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

# Muhammad Ajran Saputra (Computer Engineering UNSRI) AKHIAJRAN@STUDENTS.ILKOM.UNSRI.AC.ID

“Monitoring is a discipline” means devoting your focus as an IT professional to ensuring your network, servers, application and so on are all stable, healthy, and running at peak efficiency. It means not just being able to tell that a system has crashed, but more importantly to tell when a system will crash (predictable) and intervening so the crash is avoided.

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**

Ping send out a packet to the target device, which (if it’s up and running) sends an “I’m here” type response. The result of a ping tells you whether the device is responding at all (up) and how fast it responded (time).

1. **SNMP**

Simple Network Management Protocol (SNMP) has a few pieces that combine to provide a powerful monitoring solution. SNMP is comprised of a list of elements that return data on a particular device. It could be CPU or the average bits per second transmitted in the last five minutes. SNMP provides data based on either a Trap trigger (when one of the internal data points crosses a threshold) or an SNMP poll request.

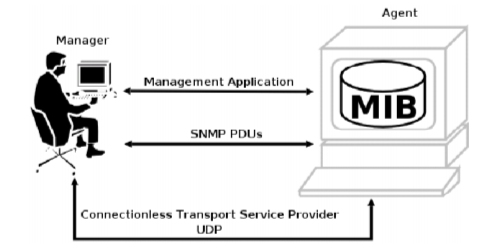
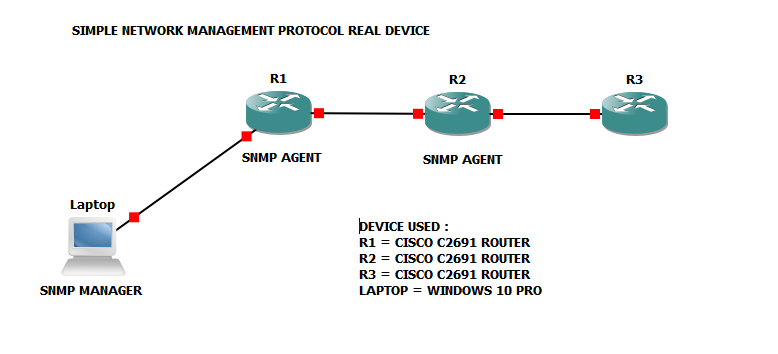


Image 1 . Structure SNMP[1]

1. **ICMP**

The internet Control Message Protocol (ICMP) is used by network devices like routers and switches to send error messages indicating that a host isn’t reachable along with some diagnostics.

Next, we will make a topology with GNS3, GNS3 (Graphical Network Simulator 3) is a software Build, Design and Test your network in a risk-free virtual environment and access the largest networking community to help. Whether you are studying for your first networking exam or building out a state-wide telecommunications network, GNS3 offers an easy way to design and build networks of any size without the need for hardware. And it allows combination of virtual and real devices, used to simulate complex networks. It used dynamips emulation software to simulate Cisco Routers IOS. [2]



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 we use windows 10 for monitoring that router.

For monitoring I use PRTG Network Monitor and The Dude. First we will try to The Dude application, after topology running well on gns3 and setup each router until connected with ospf we must discovery on the dude by discovery network until can reach all network that we built before. Don’t forget to test the router with sending a packet by a command ping destination packet 1000 send to target so that we can monitoring packet after sending with the dude

