HUB Vs SWITCH

AIM: To use traffic generator and Ethernet hub to observe the effect of collision on throughput and its impact on file transfer.

COMPONENTS REQUIRED:

Components	**Quantities**
PC	2
Laptop	1
Switch	1
Hub	1
Access Points	1

NETWORK DIAGRAM:

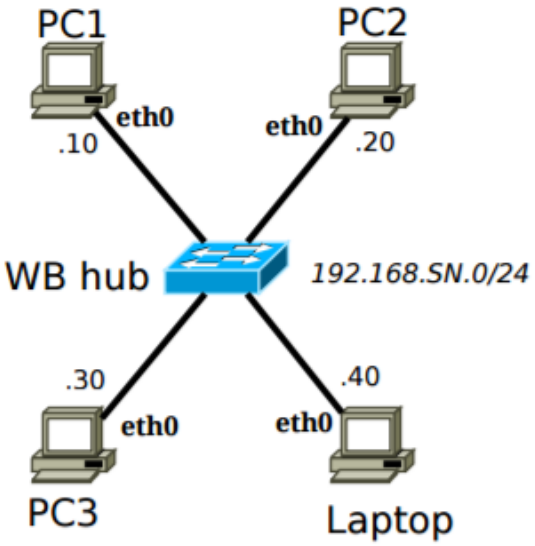


Fig 1*: IPTraf interface monitor screen*

EXPERIMENT:

A simple HUB is used to connect the workbench computers and then corresponding IP address is assigned to each computer after which packet transmission is verified using PING command that helps to verify the IP level connectivity between devices.

For the connections from Workbench 2:

PC1 to HUB to the eth0 port uses the slot PC112 in the patch panel.

PC2 to HUB to the eth0 port uses the slot PC212 in the patch panel.

PC3 to HUB to the eth0 port uses the slot PC312 in the patch panel.

Laptop to HUB to the eth0 port uses the slot LA412 in the patch panel.

IP addresses configured for the connection:

PC1: 192.168.12.10

PC2: 192.168.12.20

PC3:192.168.12.30

Laptop: 192.168.12.40

Hub: 192.168.12.0/24

Since a HUB is a physical layer device data can be transmitted between each device and the devices communicate with each other. The PING traffic is generated between PC1 and PC2 and the same is monitored from PC3 using Wireshark the results and observations of the experiment are reported.

GENERAL THEORY:

HUB Vs SWITCH

A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hubs and switches serve as a central connection for all network equipment and handles a data type known as frames. Frames carry your data. When a frame is received, it is amplified and then transmitted on to the port of the destination PC.

In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times.

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

The ability to route packages to designated end locations is one of the key advantages to using network switches. This is a great leap forward from hubs, which are only able to send packages without specification from one device to all other devices attached to their network.

RESULTS AND OBSERVATION:

1. **PING between the computers**
   Command: **ping 192.168.12.20** **%** from PC1 (192.168.12.10)
   sudo wireshark **%** to run Wireshark in PC3

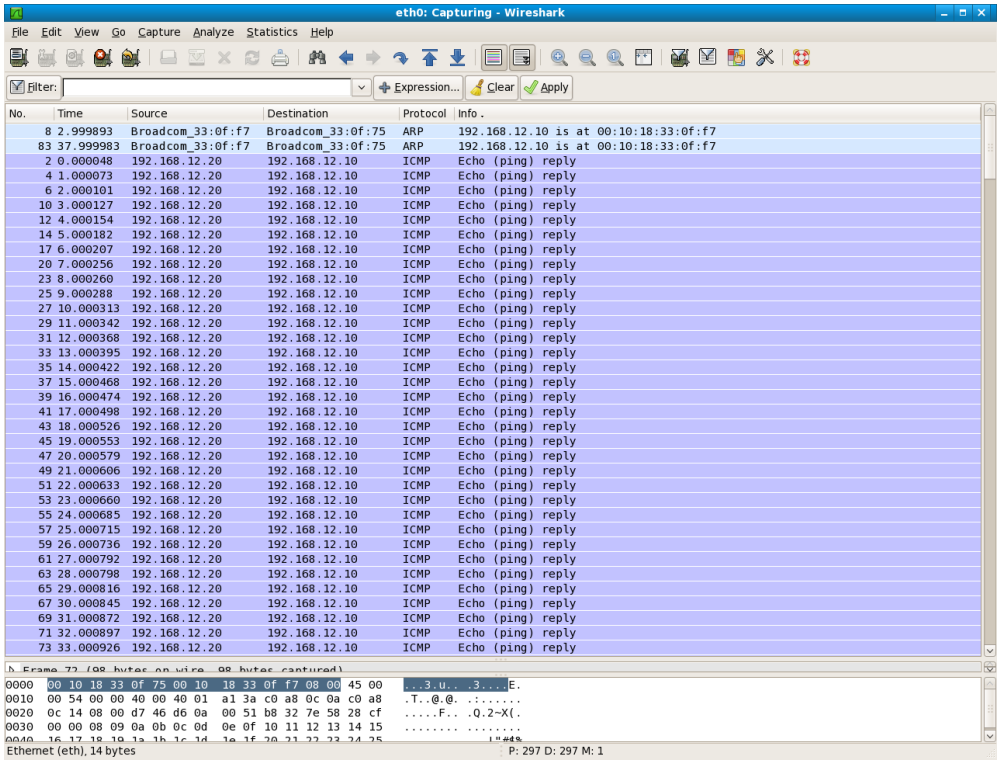


Fig 2: *Wireshark Capture from PC3*

2. ICMP PACKET STRUCTURE

After the Wireshark capture of the data the captured packets are analyzed for Ethernet header, IP header and ICMP header

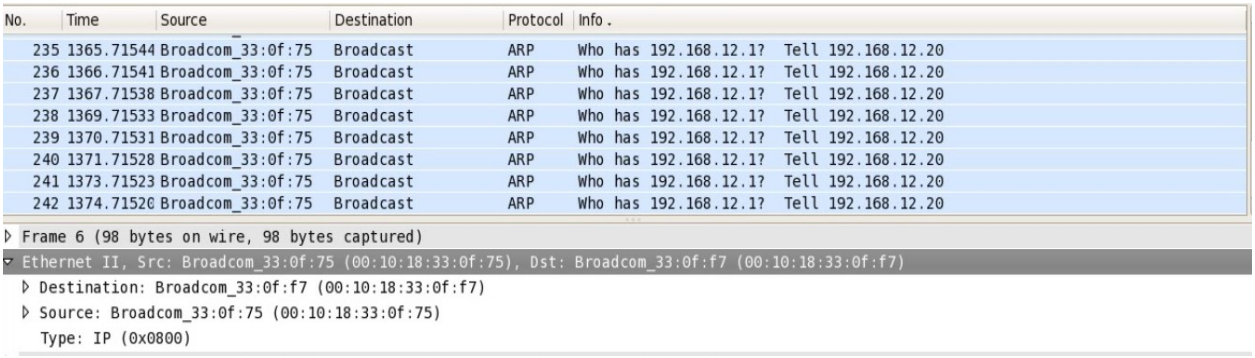


Fig 3: *Ethernet packet header*

The frame length is 98 Bytes “on the wire” which means another PC on a hub as a monitor port.

