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

Aulyah Nur Rohimah(Computer Engineering UNSRI)

09011381520069@STUDENTS.ILKOM.UNSRI.AC.ID

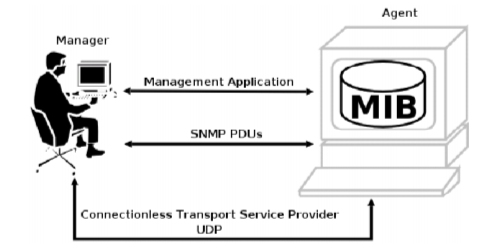
Information technology is increasingly developing, making technology a lot of help and facilitate work in various fields, including in the field of computer networks. With the availability of internet (interconnection network), the faster the exchange and delivery of information from one computer to another. the bigger and wider the network system, the more difficult it will be to organize and monitor it.  
  
 Number of Devices used in network infrastructure, it is necessary to have a good network management and monitoring system that is able to monitor the performance of the network, then a monitoring system designed to monitor the status of LAN / WAN infrastructure, ensuring that the device is normal and active, can see graphical statistics, checking signal conditions, can predict problems that will arise or can monitor data packets passing in network traffic. One popular protocol used for network management is the Simple Network Management Protocol (SNMP).

1. **SNMP**

SNMP is a popular protocol for network management. SNMP is used to collect information, and configure, network equipment, such as servers, printers, hubs, switches, and routers on Internet Protocol (IP) -based networks. SNMP can collect information such as CPU conditions, chassis temperature, and almost no limits on what SNMP can configure.

The SNMP protocol is designed to provide a "simple" method for centrally managing TCP / IP networks. If you want to manage equipment from a central computer, the SNMP protocol will facilitate the transfer of data from the client to the server side where data is centrally recorded, viewed and analyzed. SNMP consists of a set of network management standards, including application definitions in the application layer, database schema and a set of data objects. The main purpose of the SNMP protocol is only for one purpose, and is still used today, that is, to do remote management of equipment. SNMP is widely used to manage equipment on a computer network. SNMP refers to a set of standards for network management, including a protocol, a database structure specification, a set of data objects.  
SNMP was adopted as the standard for TCP / IP internet in 1989 and became very popular. Then an upgrade, known as SNMP version 2c (SNMPv2c) was adopted in 1993. SNMPv2c provides support for centralized and distributed network management strategies, and includes improvements in structure of management information (SMI), protocol operations, management architecture, and security.

SNMP uses User Datagram Protocol (UDP) and communicates through ports 161 and 162 based on a message exchange. And there are three types of messages in general:  
• Get: Allows management station to get the value of the MIB object from the agent.  
• Set: Allows the management station to set the value of the MIB object on the agent.  
• Trap: Allows the agent to notify management station of significant events.



**Image.1 SNMP**

## SNMP basic components

1. **SNMP Manager:**

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager’s key functions

* Queries agents
* Gets responses from agents
* Sets variables in agents
* Acknowledges asynchronous events from agents

1. **Managed Devices:**

A managed device or the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc...

1. **SNMP Agent:**

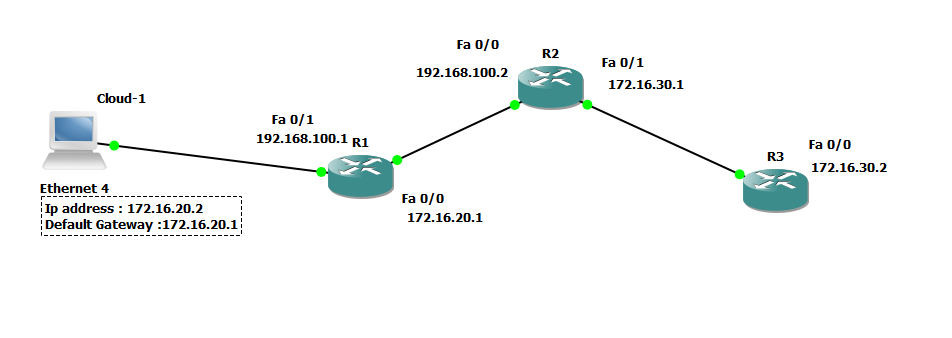
The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent’s key functions

* Collects management information about its local environment
* Stores and retrieves management information as defined in the MIB.
* Signals an event to the manager.
* Acts as a proxy for some non–SNMP manageable network node.

