National Institute of Technology (NIT), Srinagar

“ Lab File of Computer Networking”

Dt. 26th June, 23

Submitted by - Zeeshan Sharif
E.No. 2020BITE’012
6th Semester

Submitted to:
Dr. Iqra Atlaf Gillani

ITL355 - Computer Networking Lab

Lab 1. Basic Network Utilities

Dt. March 16, 2023

Network utilities are software utilities designed to analyze and configure various aspects of computer networks.

Note: Students should practice these tools on Command prompt (Windows) or Terminal (Linux/macOS). These utilities can also be checked on: https://ping.eu.

Some of the common network utility tools are as follows;

1. **ipconfig or ifconfig:**
   These commands allow you to configure your network interfaces and view information about them. For example, you can view all your configured network interfaces, their IP addresses, DNS servers, default gateways, and other information.

   Windows: `$ipconfig`
   Others: `$ifconfig`

   To get detailed information about all interfaces including MAC address use the following commands.

   Windows: `$ipconfig /all`
   Others: `$ifconfig –a`

2. **ping:**
   This is the most commonly used network tool. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. If the remote destination is configured to reply, it will respond with packets of its own and you'll be able to see how long the round-trip time is between your computer and the destination.

   However, you'll see a "request timed out" message if packet loss is occurring, and you'll see an error message if your computer can't communicate with the remote host at all.

Hence, it is mostly useful for troubleshooting Internet connection problems. It can be used with domain name or IP address.

All OS: `$ping 173.194.33.174`
or, `$ping google.com`

3. **tracert/traceroute:**
   The traceroute, or tracert command is similar to ping, but provides information about the path a packet takes. Traceroute sends packets to a destination, asking each Internet router along the way to reply when it passes on the packet. Each hop is represented by a different line in the output. Traceroute will actually send three packets of data, and measure the time taken for each. This is shown in the 3 columns after the TTL. Sometimes asterisks are seen in the output which indicate that the target server did not respond as traceroute expected before a timeout occurred.

   Windows: `$tracert google.com`
   Other OS: `$traceroute google.com`

4. **arp:**
   This network command is used to view the ARP table, which contains the mappings between the IP address and the MAC address in our local area network segment (LAN).

   All OS: `$arp -a`

5. **nslookup:**
   This command will look up the IP addresses associated with a domain name.

   For example, you can run nslookup yahoo.com to see the IP address of Yahoo's server. It also allows you to perform a reverse lookup to find the domain name associated with an IP address.

   For example, nslookup 72.30.35.9 will show you that this IP address is associated with yahoo.com.

   All OS: `$nslookup yahoo.com`
   or, `$nslookup 72.30.35.9`

6. **netstat:**
   It stands for network statistics. This command displays incoming and outgoing network connections. In particular, it can show you the open connections on your computer, which programs are making which connections, how much data is being transmitted, and

other related information. There are different options available with this command to explore these statistics. Interested readers can refer to [1]

All OS: `$netstat`

Assignment 1

1. What is the IP and Gateway of your machine?

Ans. IP Address and Gateway

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether d0:88:0c:7f:41:53
        inet6 fe80::1ccb:3317:c9a7:f734%en0 prefixlen 64 secured scopeid 0xb
        inet6 2409:4054:1c:b0db:4a5:5f0:fc71:8b36 prefixlen 64 autoconf secured
        inet6 2409:4054:1c:b0db:9887:eee:21a2:5e64 prefixlen 64 autoconf temporary
        inet 192.168.43.119 netmask 0xffffff00 broadcast 192.168.43.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

2. "Ping" is a tool used to determine if a server is responding and to estimate the round trip time of a message sent to that server. Use the ping command for the following URLs and record the success or failure statistics along with the average round trip time.

   (a) google.com
   (b) facebook.com
   (c) 208.67.222.222 (Open DNS server)

Ans.

a. Ping Google

```
➜  ~ ping google.com
PING google.com (172.217.166.14): 56 data bytes
64 bytes from 172.217.166.14: icmp_seq=0 ttl=54 time=57.108 ms
64 bytes from 172.217.166.14: icmp_seq=1 ttl=54 time=93.567 ms
64 bytes from 172.217.166.14: icmp_seq=2 ttl=54 time=69.727 ms
64 bytes from 172.217.166.14: icmp_seq=3 ttl=54 time=85.595 ms
64 bytes from 172.217.166.14: icmp_seq=4 ttl=54 time=78.517 ms
64 bytes from 172.217.166.14: icmp_seq=5 ttl=54 time=73.761 ms
64 bytes from 172.217.166.14: icmp_seq=6 ttl=54 time=142.664 ms
64 bytes from 172.217.166.14: icmp_seq=7 ttl=54 time=98.735 ms
64 bytes from 172.217.166.14: icmp_seq=8 ttl=54 time=78.230 ms
64 bytes from 172.217.166.14: icmp_seq=9 ttl=54 time=73.606 ms
64 bytes from 172.217.166.14: icmp_seq=10 ttl=54 time=751.805 ms
64 bytes from 172.217.166.14: icmp_seq=11 ttl=54 time=102.946 ms
64 bytes from 172.217.166.14: icmp_seq=12 ttl=54 time=82.411 ms
^C
--- google.com ping statistics ---
13 packets transmitted, 13 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 57.108/137.590/751.805/178.443 ms
```

b. Ping Facebook

```
➜  ~ ping facebook.com
PING facebook.com (157.240.198.35): 56 data bytes
64 bytes from 157.240.198.35: icmp_seq=0 ttl=52 time=61.484 ms
64 bytes from 157.240.198.35: icmp_seq=1 ttl=52 time=77.838 ms
64 bytes from 157.240.198.35: icmp_seq=2 ttl=52 time=93.728 ms
64 bytes from 157.240.198.35: icmp_seq=3 ttl=52 time=86.449 ms
64 bytes from 157.240.198.35: icmp_seq=4 ttl=52 time=100.826 ms
64 bytes from 157.240.198.35: icmp_seq=5 ttl=52 time=104.583 ms
64 bytes from 157.240.198.35: icmp_seq=6 ttl=52 time=97.304 ms
64 bytes from 157.240.198.35: icmp_seq=7 ttl=52 time=103.120 ms
64 bytes from 157.240.198.35: icmp_seq=8 ttl=52 time=104.277 ms
^C
--- facebook.com ping statistics ---
9 packets transmitted, 9 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 61.484/92.179/104.583/13.760 ms
```

c. Ping 208.67.222.222 (Open DNS server)

```
➜  ~ ping 208.67.222.222
PING 208.67.222.222 (208.67.222.222): 56 data bytes
64 bytes from 208.67.222.222: icmp_seq=0 ttl=50 time=157.334 ms
64 bytes from 208.67.222.222: icmp_seq=1 ttl=50 time=117.858 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=50 time=156.002 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=50 time=108.275 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=50 time=107.870 ms
64 bytes from 208.67.222.222: icmp_seq=5 ttl=50 time=101.033 ms
^C
--- 208.67.222.222 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 101.033/124.729/157.334/23.111 ms
➜  ~
```

3. Find the IP and MAC address of computers connected on your network.

Ans. IP and MAC address

```
➜  ~ arp -a
? (192.168.43.1) at 36:98:e:f3:79:a4 on en0 ifscope [ethernet]
? (192.168.43.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
➜  ~
```

4. Trace the route that is taken when you try to access:

   (a) google.com
   (b) facebook.com
   (c) 8.8.8.8

   Record the number of hops required for accessing each of the URLs. Also provide an ordered list of the geographical locations corresponding to the machines through which the packets travelled in each case. You may use http://countrycode.org to map ISO codes to country name.

Ans.

a. Traceroute Google.com

The packet went from Srinagar - Mumbai(twice) - Canberre(Aus)(twice) - Mountain View(USA)(twice) - Sydney(Aus)

```
➜  ~ traceroute google.com
traceroute to google.com (172.217.166.14), 64 hops max, 52 byte packets
 1  192.168.43.1 (192.168.43.1)  5.198 ms  4.958 ms  4.736 ms
 2  * * *
 3  10.72.72.2 (10.72.72.2)  65.063 ms
    10.72.72.3 (10.72.72.3)  52.927 ms  52.897 ms
 4  192.168.146.177 (192.168.146.177)  26.105 ms
    192.168.146.181 (192.168.146.181)  25.277 ms
    192.168.146.177 (192.168.146.177)  51.888 ms
 5  172.27.251.4 (172.27.251.4)  39.830 ms  39.558 ms  38.525 ms
 6  172.27.251.19 (172.27.251.19)  41.953 ms  41.765 ms  35.778 ms
 7  192.168.75.174 (192.168.75.174)  40.047 ms  35.318 ms  40.098 ms
 8  * * *
 9  * * *
10  * * *
11  209.85.148.118 (209.85.148.118)  142.420 ms
    142.250.161.100 (142.250.161.100)  51.352 ms *
12  * * *
13  74.125.243.97 (74.125.243.97)  80.477 ms *
    74.125.243.100 (74.125.243.100)  81.506 ms
14  209.85.251.231 (209.85.251.231)  69.800 ms
    209.85.252.45 (209.85.252.45)  58.221 ms
    74.125.244.196 (74.125.244.196)  69.771 ms
15  del03s17-in-f14.1e100.net (172.217.166.14)  58.400 ms
    108.170.251.97 (108.170.251.97)  58.264 ms
    108.170.251.113 (108.170.251.113)  58.836 ms
```

