- Introduction to Networks -

What is a Network?

A **network** is simply defined as something that *connects* things together for a specific purpose. The term *network* is used in a variety of contexts, including telephone, television, computer, or even people networks.

A **computer network** connects two or more devices together to share a nearly limitless range of *information* and *services*, including:

- Documents
- Email and messaging
- Websites
- Databases
- Music
- Printers and faxes
- Telephony and videoconferencing

Protocols are *rules* that govern how devices communicate and share information across a network. Examples of protocols include:

- **IP –** Internet Protocol
- **HTTP -** Hyper Text Transfer Protocol
- **SMTP –** Simple Mail Transfer Protocol

Multiple protocols often work together to facilitate end-to-end network communication, forming protocol **suites** or **stacks.** Protocols are covered in great detail in other guides.

Network reference models were developed to allow products from different manufacturers to interoperate on a network. A network reference model serves as a blueprint, detailing standards for how protocol communication should occur.

The **Open Systems Interconnect (OSI)** and **Department of Defense (DoD)** models are the most widely recognized reference models. Both are covered in great detail in another guide.

* * *

Basic Network Types

Network *types* are often defined by function or size. The two most common categories of networks are:

- **LANs (Local Area Networks)**
- **WANs (Wide Area Networks)**

A **LAN** is generally a high-speed network that covers a small geographic area, usually contained within a single building or campus. A LAN is usually under the administrative control of a single organization. **Ethernet** is the most common LAN technology.

A **WAN** can be defined one of two ways. The *book definition* of a WAN is a network that spans large geographical locations, usually to connect multiple LANs. This is a general definition, and not always accurate.

A more *practical definition* of a WAN is a network that traverses a public or commercial carrier, using one of several *WAN technologies***.** A WAN is often under the administrative control of several organizations (or *providers*), and does not necessarily need to span large geographical distances.

A **MAN (Metropolitan Area Network**) is another category of network, though the term is not prevalently used. A MAN is defined as a network that connects LAN's across a city-wide geographic area.

An **internetwork** is a general term describing multiple networks connected together. The **Internet** is the largest and most well-known internetwork.

Some networks are categorized by their *function*, as opposed to their *size*. A **SAN (Storage Area Network)** provides systems with high-speed, lossless access to high-capacity storage devices.

A **VPN (Virtual Private Network**) allows for information to be securely sent across a public or unsecure network, such as the Internet. Common uses of a VPN are to connect branch offices or remote users to a main office.

* * *

Network Architectures

A **host** refers to any device that is connected to a network. A host can also be defined as any device assigned a **network address**.

A host can serve one or more functions:

- A host can *request* data, often referred to as a **client.**
- A host can *provide* data, often referred to as a **server.**
- A host can both request *and* provide data, often referred to as a **peer.**

Because of these varying functions, multiple network **architectures** have been developed, including:

- **Peer-to-Peer**
- **Client/Server**
- **Mainframe/Terminal**

In a basic **peer-to-peer** architecture, all hosts on the network can both *request* and *provide* data and services. For example, two Windows XP workstations configured to share files would be considered a peer-to-peer network.

Peer-to-peer networks are very simple to configure, yet this architecture presents several challenges. Data is difficult to manage and back-up, as it is **spread across multiple devices**. Security is equally problematic, as user accounts and permissions much be configured individually on each host.

In a **client/server** architecture, hosts are assigned specific roles. *Clients* request data and services stored on *servers*. An example of a client/server network would be Windows XP workstations accessing files off of a Windows 2003 server.

There are several advantages to the client/server architecture. Data and services are now **centrally located** on one or more servers, consolidating the management and security of that data. As a result, client/server networks can scale far larger than peer-to-peer networks.

One key disadvantage of the client/server architecture is that the server can present a **single point of failure.** This can be mitigated by adding *redundancy* at the server layer.

* * *

Network Architectures (continued)

In a **mainframe/terminal** architecture, a single device (the **mainframe**) stores all data and services for the network. This provides the same advantages as a client/server architecture – centralized management and security of data.

Additionally, the mainframe performs all processing functions for the **dumb terminals** that connect to the mainframe. The dumb terminals perform *no processing whatsoever*, but serve only as input and output devices into the mainframe.

In simpler terms, the mainframe handles all *thinking* for the dumb terminals. A dumb terminal typically consists of only a keyboard/mouse, a display, and an interface card into the network.

The traditional mainframe architecture is less prevalent now than in the early history of networking. However, the similar **thin-client** architecture has gained rapid popularity. A thin-client can be implemented as either a hardware device, or software running on top of another operating system (such as Windows or Linux).

Like dumb terminals, thin-clients require a centralized system to perform all (or most) processing functions. User sessions are spawned and managed completely within the server system.

Hardware thin-clients are generally inexpensive, with a small footprint and low power consumption. For environments with a large number of client devices, the thin-client architecture provides high scalability, with a lower total cost of ownership.

The two most common thin-client protocols are:

- **RDP (Remote Desktop Protocol) –** developed by Microsoft
- **ICA (Independent Computer Architecture) –** developed by Citrix

* * *