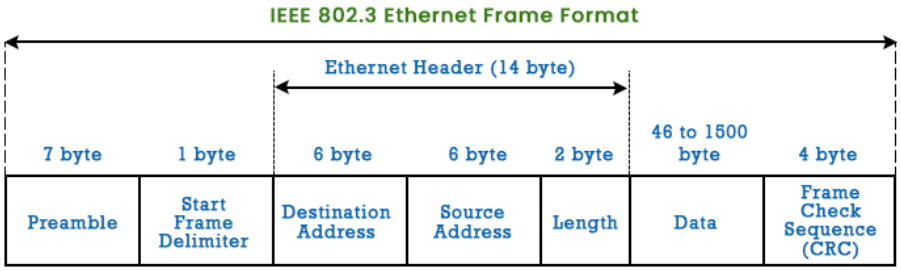
*** Security And Traffic Management***

DAY-01

Protocol: When two devices want to communicate, they have to follow certain rules which is known as protocol.

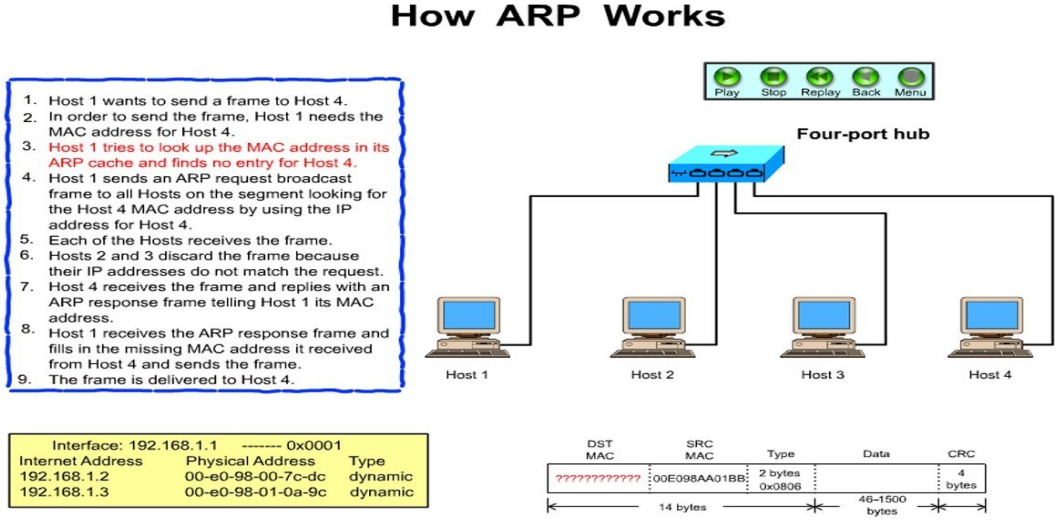
Ethernet Frame- Max frame size-1518 byte



At Data Link Layer: There are three types of MAC addresses: **Unicast, Multicast, and Broadcast**.

Need to know the Subnetting.

ARP: Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.



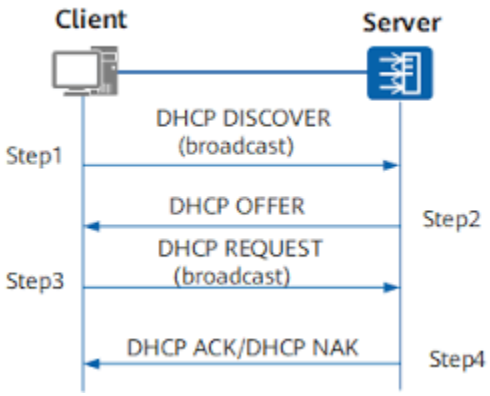
MAC address broadcast blocks at Router, That's why it is called **MAC provising**.

DHCP Sever- A DHCP Server is a network server that **automatically provides and assigns IP addresses, default gateways and other network parameters to client devices**. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

UDP port 67 is server port.

UDP port 68 is for client.

DORA===



DNS Protocol: DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.

DNS is mostly **UDP Port 53**, but as time progresses,

Server to Server DNS will rely on TCP Port 53 more heavily.

https://ns1.com/resources/dns-protocol

Commands::

1. Ipconfig /displaydns: Cache queries of websites
2. Ipconfig /flushdns: to clear the cache queries.
3. Ipconfig /release: remove the ip
4. Ipconfig /renew: renews the ip
5. Arp –a:: ARP cache
6. arp –d *: Delete the dynamic arp cache but with run as administrator

7. nslookup <website>: It gives the ip address of the website/domain. (Forward lookup)
8. nslookup <ip address>: It gives the name of the website/domain. (Reverse lookup)

TCP flags- ACK, SYN, FIN, RST, URG, PSH

A cyclic redundancy check (CRC) is **an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to digital data**. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents.

The Internet Assigned Numbers Authority (IANA) administrates the port numbers in the range of 0 - 65,535.