b. Traceroute Facebook.com

The packet went from srinagar - mumbai(twice) - Menlo Park(USA)(twice) - Dublin(Ireland)(twice)

```
➜  ~ traceroute facebook.com
traceroute to facebook.com (157.240.198.35), 64 hops max, 52 byte packets
 1  192.168.43.1 (192.168.43.1)  5.611 ms  5.674 ms  4.253 ms
 2  * * *
 3  10.72.72.19 (10.72.72.19)  344.663 ms  41.569 ms
    10.72.72.18 (10.72.72.18)  39.926 ms
 4  192.168.146.177 (192.168.146.177)  50.673 ms
    192.168.146.181 (192.168.146.181)  28.982 ms
    192.168.146.177 (192.168.146.177)  39.698 ms
 5  172.27.251.4 (172.27.251.4)  36.726 ms  38.944 ms  39.953 ms
 6  172.27.251.19 (172.27.251.19)  42.802 ms  36.195 ms  40.203 ms
 7  192.168.75.174 (192.168.75.174)  40.068 ms
    192.168.75.168 (192.168.75.168)  38.788 ms
    192.168.75.172 (192.168.75.172)  38.571 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  ae4.pr02.del1.tfbnw.net (157.240.73.118)  128.695 ms  59.190 ms  86.116 ms
14  157.240.38.135 (157.240.38.135)  68.689 ms
    po102.psw04.del1.tfbnw.net (157.240.50.169)  57.095 ms
    po102.psw01.del1.tfbnw.net (31.13.24.7)  73.647 ms
15  157.240.38.203 (157.240.38.203)  53.060 ms
    157.240.38.181 (157.240.38.181)  53.335 ms  47.784 ms
16  edge-star-mini-shv-01-del1.facebook.com (157.240.198.35)  84.587 ms  60.951 ms  82.198 ms
➜  ~
```

c. Traceroute 8.8.8.8

Delhi - Centreville(USA) - Mountain View(USA)

```
➜  ~ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
 1  192.168.43.1 (192.168.43.1)  12.652 ms  4.302 ms  6.952 ms
 2  * * *
 3  10.72.72.19 (10.72.72.19)  77.920 ms  32.567 ms  40.266 ms
 4  192.168.146.177 (192.168.146.177)  40.141 ms
    192.168.146.181 (192.168.146.181)  48.571 ms  27.163 ms
 5  172.27.251.4 (172.27.251.4)  39.803 ms  49.528 ms  31.534 ms
 6  172.27.251.19 (172.27.251.19)  71.007 ms  57.843 ms  48.962 ms
 7  192.168.75.168 (192.168.75.168)  71.237 ms
    192.168.75.170 (192.168.75.170)  46.483 ms  27.840 ms
 8  * * *
 9  * * *
10  * * *
11  72.14.195.22 (72.14.195.22)  108.846 ms
    74.125.147.192 (74.125.147.192)  78.909 ms
    142.250.47.144 (142.250.47.144)  81.858 ms
12  * * dns.google (8.8.8.8)  52.533 ms
➜  ~
```

5. Issue DNS lookup requests for the following;

   (a) 8.8.8.8
   (b) gmail.com
   (c) 209.191.88.254

Ans. DNS Lookup

```
➜  ~ nslookup 8.8.8.8
Server:         2409:4054:1c:b0db::a8
Address:        2409:4054:1c:b0db::a8#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:

➜  ~ nslookup gmail.com
Server:         2409:4054:1c:b0db::a8
Address:        2409:4054:1c:b0db::a8#53

Non-authoritative answer:
Name:   gmail.com
Address: 142.250.194.37

➜  ~ nslookup 209.191.88.254
;; Got SERVFAIL reply from 2409:4054:1c:b0db::a8, trying next server
Server:         192.168.43.1
Address:        192.168.43.1#53

** server can't find 254.88.191.209.in-addr.arpa: SERVFAIL
```

References;

[1] Understanding the Netstat command [online]
https://www.supportsages.com/understanding-the-netstat-command/ (2019)

[2] The Top 10 Basic Network Troubleshooting Tools Every IT Pro Should Know [online]

https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools (2020)

[3] Basic Network Commands that every administrator should know [online] https://pandorafms.com/blog/network-commands/ (2019)

.

.

Submission by Zeeshan Sharif (BITE'012)

Computer Networking Lab
(Lab 2)

Zeeshan Sharif
BITE'012

Aim - To introduce Devices found at different layers of the TCP/IP Model.

Theory
According to the layer, we have following devices;

Layer 1 - Hub, Repeater

a. Hub
Operates at the Physical Layer. It is a central connection point for devices in a local area network (LAN). It broadcasts incoming data to all connected devices without intelligent decision-making.

b. Repeater
It operates at the Network Interface layer. It amplifies or regenerates signals to extend network reach. It maintains signal integrity and improves network performance over long distances.

Layer 2 - Switch, Bridge

a. Switch
It Operates at the Network Interface layer. It is an Intelligent device that efficiently transmits data within a LAN. It uses MAC addresses to selectively forward data only to the intended recipient. It provides improved network performance and security compared to hubs.

b. Bridge
It operates at the Network Interface layer. It connects two separate LAN

segments. Selectively forwards network traffic based on MAC addresses. Segments networks, reduces congestion, and improves performance.

Layer 3 - Router, Collision Domain and Broadcast Domain

a. Router
It operates at the Internet layer. It connects multiple networks and forwards data packets based on IP addresses. It makes intelligent routing decisions using routing tables and protocols. It ensures efficient and reliable data transmission across networks. It directs traffic, enforces network boundaries, and provides network security.

b. Collision Domain)
A collision domain is a network segment where devices share the same physical communication medium, such as an Ethernet segment or a hub. In a collision domain, only one device can transmit data at a time. The collisions are handled using the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism in Ethernet networks. The switches and bridges can break collision domains by creating separate collision domains for each of their ports

c. Broadcast Domain
A broadcast domain is a logical division of a network where broadcast frames are forwarded. Broadcast frames are network packets that are sent to all devices in a network. In a broadcast domain, when a device sends a broadcast frame, all other devices within that domain receive and process it. Each interface on a router represents a separate broadcast domain. VLANs (Virtual LANs) can also define broadcast domains, where devices within the same VLAN can communicate using broadcast frames.

By evaluating the physical connectivity, presence of network devices, routing infrastructure, and VLAN configurations, we can determine the collision and broadcast domains within a network.

CN Lab 3 - Exploring Wireshark

Zeeshan Sharif - 2020BITE012

29 March 2023

1 The Basic HTTP GET/Response Interaction

Answer the following questions based on the captured trace of packets:

1. What is the IP address of your computer?
2. What is the IP address of the gaia.cs.umass.edu server?
3. How many bytes of content (size of file) are returned to your browser?
4. How long did it take from when the HTTP GET message was sent and response was received?

Ans:

1. The IP address of my computer is: **192.168.43.119**
2. The IP address of the gaia.cs.umass.edu server is: **128.119.245.12**
3. The size of file received is: **552 bytes (4416 bits)**
4. Response time : **0.390636000 seconds**

