

**CHAROTAR UNIVERSITY OF SCIENCE and
TECHNOLOGY**

**DEVANG PATEL INSTITUTE OF ADVANCE
TECHNOLOGY and RESEARCH**

Computer Science and Engineering

Subject Name: Data Communication and Networking

Semester: III

Subject Code: CE257

Academic year: 2020-21

ID NO :19DCS098

| NO. | AIM OF PRACTICAL |
|-----|--|
| 1. | <p><u>AIM:</u></p> <p>Configuration, Management and Administration of various networking and Internetworking Devices with explanation of layers of OSI model.</p> <p><u>THEORY/PRACTICAL:</u></p> <p>The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.</p> <p>Layers in OSI MODEL:</p> <ul style="list-style-type: none"> • Physical Layer • Datalink Layer • Network Layer • Transport Layer • Session Layer • Presentation Layer • Application Layer <p><u>PHYSICAL LAYER:</u></p> <p>❖ <u>Overview:</u></p> <ul style="list-style-type: none"> ➤ The lowest layer of OSI reference model ➤ It is responsible for actual physical connection between devices ➤ It contains information in form of bits |

- It is responsible for transmitting individual bits from one node to next

❖ **Functions:**

- Bit synchronization
- Bit rate control
- Physical topologies
- Transmission mode

❖ **Devices:**

- Hub
- Repeater
- Modem

Hubs:

- Hubs are devices commonly used to connect segments of a LAN. It contains multiple input/output ports. when signal is at any input port, this signal will be made at all output ports except the one it is coming from.

• **Cables:**

- In Wired network architecture (e.g Ethernet), cables are used to interconnect the devices.
- some of the types of cables are coaxial cable, optical fiber cable, and twisted pair cable.

• **Repeaters:**

- Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters can

only amplify the signal whereas a digital repeaters can reproduce a signal to near its original quality.

Datalink Layer:

❖ Overview:

- it is responsible for node to node delivery of the message
- it ensures that data transfer is error-free
- When packet arrives in a network datalink layer transmit it to Host using MAC address
- The packet received from network layer is further divided into frames depending on the frame size of NIC

❖ Functions:

- Framing
- Physical addressing
- Error control
- Flow control
- Access control

❖ Devices:

- Switch
- Bridge

❖ Protocol Used:

- Ethernet

Bridges:

- A bridge is a type of computer network device that provides interconnection with other networks that use the same protocol, connecting two different networks together and providing communication between them.

• Modem:

- Modem stands for Modulator/Demodulator.
- A modem converts digital signals generated by the computer into analog signals which, then can be transmitted over cable line and transforms incoming analog signals into digital equivalents.

• Network Interface Card:

- Network interface card is an electronic device that is mounted on ROM of the com that connects a computer to a computer network, usually a LAN.
- It is considered a piece of computer hardware.

Network Layer:**❖ Overview:**

- Network layer works for the transmission of data from one host to the other located in different networks
- takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available

- The sender & receiver's IP address are placed in the header by the network layer.

❖ **Functions:**

- Routing
- Logical Addressing

❖ **Devices:**

- Routers

Routers:

- A router is a switch like device that routes/forwards data packets based on their IP addresses. Routers normally connect Local Area Network (LANs) and Wide Area Network (WANs) together and have a dynamically updating routing table based on which they make decisions on routing the incoming packets.

Transport Layer:

❖ **Overview:**

- Transport layer provides services to application layer and takes services from network layer.
- The data in the transport layer is referred to as Segments.
- responsible for the End to End Delivery of the complete message
- also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

❖ **Functions:**

- Segmentation
- Reassembly

- Service Point Addressing

❖ **Devices:**

- Gateways
- Firewall

Gateways:

- In computer networking, a gateway is a component that is part of two networks, which use different protocols.
- The gateway is a protocol converter which will translate one protocol into the other.

• **Firewall:**

- A firewall is a system designed to prevent unauthorized access to or from a private network, some of the functionalities of firewall are, packet filtering and as a proxy server.

Session Layer:

❖ **Overview:**

- responsible for establishment of connection, maintenance of sessions, authentication and also ensures security

❖ **Function:**

- Session establishment
- maintenance
- termination
- Synchronization

❖ **Devices:**

- Gateways

- Firewall
- PCs/Devices

Presentation Layer:

❖ Overview:

- also called the Translation layer.
- The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

❖ Functions:

- Translation
- Encryption
- Decryption
- Compression

❖ Devices:

- Gateways
- Firewalls
- PC's.

Application Layer:

❖ Overview:

- implemented by the network applications
- These applications produce the data, which has to be transferred over the network.
- serves as a window for the application services to access the network and for displaying the received information to the user.

❖ Functions:

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

❖ Devices:

- Gateways
- Firewalls
- all end devices like PC's, Phones, Servers

| NO. | AIM OF PRACTICAL |
|-----|--|
| 2. | <p><u>AIM:</u> Illustration of various networking commands:</p> <ul style="list-style-type: none"> • Ping (types of responses) • tracert/traceroute • netstat • arp • ipconfig/ifconfig • nslookup <p><u>Theory/Practical:</u> PING:</p> <ul style="list-style-type: none"> • PING stands for “Packet Internet Grouper”. • The ping command sends packets of data to a specific IP address on a network, and then lets you know how long it took to transmit that data and get a response • It can be used to check if whether your connection is alive or not To use ping: ping hostname/IP address (To stop ping press Ctrl+C) <pre> C:\Users\Parth Patel>ping google.in Pinging google.in [172.217.27.196] with 32 bytes of data: Reply from 172.217.27.196: bytes=32 time=25ms TTL=118 Reply from 172.217.27.196: bytes=32 time=25ms TTL=118 Reply from 172.217.27.196: bytes=32 time=23ms TTL=118 Reply from 172.217.27.196: bytes=32 time=25ms TTL=118 Ping statistics for 172.217.27.196: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 23ms, Maximum = 25ms, Average = 24ms </pre> |

```
C:\Users\Parth Patel>ping 172.217.17.100

Pinging 172.217.17.100 with 32 bytes of data:
Reply from 172.217.17.100: bytes=32 time=373ms TTL=105
Reply from 172.217.17.100: bytes=32 time=372ms TTL=105
Reply from 172.217.17.100: bytes=32 time=372ms TTL=105
Reply from 172.217.17.100: bytes=32 time=373ms TTL=105

Ping statistics for 172.217.17.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 372ms, Maximum = 373ms, Average = 372ms
```

Netstat:

- Netstat is derived from “Network” and “Statistics”
- It delivers basic statistics on all network activities and informs users on which ports and addresses the corresponding connections (TCP, UDP) are running and which ports are open for tasks.
- There are various options for Netstat. Some are displayed below:

| Option | Description |
|--------|--|
| -a | Displays all connections and listening ports. |
| -e | Displays Ethernet statistics. This may be combined with the -s option. |
| -n | Displays addresses and port numbers in numerical form. |
| -p | proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP. |
| -r | Displays the routing table. |
| -s | Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default. |

```
C:\Users\Parth Patel>netstat
```

