INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Sniffer in a network

T. Prathyusha
prathyushatelaga@yahoo.in
School of Information Technology, Jawaharlal Nehru Technological University
Hyderabad, Telangana

ABSTRACT

A sniffer is a device used to read, monitor and capture network data exchange between networking devices. These are generally used by network administrators to monitor the incoming and outgoing traffic in the network. It acts like a web filter, firewall tester and troubleshoots client-server relationships. If the packets are not encrypted, it gives you a full view of data inside the packet (passwords, PINs and privacy information). When the network is slow, we need to know the bandwidth of the network and is being used by whom. Sniffer can monitor the performance by hop-by-hop network path analysis and can minimize the downtime. If there is high traffic in the network it might be an indication of a hacker in the network, it can highlight the unusual spikes in the traffic. Here two sniffers are placed in between two routers to monitor the outgoing and incoming ICMP packets in a network.

Keywords- *Sniffer, Sniffing, Packet Sniffing, Web filter, Traffic monitor, Firewall tester*

1. INTRODUCTION

A router routes the packets from source to destination using a routing table and using routing algorithms it finds the shortest path to reach its destination. Each interface of a router has a subnet connected to switch further to desktop. Two desktops can communicate with each other using switch within same subnet. Two desktop's belonging to two different subnets can communicate with each other using a router. A sniffer has two ports (incoming port and outgoing port). Incoming port of sniffer is used to monitor the incoming traffic or ICMP packet from networking devices. Outgoing port is used to monitor the outgoing traffic or ICMP packet.

2. INITIAL ASSUMPTIONS

Network can be hacked in many ways. It may be due to weak passwords, misconfigured network devices, misconfigured internet. The packet is not encrypted and is sent from one subnet to another subnet. The sniffer plays an important role in monitoring the incoming and outgoing traffic from networking devices. Since the packet is not encrypted the sniffer can read the source mac address and destination mac address of packet and even the privacy information of the packet.

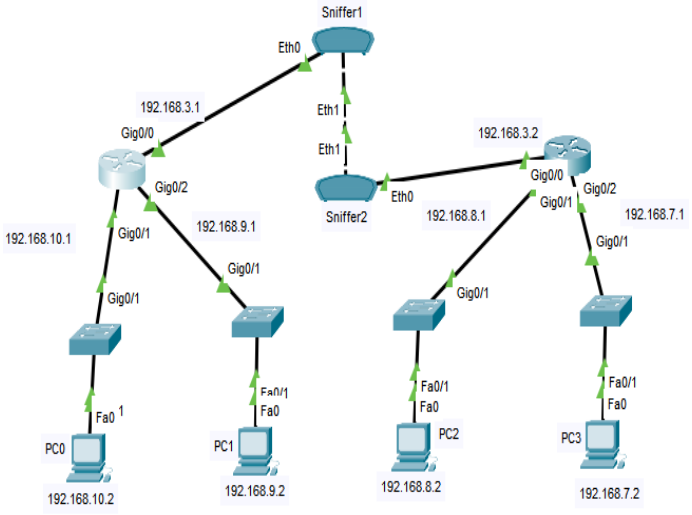


Fig. 1: Block diagram

3. EXPLANATION

A network is a collection of personal computers, switches, routers, hubs and other devices that are connected via cables to communicate with each other. Networks carry data in many locations like home, company. It consists of Ethernet network, it may be fast Ethernet, gigabit Ethernet and it is implemented in twisted pair copper cables, multi-mode fiber optic cables or some form of wireless technology. Security in networks is the biggest concern of any network administrator. The security of network lies in controlling the traffic of the network. The extent to which the administrator can control the traffic ultimately determines the security of the network. Network traffic to and from the internet, network traffic to and from the machines on the network, the behavior of each application and the network traffic generated by each application on each computer on the network, the users who can use each application. Any network that can fulfil these four points will be secure from all internal and external threats.

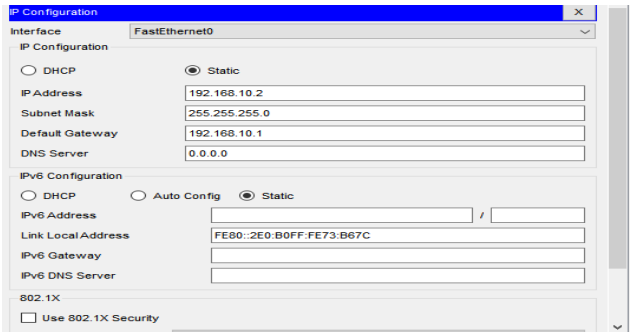
4. WORKING

The entire design explains the functionality of sniffer in a network. Here we have routers, switches and desktops

