**Classification of SNMP protocol using Wireshark with monitoring PRTG Traffic grapher and Visualization with Orange and Rapid Miner**

Nama: Andika Putra Jaya | NIM : 09011381520050

**Definition of SNMP**

Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring. These protocols are supported by many typical network devices such as routers, hubs, bridges, switches, servers, workstations, printers, modem racks and other network components and devices. Supported devices are all network-attached items that must be monitored to detect conditions. These conditions must be addressed for proper, appropriate and ongoing network administration. SNMP standards include an application layer protocol, a set of data objects and a methodology for storing, manipulating and using data objects in a database schema.

The SNMP protocol is included in the application layer of TCP/IP as defined by the Internet Engineering Task Force (IETF) [https://www.techopedia.com/definition/5473/simple-network-management-protocol-snmp]



**Component of SNMP**

* **SNMP agent:** This program runs on the hardware or service being monitored, collecting data about various metrics like [bandwidth](https://searchnetworking.techtarget.com/definition/bandwidth) use or disk space. When queried by the SNMP manager, the agent sends this information back to the management system. An agent may also proactively notify the NMS if an error occurs. Most devices come with an SNMP agent preinstalled; it typically just needs to be turned on and configured.
* **SNMP-managed devices and resources:**These are the nodes on which an agent runs.
* **SNMP manager (aka NMS):** This software platform functions as a centralized console to which agents feed information. It will actively request agents send updates via SNMP at regular intervals. What a network manager can do with that information depends heavily on how feature-rich the NMS is. There are several free SNMP managers available, but they are typically limited in their capabilities or the number of nodes they can support. At the other end of the spectrum, enterprise-grade platforms offer advanced features for more complex networks, with some products supporting up to tens of thousands of nodes.
* **Management information base (**[**MIB**](https://whatis.techtarget.com/definition/management-information-base-MIB)**):**This database is a text file (.mib) that itemizes and describes all objects used by a particular device that can be queried or controlled using SNMP. This database must be loaded into the NMS so that it can identify and monitor the status of these properties. Each MIB item is assigned an object identifier ([OID](https://whatis.techtarget.com/definition/object-ID-OID)). [https://searchnetworking.techtarget.com/definition/SNMP]

**Scenario Topology**



|  |  |
| --- | --- |
|  | **Device** |
| **Cloud 1** | **R1** | **R2** | **R3** |
| **Ip address** | **192.168.10.2** | **12.12.8.1** | **12.12.8.2** | **25.25.25.3** |

* Configuration on R1



* Configuration on R2



* Configuration on R3



First of all we make a scenario topology in GNS 3 (Graphical Network Simulator 3), we have 4 component 3 router as agent and 1 pc as Manager. After we make a scenario topology we configure every device from pc until router 3, we configure using an ip address for each deivces and connected with OSPF.

Before we open wireshark to capture the protocol we must try every device with PING! If already success we continue configure all of router for the snmp server to get protocol snmp in wireshark.

**Capturing with wireshark and Monitor with PRTG**

* Capture All protocol using Wireshark



* Capture SNMP protocol using wireshark



* Monitoring every routers with PRTG



**Visulization with Orange and Rapid Miner**

* Visualization with rapid miner

To make visualization we can get the data from wireshark with format .csv we export to rapid miner to get visualization, we can choose so many visualization in this cace we use chart pie and scatter pot in rapid miner, in rapid miner we take the data in wireshark for all protocol so we can know how many protocol we can get and make visualization

* Visualization with Orange



For orange we make visualization just snmp protocol, so we export the data from wireshark with format .csv just for snmp protocol. in axis x we have source and in axis y we have destination.