The total Bytes on the wire is 98 which is (14 bytes Ethernet header, 20 bytes IP header, 8 bytes ICMP header, 56-byte payload, equals 98. Generally, the FCS is removed from all frames.

ICMP echo request and echo reply:

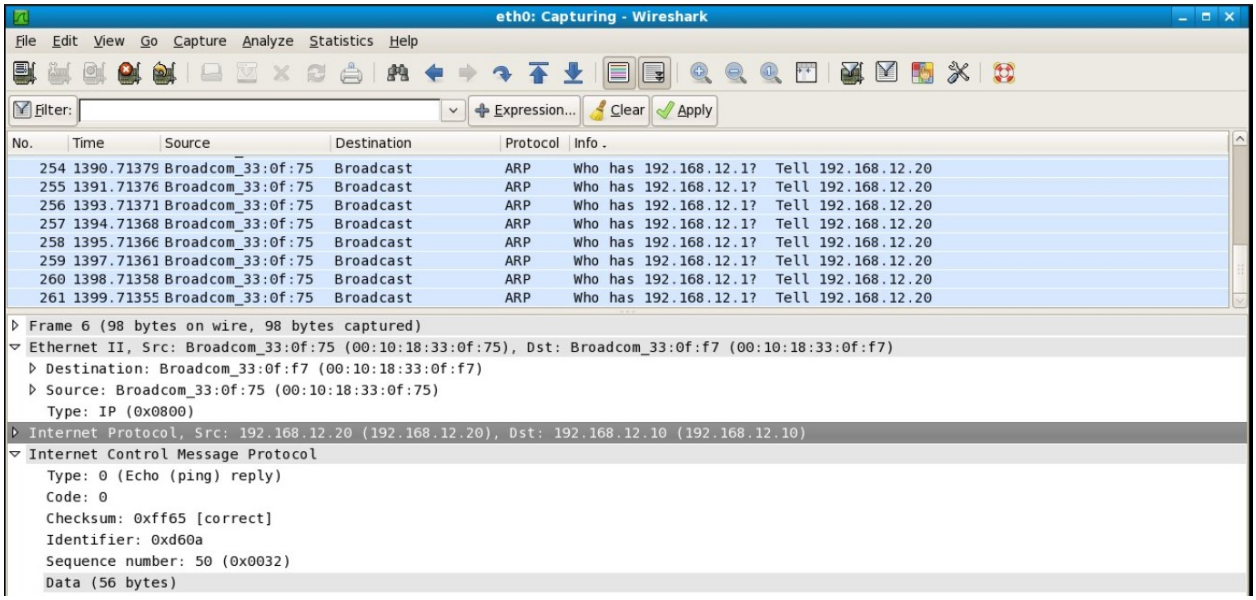


Fig 4: *ICMP Echo reply*

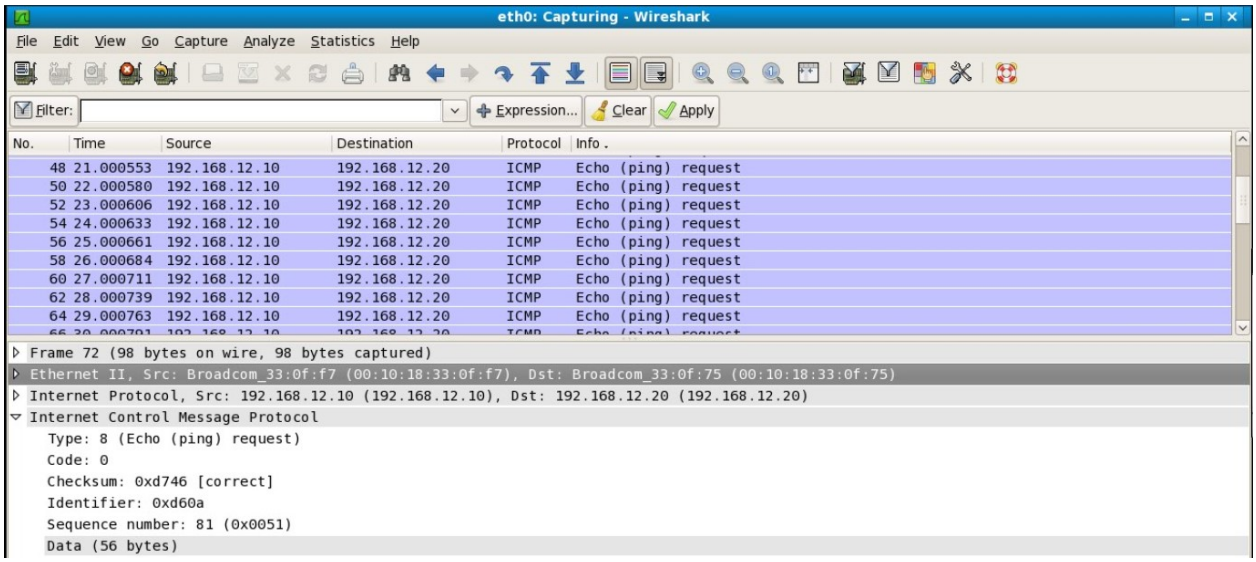


Fig 5: *ICMP Echo request*

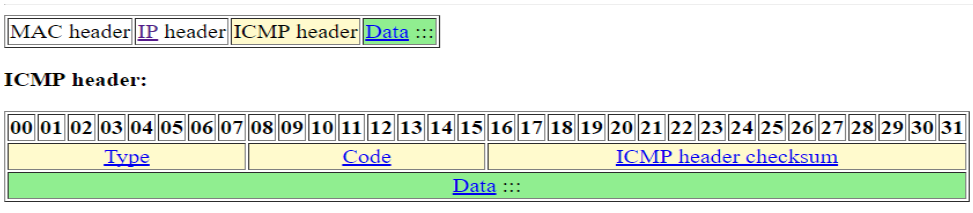


Fig 6: General *ICMP header*

ICMP messages are sent in several situations:

for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be reliable.

The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

OBSERVATION:

The data received in the echo request message must be returned in the echo reply message.

TYPE: 8 bits. Specifies the format of the ICMP message.

Type 0 denotes that it is an Echo reply

Type 8 denotes that it is an Echo request

CODE: 8 bits. Further qualifies the ICMP message.

Code 0 may be received from a gateway or a host.

