called Management information Bases (MIBS), which provide information about the network device. Each object in a MIB is identified by an object identifier (OID) and has a value associated with it.

SNMP has several versions, with SNMPV3 being the most widely used. It provides enhanced security features such as encryption; authentication and access control, making it more suitable for enterprise-level network managment. These security mechanisms help protect against unauthorized access to the network. Though they are less used nowadays.


GetRequest
Response
GetNextRequest
Response
GetBulkRequest
Response
NMS
UDP Port 161
SNMP Agent
UDP Port 161


GET command to get a value from the MIB
RESPONSE
SNMP MANAGER
TRAP is sent from device to the manager
TRAP (Important Event Notification)
MIB
MIB
MIB
SNMP AGENT
SNMP AGENT
SNMP AGENT
MANAGED DEVICES

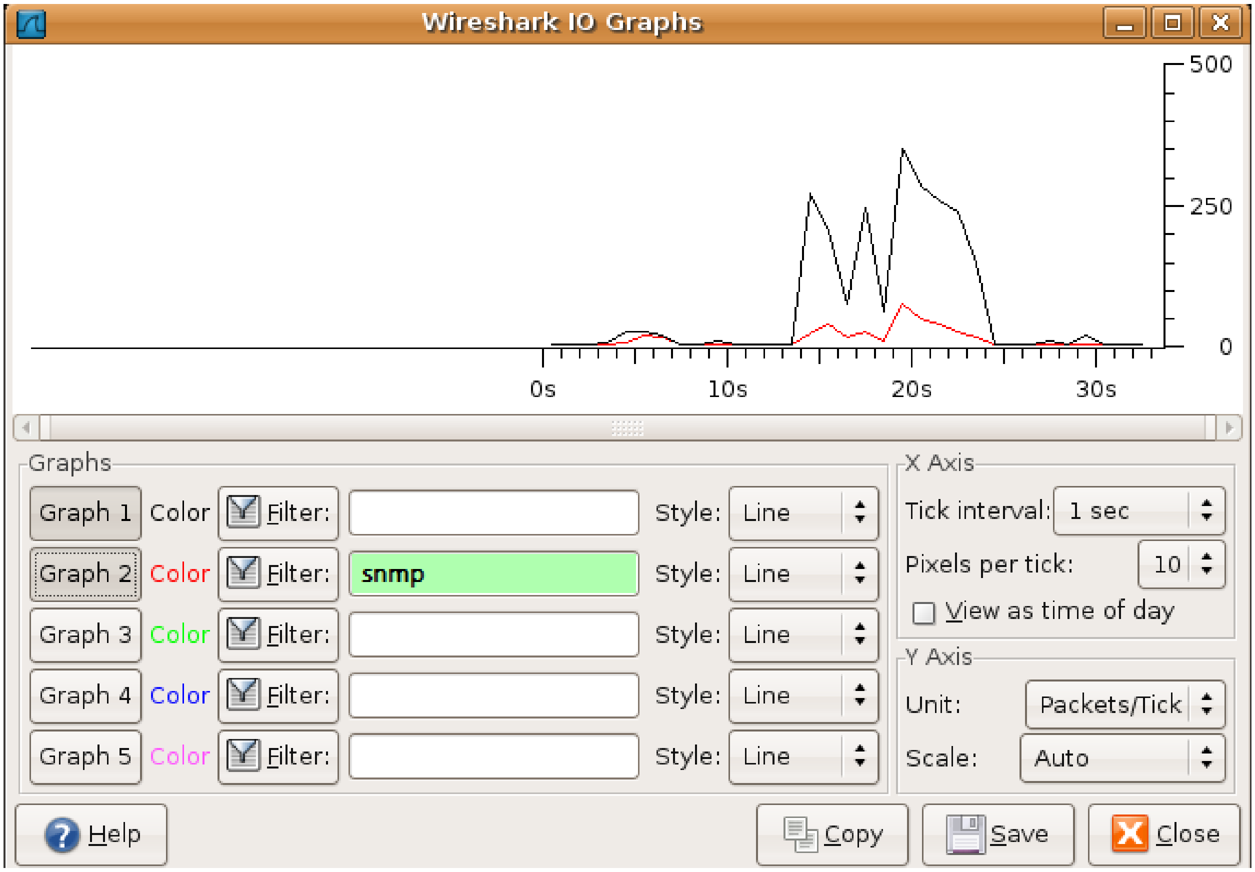
Q3. **Show the flow (I/O) graph and try to analyze the flow (Overall flow)**



SNMP follows a client-server model, where the SNMP manager sends requests to the SNMP agent, which runs on the network device being managed. The agent processes the request and sends a response back to the manager. SNMP messages are exchanged over UDP, and each message contains a header and a body.

The header contains information such as the version of SNMP being used, the type of messages (request, response, trap), and the length of the message. The body of the message contains the specific request or response data.

SNMP messages can be of diffrent types, such as get requests, ~~are used~~ set requests, and traps. Get requests are used to request information about a specific object in the MIB, while set requests are used to change the value of an object. Traps are unsolicited messages sent by the SNMP agent to the SNMP manager to notify it of an event, such as network outage or device failure.