Post Office Protocol (POP) version 3- TCP 110

Internet Message Access Protocol (IMAP) TCP 143

TCP		UDP	
FTP	20,21	DNS	53
SSH	22	BooTPS/DHCP	67
Telnet	23	TFTP	69
SMTP	25	NTP	123
DNS	53	SNMP	161
HTTP	80		
POP3	110		
IMAP4	143		
HTTPS	443		

https://www.pearsonitcertification.com/articles/article.aspx?p=1868080

ICMP (Internet Control Message Protocol) is **a network level protocol**. ICMP messages communicate information about network connectivity issues back to the source of the compromised transmission. It sends control messages such as destination network unreachable, source route failed, and source quench.

Default value of IP header ICMP have TTL (Time to Live)- In Linux=64 It is hops. (No of routers)

Windows=128

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

TTL 0 – code=0 Type=11

PING – echo_request -- code=0 Type=8

Echo_reply --code= 0 Type=0

Traceroute/tracert <domain name> --Displays hops between source to destination.

Open Wireshark (For Protocol Analysis)

Open cmd tracert www.google.com

Open Wireshark and in url tab write your ip (ip.addr==xxx.xxx.xxx.xxx) to show the packets going from base machine.

Ip.addr==ip && icmp – to see the tracert packets going outside

---

Vulnerability and exploit---- in term of VIRUS (**Vital Information Resources under Siege**)

Blaster Worm was **a virus program that mainly targeted Microsoft platforms** in 2003. The worm attacked computers by exploiting a security flaw with Microsoft remote procedure call (RPC) process using Transmission Control Protocol (TCP) port number 135.

A Trojan, or Trojan horse, is **a type of malware that conceals its true content to fool a user into thinking it's a harmless file**. Like the wooden horse used to sack Troy, the "payload" carried by a Trojan is unknown to the user, but it can act as a delivery vehicle for a variety of threats.

==========

Firewall: -

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

- 1992 - First commercial firewall DEC SEAL
- 1994 - First of the stateful firewalls appear (s/w firewall)
-

Types: - Packet Filtering, Stateful Packet Inspection, Application Gateways/proxies, Adaptive Proxies, Circuit Level Gateway

Tech: - Screening Router, DMZ Firewall, Layered Firewall, Firewall Sandwich

Packet Filtering Firewall: A packet-filtering firewall works mainly on the **network layer** of the OSI reference model, although the transport layer is used to obtain the source and destination port numbers. It examines each packet independently and does not know whether any given packet is part of an existing stream of traffic.

Advantage and Disadvantages-

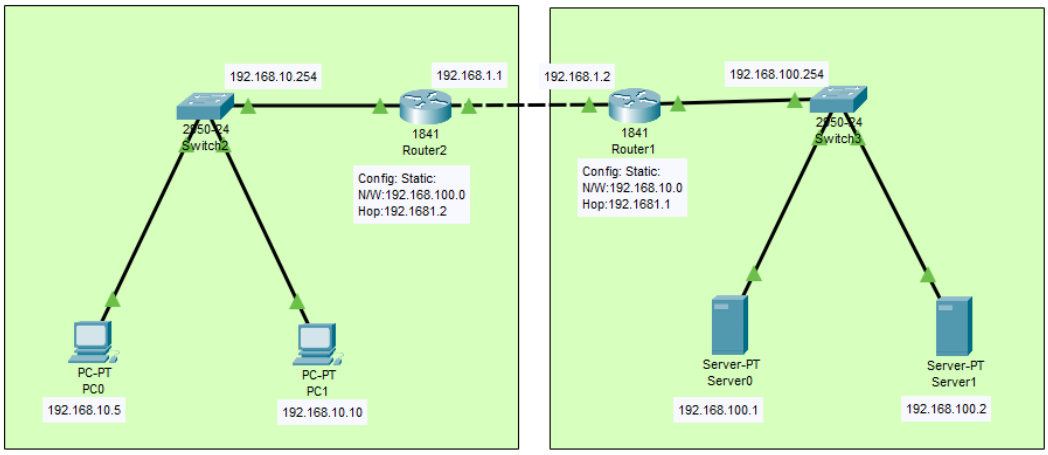
Router Has Access list 0-99

Standard Access list – source IP can be specified. Allows the source IP all traffic or blocks all traffic for that source.

Access List 100-199 = protocol, source IP, Source Port, destination IP, destination Port

++++++++++++++++++++STM LAB ++++++++++++++++++++++

1.Packet Filtering Firewall



Steps After Above Configuration:

- Go to PC -->Web-Browser -->Server IP
- Go to Server -->Services -->HTTP --> Edit Index.html

For Standard

- Packet Filter – Make an Access-list at Router 0

- Click Router 0 --> Go to CLI -->enable --> conf t --> access –list? (Tells list) --> access-list 10? -->
- Access-list 10 deny? -->access-list 10 deny host (for single ip) xxx.xxx.xxx.xxx ..