The **echo sender** may use the **identifier and sequence number** to aid in matching the replies with the echo requests.

the sequence number might be incremented on each echo request sent. (Here corresponding packets are not expanded)

3. FILE TRANSFER AND SPEED OF THE LINK:

Command: **sudo ethtool eth0** %view the interface

sudo ethtool -s eth0 autoneg off %to turn off autoneg

sudo ethtool autoneg off speed 10 %to set the speed manually

scp /var/labs/lab02/large.file team12@192.168.11.20 :/tmp/test1 .mpg %large file transfer

sudo hping -n –udp -k -p 3000 -i u2000 -d 1222 -I eth0 192.168.12.40 %UDP traffic with rate 5 Mbps

sudo iptables -A INPUT -p udp –dport 3000 j DROP %to drop UDP packets coming to port 3000

The speed of the file transfer between two PCs is monitored when there is an ongoing packet transfer between other two PCs. When all these PCs are connected to a hub.

The speed of the link is set as 10 Mbps and the corresponding LED lights in the hub are observed to monitor the change in the speed

File transfer is initiated from PC1 to PC2 and the status of file transfer is observed. The transfer rate is observed.

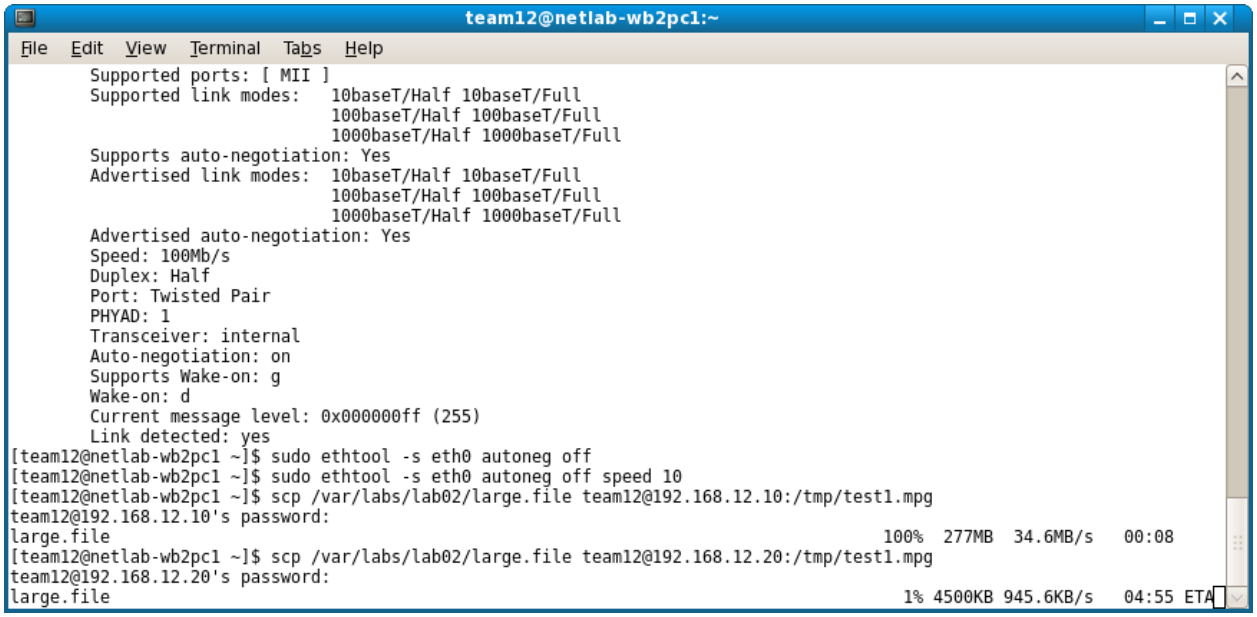


Fig 7 *Transfer Rate*

Proceeding with this an UDP traffic is generated between PC3 and Laptop. The UDP packet increases the load in the network thereby reducing the file transfer rate, The UDP port 3000 in the Laptop is then configured such that the incoming UDP traffic is dropped and making the hub unloaded of the hping traffic.

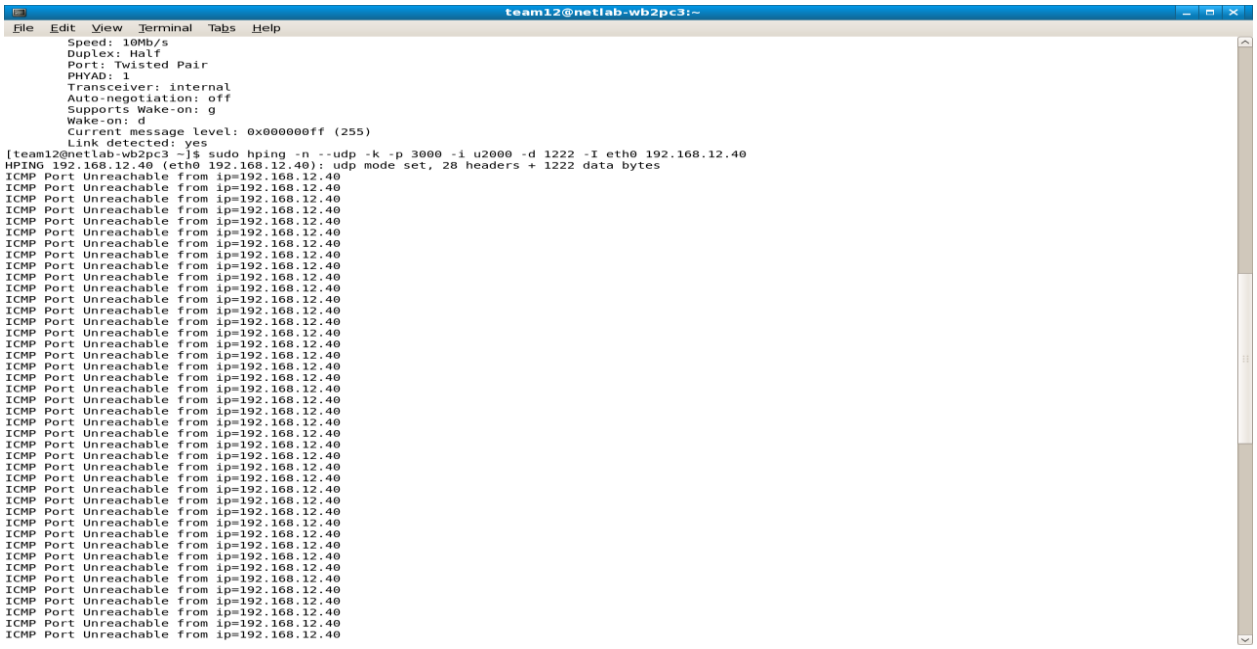


Fig *8 ICMP port unreachable message from PC3*

IPtraf application is started in the PC3 in the monitor mode and the UDP port is monitored the traffic rate is observed and it is seen that the rate is 4.6 Mbps since there is no UDP flooding the spped is almost same.