Active Connections

| Proto | Local Address | Foreign Address | State |
|-------|-------------------|-----------------------|-------------|
| TCP | 127.0.0.1:59443 | DESKTOP-B4NA290:59444 | ESTABLISHED |
| TCP | 127.0.0.1:59444 | DESKTOP-B4NA290:59443 | ESTABLISHED |
| TCP | 127.0.0.1:59449 | DESKTOP-B4NA290:59450 | ESTABLISHED |
| TCP | 127.0.0.1:59450 | DESKTOP-B4NA290:59449 | ESTABLISHED |
| TCP | 127.0.0.1:59454 | DESKTOP-B4NA290:59455 | ESTABLISHED |
| TCP | 127.0.0.1:59455 | DESKTOP-B4NA290:59454 | ESTABLISHED |
| TCP | 127.0.0.1:59457 | DESKTOP-B4NA290:59458 | ESTABLISHED |
| TCP | 127.0.0.1:59458 | DESKTOP-B4NA290:59457 | ESTABLISHED |
| TCP | 127.0.0.1:63819 | DESKTOP-B4NA290:63820 | ESTABLISHED |
| TCP | 127.0.0.1:63820 | DESKTOP-B4NA290:63819 | ESTABLISHED |
| TCP | 127.0.0.1:63862 | DESKTOP-B4NA290:63863 | ESTABLISHED |
| TCP | 127.0.0.1:63863 | DESKTOP-B4NA290:63862 | ESTABLISHED |
| TCP | 192.168.2.5:51313 | 40.119.211.203:https | ESTABLISHED |
| TCP | 192.168.2.5:51589 | 74.125.24.188:5228 | ESTABLISHED |

Ipconfig/ifconfig:

- Ipconfig stands for “Internet Protocol Configuration”.
- This command is used to view all the current TCP/IP network configurations values of the computer.
- ifconfig stands for “Interface Configuration.”
- This command is the same as ipconfig, and is used to view all the current TCP/IP network configurations values of the computer.
- ipconfig/all: It gives the full configuration of the system.
- ipconfig/registerdns: This command refreshes all DHCP leases and reregisters the DNS names.
- ipconfig/displaydns: It displays the information that is stored in the DNS Resolver cache. It has all the DNS information that has been used earlier.
- ipconfig/showclassid adapter: It displays all the class id’s that are allowed for the adapter.
- ipconfig/setclassid adapter [classid]: This command is used to modify the DHCP class id.

```
C:\Users\Parth Patel>ipconfig

Windows IP Configuration

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:
```

Tracert:

- tracert stands for “Trace Route”

- Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between.
- Traceroute also records the time taken for each hop the packet makes during its route to the destination.

Options:

```
-d          Do not resolve addresses to hostnames.
-h maximum_hops  Maximum number of hops to search for target.
-j host-list     Loose source route along host-list (IPv4-only).
-w timeout      Wait timeout milliseconds for each reply.
-R            Trace round-trip path (IPv6-only).
-S srcaddr      Source address to use (IPv6-only).
-4            Force using IPv4.
-6            Force using IPv6.
```

```
C:\Users\Parth Patel>tracert google.in
```

```
Tracing route to google.in [172.217.27.196]
over a maximum of 30 hops:
```

```
  1    2 ms    2 ms    2 ms  192.168.2.1
  2   20 ms   18 ms   27 ms  100.67.0.1
  3   14 ms   21 ms   18 ms  vad-core01.youbroadband.in [203.187.193.1]
  4   27 ms   44 ms   32 ms  97-193-187-203.static.youbroadband.in [203.187.193.97]
  5   25 ms   32 ms   26 ms  142.250.160.122
  6   28 ms   31 ms   31 ms  209.85.245.11
  7   31 ms   27 ms   27 ms  216.239.56.115
  8   41 ms   55 ms   47 ms  bom07s15-in-f4.1e100.net [172.217.27.196]
```

```
Trace complete.
```

ARP:

- Arp stands for “Address Resolution Protocol”.
- This protocol is used by network nodes to match IP addresses to MAC addresses.

| Option | Description |
|-----------|---|
| -a | Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed. |
| -g | Same as -a |
| inet_addr | Specifies an internet address |
| -N | if_addr Displays the ARP entries for the network interface specified by if_addr |
| -d | Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts |
| -s | Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent |
| eth_addr | Specifies a physical address |

```
C:\Users\Parth Patel>arp -a

Interface: 192.168.2.5 --- 0x4
    Internet Address      Physical Address      Type
    192.168.2.1           00-17-7c-5d-0d-17    dynamic
    192.168.2.7           c4-95-00-e5-7e-93    dynamic
    192.168.2.255         ff-ff-ff-ff-ff-ff    static
    224.0.0.2             01-00-5e-00-00-02    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Nslookup:

- Nslookup stands for “Network Server lookup”.
- nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.

```
C:\Users\Parth Patel>nslookup google.in
Server: 66-193-187-203.static.youbroadband.in
Address: 203.187.193.66

