Classification of SNMP in Traffic Data Using Wireshark and Visualisation with ORANGE



Aditiya Muaffan

09011381520071

Sistem Komputer

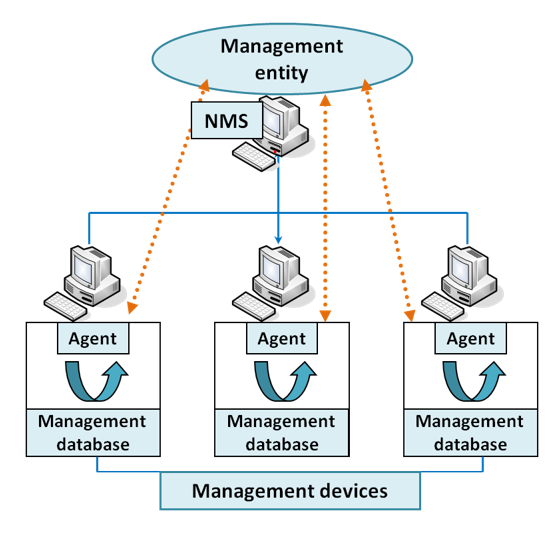
Fakultas Ilmu Komputer

Universitas Sriwijaya

**SNMP**

The Simple Network Management Protocol (SNMP) has become the de facto standard for network management. Because SNMP provides a simple solution, and only requires a little code.

Network management system with SNMP has two main entities: Manager and agent. Manager is a place where network administrators control network management functions. An agent is an entity that is attached to a device that is actually managed. Switch, Router or network server are examples of managed devices.

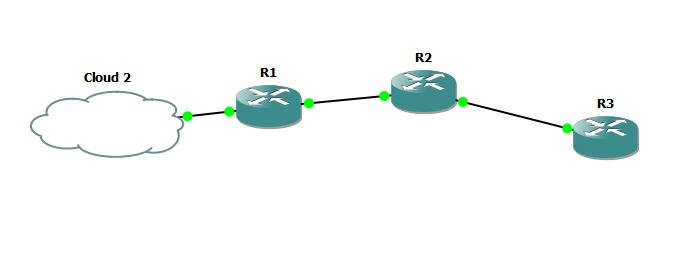


SNMP is based on the Manager / agent model. SNMP is referred to as "simple" because agents need very little software. Data processing and storage are in the System Manager, while the complementary parts of the functions are in the managed system.

The data exchanged in SNMP is a simple value such as a string that has a number called OID (Object Identifier). This OID is managed in a database in the agent and is usually called MIB (Management Information Base). Management databases / tables of objects are also not included in the SNMP protocol standard, but are separate standards. So SNMP is only a communication protocol to exchange information.