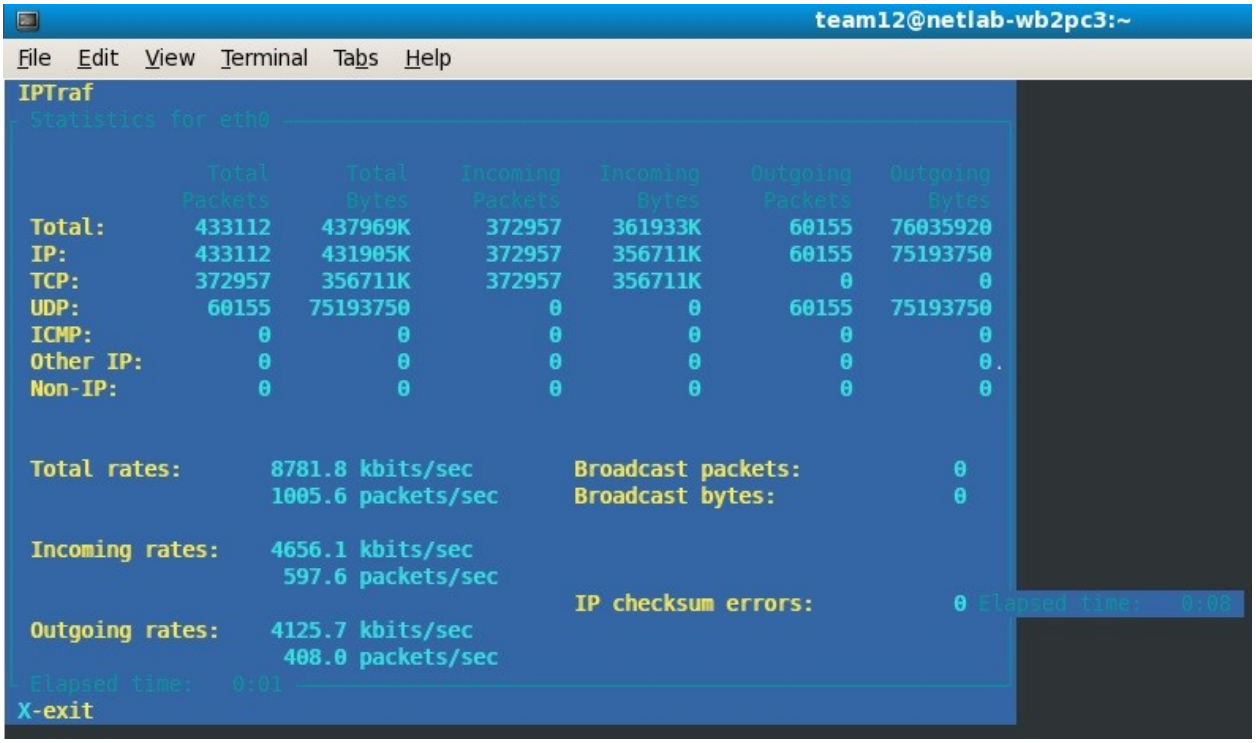


Fig 9 *UDP and file transfer rate monitored*

The file transfer process is repeated and the transfer rate is observed for the switch and it is seen that the rate of transfer in switch is greater than that of the hub.