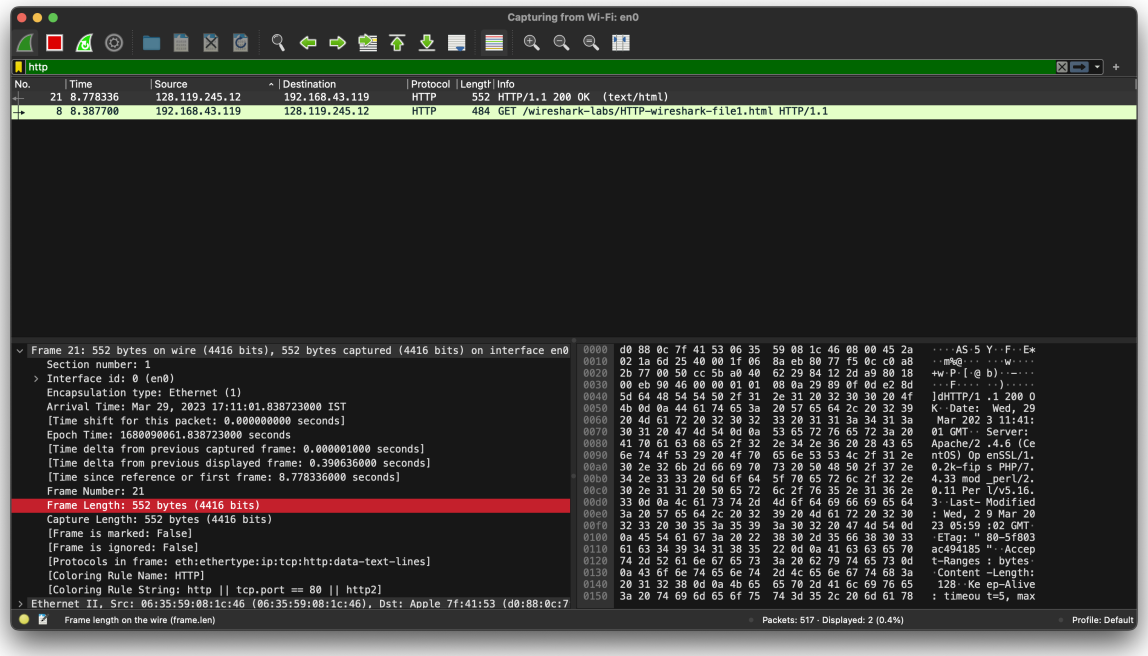


Figure 1: IP addresses

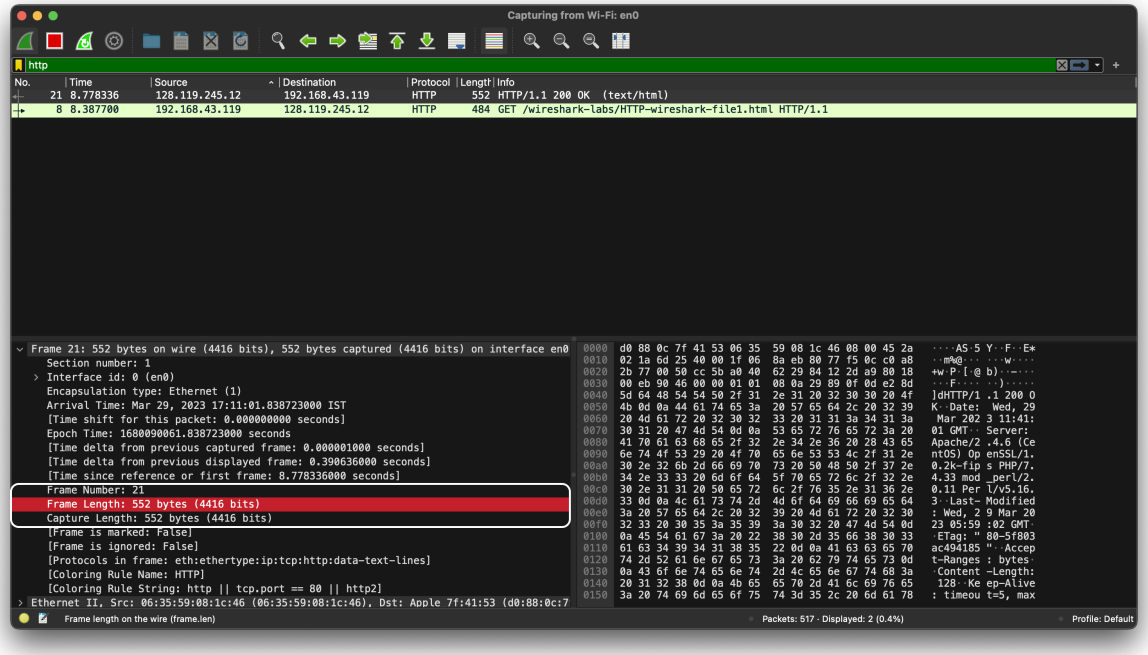


Figure 2: Size of file received

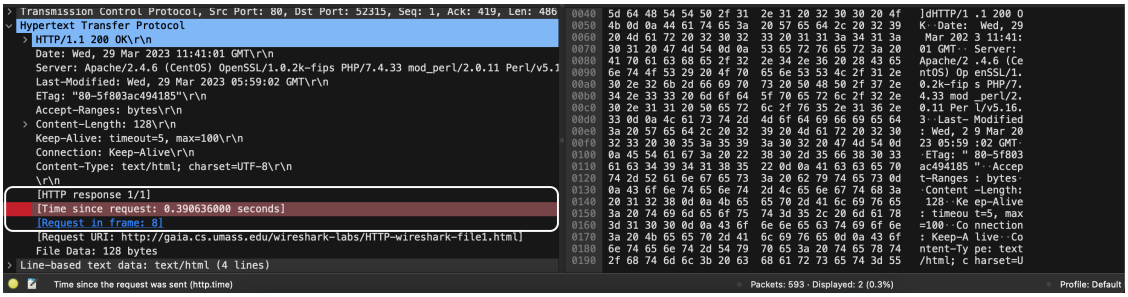


Figure 3: Time since request

2 DNS

Answer the following questions based on the captured trace of packets:

1. Which transport layer protocol is used to carry DNS query & response?
2. What is source port of DNS response? Is this a standard port number?
3. What information did you get from DNS response?

Ans:

1. **User Datagram Protocol (udp)** is used to carry DNS query and response.
2. Source port : **53** . Yes, it is a standard port number.
3. Following is the information received from DNS response :

a. Name of the host : **www.tue.nl**
b. The Type of address : **A (HOST address)**
c. The IP address : **167.235.218.203**

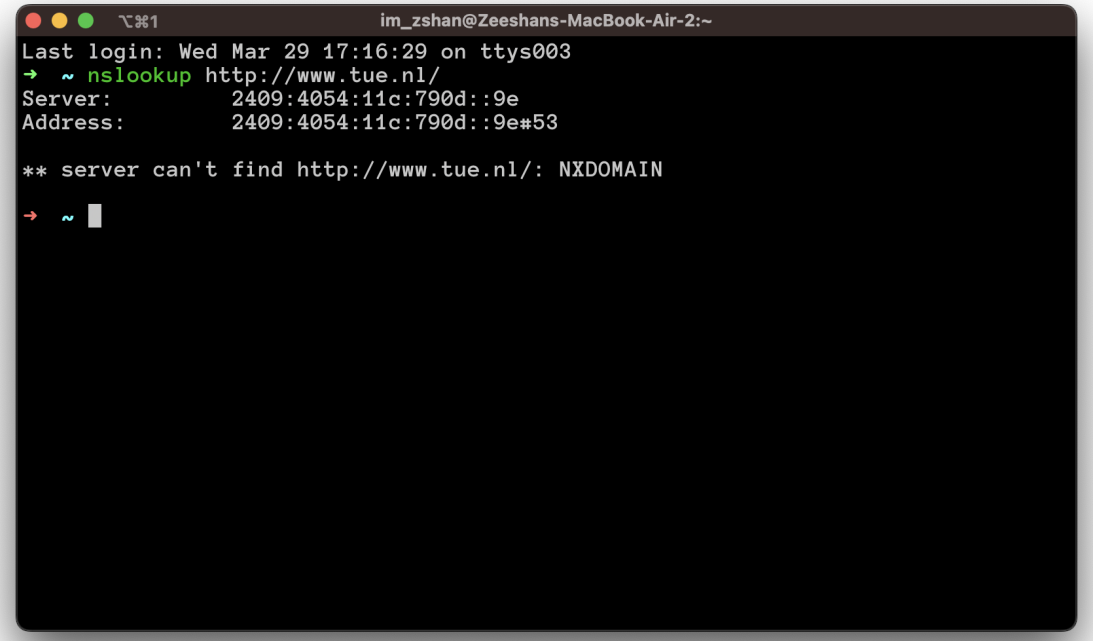


Figure 4: Doing nslookup on www.tue.nl.

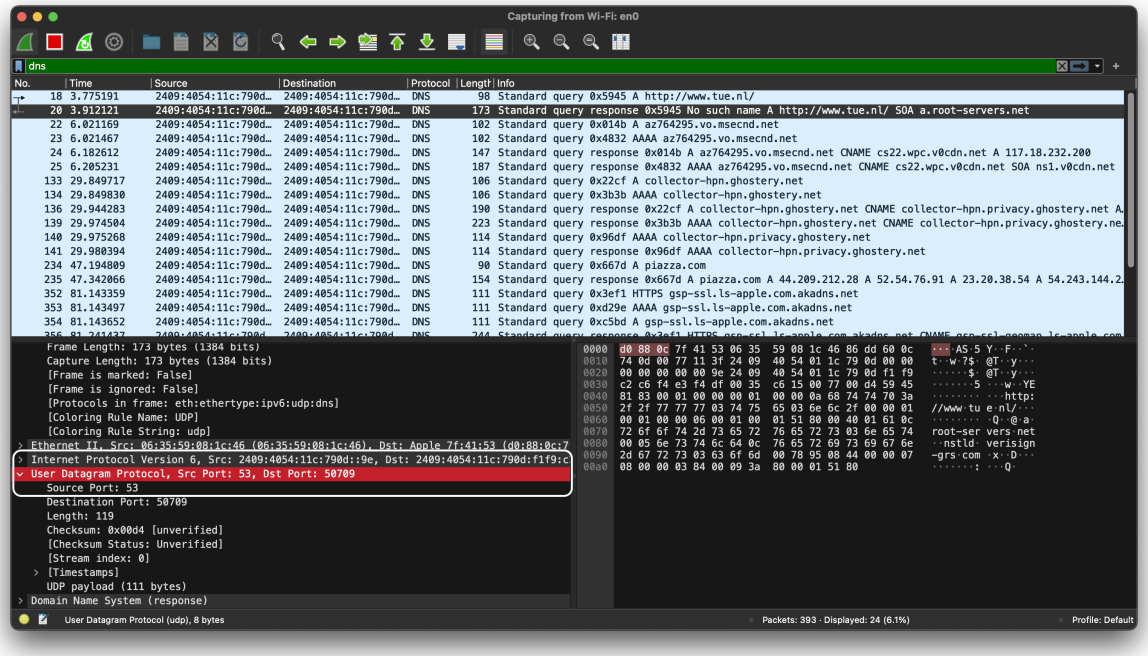


Figure 5: Transport Layer Protocol for DNS request

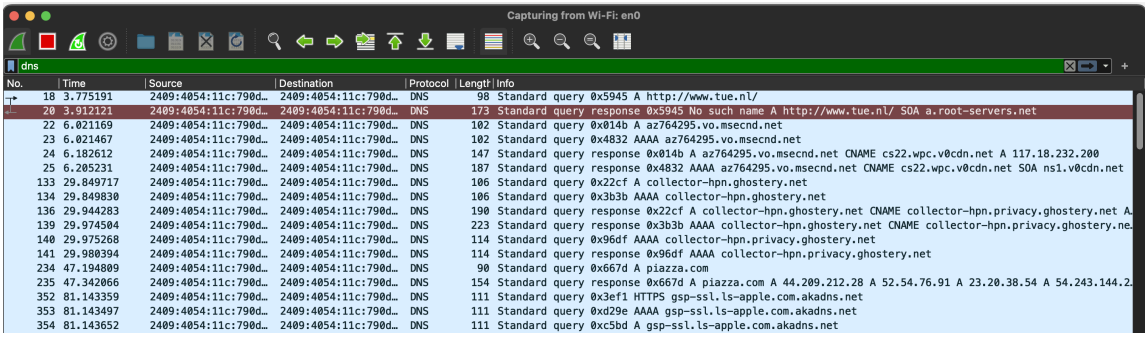


Figure 6: Information from DNS response

3 ICMP

Answer the following questions based on the captured trace of packets:

1. What is the destination IP address?
2. Report the response time of the first packets ent.

Ans:

1. Destination IP address : **202.165.107.50**
2. Response Time of first packet : **129.155 ms**

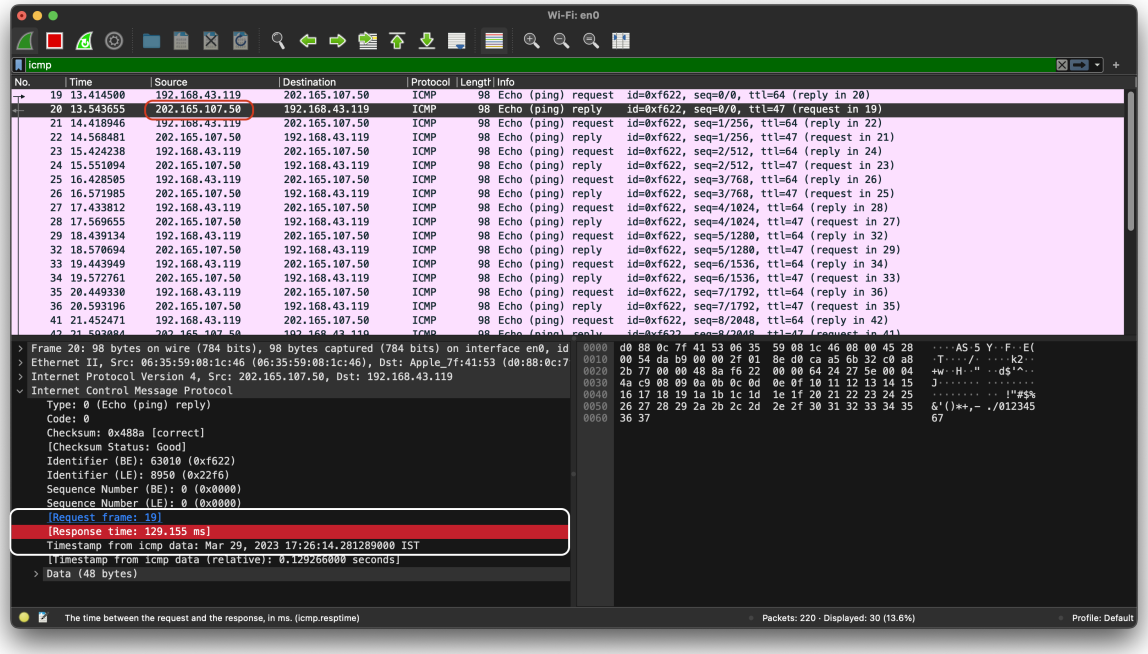


Figure 7: Destination IP and its Response time

The End

Computer Networking Lab
(Lab 4)

Zeeshan Sharif
BITE'012

Aim - To understand Cisco Packet Tracer and Create a LAN using hubs and switches and understand their working, address learning in a switch.

Theory

1. Cisco Packet Tracer

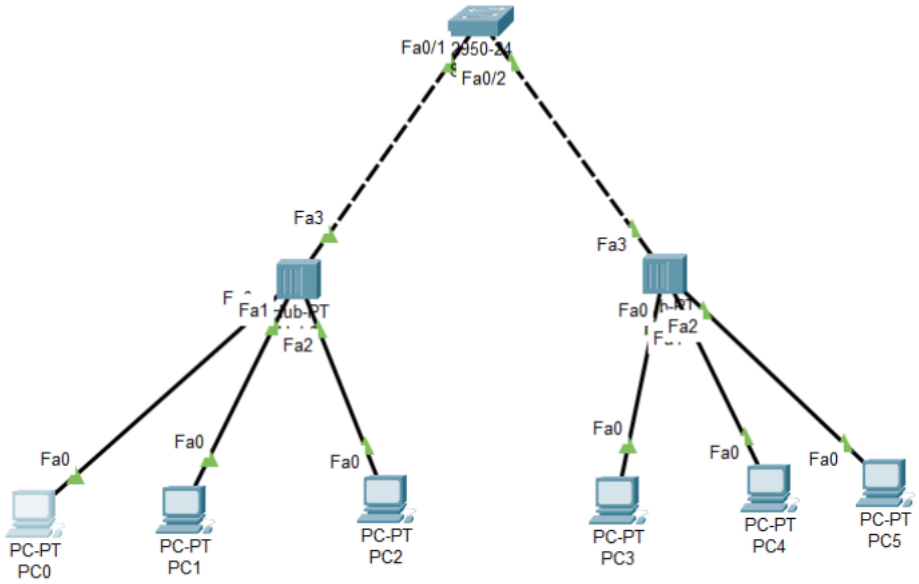
Cisco Packet Tracer is a network simulation tool that allows users to design, configure, and troubleshoot network typologies. It provides a virtual environment to experiment with network setups without the need for physical devices. The users can simulate routers, switches, hubs, PCs, and other network components to create and analyze network configurations.

2. LAN Creation Using Hubs and Switches

Local Area Networks (LANs) can be created using hubs and switches to interconnect multiple devices. The Hubs operate at the Physical layer and pass incoming data to all connected devices without any intelligent decision-making. The switches operate at the Data Link layer (Link layer) and selectively forward data based on MAC addresses, improving network performance compared to hubs.

3. Address Learning in a Switch

Switches use a process called address learning to build and maintain a MAC address table. When a switch receives a frame, it examines the source MAC address and associates it with the incoming port in its MAC address table. Subsequently, when the switch receives a frame with a destination MAC address, it looks up the address in the table and forwards the frame only to the port associated with that address, reducing unnecessary network traffic.



Implementation
To conduct this experiment, the following steps were followed:

Step 1: Open Cisco Packet Tracer, Take a switch, Two Hubs and connect these hubs with switch and then take end devices (atleast 4) and connect each of two with a hub.

Step 2: On each end devices, click on it and go to Desktop and then select IP configuration in which allocate IP address (either static or DHCP) and IP6 address(if you want).

ping 192.168.2.29

Step 3: Once all above steps done, choose a end device and ping another device with its IP address in command Prompt.
As example: -

192.168.2.29 is the IP address of another device whom we want to ping

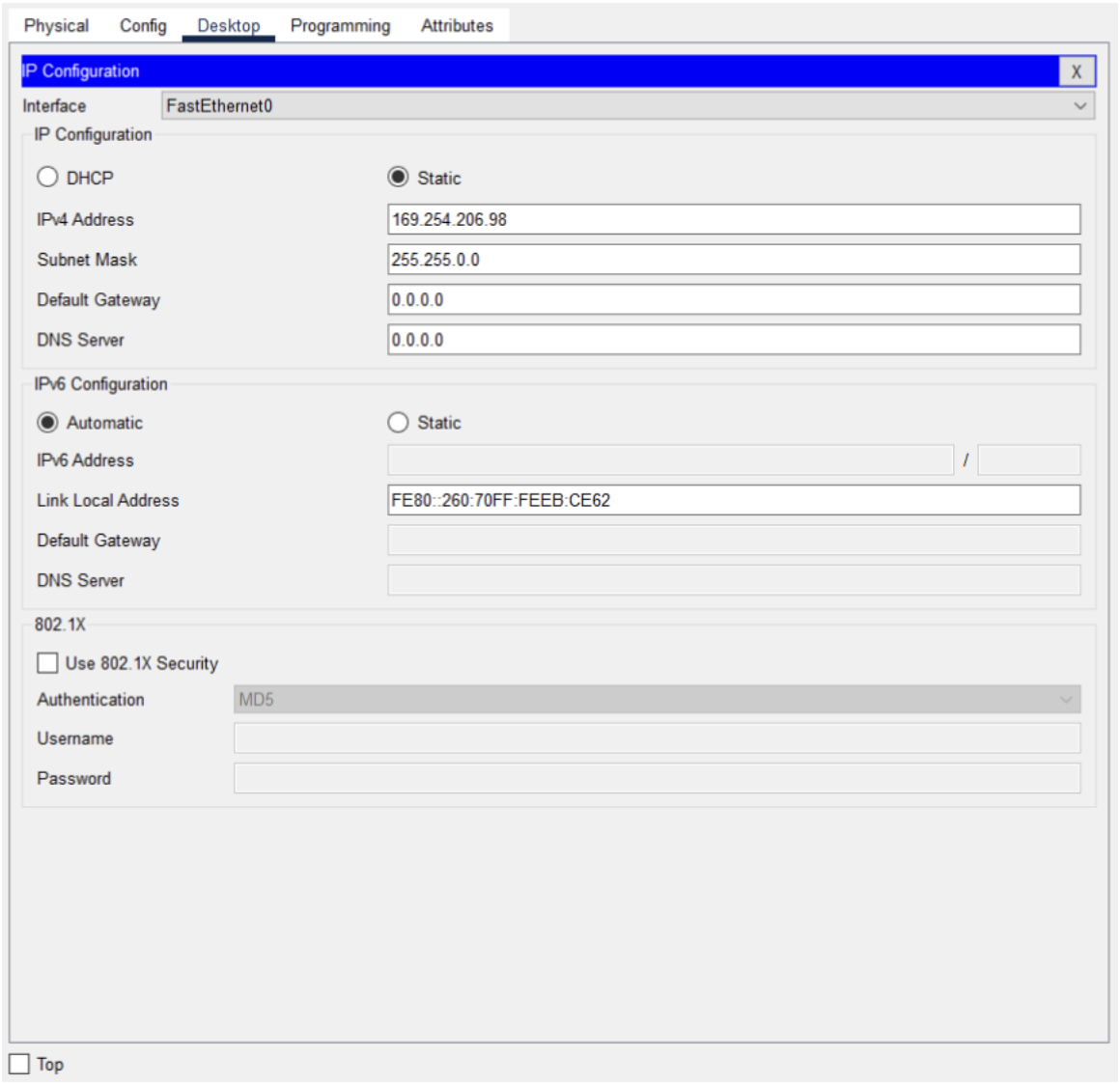


Figure 1: Allocating IP Address to PC0

Inferences

Based on the experimental results and observations, the following inferences can be made:

• Cisco packet Tracer provides a user-friendly platform for network simulation, allowing user to design and configure virtual networks.