Non-authoritative answer:
Name:    in.domain.name
Address: 78.47.226.171
Aliases: google.in.domain.name
```

Conclusion:

- By performing the above practical, we got to know about various networking commands that will be useful in networking.

| NO | AIM OF PRACTICAL |
|----|---|
| 3. | <p><u>Aim:</u> List different types of network cables. Create understanding of straight through and cross over cable using a twisted-pair cable and RJ-45 connector.</p> <p><u>Theory/Practical:</u></p> <p><u>Step 1:</u> Unroll the required length of network cable and add a little extra wire, just in case. If a boot is to be fitted, do so before stripping away the sleeve and ensure the boot faces the correct way.</p> <p><u>Step 2:</u> Carefully remove the outer jacket of the cable. Be careful when stripping the jacket as to not nick or cut the internal wiring. One good way to do this is to cut lengthwise with snips or a knife along the side of the cable, away from yourself, about an inch toward the open end. This reduces the risk of nicking the wires' insulation. Locate the string inside with the wires, or if no string is found, use the wires themselves to unzip the sheath of the cable by holding the sheath in one hand and pulling sideways with the string or wire. Cut away the unzipped sheath and cut the twisted pairs about 1 1/4" (30 mm). You will notice 8 wires twisted in 4 pairs. Each pair will have one wire of a certain colour and another wire that is white with a coloured stripe matching its partner (this wire is called a tracer)</p> <p><u>Step 3:</u> Inspect the newly revealed wires for any cuts or scrapes that expose the copper wire inside. If you have breached the protective sheath of any wire, you will need to cut</p> |

the entire segment of wires off and start over at step one. Exposed copper wire will lead to cross-talk, poor performance or no connectivity at all. It is important that the jacket for all network cables remain intact.

Step 4:

Untwist the pairs so they will lay flat between your fingers. The white piece of thread can be cut off even with the jacket and disposed (see Warnings). For easier handling, cut the wires so that they are 3/4" (19 mm) long from the base of the jacket and even in length.

Step 5:

Arrange the wires based on the wiring specifications you are following. There are two methods one is 568A and second is 568B. Which one you use will depend on what is being connected. A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC). Two like devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568B, while a crossover cable has one end wired 568A and the other end wired 568B. For our demonstration in the following steps, we will use 568B, but the instructions can easily be adapted to 568A.

Step 6:

Press all the wires flat and parallel between your thumb and forefinger. Verify the colours have remained in the correct order. Cut the top of the wires even with one another so that they are 1/2" (12.5 mm) long from the base of the jacket, as the jacket needs to go into the 8P8C connector by about 1/8", meaning that you only have a 1/2"

of room for the individual cables. Leaving more than 1/2" untwisted can jeopardize connectivity and quality. Ensure that the cut leaves the wires even and clean; failure to do so may cause the wire not to make contact inside the jack and could lead to wrongly guided cores inside the plug.

Step 7:

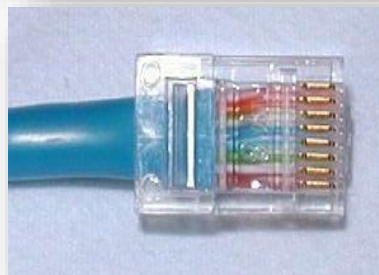
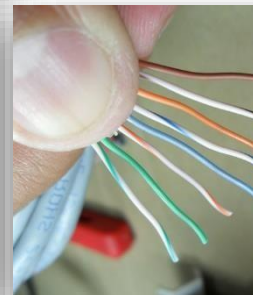
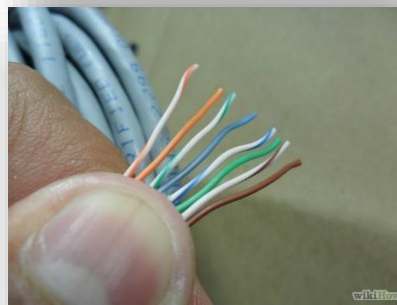
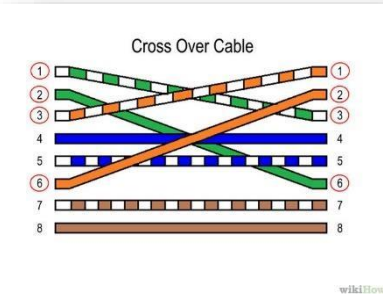
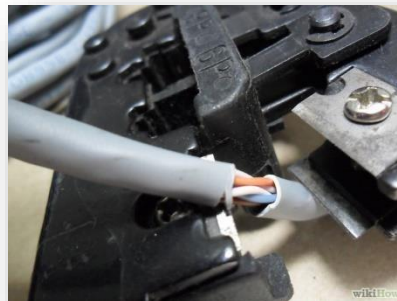
Keep the wires flat and in order as you push them into the RJ-45 plug with the flat surface of the plug on top. The white/orange wire should be on the left if you're looking down at the jack. You can tell if all the wires made it into the jack and maintain their positions by looking head-on at the plug. You should be able to see a wire located in each hole, as seen at the bottom right. You may have to use a little effort to push the pairs firmly into the plug. The cabling jacket should also enter the rear of the jack about 1/4" (6 mm) to help secure the cable once the plug is crimped. You may need to stretch the sleeve to the proper length. Verify that the sequence is still correct before

Step 8:

Place the wired plug into the crimping tool. Give the handle a firm squeeze. You should hear a ratcheting noise as you continue. Once you have completed the crimp, the handle will reset to the open position. To ensure all pins are set, some prefer to double-crimp by repeating the step.

Step 9:

Repeat all of the above steps with the other end of the cable. The way you wire the other end (568A or 568B) will depend on whether you're making a straight-through, rollover, or crossover cable.

Output:

Question-Answers:

1) Explain RJ- 45 connector and crimping tool ?

- **RJ-45 connector** - RJ-45 connectors - They usually come in bags of 50, 100 etc. and cost less than a quarter each. Pay attention to the type of RJ-45 connector you get and make sure it is intended for the type of Cat5 wire you're using. There are two different kind of RJ-45 connectors, depending on whether you use them with solid or stranded wire cable as mentioned above. Using the wrong kind with the wrong cable will most likely result in a bad connection.