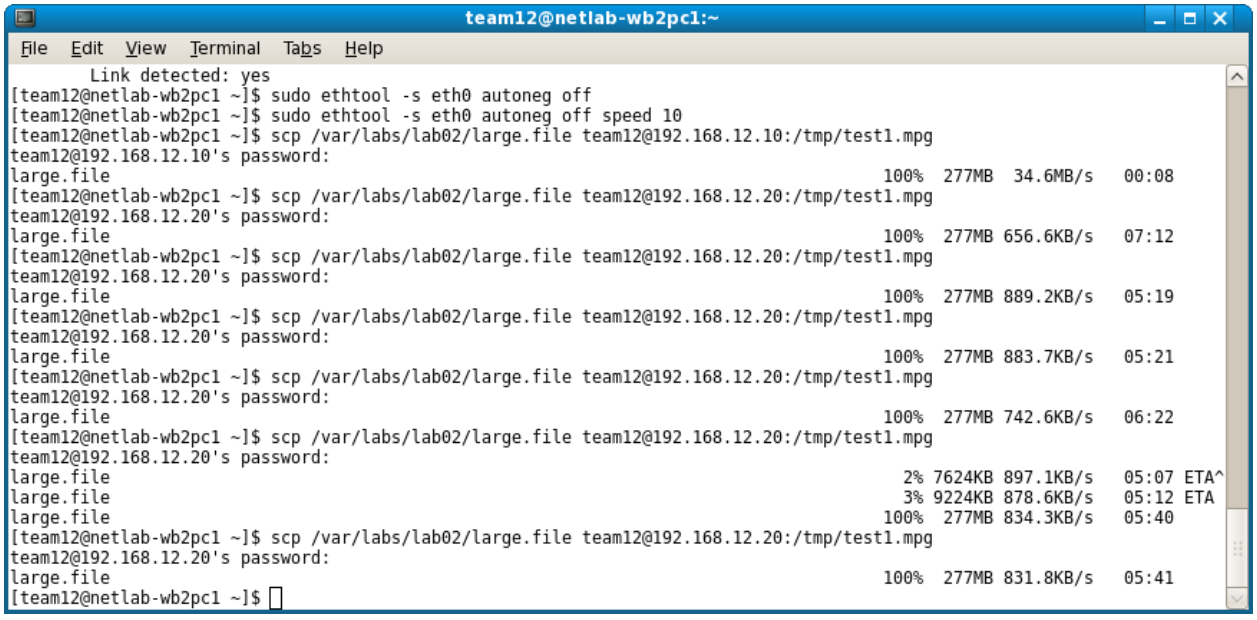


Fig 10 File transfer rate with switch

Wireless – BSS

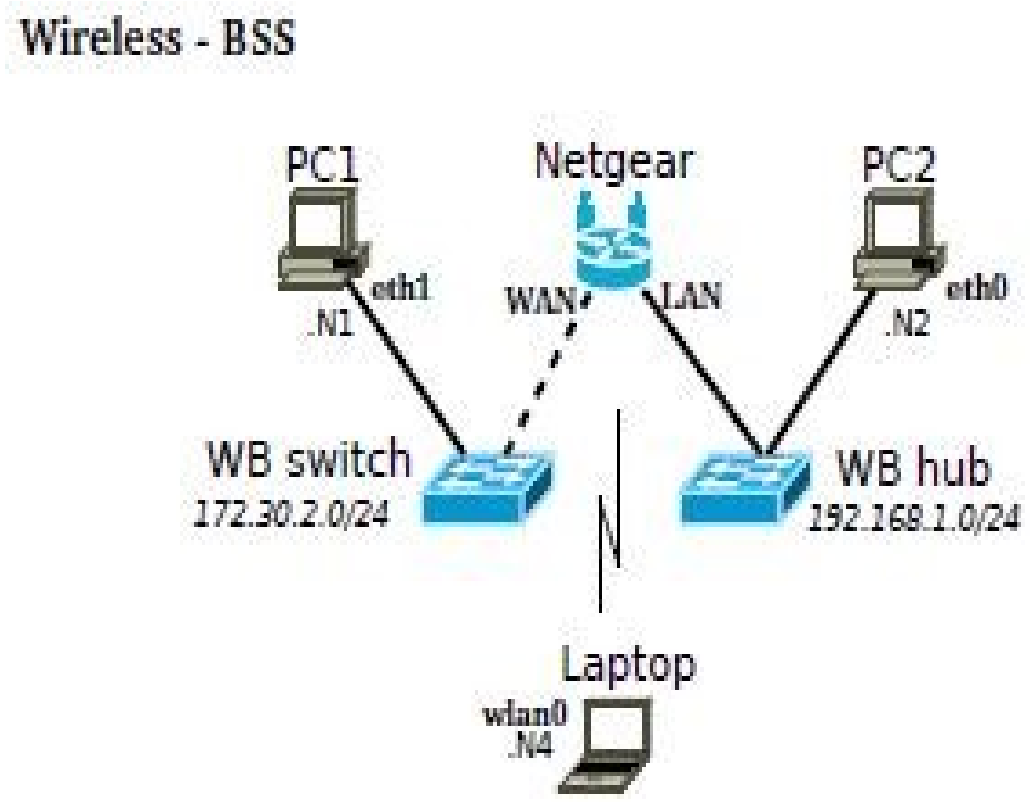
Aim:

To implement a Basic Service Set which consists of two Pc's, laptop, a switch, a hub and Access Point (AP). The AP functions as a bridge. The AP is configured using the WAN ports.

Components Used:

Components	Quantities
PC	2
Laptop	1
Switch	1
Hub	1
Access Points	1

Network diagram:



Setup:

Here we assume that Workbench 2 is used for the entire experiment.
For PC1, eth1 interface is used and the IP address is 172.30.2.21/24
For PC2, eth0 interface is used and the IP address is 172.30.2.22/24
For laptop, wlan0 is used and the IP address is 172.30.2.24/24
One access point is connected with switch using WAN and with hub using LAN
The default gateway is 172.30.2.1 for switch & 192.168.1.1 for hub.

Process:

Command:

sudo /etc/init.d/network restart . **%**The default mode is set using the following command,

Then the Ethernet interfaces are made to run at 100Mbps. Then PC1, is opened and the URL http://172.30.2.27:8080 is connected. The username is entered as **admin** and the password is **password.** Then under, Setup Wireless Setting is chosen and the SSID is **netlabwb12**. The Mode is selected as Up to 54Mbps and the Security Options is chosen as none. Since we are using workbench 2 , the channel we must consider here is 6. After this, we move to the Laptop. Make sure that wireless interface switch is in ON position. Then type the following commands in the terminal,

- **sudo ifconfig wlan0 up** %activate wireless interface
- **iwconfig wlan0 essid <netlabwbSN> mode Managed channel <channel> ap <MAC-address>** %configure wireless interface
- **sudo ifconfig wlan 192.168.1.24/24** %set IP address for wireless interface

Then, a file transfer is done from laptop to PC2 using **scp** command and the data rate is observed as laptop is moved away from AP. The signal strength is also measured using Kismet command.

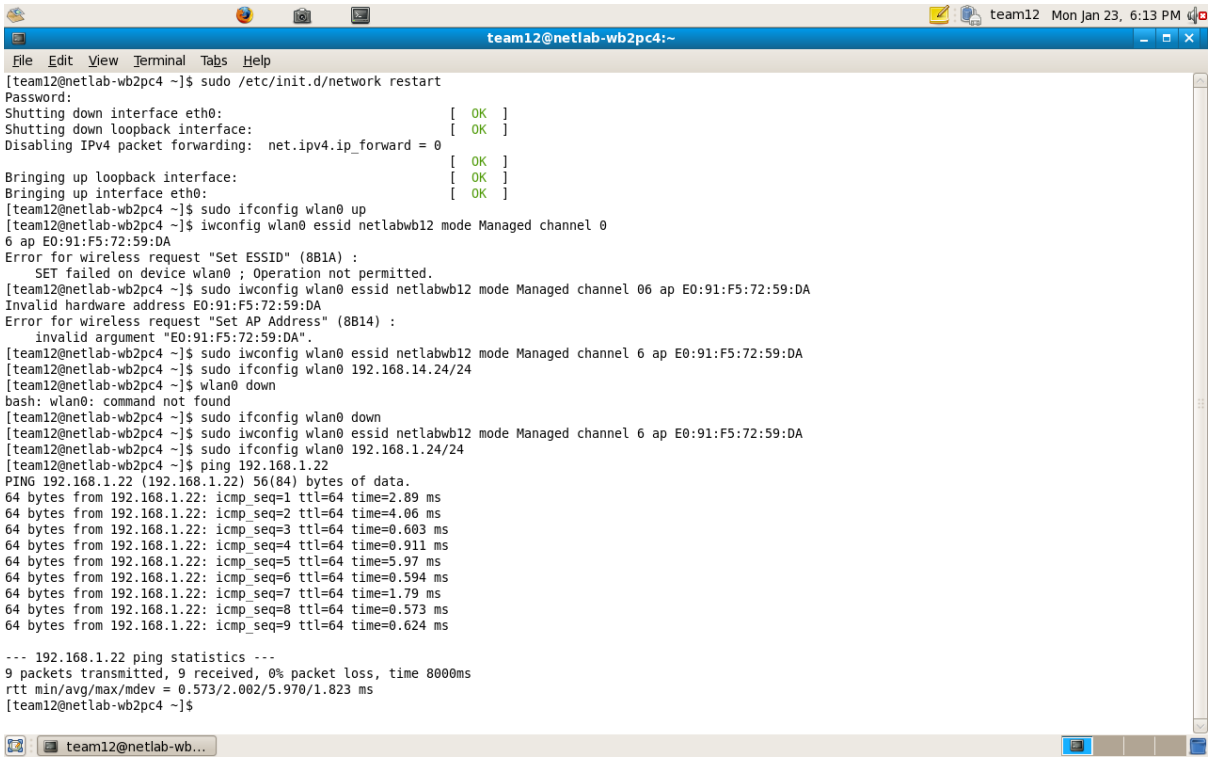


Fig 1 : *File transfer from laptop to PC2*

Then, a file transfer is done from laptop to PC2 using **scp** command and the data rate is observed as laptop is moved away from AP. When the laptop is near the AP, following data rate is observed