The following is the experimental topology using the GNS3 application. GNS3 is a GUI-based (Graphical User Interface) modeling software. This software can be said to be a combination of Cisco Tracer and Virtualbox Packages, but this software better describes the real conditions in configuring the router directly compared to Cisco Tracer Packages. GNS3 also allows complex network simulations, because it uses the original operating system from network devices such as Cisco and Juniper.

The working principle of GNS3 is to emulate Cisco IOS on your computer, so that your PC or Laptop can function like a router or even a switch, by activating functions from EthernetSwicth Card. GNS is an open source program, this program is free and can be used on several Operating Systems such as Windows, Linux, and MacOS X.



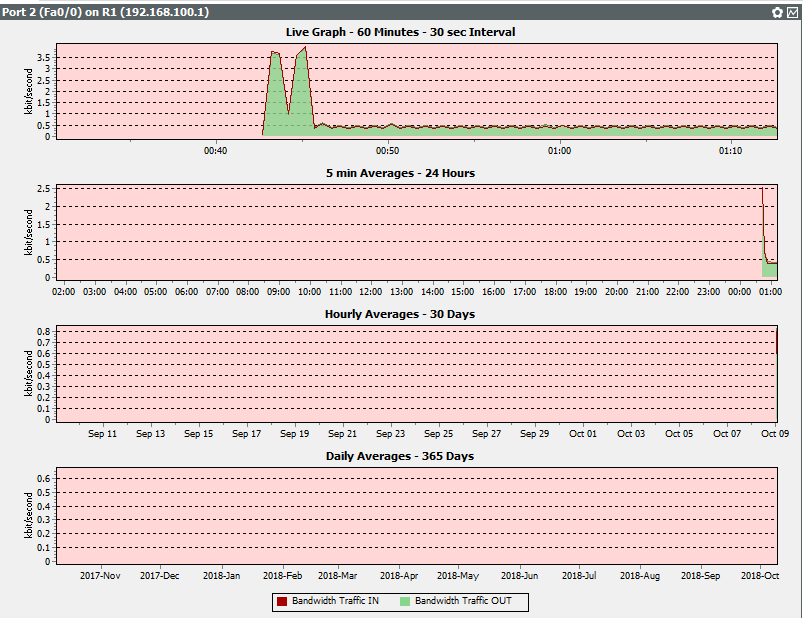
**Image 2.** Designed Network Topology

|  |  |
| --- | --- |
| **Device** | **IP Address** |
| Router(R1) | 192.168.100.1 |
| Router(R2) | 192.168.100.2 |
| Router(R3) | 172.16.30.2 |
| PC | 0 |

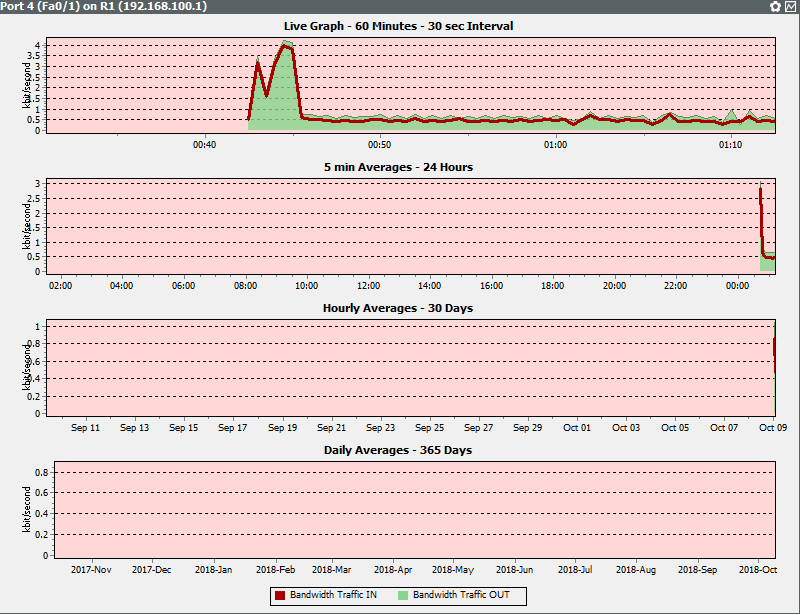
**Tabel 1**. Informasi Device

Here is the traffic from each device:

* **RI**
* **Port2**

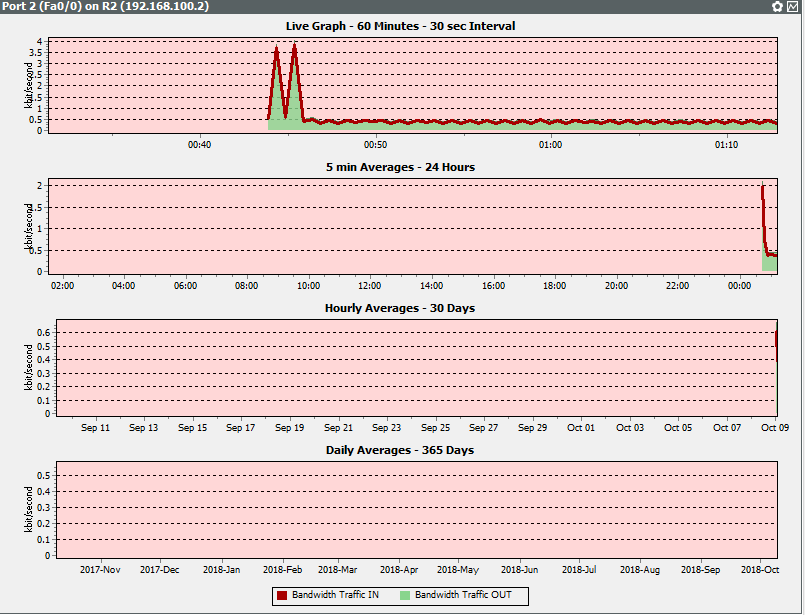
****

* **Port 4**

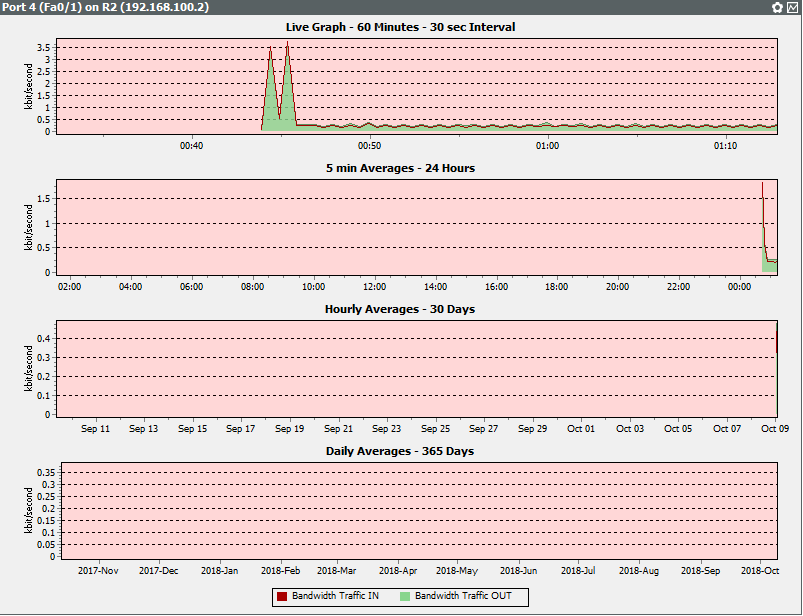
****

**Image 3.**Traffic R1

* **R2**
* **Port2**

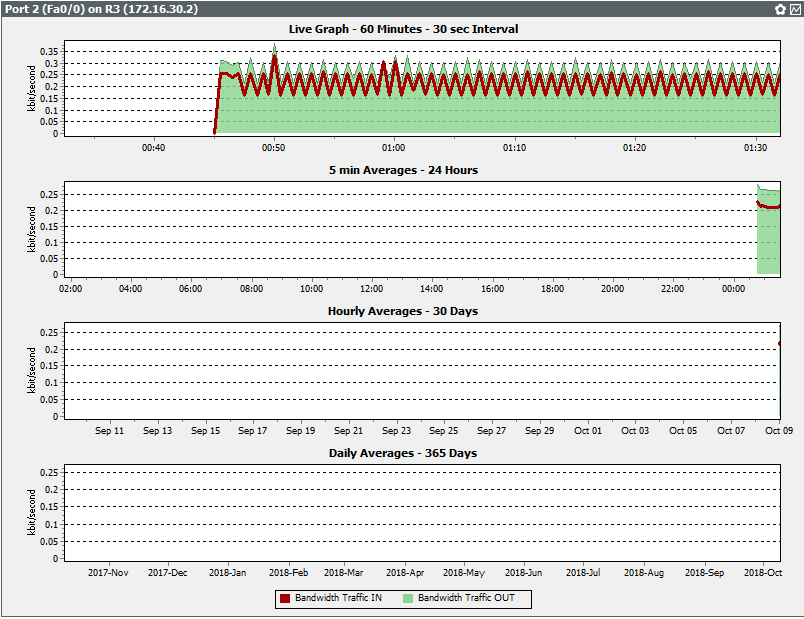
****

* **Port 4**

****

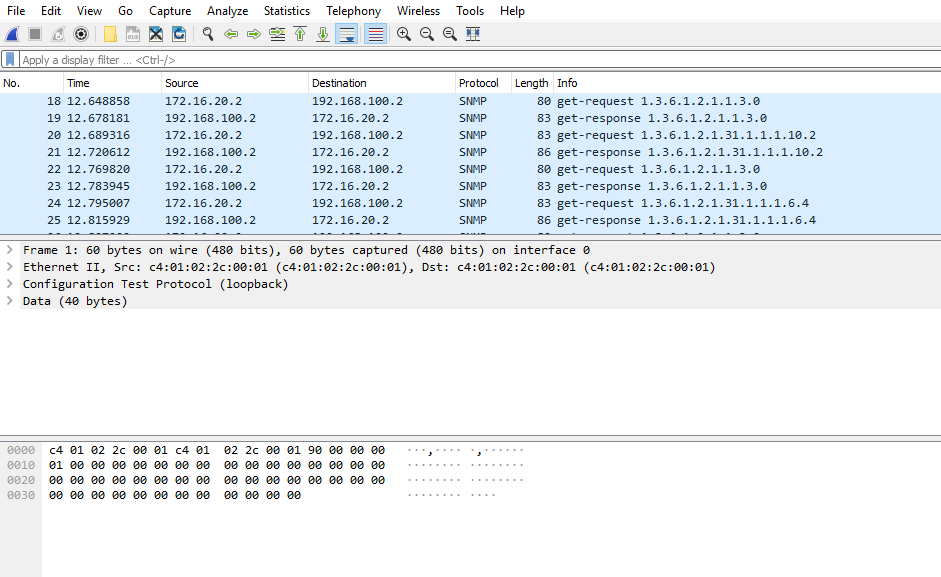
**Image 4.** Traffic R2

* **R3**
* **Port2**

****

**Image 5.** Traffic R3

After conducting an experiment, the SNMP capture results are obtained



**Image 6.**Hasil Capture Wireshark

Based on the image (so many), we can see in the INFO section that each SNMP message has a Protocol Data Unit (PDU). PDU is a data unit consisting of a header and some data that is pasted. SNMP PDU is used for  
communication between the SNMP manager and the SNMP Architecture SNMP agent defines the messages from the PDU as follows:

* 1. GetRequest

A manager-to-agent request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (the value field is not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