- **RJ-45 crimping tool** - Crimping tool - While this is the expensive part of making your own cables, it's only a one-time startup cost. They run anywhere from 10 to 50 bucks depending on the quality and features. Keep in mind that the crimpers will pay for themselves after you make a few cables. A good crimping tool has a pair of wire cutters built in, as well as a blade to strip insulation. It also might support crimping of other connectors such as RJ-11.



2) Give difference between straight through and cross over cable?

A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC). Two like devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568B, while a cross-over cable has one end wired 568A and the other end wired 568B

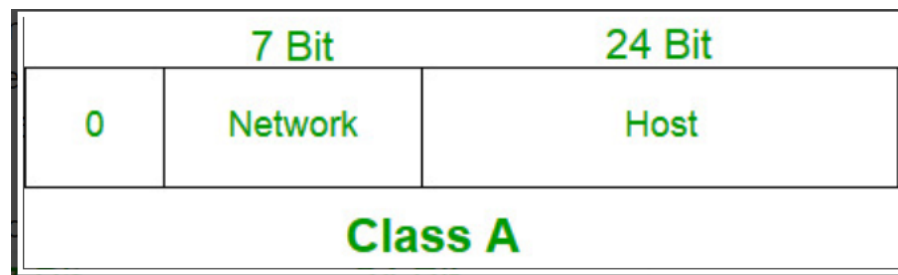
| Straight through Cable (pc to hub) | | Cross over cable (pc to pc) | |
|---|-------------------|--|-------------------|
| <i>Sequence-1</i> | <i>Sequence-2</i> | <i>Sequence-1</i> | <i>Sequence-2</i> |
| Orange White | Orange White | Orange White | Green White |
| Orange | Orange | Orange | Green |
| Green White | Green White | Green White | Orange White |
| Blue | Blue | Blue | Blue |
| Blue White | Blue White | Blue White | Blue White |
| Green | Green | Green | Orange |
| Brown White | Brown White | Brown White | Brown White |
| Brown | Brown | Brown | Brown |

| | |
|--|---|
| | <p><u>Conclusion:</u></p> <ul style="list-style-type: none">• In this practical, we came to know about making a 568B cable for connection. |
|--|---|

| NO. | AIM OF PRACTICAL | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|---|---------|---------|---------|--------|--------|---------|--------|---------|--|--|---------|--------|--|---------|--|---------|--------|--|--|---------|---------|-------------------|--|--|--|---------|----------|--|--|--|
| 4. | <p><u>AIM:</u> Work on Classful Addressing in IPv4, Network Address, Broadcast Address in each Class.</p> <p><u>PRACTICAL/THEORY:</u></p> <ul style="list-style-type: none">IP address is an address having information about how to reach a specific host, especially outside the LAN.An IP address is a 32 bit unique address having an address space of 2³². <p>IP Addressing is two types:</p> <ul style="list-style-type: none">Classless addressingClassful addressing <p>Classful Addressing:</p> <ul style="list-style-type: none">The 32-bit IP Address is divided into five sub-classes.They are as follows:<ul style="list-style-type: none">Class AClass BClass CClass DClass E <div><table><tr><td></td><td>Byte 1</td><td>Byte 2</td><td>Byte 3</td><td>Byte 4</td></tr><tr><td>Class A</td><td>NET ID</td><td colspan="3">HOST ID</td></tr><tr><td>Class B</td><td colspan="2">NET ID</td><td colspan="2">HOST ID</td></tr><tr><td>Class C</td><td colspan="3">NET ID</td><td>HOST ID</td></tr><tr><td>Class D</td><td colspan="4">MULTICAST ADDRESS</td></tr><tr><td>Class E</td><td colspan="4">RESERVED</td></tr></table></div> | | Byte 1 | Byte 2 | Byte 3 | Byte 4 | Class A | NET ID | HOST ID | | | Class B | NET ID | | HOST ID | | Class C | NET ID | | | HOST ID | Class D | MULTICAST ADDRESS | | | | Class E | RESERVED | | | |
| | Byte 1 | Byte 2 | Byte 3 | Byte 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Class A | NET ID | HOST ID | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Class B | NET ID | | HOST ID | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Class C | NET ID | | | HOST ID | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Class D | MULTICAST ADDRESS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Class E | RESERVED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

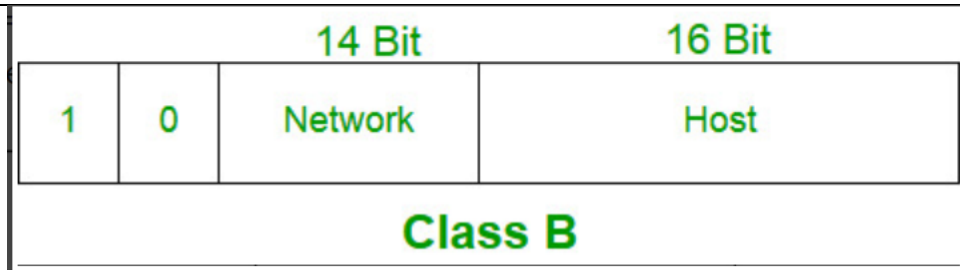
CLASS A:

- IP address belonging to class A are assigned to the networks that contain a large number of hosts
- The network ID: 8 bits
- The host ID: 24 bits
- class A has a total of:
 - $2^7 - 2 = 126$ network ID
 - $2^{24} - 2 = 16,777,214$ host ID
 - IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x



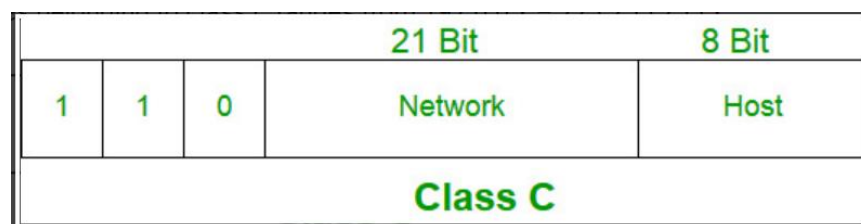
Class B:

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks
- The network ID: 16 bits
- The host ID: 16 bits
- Class B has a total of:
 - $2^{14} = 16384$ network address
 - $2^{16} - 2 = 65534$ host address
 - IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.



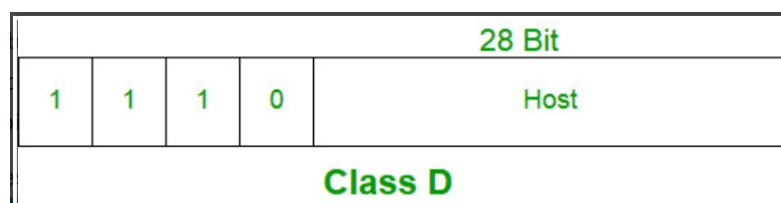
Class C:

- IP address belonging to class C are assigned to small-sized networks
- The network ID: 24 bits
- The host ID: 8 bits
 - $2^{21} = 2097152$ network address
 - $2^8 - 2 = 254$ host address
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x



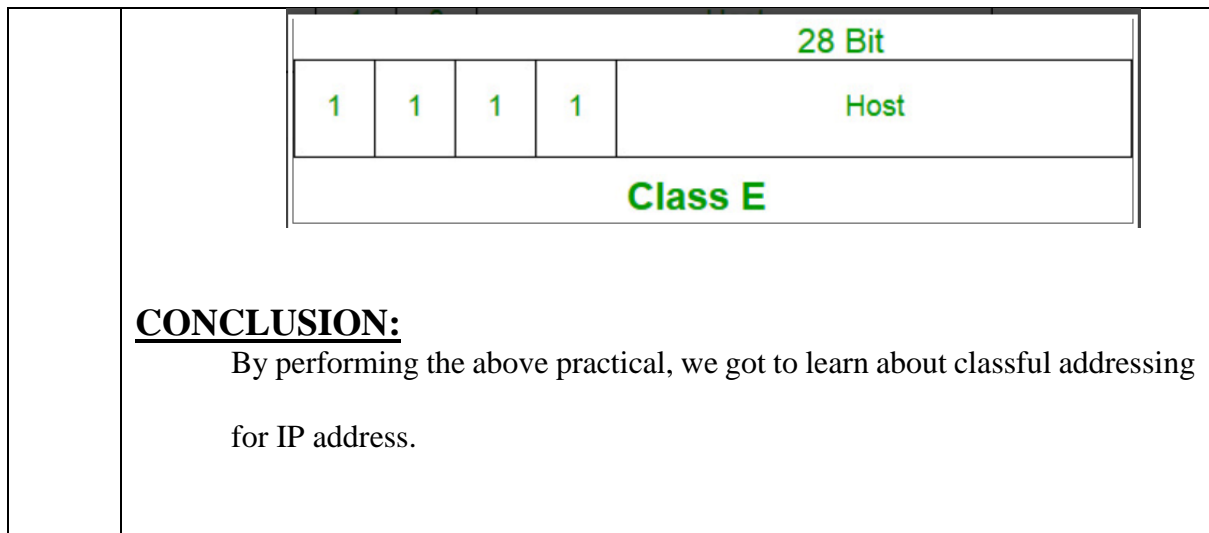
Class D:

- IP address belonging to class D are reserved for multi-casting.
- Class D does not possess any sub-net mask
- IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E:

- IP addresses belonging to class E are reserved for experimental and research purposes
- IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254



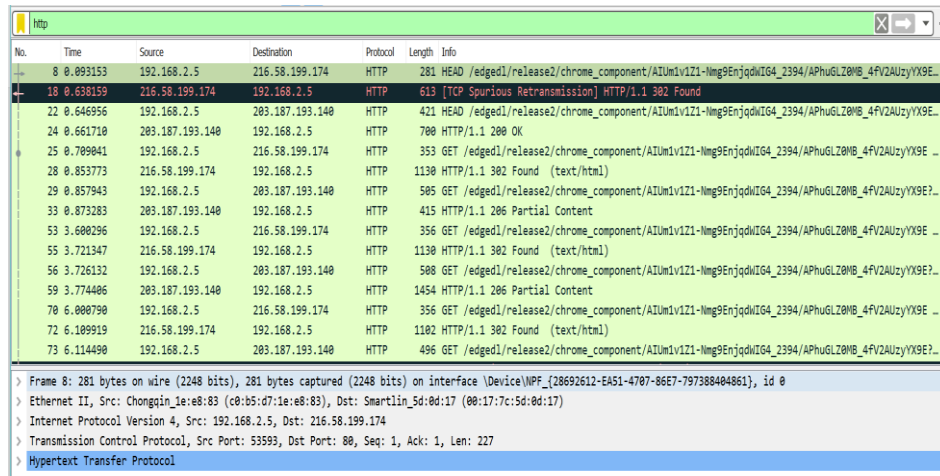
| NO. | AIM OF PRACTICAL |
|-----|---|
| 5. | <p><u>AIM:</u> Understand basic networking concept using Wireshark. Use of different Wireshark Display Filters.</p> <p><u>PRACTICAL/THEORY:</u></p> <ul style="list-style-type: none"> • Wire shark is a free and open source packet analyser. • It is used for network troubleshooting, analysis, software and communications protocol development, and education. <p><u>USAGE:</u></p> <ul style="list-style-type: none"> • Network administrators use it to troubleshoot network problems • Network security engineers use it to examine security problems <p><u>FEATURES:</u></p> <ul style="list-style-type: none"> • Live capture and offline analysis • Live capture and offline analysis • The most powerful display filters in the industry • Coloring rules can be applied to the packet list for quick, intuitive analysis • Output can be exported to XML, PostScript®, CSV, or plain text <p><u>PROS and CONS:</u></p> <p><u>PROS:</u></p> <ul style="list-style-type: none"> • Captures all kinds of packet data in network traffic • Save & restore captured packed data • Show errors and issues in levels below the HTTP protocol <p><u>CONS:</u></p> <ul style="list-style-type: none"> • Can't modify or manipulate things/data on the network (only records data) |

- A better interface would be nice - it's functional as-is, but it could use some polish

DIFFERENT FILTERS:

HTTP:

- HTTP stands for “Hyper Text transfer Protocol”
- To capture it in wireshark, apply http filter and you can see all http packages

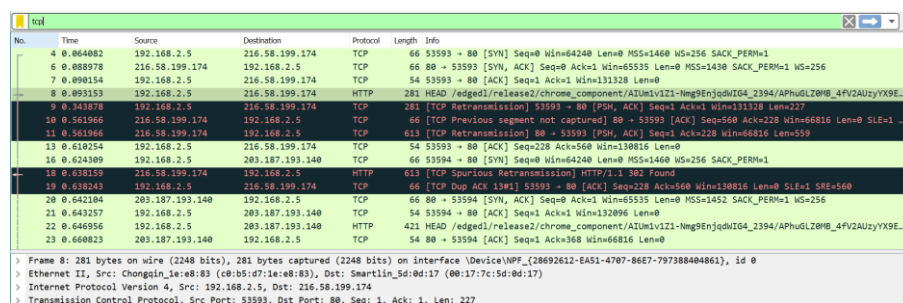


| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|--|
| 8 | 0.093153 | 192.168.2.5 | 216.58.199.174 | HTTP | 281 | HEAD /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 18 | 0.638159 | 216.58.199.174 | 192.168.2.5 | HTTP | 613 | [TCP Spurious Retransmission] HTTP/1.1 302 Found |
| 22 | 0.646956 | 192.168.2.5 | 203.187.193.140 | HTTP | 421 | HEAD /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 24 | 0.661710 | 203.187.193.140 | 192.168.2.5 | HTTP | 700 | HTTP/1.1 200 OK |
| 25 | 0.709041 | 192.168.2.5 | 216.58.199.174 | HTTP | 353 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 28 | 0.853773 | 216.58.199.174 | 192.168.2.5 | HTTP | 1130 | HTTP/1.1 302 Found (text/html) |
| 29 | 0.857943 | 192.168.2.5 | 203.187.193.140 | HTTP | 505 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E? |
| 33 | 0.873283 | 203.187.193.140 | 192.168.2.5 | HTTP | 415 | HTTP/1.1 206 Partial Content |
| 53 | 3.600296 | 192.168.2.5 | 216.58.199.174 | HTTP | 356 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 55 | 3.721347 | 216.58.199.174 | 192.168.2.5 | HTTP | 1130 | HTTP/1.1 302 Found (text/html) |
| 56 | 3.726132 | 192.168.2.5 | 203.187.193.140 | HTTP | 508 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E? |
| 59 | 3.774406 | 203.187.193.140 | 192.168.2.5 | HTTP | 1454 | HTTP/1.1 206 Partial Content |
| 70 | 6.000790 | 192.168.2.5 | 216.58.199.174 | HTTP | 356 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 72 | 6.109919 | 216.58.199.174 | 192.168.2.5 | HTTP | 1102 | HTTP/1.1 302 Found (text/html) |
| 73 | 6.114490 | 192.168.2.5 | 203.187.193.140 | HTTP | 496 | GET /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E? |

> Frame 8: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface \Device\NPF_{28692612-EA51-4707-86E7-797388404861}, id 0
 > Ethernet II, Src: Chonglin_1e:e8:83 (c0:b5:d7:1e:e8:83), Dst: Smartlin_5d:0d:17 (00:17:7c:5d:0d:17)
 > Internet Protocol Version 4, Src: 192.168.2.5, Dst: 216.58.199.174
 > Transmission Control Protocol, Src Port: 53593, Dst Port: 80, Seq: 1, Ack: 1, Len: 227
 > Hypertext Transfer Protocol

TCP:

- TCP stands for “Transmission Control protocol”
- Apply tcp filter and then you can see the Tcp packages



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|----------|--------|--|
| 4 | 0.064002 | 192.168.2.5 | 216.58.199.174 | TCP | 66 | 53593 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 6 | 0.068978 | 216.58.199.174 | 192.168.2.5 | TCP | 66 | 80 → 53593 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256 |
| 7 | 0.090154 | 192.168.2.5 | 216.58.199.174 | TCP | 54 | 53593 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 8 | 0.093153 | 192.168.2.5 | 216.58.199.174 | HTTP | 281 | HEAD /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 9 | 0.093153 | 192.168.2.5 | 216.58.199.174 | TCP | 22 | [TCP Retransmission] 53593 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=227 |
| 11 | 0.561966 | 216.58.199.174 | 192.168.2.5 | TCP | 66 | [TCP Previous segment not captured] 80 → 53593 [ACK] Seq=500 Ack=228 Win=66816 Len=0 SLE=1 |
| 13 | 0.610254 | 192.168.2.5 | 216.58.199.174 | TCP | 613 | [TCP Retransmission] 80 → 53593 [PSH, ACK] Seq=1 Ack=228 Win=66816 Len=559 |
| 16 | 0.624309 | 192.168.2.5 | 203.187.193.140 | TCP | 54 | 53593 → 80 [ACK] Seq=228 Ack=560 Win=130816 Len=0 |
| 18 | 0.632157 | 192.168.2.5 | 203.187.193.140 | TCP | 66 | 53594 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 19 | 0.630245 | 192.168.2.5 | 216.58.199.174 | HTTP | 613 | [TCP Spurious Retransmission] HTTP/1.1 302 Found |