When the Laptop is very close to the range of the AP the data rate observed is comparatively greater than the AP being far away

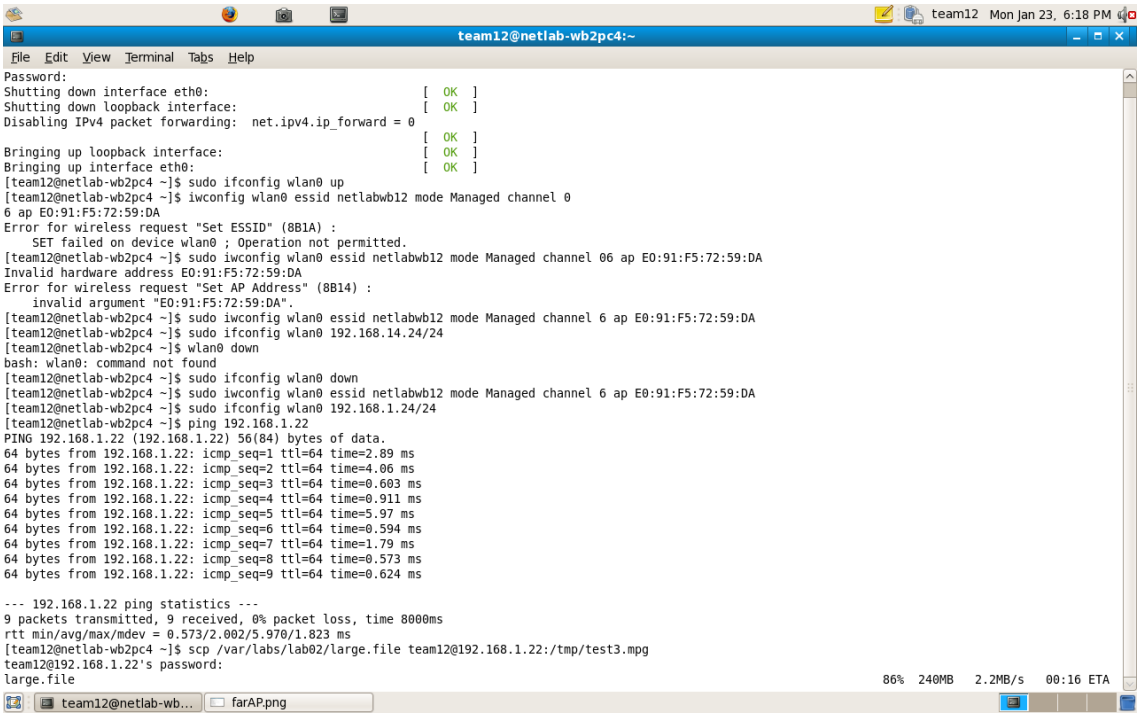


Fig 2: *When near the AP range*

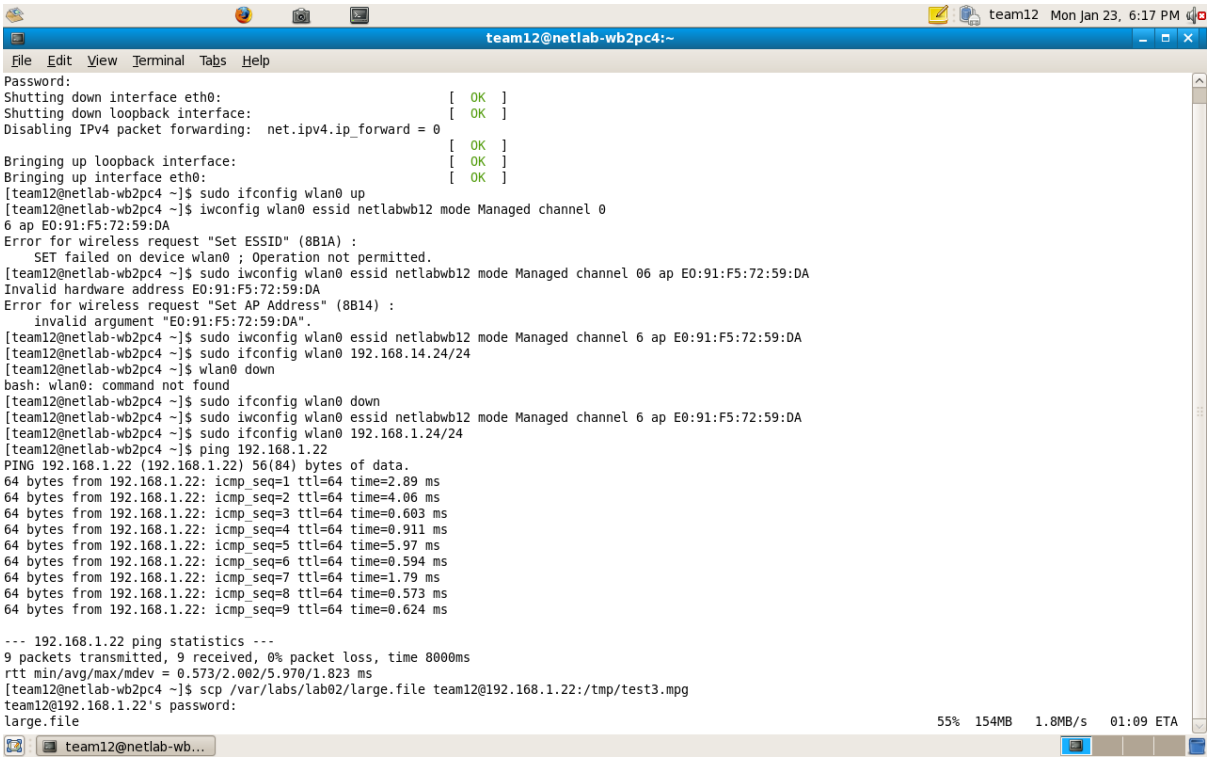


Fig 3: *When far away from the AP*

The signal strength is also measured using Kismet command as follows,

sudo kismet %opens up kismet terminal

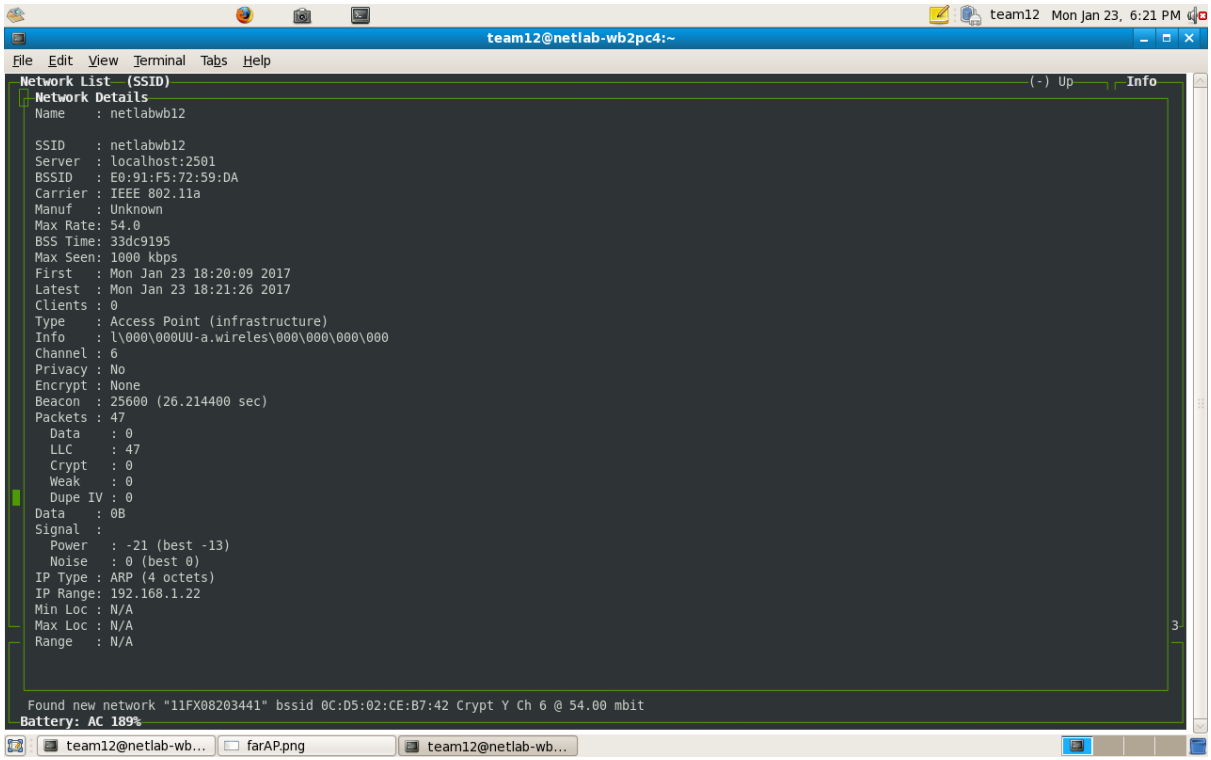


Fig 4: *The signal and the noise strength of The AP*

