Om Shete
THADOMAL SHAHANI TSEC ENGINEERING COLLEGE
TE C32
2103163

Assignment 2

Q.1 Write short notes on the
i) Ethernet ii) IPv6 iii) ssh

⇒

i) Ethernet

⇒

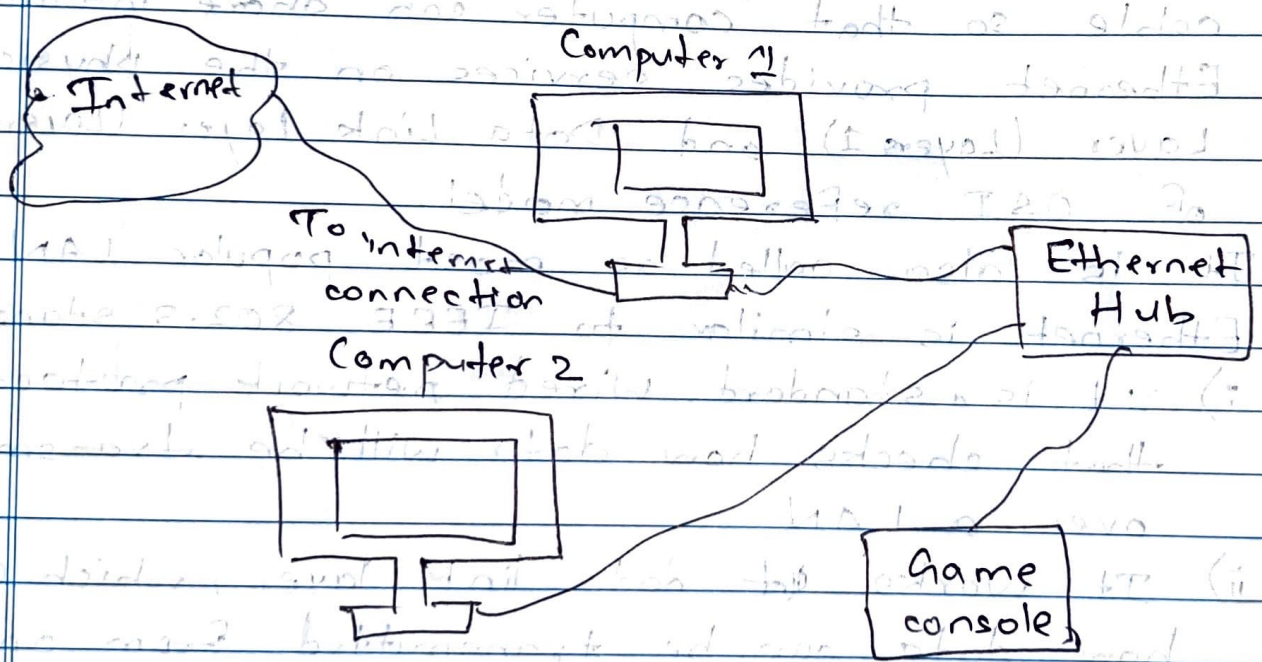
- Ethernet is a computer network technology which is used for connecting number of computers to which form a LAN.
- Ethernet connects computers together with cable so that computer can share information.
- Ethernet provides services on the physical Layer (Layers 1) and Data Link Layer (Layers 2) of OSI reference model.
- It is also called as most popular LAN.
- Ethernet is similar to IEEE 802.3 standard
  i) It is a standard wired network protocol that checks how data will be transmitted over a LAN.
  ii) It works at data link layer, which checks how data can be transmitted from one device to other device over same network segment.
- For connection Ethernet cable is inserted into the Ethernet port of our system. It can travel over speed of one Gigabyte per second.
- Ethernet is standard communication protocol embedded in software and hardware devices.

- There are two types of Ethernet Networks:
  i) Wired Ethernet Network
  ii) Wireless Ethernet.

i) Wired Ethernet

⇒

1) The ethernet technology mainly works with the fibre optic cables that connects devices within a distance of 10 km. The Ethernet supports 10 Mbps.



2) A computer network interface card (NIC) is installed in each computer, and is assigned to a unique address.
3) An Ethernet cable runs from each NIC to the central switch or hub.