• Hubs, operating at the Physical layer, transmit data to all connected devices, resulting in increased network congestion and potential performance issues.

• Switches, operating at the Data Link layer, offer superior performance compared to hubs by selectively forwarding data based on MAC addresses. Address learning of Switch plays a very crucial role in forwarding frames.

Computer Networking Lab
(Lab 5)

Zeeshan Sharif
BITE'012

Aim - Router configuration in Cisco Packet Tracer to do following: -

1. Introduction to various router CLI Modes.
2. Classful IP address assignment to end-devices and routers interfaces.
3. Classless IP address assignment to end-devices and router interfaces(Assignment)

Theory

1. Router CLI Modes
Cisco routers have different CLI (Command Line Interface) modes that provide different levels of access and functionality. The three main CLI modes are User EXEC mode, Privileged EXEC mode, and Global Configuration mode. **User EXEC mode** is the default mode after accessing the router, providing limited access for basic commands. **Privileged EXEC mode** offers more control and advanced commands, typically requiring a password for access. **Global Configuration mode** allows for configuring specific parameters for the router, including interface settings, routing protocols, and security features.

2. Classful IP Address Assignment
Classful IP addressing is a method of assigning IP addresses based on specific address classes defined by the original IP addressing scheme. There are five classes: A, B, C, D, and E. Classes A, B, and C are commonly used for network assignments, while classes D and E have specific purposes. Each class has a predetermined range of IP addresses and a default sub-

net mask. Classful IP addressing does not support variable-length subnet masks (VLSM) or subnetting within a classful network.

3. Classless IP Assignment
Classless Inter-Domain Routing (CIDR) allows for more flexible allocation of IP addresses by using variable-length subnet masks (VLSM). CIDR allows networks to be subnetted into smaller subnets, based on the specific requirements of each network. Classless addressing does not strictly adhere to the fixed class boundaries defined in classful addressing.

Implementation
To conduct this experiment, the following steps were followed:

Step 1: Allocating IP Address to PC: Select and click on PC, then Go to IP configuration and then Write IP address along with Subnet mask and default Gateway IP address.

Step 2: Allocating IP Address to Router Interface: Select and click on Router, Choose CLI and Go to interface mode from User Exec Mode with the help of following command:- Select Interface to enter in interface mode: let's say fa0/0

Router# enable
Router# conf t
Router(config)# int fa0/0
Router(config-if)# ip address IP Address Subnet Mask

If you want to use classless IP address, just change the subnet mask accordingly.

Inferences
Based on the experimental results and observations, the following inferences can be made:

• Router CLI modes provide different levels of access and functionality for managing and configuring Cisco routers.

• Classful IP address assignment follows fixed class boundaries (Class A, B, and C) but may lead to inefficient address utilization.

• Classless IP address assignment using CIDR and VLSM offers more flexibility in subnetting and efficient utilization of IP addresses.

Computer Networking Lab
(Lab 6)

Zeeshan Sharif
BITE'012

Aim - Configuring static routing on a network. Assignment: Default routing.

Theory

Routing is an essential component of computer networking as it facilitates the transmission of data packets from one network to another. Static routing is a configuration approach employed in networks to establish the path for data transmission through manually defined routes. This lab primarily concentrates on default routing, which is a specialized form of static routing utilized when a router intends to forward packets to destinations outside its directly connected networks.

1. Default Routing

Default routing is a type of static routing used when a router needs to send packets to destinations outside of its directly connected networks. It involves configuring a router to forward any packet that doesn't match a specific route in its routing table to a default gateway or next-hop address. This allows the router to handle traffic intended for external networks efficiently.

Configuration Process of Default Routing

The configuration process for default routing in Cisco routers involves the following steps:

1. Access the Router: Connect to the Cisco router through a console cable and a terminal emulation program like PuTTY or SecureCRT. Use the appropriate login credentials to access the router's command-line interface (CLI).

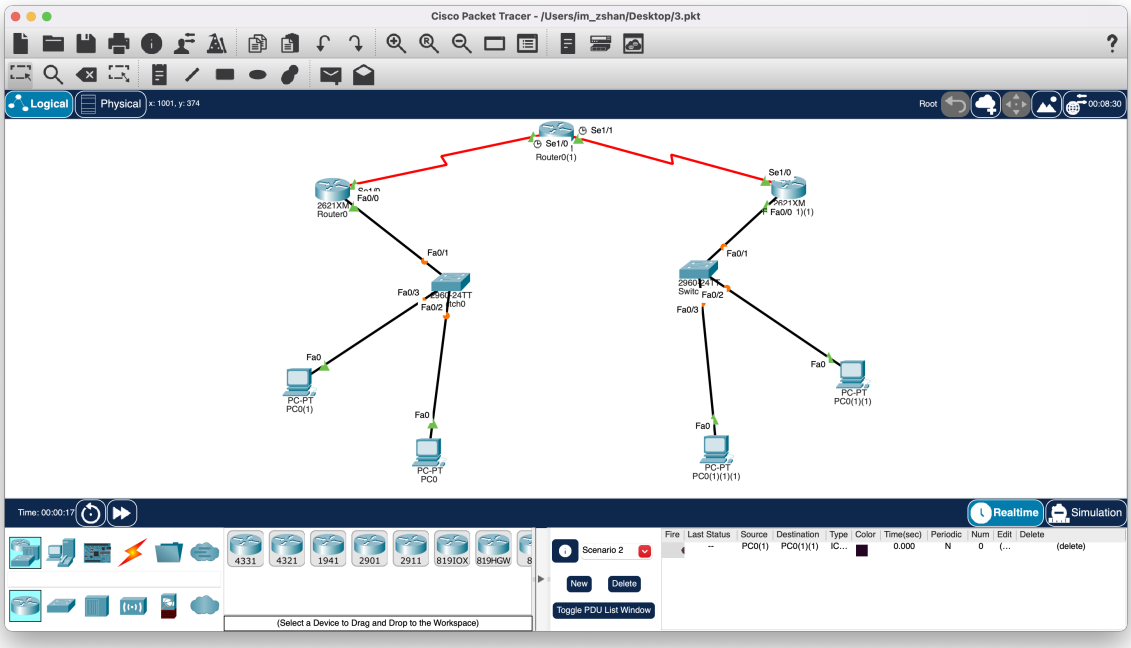
2. Enter Privileged Exec Mode: Once logged in, enter privileged exec mode by typing enable and providing the privileged password. This grants you administrative privileges to make configuration changes.

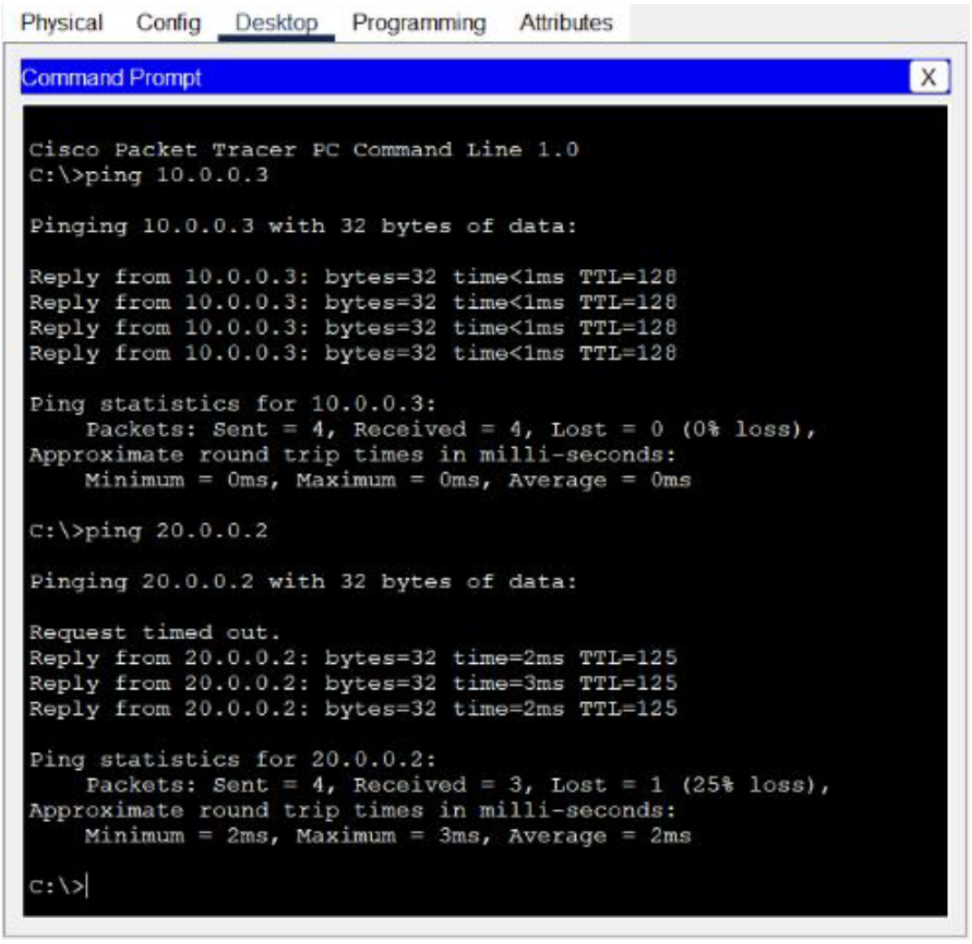
3. Enter Global Configuration Mode: Enter global configuration mode by typing configure terminal or simply conf t. This mode allows you to make changes to the router's configuration.