Now the interface is checked whether wlan0 is in Monitor Mode or managed mode and the MAC address is identified by the packets captured using Wireshark. wlan0 is made down using

sudo ifconfig wlan0 down %de-activate wireless interface

sudo iwconfig wlan0 mode Managed **%** Managed mode

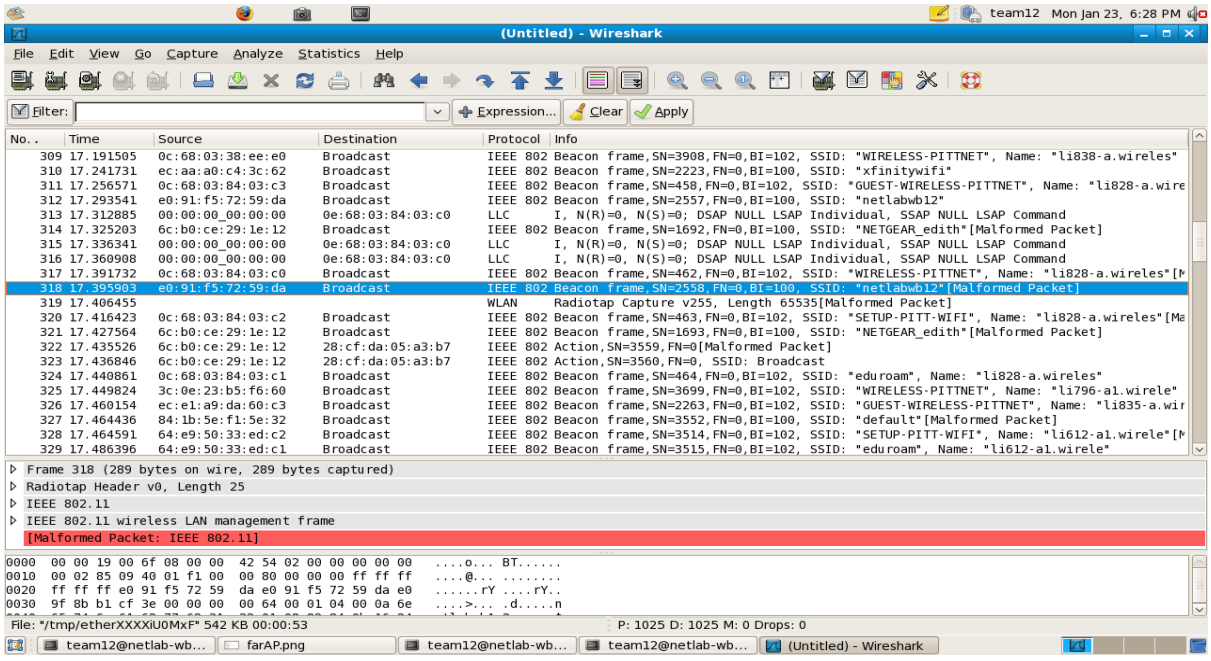


Fig 5*: Wireshark data capture*

Wireless – WDS

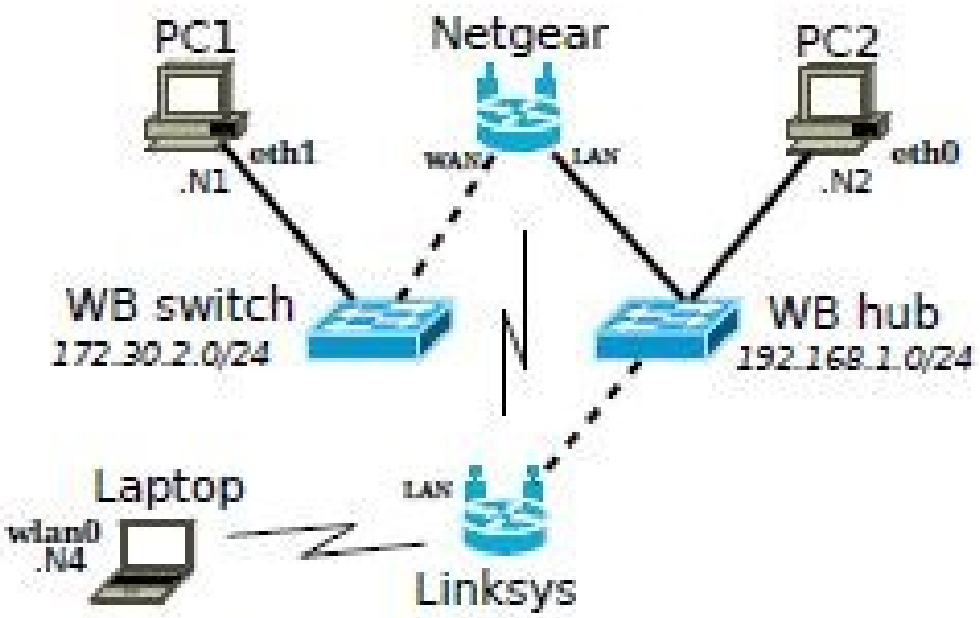
Aim:

To implement a Extended Service Set which consists of two Pc's, laptop, a switch, a hub and two Access Points. Pinging is also done between the nodes connected in this network.

