Introduction to Computer Networks

A network can be any connected devices. It can be as small as two computers or as complex as a multisite network such as a telecommunications infrastructure that contains 100s if not 1000s of computers that are connected together.
The common uses of a network are:

- **Communication –** video conferencing, email, chats, learning, etc…
- **Sharing Hardware –** printers, scanners, storage…
- **Sharing data –** files.
- **Sharing applications –** Microsoft word, spread sheet, specialised software, etc.
- **Data Backup and retrieval**

1.1 Types of Networks

1.1.1 LANs and WANs

They types of network used are dictated by the number of locations they span.

LANs – Local Area Networks are restricted to a single location (building, office, school).
WANs – Wide Area Networks spread over multiple geographic locations. They are slower than LANs and more expensive and they tend to use different technologies to connect LANs together to create an internetwork.
Between these networks are other types of networks that you might experience:
MANs – Metropolitan Area Networks spread over geographic locations; they're not large enough to be called WANs and not too big to be called LANs, which is why on many occasions MANs are referred to as WANs because there is no rule or guideline to differentiate between the two.
CANs – Campus Area Networks are restricted to one location, similar to LANs but they're too small to be called LANs.
PANs – Personal Area Networks are small networks that are used to connect personal devices together, such as connecting a laptop to a PDA device.

1.1.2 Peer-to-Peer and Client/Server Networks

Wired networks use two basic models, peer-to-peer and client/server:

Peer-to-Peer Networks
Peer-to-peer networks are made of a small number of computers (usually not more than 10 PCs) that are connected together and each one of these PCs is responsible for their own security and resource management. It is sometimes called decentralised network because there is no method to centralise the management of resources.

Advantages of Peer-to-Peer:
- Low cost, no requirement for expensive servers.
- Easy to implement.

- Easy to maintain (the lower the number of devices the easier it is).

Disadvantages:

- Security needs to be applied, managed and maintained separately on each device.
- Data Backup needs to be performed separately on each device.
- Limited number of PCs, although you can install more than 10 PCs or devices however managing these devices gets harder and unfeasible as the number of these devices increases.

1.1.3 Client/Server Network

Client/server networks on the other hand are the most common networks you'll see installed in organisations even small businesses because although they're more expensive the following advantages makes them the number one choice chosen by all businesses.

Advantages of client/server networks:

- Scalable, very easy to expand and add as many devices as needed.
- Centralised management.
- Enhanced Security.
- Simplified backup.

1.1.4 Hybrid Networks

A hybrid network describes a network that takes advantage of a number of other network types to operate. Like for example a network utilising a client/server technology and at the same time the network or part of it operates in peer-to-peer.

1.1.5 Distributed and centralised computing

Distributed computing is when the work or load of the network traffic is distributed or spread over to different systems. It also describes a network that uses client/server network but at the same time some of the load is distributed to the client. Like for example a hotel booking system; the booking system could be held on the mainframe, while the email system used to correspond to customers is held on the PC-based server.

1.1.6 VPN (Virtual Private Network)

VPNs are used to connect two networks of different locations by creating an encrypted point-to-point tunnel via public networks (internet). They provide a secure point-to-point dedicated link between the two networks over the internet. It can be thought of as a sort of a WAN connection. VPNs provide a cost effective way to expand the network, provide network connectivity over long distances, can be used to connect a private LAN to another (LAN-to-LAN internetworking), allow remote workers to connect to the company network as if they were inside and provides security; without the need of a leased line.

The following are the important elements that are involved when establishing a VPN connection:

- VPN Client – The remote client that starts a connection.
- VPN Server – Authenticate connections.
- Access Method – internet or intranet.

- VPN protocols – required to establish, manage and secure the data over the VPN connection. The VPN connection is managed by the **PPTP (Point-to-Point Tunnelling Protocol)** and the **L2TP (Layer 2 Tunnelling Protocol).** They enable authentication and encryption. The VPN connection supports analogue modems, ISDNs, Wireless and Broadband connections (cable or DSL).

Advantages of VPNs:

- **Cost –** no need for leased lines.
- **Network Scalability –** allows expansion without the need to change the network infrastructure.
- **Simplified admin –** Authentication server can easily add or remove clients.
- **Security –** all data travels over the internet via an encrypted tunnel.

Disadvantages of VPNs:

- **Security and complexity –** Admins need a good understanding of security protocols and the need to properly setup, configure and manage a VPN connection.
- **Reliability –** Dependant on the ISP (how reliable the ISP is). The ISP is short for Internet Service Provider (Plusnet, BT Broadband, SkyNet).
-

1.1.7 VLANs (Virtual Local Area Networks)

VLANs are used for segmentation. This is a strategy to improve:

- Network Performance.
- Can increase security.
- Removes Performance bottle neck.

A VLAN is a group of connected computers that act as if they're on their own network segment even though they might not be. They're a group of logically connected systems and configure through an interface on a switch or router. For example we have a multi-storey building that has employees from the same department but on different floors; the VLAN can be used to group these employees under one virtual segment where they can connect and use all the resource that are specialised for that department.

Advantages of VLANs:

- Increase security and performance.
- Organisation – network users and resources that are linked and communicate frequently can be grouped together in a VLAN.
- Simplified Admin – easier to remove or reconfigure switches or routers, moving users between LAN segments and it is easier to re-cable and address new stations.

VLAN Membership

- Protocol-based – assigns a membership based on the protocol and IP address used.
- Port-based – assigns membership based on ports.
- MAC-address – membership assignment is based on the MAC address of the device. The MAC address (Media Access Control) is an address assigned by the manufacturer of the device, which is hardcoded into the device. This MAC address is made of a part that Identifies the manufacturer of the device and a part made of a sequence number of the device.

Source : http://infosectutorials.com/2012/02/05/1-introduction-to-computer-networks/