* 1. SetRequest

A manager-to-agent request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A *Response* with (current) new values for the variables is returned.

* 1. GetNextRequest

A manager-to-agent request to discover available variables and their values. Returns a *Response* with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

* 1. GetBulkRequest

A manager-to-agent request for multiple iterations of *GetNextRequest*. An optimized version of *GetNextRequest*. Returns a *Response* with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific *non-repeaters* and *max-repetitions* fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

* 1. Response

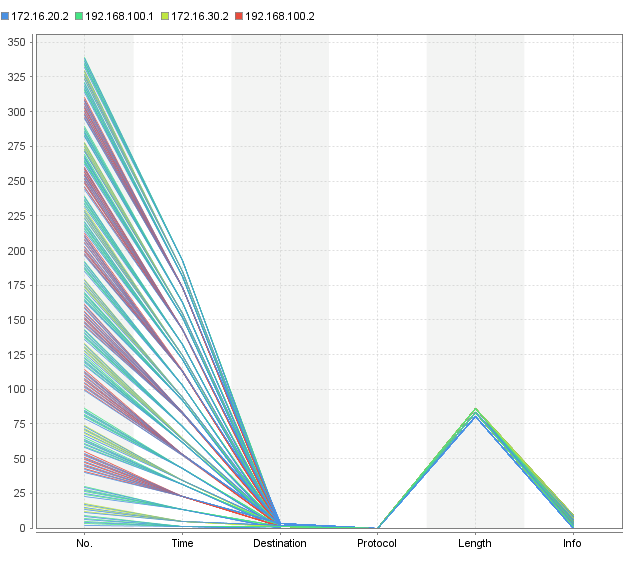
Returns variable bindings and acknowledgement from agent to manager for *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest* and *InformRequest*. Error reporting is provided by *error-status* and *error-index* fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.