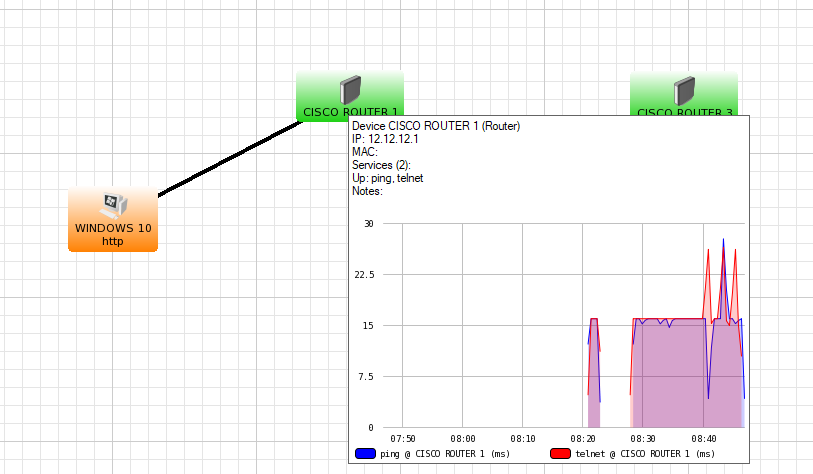
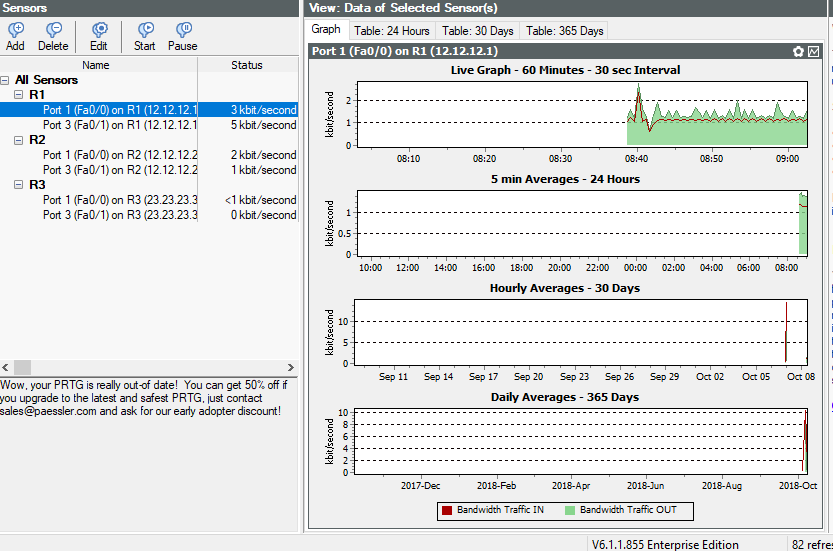


Image 2 . R1 monitor the dude

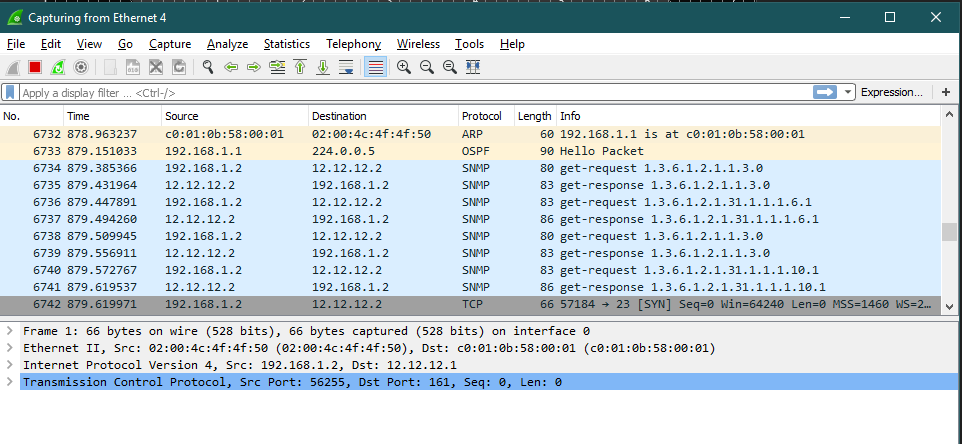
According image above, we can see packet sending before with ping at time I start monitored at 08:20 until now, still sending a packet and if I send bulk packet like a command ping *“ping 12.12.12.1 -l 10000”* it must graphic will be high continuously until stop sending packet.

We can started PRTG Network Monitor too and I assumed we already setup and install software, config and setting alarms if one of the routers have to down or crash. With PRTG Network Monitor, the routers identified as sensor in that application.