Components Used:

Components	Quantities
PC	2
Laptop	1
Switch	1
Hub	1
Access Points	2

Network diagram:



The network is implemented as above and the following results are observed.

- Pinging is done from laptop to PC2

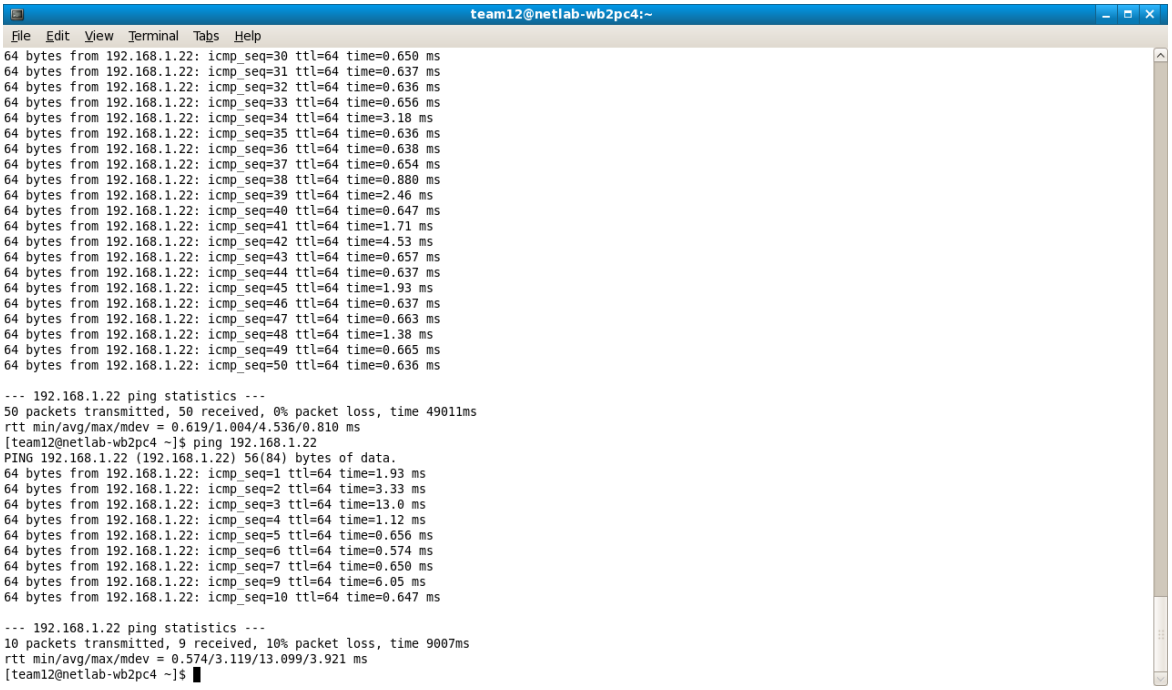


Fig 1: *PING command in WDS*

- Wireshark in laptop from another workbench is used to capture the traffic and the MAC addresses of both APs are identified.

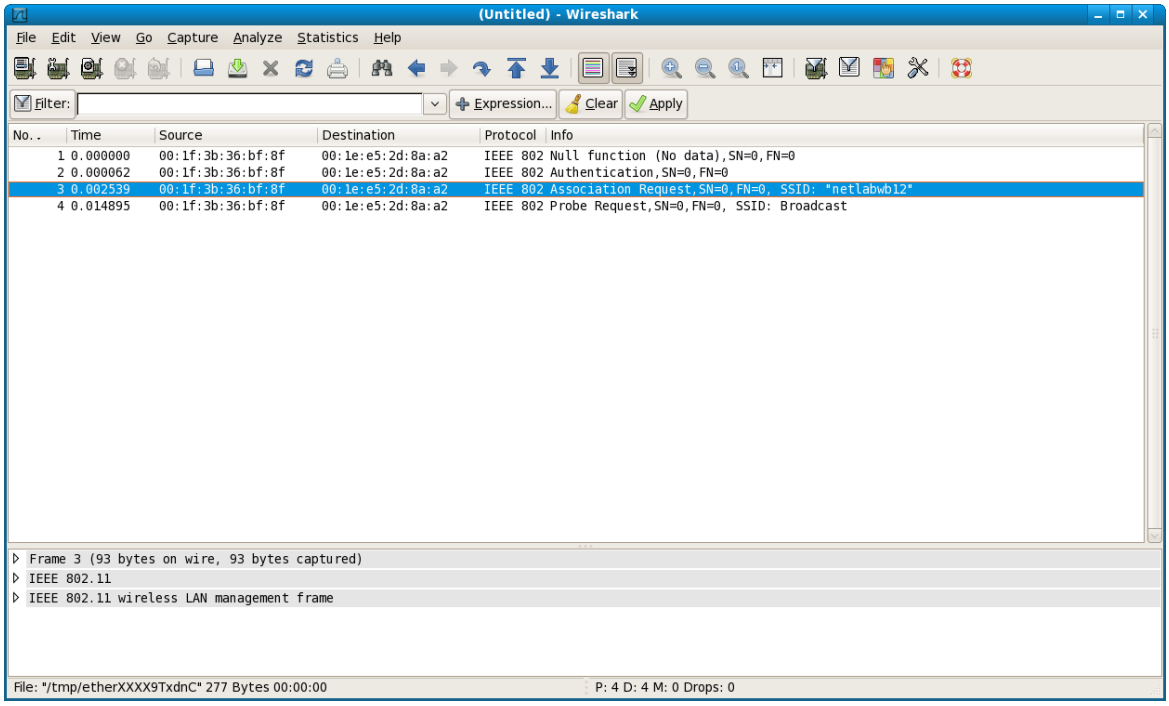


Fig 2*: Wireshark data capture from a remote node in WDS*

REFERENCES:

http://www.webopedia.com/TERM/H/hub.html

http://www.ebay.com/gds/Network-Switches-vs-Hubs-Advantages-and-Disadvantages-/10000000177330010/g.html