| 20 | 0.642104 | 203.187.193.140 | 192.168.2.5 | TCP | 66 | 80 → 53594 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 WS=256 |
| 21 | 0.643257 | 192.168.2.5 | 203.187.193.140 | TCP | 54 | 53594 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0 |
| 22 | 0.646956 | 192.168.2.5 | 203.187.193.140 | HTTP | 421 | HEAD /edgedl/release2/chrome_component/AIUm1v1Z1-nmg9EnjqdwIG4_2394/APhuGLZ0NB_4FV2AUzyYX9E... |
| 23 | 0.660823 | 203.187.193.140 | 192.168.2.5 | TCP | 54 | 80 → 53594 [ACK] Seq=1 Ack=368 Win=66816 Len=0 |

> Frame 8: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface \Device\NPF_{28692612-EA51-4707-86E7-797388404861}, id 0
 > Ethernet II, Src: Chonglin_1e:e8:83 (c0:b5:d7:1e:e8:83), Dst: Smartlin_5d:0d:17 (00:17:7c:5d:0d:17)
 > Internet Protocol Version 4, Src: 192.168.2.5, Dst: 216.58.199.174
 > Transmission Control Protocol, Src Port: 53593, Dst Port: 80, Seq: 1, Ack: 1, Len: 227

UDP:

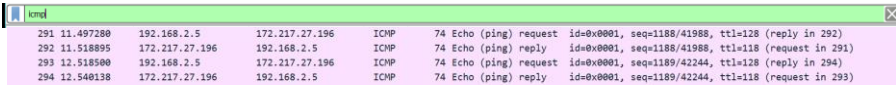
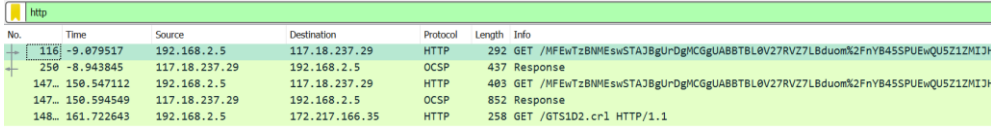
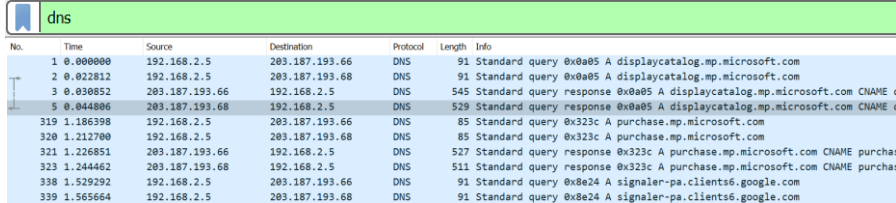
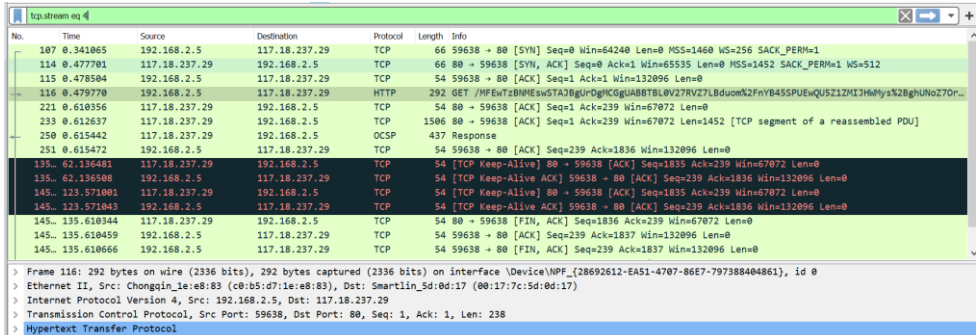
- UDP stands for “User Defined Protocol”
- Apply tcp filter and then you can see the udp packages

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 1 | 0.000000 | 192.168.2.5 | 203.187.193.66 | DNS | 79 | Standard query 0x780f A redirector.gvt1.com |
| 2 | 0.004524 | 192.168.2.5 | 203.187.193.68 | DNS | 79 | Standard query 0x780f A redirector.gvt1.com |
| 3 | 0.002157 | 203.187.193.66 | 192.168.2.5 | DNS | 350 | Standard query response 0x780f A redirector.gvt1.com A 216.58.199.174 NS ns2.google.com NS... |
| 4 | 0.073304 | 203.187.193.68 | 192.168.2.5 | DNS | 350 | Standard query response 0x780f A redirector.gvt1.com A 172.217.168.206 NS ns1.google.com NS... |
| 5 | 0.568850 | 192.168.2.5 | 203.187.193.66 | DNS | 94 | Standard query 0xb9c0 A r1---sn-tv8gv5qc5o-cq9e.gvt1.com |
| 6 | 0.611773 | 192.168.2.5 | 203.187.193.68 | DNS | 94 | Standard query 0xb9c0 A r1---sn-tv8gv5qc5o-cq9e.gvt1.com |
| 7 | 0.622415 | 203.187.193.66 | 192.168.2.5 | DNS | 403 | Standard query response 0xb9c0 A r1---sn-tv8gv5qc5o-cq9e.gvt1.com CNAME r1.sn-tv8gv5qc5o... |
| 8 | 0.633108 | 203.187.193.68 | 192.168.2.5 | DNS | 403 | Standard query response 0xb9c0 A r1---sn-tv8gv5qc5o-cq9e.gvt1.com CNAME r1.sn-tv8gv5qc5o... |
| 9 | 1.673072 | 192.168.2.3 | 192.168.2.255 | UDP | 77 | 55864 → 15600 Len=35 |
| 10 | 6.372564 | 192.168.2.5 | 216.58.196.68 | UDP | 319 | 54926 → 443 Len=277 |
| 11 | 6.486444 | 216.58.196.68 | 192.168.2.5 | UDP | 68 | 443 → 54926 Len=26 |
| 12 | 6.486444 | 216.58.196.68 | 192.168.2.5 | UDP | 185 | 443 → 54926 Len=63 |
| 13 | 6.486604 | 216.58.196.68 | 192.168.2.5 | UDP | 68 | 443 → 54926 Len=26 |
| 14 | 6.493022 | 192.168.2.5 | 216.58.196.68 | UDP | 75 | 54926 → 443 Len=33 |
| 15 | 6.493919 | 192.168.2.5 | 203.187.193.66 | DNS | 70 | Standard query 0xdb2b A google.com |

> Frame 5: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface \Device\NPF_{28692612-EA51-4707-B6E7-797388404861}, id 0
 > Ethernet II, Src: Smartlin_56:8d:17 (00:17:7c:5d:8d:17), Dst: Chongqin_1e:e8:83 (c8:b5:d7:1e:e8:83)
 > Internet Protocol Version 4, Src: 203.187.193.68, Dst: 192.168.2.5
 > User Datagram Protocol, Src Port: 53, Dst Port: 59626
 > Domain Name System (response)

CONCLUSION:

By performing the above practical, we got to know about basics of Wireshark and different filters that can be used for capturing and for analysis

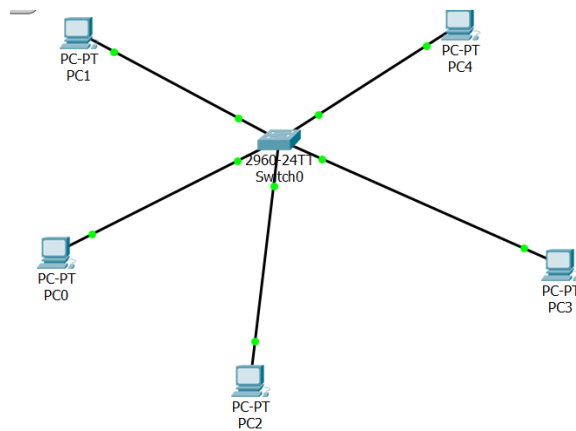
| NO. | AIM OF PRACTICAL |
|-----|---|
| 6. | <p>AIM: Capture HTTP & ICMP Traffic using Wireshark. 2. Understand DNS packet format through captured Traffic. 3. Follow TCP/UDP Stream to look inside packet</p> <p>ICMP:</p>  <p>HTTP:</p>  <p>DNS:</p>  <p> > User Datagram Protocol, Src Port: 53, Dst Port: 49773 v Domain Name System (response) Transaction ID: 0x0a05 > Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 4 Authority RRs: 10 Additional RRs: 5 </p> <p>UDP/TCP:</p>  |

30

| NO. | AIM OF PRACTICAL |
|-----|---|
| 7. | <p><u>AIM:</u> Understand basic configuration (Password/Switch name/time) of Switch using Packet Tracer CLI & Actual Device. Create Star topology</p> <p><u>THEORY/PRACTICAL:</u></p> <ul style="list-style-type: none"> • A star topology is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch • Main Controller in star topology is Switch. • Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. • Switch is operated on Data link layer. • In this packet filtering is available. • It is type of full duplex transmission mode and it is also called efficient bridge. <p><u>STEPS:</u></p> <ul style="list-style-type: none"> • Select Switch and click on it. • Then open CLI • Perform the following steps |

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Switch(config)#hostname switch-1
switch-1(config)#enable password 1234
switch-1(config)#service password-encryption
switch-1(config)#banner motd "Invalid USer"
switch-1(config)#line console 0
switch-1(config-line)#password 8980
switch-1(config-line)#login
switch-1(config-line)#exit
```