Graphs

Graph 1 Color Filter: Style: Line

Graph 2 Color Filter: snmp Style: Line

Graph 3 Color Filter: Style: Line

Graph 4 Color Filter: Style: Line

Graph 5 Color Filter: Style: Line

X Axis

Tick interval: 1 sec

Pixels per tick: 10

☐ View as time of day

Y Axis

Unit: Packets/Tick

Scale: Auto

Q4. Show the protocol hierarchy of the specified protocol and explain all the layers it has.

SNMP operates all the application layer of the OSI model. The protocol hierarchy can be represented as follows

Application layer (SNMP)

SNMP Message

SNMP version

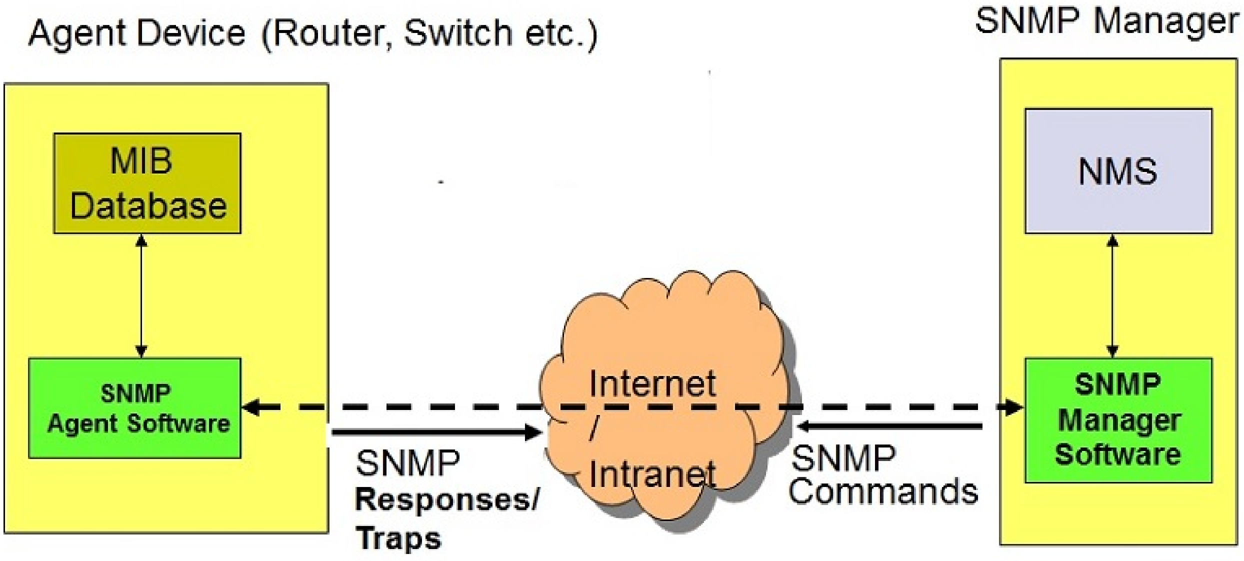
SNMP Header

SNMP PDU

The length of an SNMP packet depends on the size of the SNMP message, which includes the SNMP header and SNMP PDU. The SNMP header is 20 bytes in length and contains information such as the version of SNMP being used, type of message, length of message, ID of message.

The SNMP PDU varies in size - depending on the type of message being sent

SNMP Architecture



eg: A get request PDU consists of the following

Request ID (4 bytes)

Error Status (1 byte)

Error Index (1 byte)

variable bindings (variable length)

The variable bindings contain OID and value of the object being requested. The length of the variable bindings varies with the number of objects being requested.

Q5 Explain the structure of Wireshark

Wireshark is a network protocol analyser that allows you to capture and view network traffic in real-time. The structure of Wireshark can be divided into 4 main parts

Capture options : This selection allows you to select the network interface you want to capture traffic on and configure ~~traffic on~~ capture options such as the capture filter, snap length & buffer size

Packet List pane : This section displays a list of captured packets, with each row representing a single packet. The columns in the packet list pane show various packet details such as the time of capture, source and destination addresses & protocol type

Packet detail pane : This section displays the details of the selected packet in a tree-like structure with each layer of the protocol stack represented as a node. You can expand and collapse each node to view details of each layer.

Packet bytes pane : This section displays the hexadecimal representation of the selected packet, with each byte of packet displayed in 2 digit format. You can use this pane to view the raw data of the packet.

Wireshark also provides various tools & features to help you analyse network traffic such as filters, colouring rules, statistics and graphs. These tools can help you identify network problems, troubleshoot issues and optimize network performance.

SNMP Packet generation was done in two ways -

1. Used iReasoning SNMP Simulator (Used Cisco 6500 switch to generate packets)
2. Used SNMPBulkWalk (Linux package to generate bulk packets)

Both methods' screenshots are provided in the /screenshot folder.
(Please have a look)

Thank You, Sir

- Document by Daksh Dadhania
- Written by Prashanth, Ayushi, and Ojas