* 1. Trap

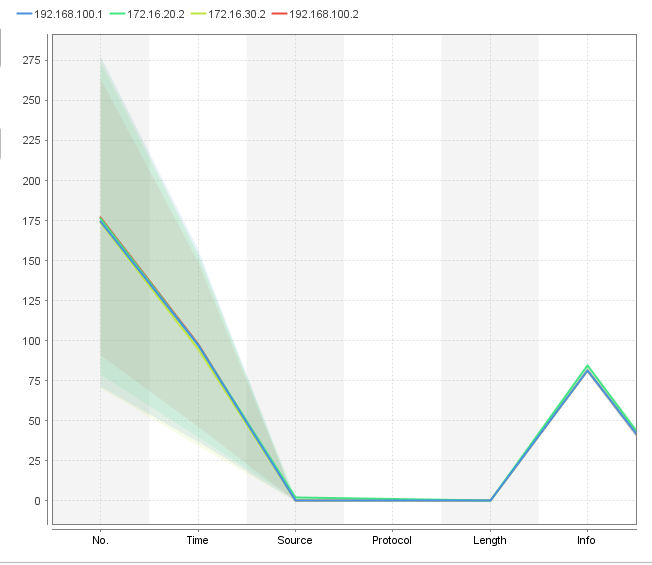
Asynchronous notification from agent to manager. While in other SNMP communication, the manager actively requests information from the agent, these are PDUs that are sent from the agent to the manager without being explicitly requested. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Trap PDUs include current *sysUpTime* value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed *SNMPv2-Trap*.

* 1. InformRequest

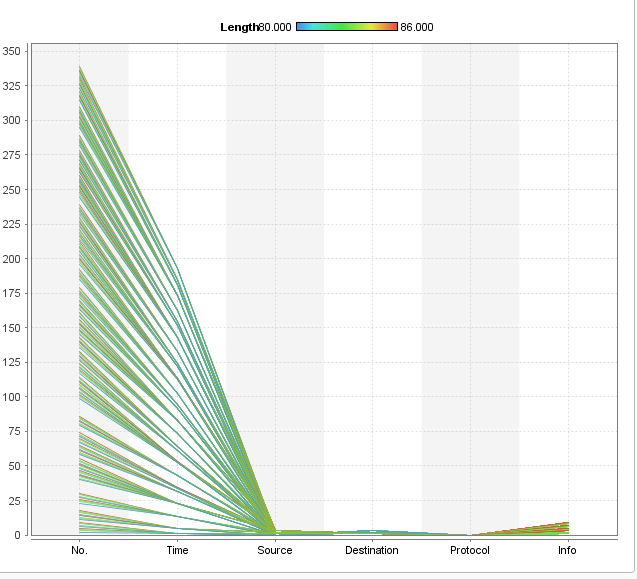
Acknowledged asynchronous notification. This PDU was introduced in SNMPv2 and was originally defined as *manager to manager* communication.Later implementations have loosened the original definition to allow *agent to manager* communications. Manager-to-manager notifications were already possible in SNMPv1 using a *Trap*, but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a *Trap* was not guaranteed. *InformRequest* fixes this as an acknowledgement is returned on receipt.



**Image 7.**Visualisasi Source pada SNMP



**Image 8**. Visualisasi Destination pada SNMP



**Image 9**.Visualisasi Info pada SNMP

**DAFTAR PUSTAKA**

1. wikipedia.org/wiki/Simple\_Network\_Management\_Protocol, diakses 6 Oktober 2108
2. www.manageengine.com/network-monitoring/what-is-snmp.html,diakses 6 Oktober 2018
3. http://www.cisco.com/en/US/docs/internetworking/technology/handbook /SNMP.html, diakses 7 Oktober 20018