**Analysis of SNMP Using Wireshark with Classification Traffic and Monitoring with PRTG Traffic Grapher**

# Kurnia Santy Lingsing Puteri (Computer Engineering UNSRI) 09011381520060

Monitoring is done of communications which occur in a network of nodes, each communication being effected by a transmission of one or more packets among two or more communicating nodes, each communication complying with a predefined communication protocol selected from among protocols available in the network. The contents of packets are detected passively and in real time, communication information associated with multiple protocols is derived from the packet contents. [1]

Regardless of what monitoring vendors will have you believe, a finite and limited number of technologies can be used to monitor. So this is kind of monitoring tech :

1. **PING**

This is a network admin tool that is used to test the reachability and availability of a host in an IP network. The data from ping results can determine whether a host in the network is active or not. Furthermore, it can measure the transmission time and packet loss when communicating with a host. [2]

1. **SNMP**

SNMP is a network management protocol that is used for exchanging information between hosts in a network that includes network monitoring software. This is the most widely used protocol for management and monitoring of the network and includes the below components: Managed device: The node in the network that supports SNMP and access to specific information.

**Managed device:**The node in the network that supports SNMP and access to specific information.

**Agent:**A software that is part of the monitored device. An agent has access to the MIB (management information database) of the device and allows NMS systems to read and write to the MIB.

**Network Management System (NMS):**An application on a system that monitors and controls the managed devices through the agent using SNMP commands.

SNMP data is collected or sent to a managed device, either by polling or using traps. Traps allow an agent to send information to an NMS about events on the device.

The MIB holds information about the structure of the data on a device for management. The MIBs contain OID (object identifiers) which is the actual identifier for the variable to be read from the device or set on the device. [2]



Image 1 . Structure SNMP[1]

1. **ICMP**

The Internet Control Message Protocol is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. [3]

Next, we will make a topology with GNS3, GNS3 (Graphical Network Simulator 3) is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud. GNS3 can help you prepare for certification exams such as the Cisco CCNA, but also help you test and verify real world deployments [4]



Image 2. Topology With GNS3

After creating the topology, we assume the topology work with *ping protocol* each other used OSPF to connecting between devices and don’t forget to use snmp-protocol command to each router. We used 3 with 2 router as snmp agent and 1 laptop as snmp manager, router from cisco C6291 we can download the firmware to embedded GNS3 from official website and using windows 10 for monitoring the router.

For monitoring I use PRTG Network Monitor. First we should open PRTG Network Monitor application, and make sure topology running well on gns3 and setup each router until connected with ospf.



Image 3. Routers 1 monitored



Image 4. Routers 2 monitored



Image 5. Routers 3 monitored

Wireshark captured at port ethernet we connected with routers and we can see the classification protocol that passed way at ethernet to router and so on upstream downstream, length, info , time and destination.

Image 6. Wireshark classification

After we captured the wireshark we can export to csv (excel file) for make a visualization to Orange Biolabs like this:



Image 7. Orange Biolabs Visualization

And I also make a visualization with RapidMiner Studio like this:



Image 8. RapidMiner Visualization

**DAFTAR PUSTAKA**

**[1]** Engel, F., Jones, K.S., Robertson, K., Thompson, D.M. and White, G., Concord Communications Inc, 2000. *Network monitoring*. U.S. Patent 6,115,393.

**[2]** https://www.solarwinds.com/basics-of-network-monitoring

**[3]**https://en.wikipedia.org/wiki/Internet\_Control\_Message\_Protocol#cite\_note-Forouzan-1

**[4]**https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9\_aLY8kkdhgaMB0wPCz8a38/index.html