**Topology**

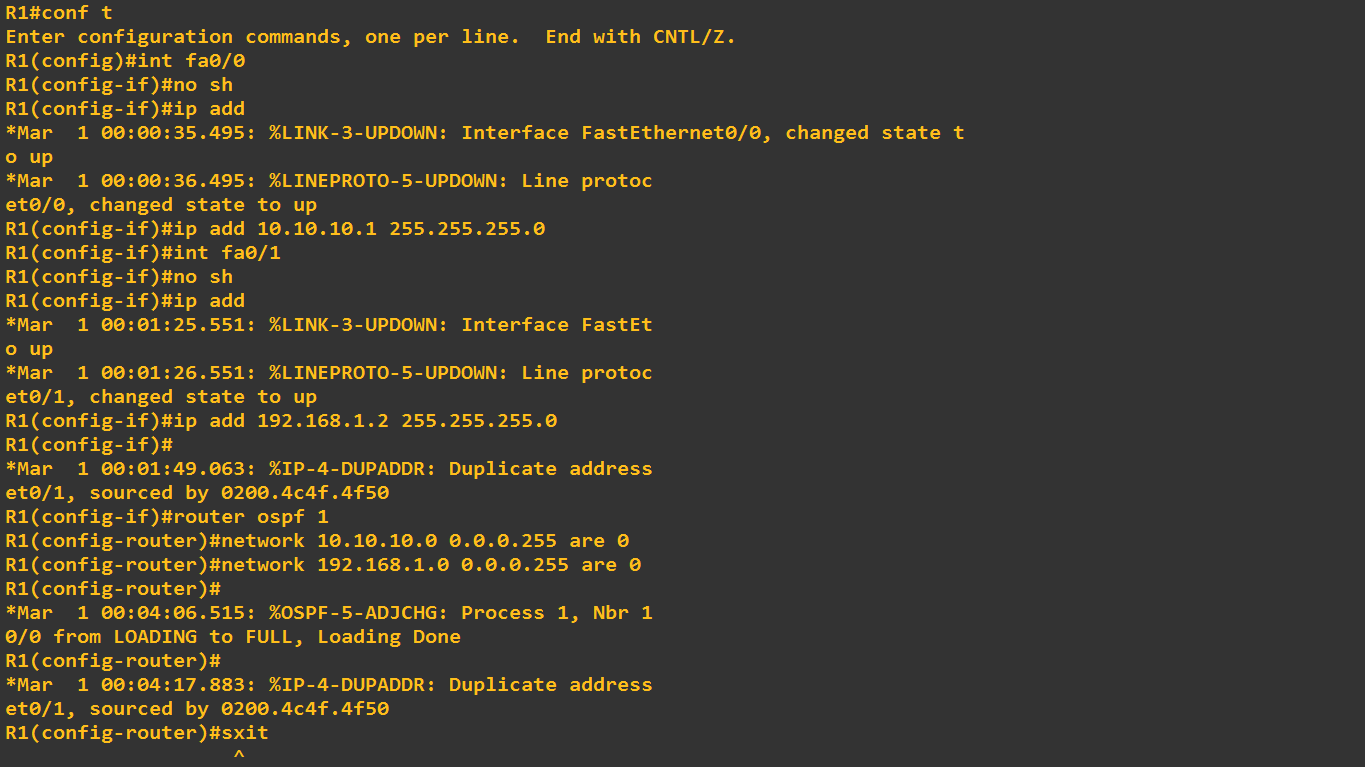
To make topology network, we use GNS3, GNS3 (Graphical Network Simulator 3) is a software Build, Design and Test your network in a risk-free virtual environment and access the largest networking community to help. Whether you are studying for your first networking exam or building out a state-wide telecommunications 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.