For Extended

- #Access list 100? --> permit--> access-list 100 tcp? (For websites) -->access-list 100 tcp host? -->
- Access-list 100 tcp host xxx.xxx.xxx.xxx(PC 0)? --> Access-list 100 tcp host xxx.xxx.xxx.xxx host xxx.xxx.xxx.xxx(Server-1)?

- --> Access-list 100 tcp host xxx.xxx.xxx.xxx eq 80?

Overall= access-list 100 permit tcp host 192.168.10.5 host 192.168.100.1 eq 80

do sh run ---> to see access-list

Where to put the firewall in the router: -

Select Router 0--> Select interface (0/0,0/1.): **int fa0/0** -->

Ip access-group 100? --> **Ip access-group 100 in.**

To add rule for ping:

Enable-->config t --> **do show ip route** (to check route list)

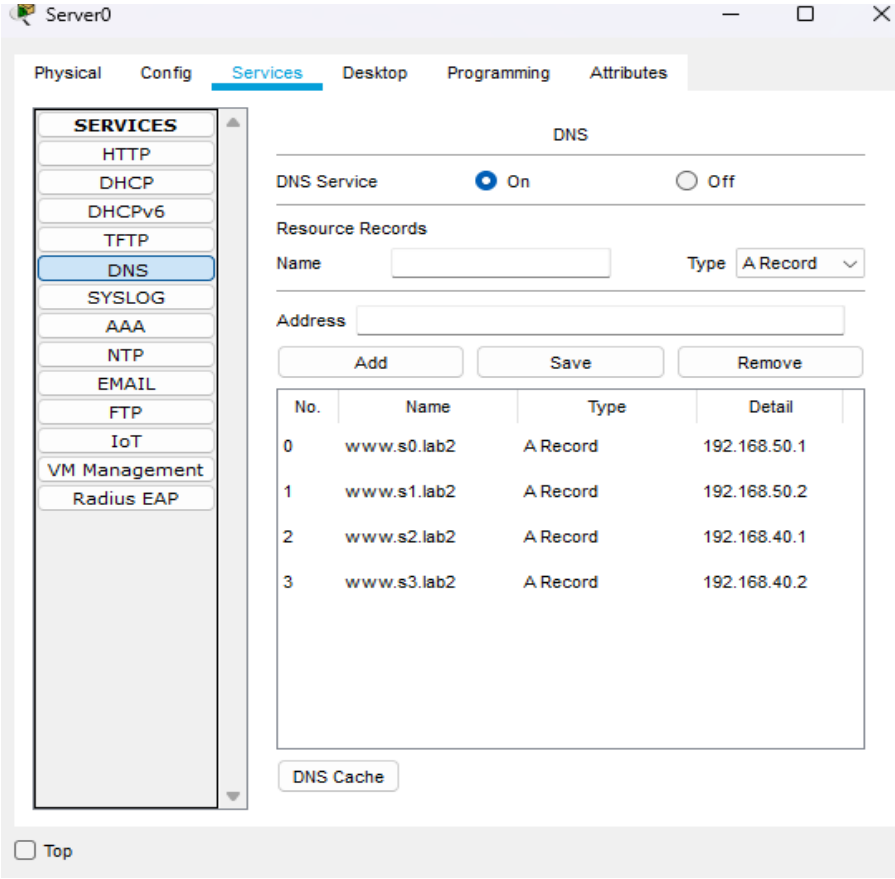
To delete the access group --> **no access-list 100**

TO SEE THE ACCESS-LIST **= do sh run**

Click on server 0:

- Services---->DNS --> Name=www.web1.lab Address=192.168.20.1

  Name=ftb.web1.lab Address=192.168.20.2



- Go to all PC and Input DNS Server Address of above entry Server.
- In browser you can access this website via name.

Go to Individual PC's: -0

- In cmd **nslookup <Name>**
- You can able to find the ip of the website.

Assignment::

Access-list Problems:

- 192.168.30.0 entire n/w should access DNS on 192.168.20.1
- 192.168.30.1 can access website on 192.168.20.1
- 192.168.30.5 can access website on 192.168.20.2
- 192.168.30.10 can access both websites and ping to both computers.

Solution:

- access-list 100 permit udp 192.168.30.0 0.0.0.255 host 192.168.20.1 eq domain
- access-list 100 permit tcp host 192.168.30.1 host 192.168.20.1 eq www

- access-list 100 permit tcp host 192.168.30.5 host 192.168.20.2 eq www
- access-list 100 permit tcp host 192.168.30.10 host 192.168.20.1 eq www
- access-list 100 permit icmp host 192.168.30.10 host 192.168.20.1 echo
- access-list 100 permit icmp host 192.168.30.10 host 192.168.20.2 echo
- access-list 100 permit tcp host 192.168.30.10 host 192.168.20.2 eq www