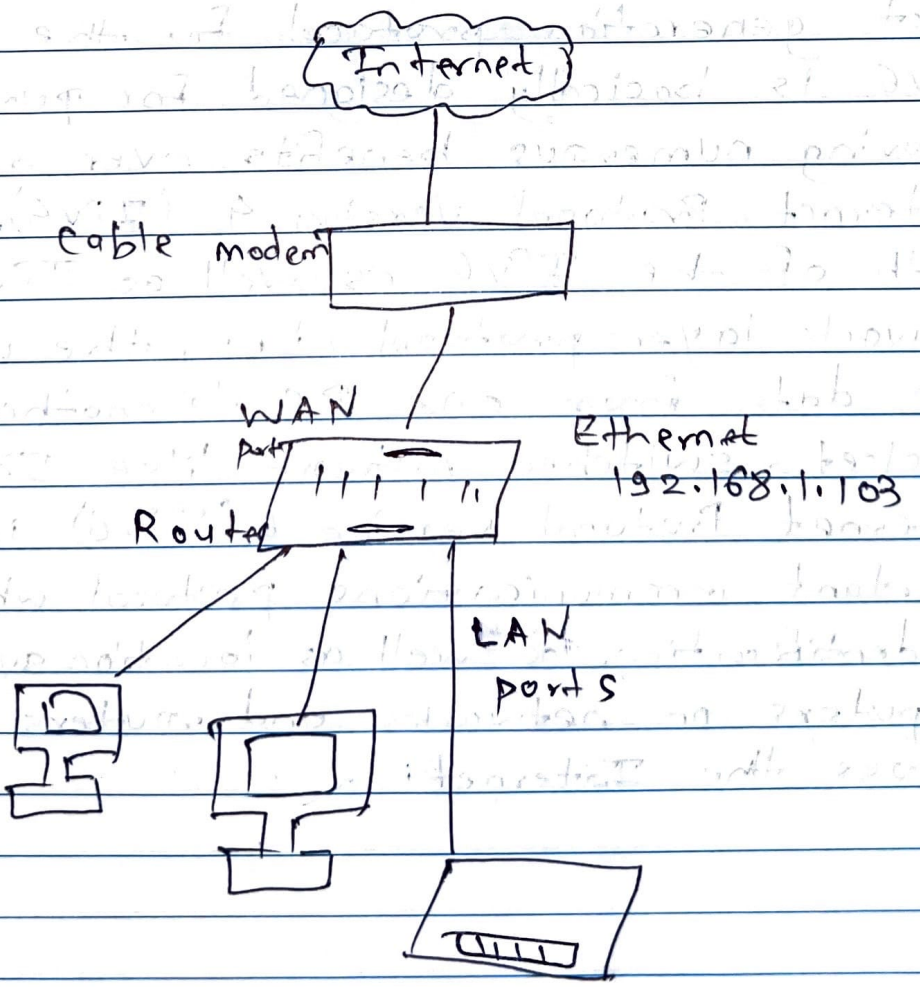
THADOMAL SHAHANI
TSEC
ENGINEERING COLLEGE

?i) Wireless Ethernet

⇒

1) Ethernet networks can also be wireless. Rather than using ethernet cable to connect the computers, wireless NICs use radio waves for two-way communication with a wireless switch or hub.

2) It consists of Ethernet ports, wireless NICs switches and hubs. Wireless network technology can be more flexible to use, but also requires extra care in configuring security.



ii) IPV6

⇒

- Shortcomings of IPV4 like address depletion prompted a new version of IP in the early 1990s. The next or new version, which is called Internet Protocol version 6 (IPV6). It is also called as IP new generation (IPng) protocol.
- IPV6 has increased the address space immensely and also redesign the format of IP packet. It has also revise some of the auxillary protocol for e.g., ICMP
- IP V6 or Internet protocol version 6 is the next generation protocol for the Interned.
- IPV6 is basically designed for purpose of proving numerous benefits over current Internet Protocol Version 4 (IPV4).
- Both of the IPV6 as well as IPV4 define network layer protocol, i.e., the way to send the data from one PC to another PC over packet-switched network like Internet.
- Internet Protocol version 6 (IPV6) is an important communications protocol which provides an identification as well as location system for computers on networks and routers traffic across the Internet.