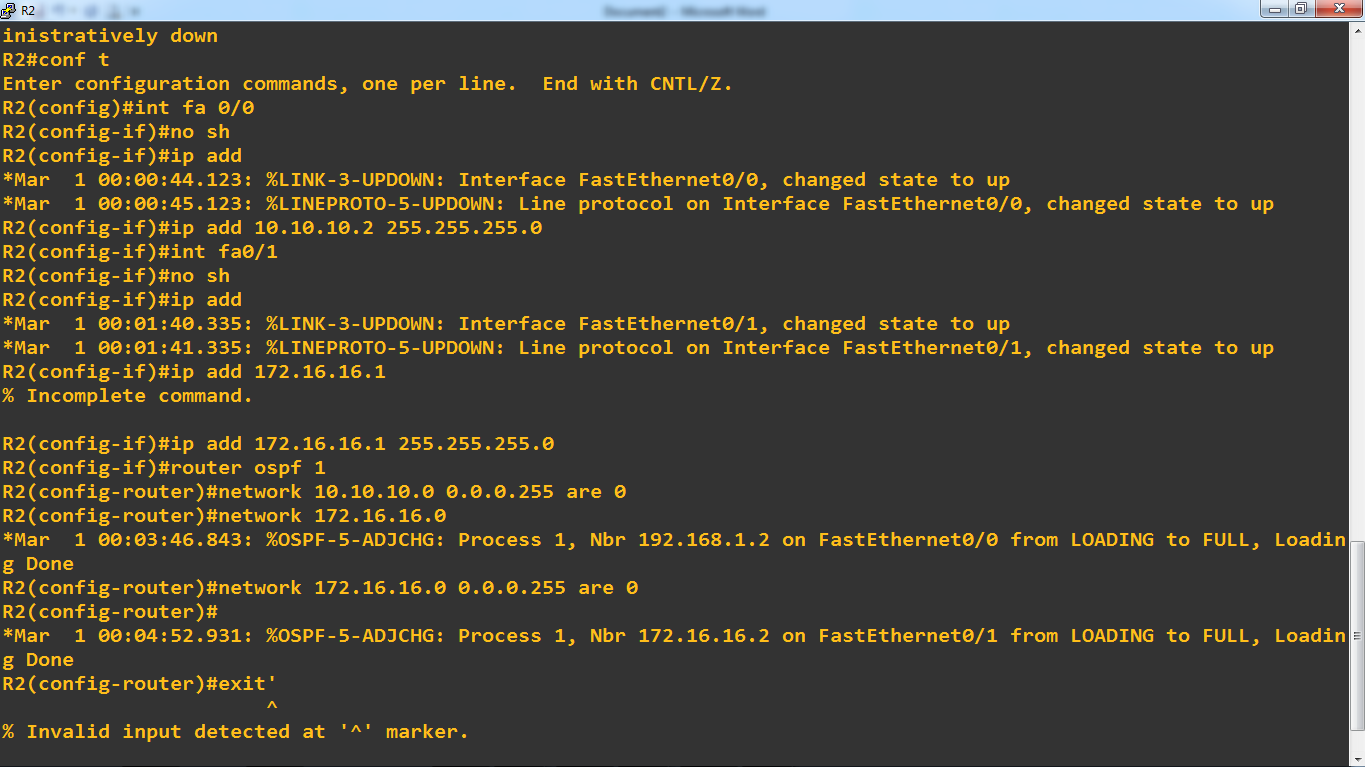


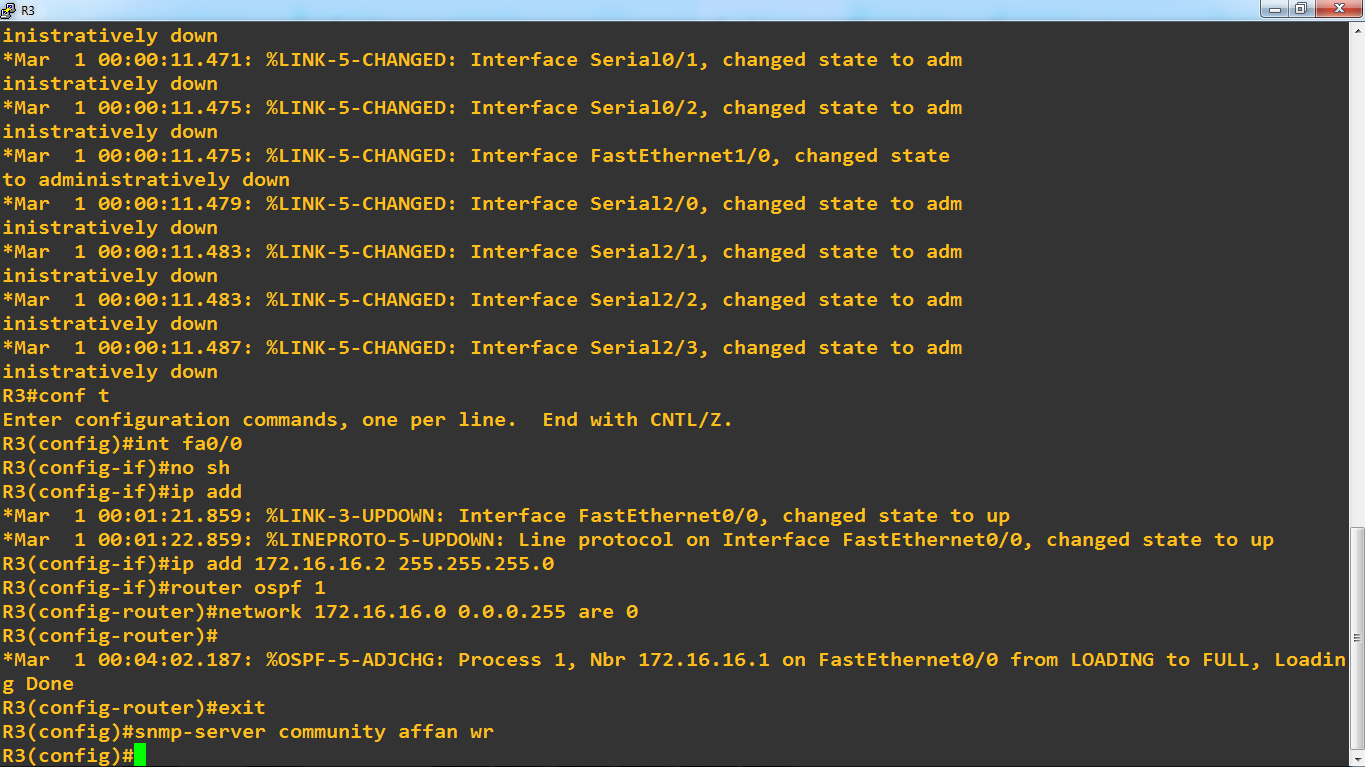
|  |  |  |
| --- | --- | --- |
| R1 | 10.10.10.1 | 255.255.255.0 |
| 192.168.1.2 | 255.255.255.0 |
| R2 | 10.10.10.2 | 255.255.255.0 |
| 172.16.16.1 | 255.255.255.0 |
| R3 | 172.16.16.2 | 255.255.255.0 |
| PC | 192.168.1.1 |  |
| Gate way | 192.168.1.2 |