4. Define a Default Route: Configure the default route by using the ip route command. Specify the default route destination as 0.0.0.0 with a subnet mask of 0.0.0.0. Assign the next-hop IP address of the default gateway or the exit interface where the default route should be forwarded.

4. Verify and Save Configuration: Verify the configuration by entering the command show ip route to ensure that the default route entry appears in the routing table. To save the configuration, use the write memory command or its shortcut wr to save the changes to the router's running configuration to the startup configuration, which will persist after a reboot.

5. Test Connectivity: Verify the functionality of the default route by testing connectivity to destinations outside the router's directly connected networks. Send packets to remote IP addresses and ensure they are correctly forwarded to the default gateway or next-hop address.


Cisco Packet Tracer - /Users/im_zshan/Desktop/3.pkt
Logical
Physical
Root
Router0(1)
Router0
Fa0/0
Fa0/1
Fa0/2
Fa0/3
Fa0
PC-PT
PC0(1)
PC0
PC0(1)(1)
Time: 00:00:17
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
Scenario 2
New
Delete
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
PC0(1)
PC0(1)(1)
0.000
(delete)


Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3
Pinging 10.0.0.3 with 32 bytes of data:
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Ping statistics for 10.0.0.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 20.0.0.2
Pinging 20.0.0.2 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.2: bytes=32 time=2ms TTL=125
Reply from 20.0.0.2: bytes=32 time=3ms TTL=125
Reply from 20.0.0.2: bytes=32 time=2ms TTL=125
Ping statistics for 20.0.0.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>

Computer Networking Lab
(Lab 7)

Zeeshan Sharif
BITE'012

Aim - Configuring distance vector routing (Dynamic routing via RIP) on a network.

Theory
Routing plays a critical role in computer networking as it involves finding the best paths for transmitting data within a network. Dynamic routing protocols facilitate the exchange of information among routers, allowing them to update their routing tables dynamically and adapt to network changes. In this lab, our focus is on configuring distance vector routing using the Routing Information Protocol (RIP).

1. Distance Vector Routing
Distance vector routing is a type of routing algorithm used in computer networks to determine the best path for data transmission between routers. It operates based on the concept of vectors, where each router maintains a table containing the distance (or cost) to reach other routers in the network

2. Routing Information Protocol (RIP)
The Routing Information Protocol (RIP) is a distance vector routing protocol used in computer networks. It enables routers to exchange information about network topology and update their routing tables accordingly. RIP uses hop count as the metric to determine the best path for data transmission. It employs a maximum hop count limit to avoid routing loops. RIP is a simple and widely supported routing protocol, commonly used in small to medium-sized networks.

Configuration Process of Distance Vector Routing
The configuration process for Distance Vector Routing in Cisco routers involves the following steps:

1. Access the Router: Connect to the Cisco router through a console cable and a terminal emulation program like PuTTY or SecureCRT. Use the appropriate login credentials to access the router's command-line interface (CLI).

2. Enter Privileged Exec Mode: Once logged in, enter privileged exec mode by typing enable and providing the privileged password. This grants you administrative privileges to make configuration changes.

3. Enter Global Configuration Mode: Enter global configuration mode by typing configure terminal or simply conf t. This mode allows you to make changes to the router's configuration.

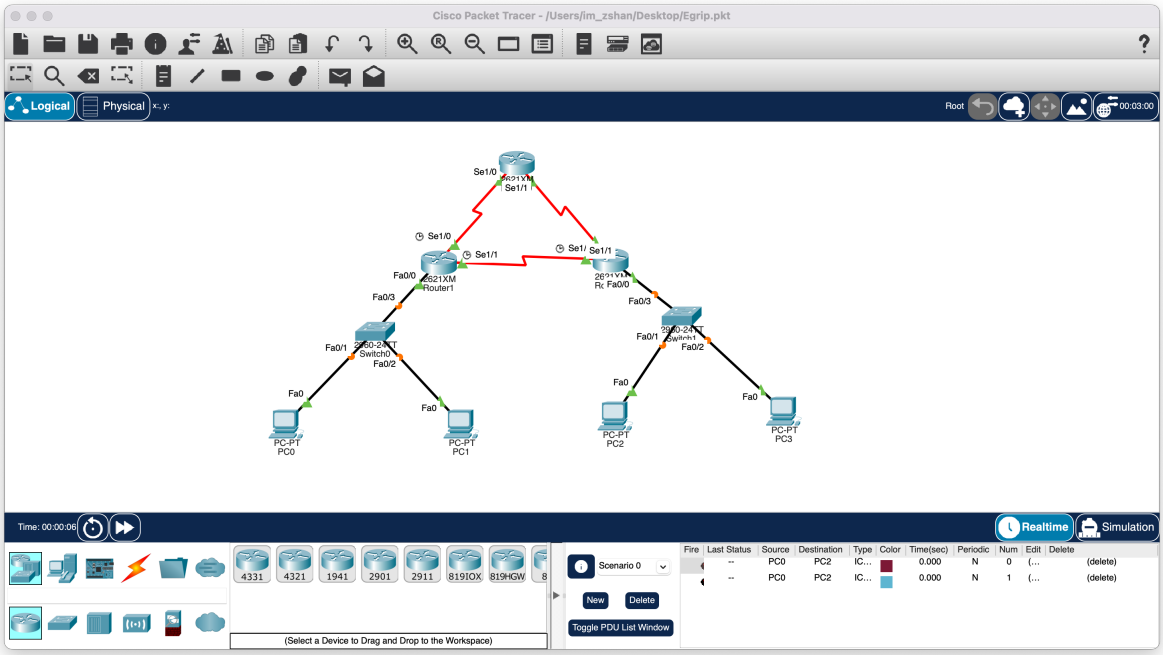
4. Enable RIP Routing: Enable RIP routing on the router by using the router rip command. This puts you into the RIP configuration mode. Here's an example command:
$ router rip

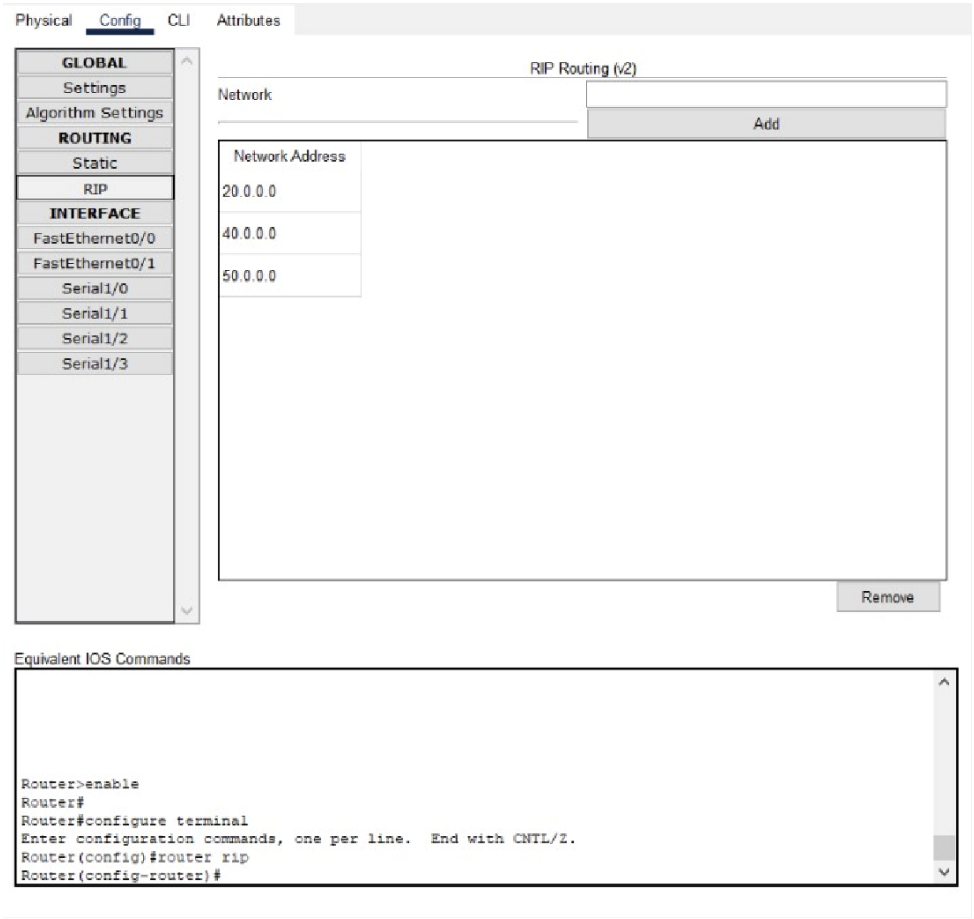
Define Network Interfaces: Specify the network interfaces that will participate in RIP routing by using the network command followed by the network address and wildcard mask. Here's an example command:
$ network 192.168.0.0

4. Verify and Save Configuration: Verify the RIP configuration by entering the command show ip protocols to ensure that RIP is enabled on the desired interfaces and networks. To save the configuration, use the write memory command or its shortcut wr to save the changes to the router's running configuration to the startup configuration, which will persist after a reboot.