- After following the above steps
- Connect the PCs shown in the image
- Also, Configure their IP address
- Test the connection by PING test.

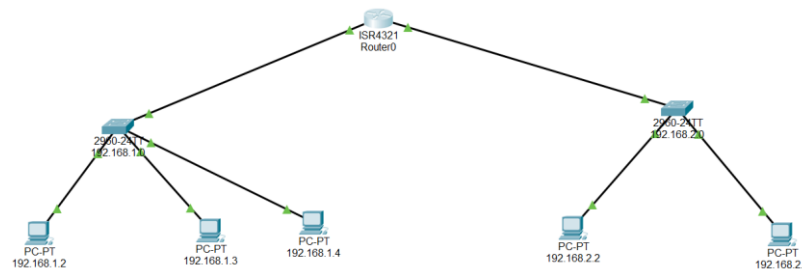


| | |
|--|--|
| | <pre> C:\>ping 192.168.1.4 Pinging 192.168.1.4 with 32 bytes of data: Reply from 192.168.1.4: bytes=32 time=11ms TTL=128 Reply from 192.168.1.4: bytes=32 time<1ms TTL=128 Reply from 192.168.1.4: bytes=32 time=11ms TTL=128 Reply from 192.168.1.4: bytes=32 time=5ms TTL=128 Ping statistics for 192.168.1.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 11ms, Average = 6ms </pre> <p><u>CONCLUSION:</u> By performing the practical, we learned about basic configuration of switch and also how to create star topology in Cisco Packet Tracer</p> |
|--|--|

| NO. | AIM OF PRACTICAL |
|-----|---|
| 8. | <p><u>AIM:</u> Static routing configuration using Cisco Packet Tracer</p> <p><u>PRACTICAL/STEPS:</u></p> <ul style="list-style-type: none"> • Take 5 Host and configure their respective IP address. • Then take two switches. • To one switch connect 3 hosts and to other connect the remaining with the wires. • Configure the Switch name and wait for 10-15 seconds so that switch and hosts establish connections. • Then run ping tests to check if the switch and hosts are properly working. • Then take one router. • Connect the router with the two switches with the wires. |

- Then do the necessary IP configuration in the router so it acts as a gateway for the switches.
- Then set the default gateway in all the hosts and check if the topology is working or not.