* Cloud 2 (PC) as Manager
* R1, R2, R3 as Agent
* R = Router

Next, we configure every Routers

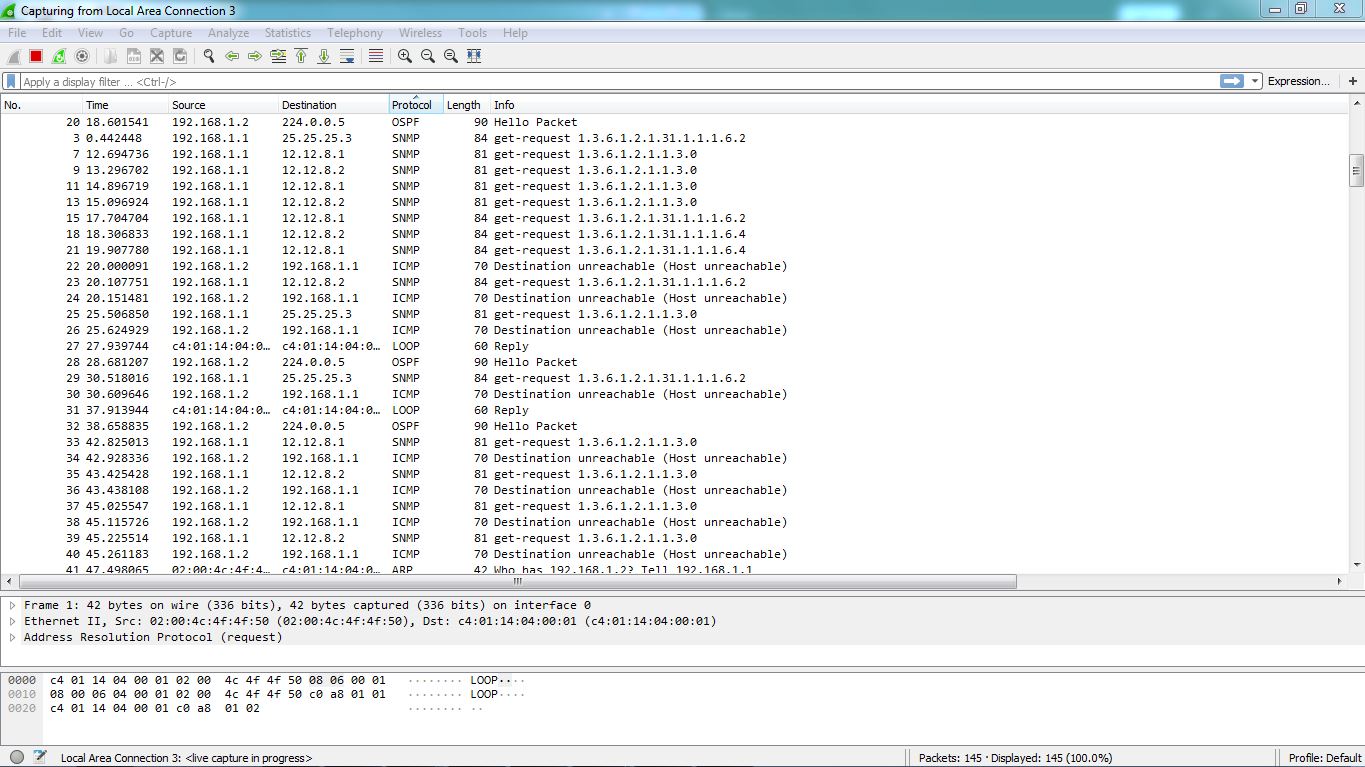




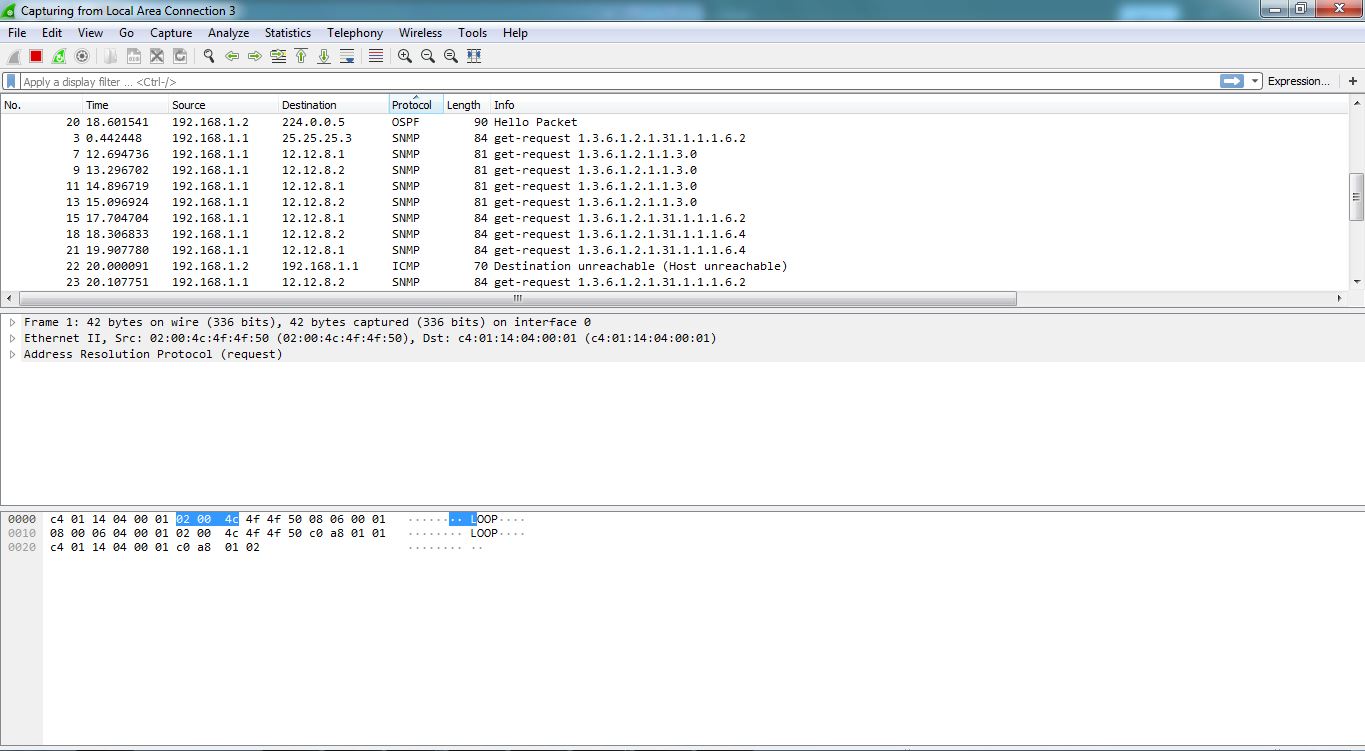


After creating the topology, we assume the topology work with *ping protocol* each other used OSPF to connecting between devices and don’t forget to use snmp-protocol command to