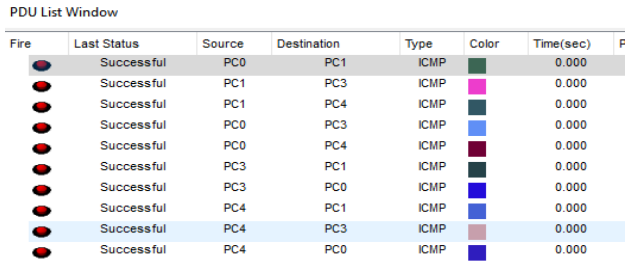
connected to each other. One interface of the router(R1) is connected to one switch and a desktop(PC0). The other interface is connected to another switch and a desktop(PC1). The PDU packets can be sent and received by PC0 and PC1 internally through router(R1). Similarly, router(R2) is connected to two switches and desktops PC2 and PC3 respectively. The Routers R1 and R2 are connected to each other. Now the PDU packets can be sent and received by all the desktops within the network. A Sniffer 1 is a device which is connected to a router R1 to sniff the incoming traffic and sniffer 2 is connected to router R2 to sniff the incoming traffic. These two sniffers and connected to each other to view the traffic from both the routers. ICMP packet stores the source MAC address and destination MAC address. The packets are not encrypted so even the information inside the packet can also be viewed.

5. IMPLEMENTATION

This block diagram implementation is done using a tool cisco packet tracer 7.3.0. the devices are configured using cables end-on-end.

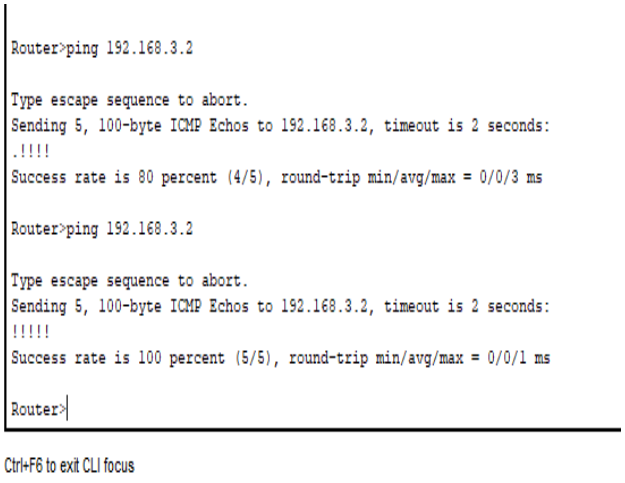


IP address of desktops and routers are configured.
ICMP packet successful ratio between the desktop's is as follows.

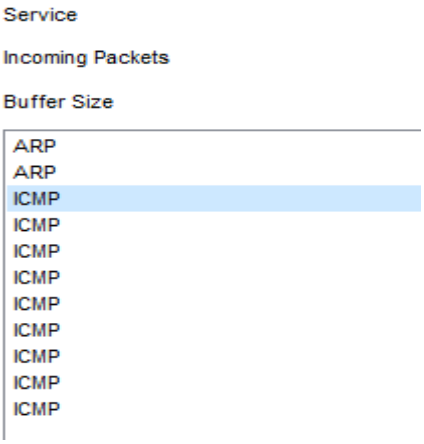


Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC0	PC1	ICMP		0.000
	Successful	PC1	PC3	ICMP		0.000
	Successful	PC1	PC4	ICMP		0.000
	Successful	PC0	PC3	ICMP		0.000
	Successful	PC0	PC4	ICMP		0.000
	Successful	PC3	PC1	ICMP		0.000
	Successful	PC3	PC0	ICMP		0.000
	Successful	PC4	PC1	ICMP		0.000
	Successful	PC4	PC3	ICMP		0.000
	Successful	PC4	PC0	ICMP		0.000

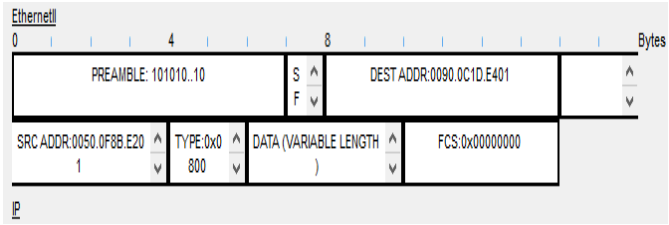
Sniffer is connected to the Router and incoming packets are sniffed.
Traffic from Router1 is as follows:



This PDUs are received by the sniffer1 is as follows:



ICMP packet contains the source MAC address, Destination MAC address and the data part. If the data is not encrypted it can also be easily viewed with the help of sniffer.



6. CONCLUSION

The Sniffer is used to monitor the traffic and read the PDU sent and received by the routers in the network. Two sniffers and placed so as to monitor the incoming and outgoing PDUs of both the routers in the network.

7. REFERENCES

[1] Priscilla Oppenheimer. Top-Down Network Design.
[2] Etutorials. Flat Network Topology URL: http: //etutorials.org/Networking.
[3] Understanding Network models from webpronews.
[4] Cisco.Network Topology. URL: http:// ns/books /ciscopress/samples.
[5] CCNP1: Advanced Routing.
[6] CCNA Exploration LAN Switching and Wireless.
[7] CCNP Security.
[8] John E. Canavan. Fundamentals of Network Security.
[9] R. Shirey, editor. Internet Security.
[10] Gregory B. White, w. Pooch. Computer System and Network Security.
[11] Randy Marchany. Computer and network security in Higher Education.
[12] Packet sniffer. Dnsstuff.com.