5. Test Connectivity: Verify the functionality of the RIP configuration by testing connectivity between routers and networks. Ensure that routing updates are being exchanged and that routers can reach their in-

tended destinations.





Computer Networking Lab
(Lab 8)

Zeeshan Sharif
BITE'012

Aim - Implement EIGRP protocol. Introduction to traffic filtering via access lists. Configuring traffic filtering on routers via standard access list (block a host).

Theory

The Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol commonly used in computer networks. It facilitates the exchange of routing information among routers and enables efficient routing decision-making.

Access lists are employed to filter network traffic, allowing network administrators to control which packets are permitted or denied based on specific criteria. By implementing a standard access list, administrators can effectively block a particular host by specifying its IP address. This enhances network security and provides control over the flow of network traffic.

Configuration Process of EIGRP in Cisco

The configuration process for Enhanced Interior Gateway Routing Protocol (EIGRP) in Cisco routers involves the following steps:

1. Access the Router: Connect to the Cisco router through a console cable and a terminal emulation program like PuTTY or SecureCRT. Use the appropriate login credentials to access the router's command-line interface (CLI).

2. Enter Privileged Exec Mode: Once logged in, enter privileged exec mode by typing enable and providing the privileged password. This

grants you administrative privileges to make configuration changes.

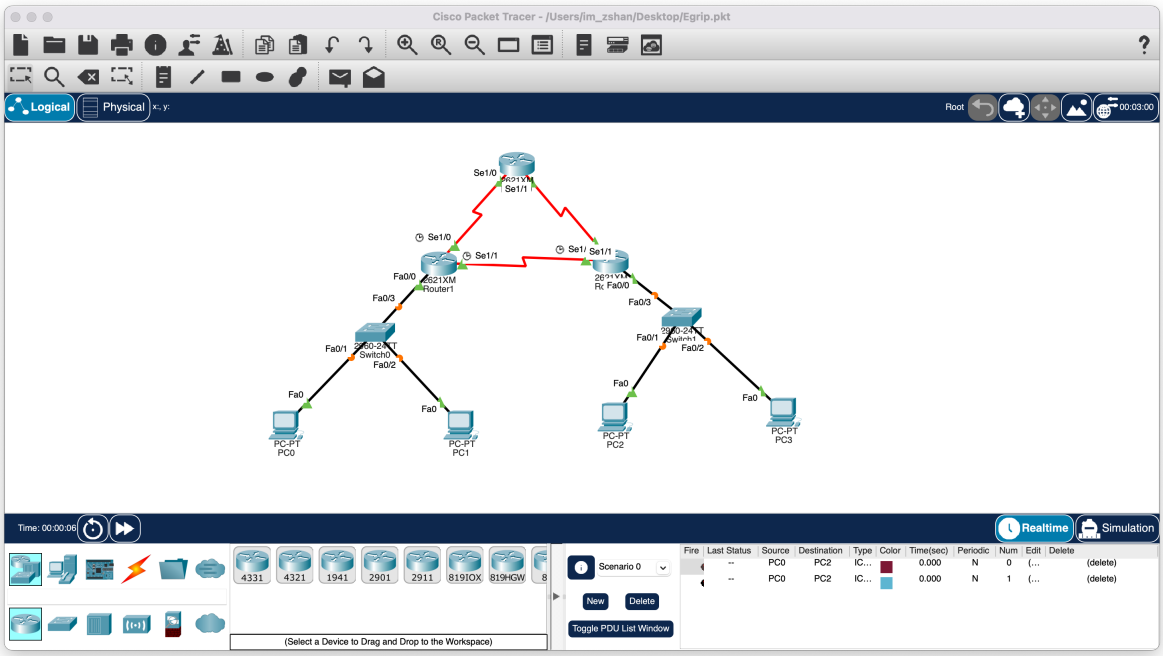
3. Enter Global Configuration Mode: Enter global configuration mode by typing configure terminal or simply conf t. This mode allows you to make changes to the router's configuration.

4. Enable EIGRP Routing: Enable EIGRP routing on the router by using the router eigrp command followed by an autonomous system (AS) number. The AS number is a unique identifier for EIGRP within your network. Here's an example command:
$ router eigrp 100

5. Define Network Interfaces: Specify the network interfaces that will participate in EIGRP routing by using the network command followed by the network address and wildcard mask. Here's an example command:
$ network 192.168.0.0 0.0.0.255

6. Verify and Save Configuration: Verify the EIGRP configuration by entering the command show ip protocols to ensure that EIGRP is enabled on the desired interfaces and networks. To save the configuration, use the write memory command or its shortcut wr to save the changes to the router's running configuration to the startup configuration, which will persist after a reboot.

7. Test Connectivity: Verify the functionality of the EIGRP configuration by testing connectivity between routers and networks. Ensure that routing updates are being exchanged and that routers can reach their intended destinations.


Cisco Packet Tracer - /Users/im_zshan/Desktop/Egrip.pkt
Logical
Physical
Root
00:03:00
Se1/0
Se1/1
Router1
Fa0/0
Fa0/3
Fa0/1
Fa0/2
Switch0
Switch1
Fa0
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Time: 00:00:06
Realtime
Simulation
4331
4321
1941
2901
2911
819IOX
819HGW
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
PC0
PC2
0.000
(delete)

Computer Networking Lab
(Lab 9)

Zeeshan Sharif
BITE'012

Aim - Configuring traffic filtering on routers via standard access lists (block full network) and extended access-list (block only HTTP port of a server).

Theory

Traffic filtering is an essential aspect of network security, enabling administrators to exercise control over network traffic based on specific criteria. Access lists (ACLs) are widely used to define rules that either permit or deny traffic at a router interface.

Standard Access Lists - Blocking a Full Network:

Standard access lists are used to filter traffic based on source IP addresses. They allow or deny entire networks or specific hosts. In this lab, we utilize a standard access list to block a full network.

Configuration Process of Standard Access List in Cisco

The configuration process for Standard Access List in Cisco routers involves the following steps:

1. Create a Standard Access List: Define a standard access list using the access-list command followed by an access list number. Specify the network IP address or subnet to be blocked using the deny statement. Here's an example command to create an access list with number 10:

2. Apply the Access List to an Interface: Apply the created access list to the appropriate interface using the interface command followed by the interface name. Then, use the ip access-group command to apply the access list

3. Verify the Traffic Filtering Configuration: Verify the effectiveness of the access list by testing network connectivity from a host within the blocked network to other destinations. Ensure that the desired traffic is being blocked and the network access is restricted as intended.

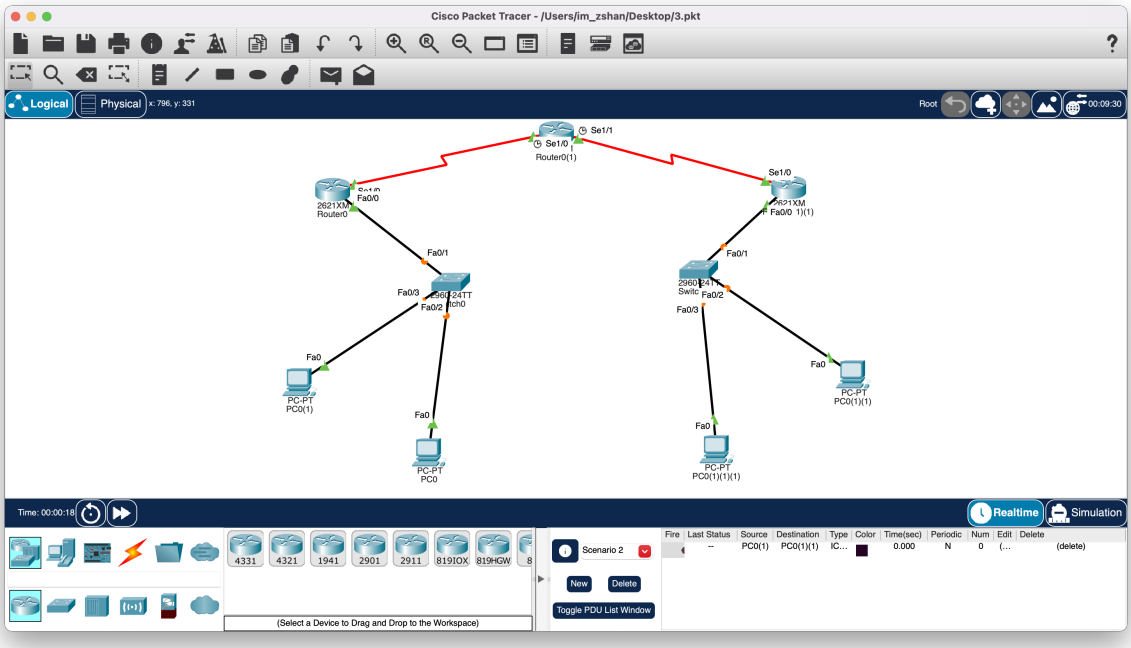
 # Extended Access Lists - Blocking Only the HTTP Port of a Server: Extended access lists provide more granular control over traffic filtering by considering source and destination IP addresses, port numbers, and protocols. In this lab, we use an extended access list to block only the HTTP port (port 80) of a server.