each router. We used 3 with 2 router as snmp agent and 1 laptop as snmp manager, router from cisco C3745 we can download the firmware to embedded GNS3 from official website.

**Capturing**

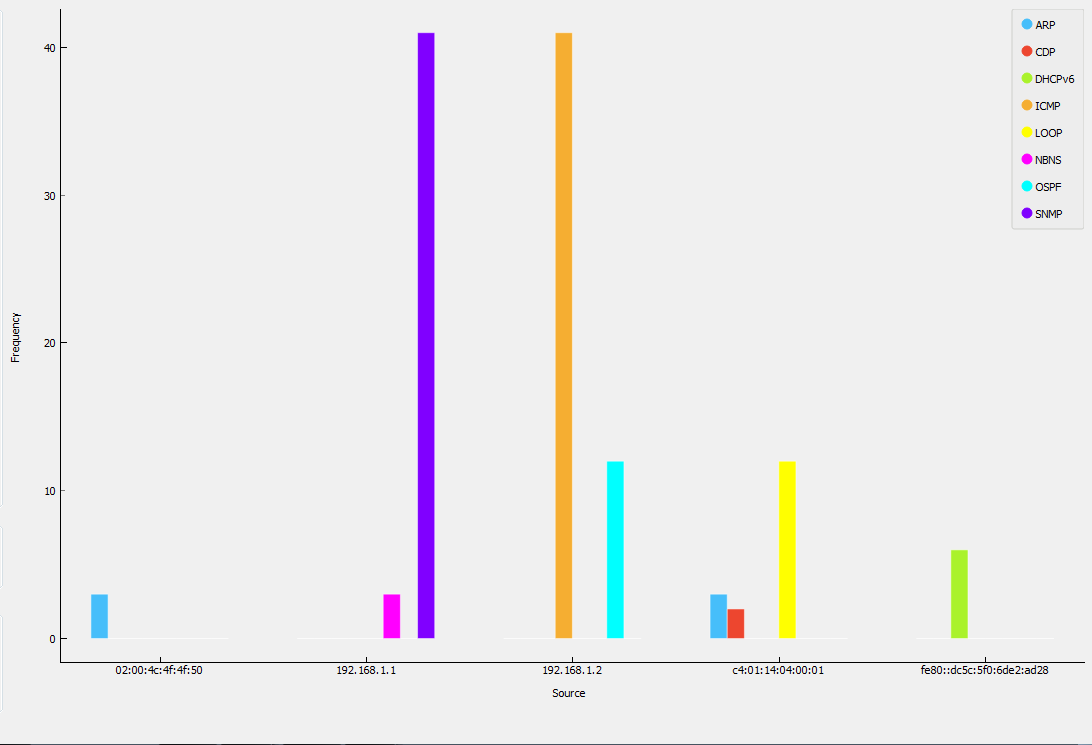
We already have network topology and it works well. then we will capture the data traffic in the topology, to do it we use WIRESHARK