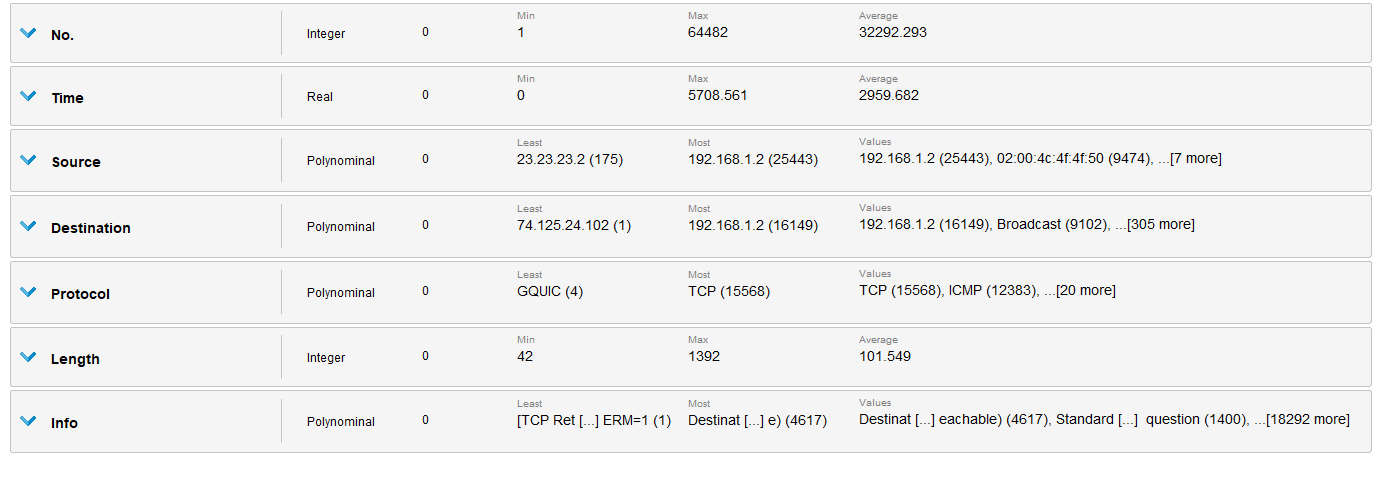
 Image 3. Routers 1 monitored

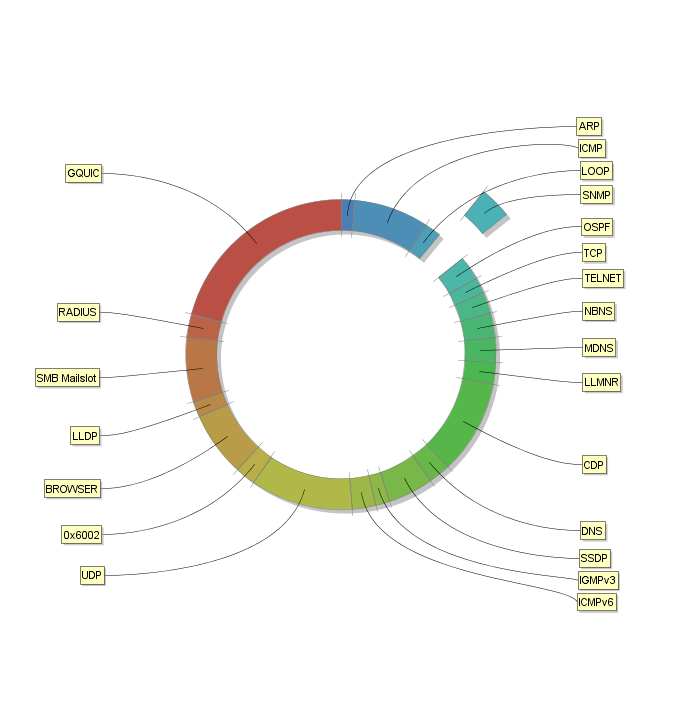
About router I monitored especially on routers 1, I start at 08:38 with idle communication until stopped monitored at 09:10. I choose idle communication for 2 minutes first time, to check how much traffic reach the high limit, so at 08:41 I send a bulk information with many ping on routers to give me information about threshold at routers 1. So the graph upstream and downstream will show at live graph about 1 hours first we start 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 4. Wireshark classification

After we captured the wireshark we can export to csv (excel file) for make a visualization to Orange Biolabs or Rapid Miner data science and then we put on plotting or schematics at visualization for a data from wireshark captured I can store at programs consist of Number Packet, Time , Source, Destination, Protocol, Length and Info

 image 5. Data category

 Image 6. Visualization

Conclusion visualization, with data that I have collected, I get 12667 from captured on wireshark at one shoot captured and make visualization at the picture above, I separate for SNMP only from length of average each packet up and down. SNMP from wireshark just get response and get request like a snmp manager and snmp agent at the routers and host. If snmp managers want to know about routers (monitored) snmp agent will get request from snmp managers, and otherwise will get response from snmp managers and how long length we snmp or agent gets? It’s according with packet sending, the big packet we sending, so make a more longer length at snmp so on visualization is a average from value length from all I captured from wireshark.