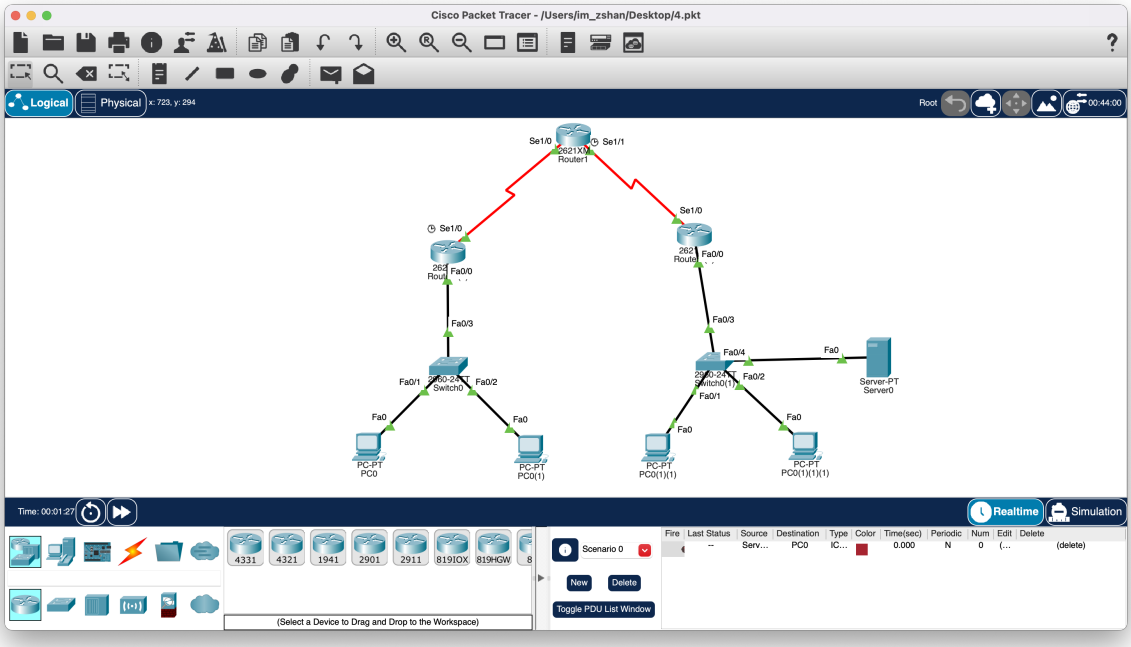
Configuration Process of Extended Access Lists in Cisco
The configuration process for Extended Access Lists in Cisco routers involves the following steps:

1. Create an extended access list: To block the HTTP port of a server, an extended access list needs to be created. This involves specifying the access list number and defining a rule that denies traffic with the source IP address of the server and the destination port number of 80 (HTTP).

2. Apply the Access List to an Interface: Once the extended access list is defined, it needs to be applied to the appropriate interface on the router. Similar to the standard access list configuration, the access-group command is used to apply the access list in the desired direction.

3. Verify the Traffic Filtering Configuration: After applying the access list, it is crucial to verify its effectiveness. This can be done by attempting to access the server's HTTP service from a client and confirming that the connection is being blocked on port 80.


Cisco Packet Tracer - /Users/im_zshan/Desktop/3.pkt
Logical
Physical
Root
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Toggle PDU List Window


Cisco Packet Tracer - /Users/im_zshan/Desktop/4.pkt
Logical
Physical
Root
Realtime
Simulation
(Select a Device to Drag and Drop to the Workspace)
Toggle PDU List Window

Computer Networking Lab
(Lab 10)

Zeeshan Sharif
BITE'012

Aim - Introduction to Ethernet, its types, specifications, UTP standards, and different cable constructions: straight-through, crossover, and rollover. Practical demonstration of creating straight-through cable.

Theory
Ethernet is a widely adopted networking technology that enables devices to communicate within a local area network (LAN). It provides a standard set of rules and protocols for transmitting data packets between computers, servers, printers, and other networked devices. Ethernet operates at the data link layer of the OSI model and utilizes a variety of physical media, such as copper cables or fiber optics, to transmit data. With its scalability, reliability, and high-speed capabilities, Ethernet has become the de facto standard for local network connectivity, supporting a wide range of applications and facilitating seamless data exchange in modern networks.

 # Types of Ethernets:

1. Ethernet (10BASE-T):
Also known as "twisted pair Ethernet," it uses unshielded twisted pair (UTP) cables to transmit data at a maximum speed of 10 Mbps. It is one of the earliest Ethernet standards and is still in use today for some legacy systems.

2. Fast Ethernet (100BASE-T):
This Ethernet standard supports data transfer rates of up to 100 Mbps. It uses UTP cables and is backward compatible with Ethernet (10BASE-T), allowing for seamless integration into existing networks.

3. Gigabit Ethernet (1000BASE-T):
Gigabit Ethernet provides data transmission speeds of up to 1 Gbps (1,000 Mbps). It uses UTP cables and is widely deployed in modern networks, offering significantly faster data transfer compared to Fast Ethernet.

 # UTP Standards!
UTP (Unshielded Twisted Pair) cables are widely used in Ethernet networking for transmitting data. Several standards define the performance characteristics of UTP cables. Here are some commonly known UTP standards:

a. Category 5e (Cat 5e): Cat 5e is an enhanced version of Category 5 (Cat 5) UTP cable. It supports data transmission at speeds up to 1 Gbps (Gigabit Ethernet) with reduced crosstalk and improved performance compared to Cat 5. Cat 5e cables are widely used in Ethernet networks.

b. Category 6 (Cat 6): Cat 6 UTP cable provides improved performance and is designed to support higher data transfer rates. It can handle data transmission at speeds up to 10 Gbps over shorter distances. Cat 6 cables have more stringent specifications for crosstalk and system noise compared to Cat 5e.

c. Category 6a (Cat 6a): Cat 6a UTP cable is an augmented version of Cat 6. It offers even higher performance and can support data transmission at speeds up to 10 Gbps over longer distances (up to 100 me-

ters). Cat 6a cables have improved crosstalk and noise resistance compared to Cat 6.

d. Category 7 (Cat 7): Cat 7 UTP cable is designed to support higher bandwidths and offer superior performance compared to previous categories. It can handle data transfer rates of up to 10 Gbps and has improved shielding to reduce interference and crosstalk.

 # Different Cable Constructions:
There are different cable constructions used in networking, each designed for specific purposes and performance requirements. Here are some common cable constructions used in networking:

1. Unshielded Twisted Pair (UTP): UTP cables consist of multiple pairs of insulated copper wires twisted together. They are widely used in Ethernet networking due to their cost-effectiveness and ease of installation. UTP cables are available in different categories, such as Cat 5e, Cat 6, and Cat 6a, with varying levels of performance and data transmission capabilities.

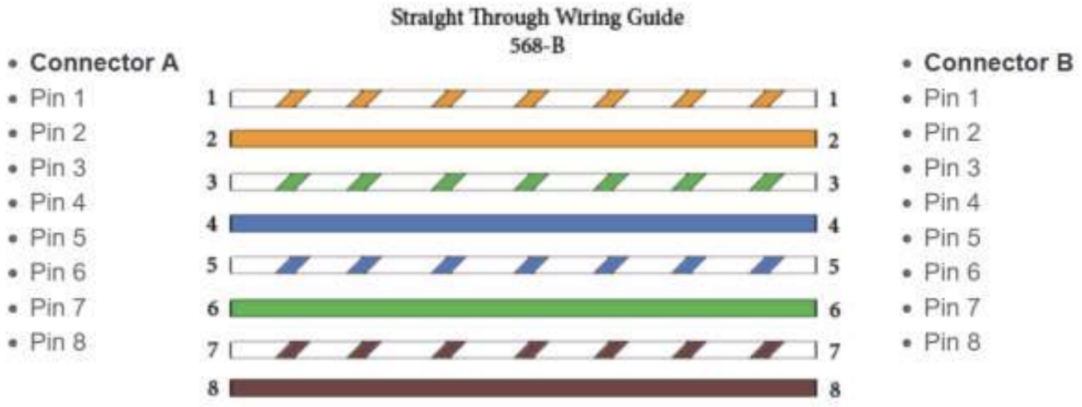
2. Shielded Twisted Pair (STP): STP cables are similar to UTP cables but have an additional layer of shielding for each twisted pair. The shielding helps reduce electromagnetic interference (EMI) and crosstalk, resulting in improved signal integrity. STP cables are commonly used in environments with higher levels of interference or where EMI protection is required.

3. Coaxial Cable: Coaxial cables consist of a central conductor surrounded by insulation, a metallic shield, and an outer jacket. They are commonly used in cable television (CATV) and broadband internet applications. Coaxial cables provide better shielding against EMI and offer higher bandwidth capabilities.

4. Fiber Optic Cable: Fiber optic cables use strands of glass or plas-

tic fibers to transmit data as pulses of light. They offer high bandwidth, long-distance transmission capabilities, and immunity to electromagnetic interference. Fiber optic cables are widely used in high-speed data networks, telecommunications, and long-haul communications.

5. Ethernet Cables with Power (PoE): Ethernet cables with Power over Ethernet (PoE) capability are designed to deliver both data and electrical power to network devices. They allow for the simultaneous transmission of data and power, eliminating the need for separate power cables for certain devices such as IP cameras, wireless access points, and VoIP phones.



Lab File Submitted to Dr. Iqra Altaf Gillani

— The End —