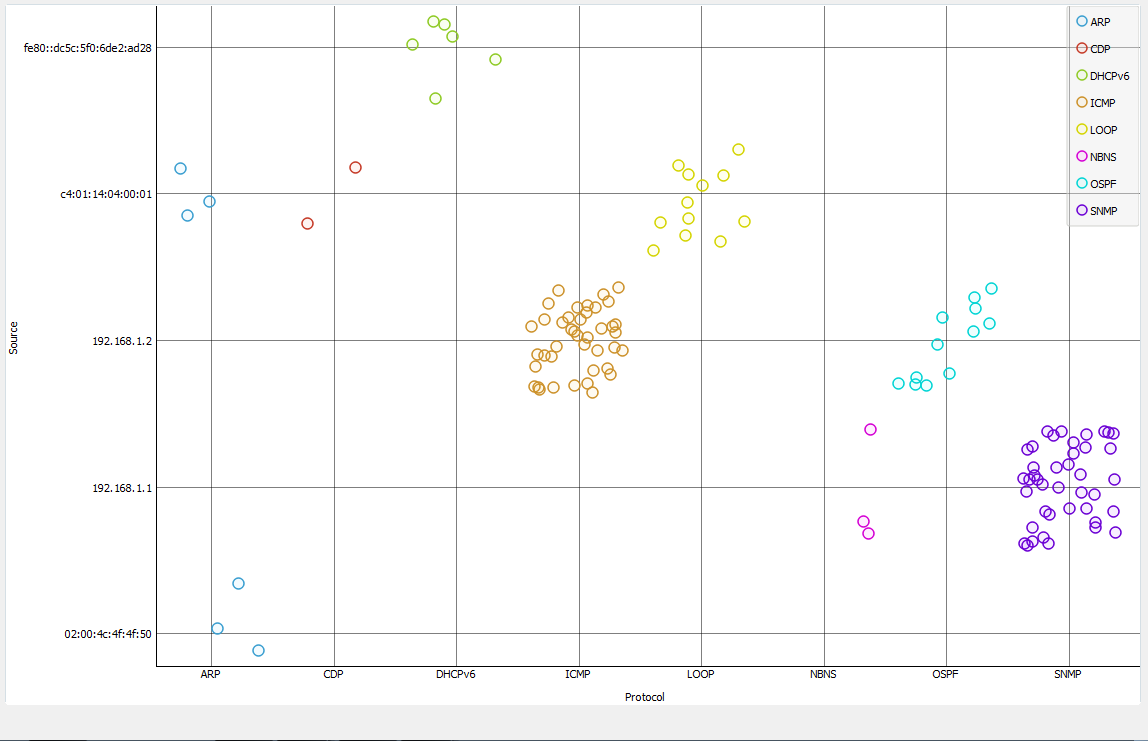
Wireshark captured at port ethernet we connected with routers and we can see the classification protocol that passed way at ethernet to router and so on upstream downstream, length, info , time and destination. In this task we will calcify the snmp protocol.



**Visualisation**

In Wireshark we can save the captured data by saving the format .csv (excel) to make visualitation with ORANGE.





Distribution and Scatter Plot type