- IETF has developed IPv6 with the very old problem regarding IPv4 address exhaustion. The basic intention of IPv6 is to replace IPv4. Devices which are present on the Internet are assigned a unique IP address for the purpose of identification as well as location definition.
- Advantages of IpV6 :

1) Increased address space.
2) More efficient routing
3) Reduced management requirements
4) Improved methods to change ISP
5) Better mobility support.
6) Multi-homing
7) Security.
8) Scoped address : link-local, site-local and global-address space.

iii) ssh

⇒

- SSH (Secure Shell) is access credential that is used in the SSH protocol.
- In other words, it is a cryptographic network protocol that is used in for transferring encrypted data over network.
- It allows you to connect to a server, or multiple servers, without having you to remember or enter your password for each system that is to login remotely from one system into another.
- It always comes in "key pair":

1) Publickey ⇒ Everyone can see it, no need to protect it
2) Private key ⇒ Stays in computer, must be protected.

- Key pairs can be of following types:

1) User key ⇒ If public key and private key remain with the user.
2) Host key ⇒ If public key and private key are on a remote system.
3) Session key ⇒ Used when large amount of data is to be transmitted.

Q.2 Explain the purpose of following protocols with their header format.

i) ARP

⇒

- Address Resoultion Protocol (ARP) is used to map an IP address to a physical (MAC) address on a local network.
- ARP operates at the link layer of the OSI model.
- ARP is primilary used to resolve the layer 3 (IP) addresses to layer 2 (MAC) addresses. When a local device on a local network needs to communicate with another device on the same network, it must know the MAC address of the target device. ARP helps in finding the MAC address that corresponds to given IP address within the local network.
- In many local networks, device obtain IP addresses dynamically using protocols like DHCP. ARP plays crucial role in the dynamic allocation of IP addresses by helping devices find the MAC addresses corresponding to their IP address.

- ARP Header Format :

Octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 byte)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 byte)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 byte)	
20	(last 2 byte)	
22	(last 2 byte)	
24	Target protocol address (TPA) (first 2)	
26	(last 2 byte)	

ii) ICMP

=>

- Internet Control Message Protocol (ICMP), is another important network protocol that operates at the network layer (layers 3) of the OSI model.
- ICMP is primilary used for reporting errors and conditions related to the IP packet delivery process.
- ICMP includes a function for network troubleshooting known as the "ping" utility.
- A device can send an ICMP Echo Request message to another device, and if the target device is reachable and operational, it will reply with an ICMP Echo Reply Message.
- The header format :

Type (8 bit)	Code (8 bit)	Checksum (16bit)
Extended Header (32 bit)		
Data / Payload (Variable length)		

- ICMP can be used for network management and control.

iii) DNS

⇒

- Domain Name system (DNS) is a critical protocol used in computer networks to translate human-readable domain names into IP addresses that computers use to identify each other on the internet.
- DNS is primilary used to resolve domain names to IP addresses. When you enter a website's URL in a web browser or send an email to a domain, DNS is responsible for translating the human-readable domain name into the corresponding IP address so that data can be routed to correct destination.
- DNS can be configured with redundant servers and failover mechanisms.
- If one DNS server becomes unavailable, DNS can automatically direct traffic to an alternative server to ensure service continuity.
- DNS is also used for reverse lookups, where an IP address is translated back into a domain name.
- This is often used for security and logging purposes.

Q.3 Discuss Persistent and Non-persistant protocols used in Transport and Application layer of TCP/IP protocol suite.

⇒

- **Persistent HTTP:**

- With persistent connections, the servers leaves the TCP connection open after sending responses and hence the subsequent requests and responses between the same client and server can be sent.
- Multiple objects can be sent over a single TCP connection between client and server.
- Fewer RTTs and less slow start.
- HTTP 1.1 uses persistent HTTP in default mode.

- **Non-Persistent HTTP:**

- A non-persistent connection is the one that is closed after the server sends the requested object to the client.
- At most one object is sent over a TCP connection.
- 2 RTTs to fetch each object.
- HTTP 1.0 uses non-persistent HTTP.

02/10/23