OUTPUT:



```

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=11ms TTL=128
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=6ms TTL=128
Reply from 192.168.2.2: bytes=32 time=4ms TTL=128
Reply from 192.168.2.2: bytes=32 time=4ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 3ms
  
```

PING test for switch-1(192.168.1.0)

PING test for switch-2(192.168.2.0)

```

C:\>ping 192.168.2.2

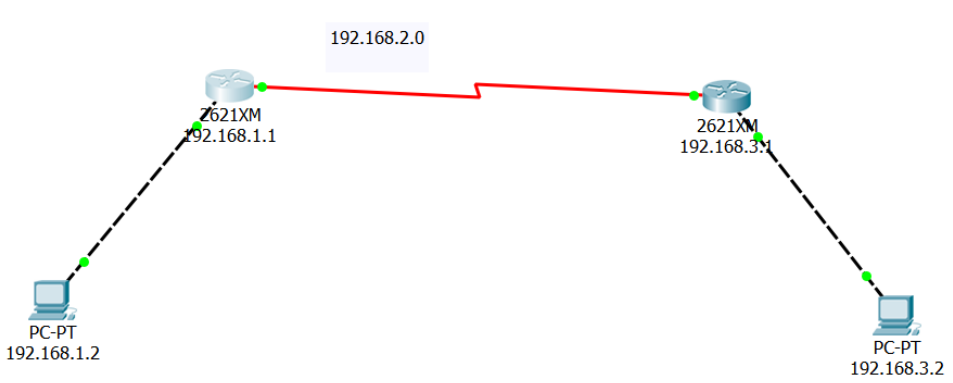
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=11ms TTL=127
Reply from 192.168.2.2: bytes=32 time=16ms TTL=127
Reply from 192.168.2.2: bytes=32 time=16ms TTL=127
Reply from 192.168.2.2: bytes=32 time=23ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 23ms, Average = 16ms
  
```

PING test to check if router works as a gateway

| | |
|--|---|
| | <p><u>CONCLUSION:</u></p> <p>Thus, above shown is the procedure to connect devices to switch and to the routers using CISCO packet tracer.</p> |
|--|---|

| NO . | AIM OF PRACTICAL |
|---------|--|
| 9. | <p>AIM: Configuration of Wireless Router using CLI and create traffic in Three LAN Architecture using Cisco Packet Tracer.</p> <p>PRACTICAL/THEORY:</p> <ul style="list-style-type: none"> Firstly, take two PCs and two router and then, connect them. Switch-off both the routers and add WIC-1T card to both and again switch on the routers Then configure both the routers using CLI so that they can get connected wirelessly <pre> Router>en Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R0 R0(config)#int f0/0 R0(config-if)#ip add % Incomplete command. R0(config-if)#ip add 192.168.1.1 255.255.255.0 R0(config-if)#no shut R0(config-if)# %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up R0(config)#int s0/0 R0(config-if)#ip add 192.168.2.1 255.255.255.2 Bad mask 0xFFFFF02 for address 192.168.2.1 R0(config-if)#ip add 192.168.2.1 255.255.255.252 R0(config-if)# no shut %LINK-5-CHANGED: Interface Serial0/0, changed state to down R0(config-if)#int s0/0 R0(config-if)#clock rate 64000 R0(config-if)#exit R0(config)# %LINK-5-CHANGED: Interface Serial0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up </pre> <ul style="list-style-type: none"> Then assign IP address and Default gateway to both PCs Run ping test  |

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=9ms TTL=126
Reply from 192.168.1.2: bytes=32 time=7ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 4ms
```

CONCLUSION:

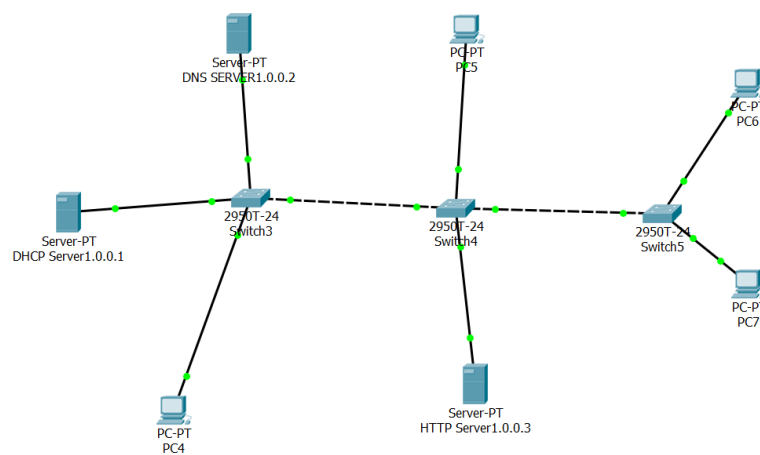
By performing the above practical, we got to know how we can configure wireless connection between two networks

| NO. | AIM OF PRACTICAL |
|-----|--|
| 11. | <p><u>AIM:</u> Configure DHCP, DNS and HTTP services using single Server in Cisco packet tracer</p> <p><u>THEORY/PRACTICAL:</u></p> <p>SWITCH:</p> <p>Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on Data link layer. In this packet filtering is available. It is type of full duplex transmission mode and it is also called efficient bridge</p> <p>HTTP SERVER:</p> <p>An HTTP server is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages). An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device</p> <p>DNS SERVER:</p> <p>DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested</p> <p>DHCP SERVER:</p> |

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.

Steps:

- First, take 3 switches, 4 PCs, 3 Generic Servers
- Then configure one server as HTTP server, second DNS server and last one as DHCP
- When all servers are configured with each other, now we assign the IP address to the PCs using
- DHCP Server
- Test the Network



Physical Config Services Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

DHCP

Interface

FastEthernet0

Service

☒ On ☐ Off

Pool Name

serverPool

Default Gateway

0.0.0.0

DNS Server

0.0.0.0

Start IP Address :

1

0

0

0

Subnet Mask:

255

0

0

0

Maximum Number of Users :

512

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max Jse | TFTP Server | WLC Address |
|--------------|-----------------|------------|------------------|-------------|---------|-------------|-------------|
| serverPool-1 | 0.0.0.0 | 0.0.0.0 | 1.0.0.0 | 255.0.... | 512 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 1.0.0.0 | 255.0.... | 512 | 0.0.0.0 | 0.0.0.0 |

IP Configuration

IP Configuration

☒ DHCP ☐ Static

IP Address

1.0.0.5

Subnet Mask

255.0.0.0

Default Gateway

0.0.0.0

DNS Server

1.0.0.2

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:

[A small page](#)
[Copyrights](#)
[Image page](#)
[Image](#)

CONCLUSION:

By performing the above Practical, we learnt how to configure DHCP, DNS, HTTP server