**COMPUTER COMMUNICATIONS LAB 01**

**UNIT 1**

**Hosts**

A host (also called an end or client) device is connected to a network and participates directly in network communication. Specifically, these devices are assigned a communication address called an IP (internet protocol) which is a unique identifier.

**Intermediary Device**

These devices connect the end devices to the network. They use the destination end device address along with information about the network interconnects to determine the path the messages should flow through a network. They can transmit signals, redirect data, classify and prioritise data and permit or deny the flow of data. Eg. Router, switch, firewall.

**Server**

Computers with software that allow them to provide information to other end devices on the network. Eg. Email servers, web pages, file.

**Peer-To-Peer**

A basic setup where a computer is both a client and a server connected to each other.

Advantages:

* Easy setup
* Simple setup
* Lower cost as fewer devices
* Can be used for simple tasks like transferring files and sharing printers.

Disadvantages:

* No centralised admin
* Not as secure
* Not scalable
* Slow performance as each device is both client and host.

**Transmission of Information**

Choosing between transmission depends on distance, environment, amount of data and also the cost.

**Metal Wires** – Data is encoded into electrical impulses

**Glass/Plastic Fibre** – Data is encoded into pulses of light

**Wireless** – Data is encoded via modulation of specific frequencies of electromagnetic waves.

**Network Interface Card (NIC)** – connects the end device to the network.

**Physical Port** – An outlet on a networking device where media connects to an end device or another networking device.

**Interface** – Specialised port on a networking device that connects to individual networks. The ports on a router is referred to as network interfaces.

**Physical Topology Diagram**

Shows the physical location of intermediary devise and cable installation.

**Logical Topology Diagram**

Shows which end devices are connected to which intermediary devices,

**SOHO Networks**

Small office and home office networks.

**LAN** – Local area network. Fast transfer over small distance. Limited by area.

**WAN** – Wide area network. Slower transfer over larger area. Usually controlled by ISPs.

**Internet** – A collection of LANs and WANs.

**Intranet** – A term used to refer to a private collection of networks that belong to an organisation.

**Extranet –** A company may use an extranet to provide secure and safe access to individuals who work for a different organisation but require access to the organisations data.

**Network internet connections**

Networks used to be independent for phone, file and broadcast purposes however they are now converged for the internet.

* **Cable** – Typically offered by cable television providers. It has high bandwidth, high availability and an always-on connection to the internet.
* **DSL** – Digital Subscriber lines. Mostly for home/small office. High bandwidth, high availability and always-on connection to internet. ADSL is more common – upload is slower than download.
* **Cellular** – Uses a cell phone to connect, dependent on whether you can get a signal. Limited by capability of phone and the cell tower.
* **Satellite** – Availability of satellite internet is benefit for areas that are remote or don’t have access. Must have a clear line of site to satellite.
* **Dial-Up** – Inexpensive and used phone line and modem. Low bandwidth and not sufficient for large data transfer but useful for mobile access while traveling.

For business:

* **Dedicated Leased Line** – private circuits that connect for private networking.
* **Metro Ethernet** – Extends LAN networks into the WAN.
* **Business DSL** – Similar to consumer for SDSL – upload and download the same.

**Good Network Design**

* **Fault Tolerance –** Limits the effects of a failure in a network.
* **Scalability** – Allows new users and applications without degrading performance.
* **Quality of Service** – Ensures speed and priority with congestion of bandwidth problems.
* **Network Security** – Protects data and infrastructure from unauthorised access.

**Network Trends**

* **Bring your own device** – Freedom for employees and students to access information and communicate.
* **Online Collaboration** – Allows for individuals to collaborate with each other ( Skype).
* **Video Communications** – Used for communication, collaboration and entertainment.
* **Cloud Computing** – Allows the storing of data online.
  + Public – pay-per-use models.
  + Private – set up for an organisation usually
  + Hybrid – combination of public and private
  + Community – for organisations like hospitals. Levels of security/privacy.

**Powerline** allows LAN within a home using electrical outlets.

**Wireless Internet Service Provider** **(WISP)** is an ISP that allows subscribers to access point of hot spots in their homes. Usually has an antenna or dish.

**Threats to Networks**

* **Viruses, worms and trojan horses** – malicious code running on a user device.
* **Spyware and adware** – Steals user information using software on a device.
* **Zero-day attacks** – occur on the first day that a vulnerability becomes known.
* **Threat actor attacks** – malicious person attacks user devices or network.
* **Denial of service attacks** – Attacks that slow or crash processes on a network.
* **Data interception and theft** – Captures private information from a network.
* **Identity theft** – Steals login credentials to access private data.