Networks — How the Internet Works

"The Internet is a Network of Networks" — Thus in order to gain an understanding of the Internet we need to define:

- What a simple network is.
- How computers communicate over a network.
- The need for a variety of protocols to govern communication.
- How we connect networks together.




What is a Network?

A network can be:

- as simple as two computers connected together, or
- as complex as 150 Million connected together (The Internet).

Other devices can be connected to a network:
For example, printers, disk drives, terminal server and communication servers.
Computers can and will be of a different type

Thus, over a network, resources can be shared.

For a company (or university) this can

- maximise use of resources (share expensive computers, color printers), and
- all sorts of information (programs, data *etc*) can be easily exchanged or shared (over Email, Ftp, Telnet, Local network sharing — file servers).



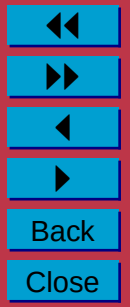

Departmental Networks

Many computer networks exist in this department.
We have local networks of

- Unix/Linux Workstations (Research and Teaching Labs)
- Macintosh Power PCs (Multimedia Lab)
- IBM compatible PCs (Two Teaching Labs)
- Specialist machines (Parallel Computers, GRID computers, High performance Graphics).

Many of these computers (UNIX, PC, Mac Labs) all exist on a local (individual) network that share local printer resources.

However, they all connect to a large department layer of network and even to the Universities network before going onto the Internet.



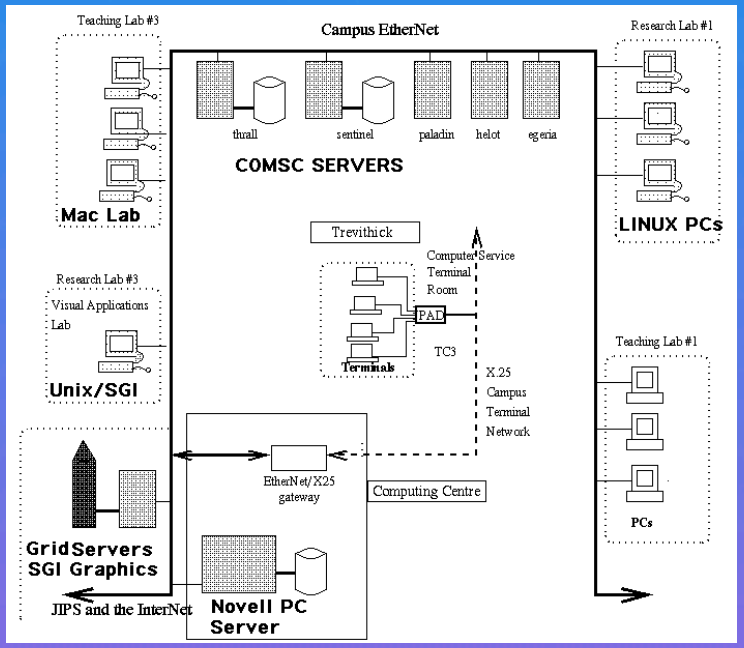


Figure 2: Department Local Networks and Internet Connectivity

(This picture may be a little out of date w.r.t. computer resources but the network is still accurate)




Back

Close

Communication — Protocol

The need for a protocol

A set of rules is needed for any means of communication:

- Human intercommunication (in pairs or larger groups) requires rules of conversation (do not speak if someone else is speaking) to function effectively.
- Computers are no different.
  Consider the following simplistic analogy:
  - Two computers connected via a single connection — Imagine two people talking via two tin cans connected via piece of string:

    If the two people talk at the same time then we get what is known (in networking terms) as *data collision*.




Back
Close

Protocols (Cont.)

- For any inter-computer communcation, we need regulations and rules to how we communicate over a computer network.
  For example to remote login (telnet), FTP, email, access web pages (HTTP, CGI)
- The set of rules and regulations is called a *Protocol*.




What exactly does an Internet (Network) Protocol do?

A network protocol has to define how:

- all the operations within a network, *and also*
- how entities outside the network must interact.

Typical network protocols define:

- How data gets from point A to Point B
- How computers and devices communicate, For example:
- How a file is printed on a printer
- How data is transmitted over a telephone line.




The Client Server Model — Another view of the Internet

We can to distinguish between computers that

- access information and
- provide information.

A computer can be either of both at the same time.

Client Server Definitions

The Internet is made up of **client** computers which can access information and **servers** which sort and distribute information.

- A program becomes a *client* when it sends a request to a server a awaits a response. The client runs on the computer you are using. It facilitates your access to information provided by the server.
- A *server*is a program that offers a service that can be obtained over the network.




Client Examples

Examples of Clients

- WWW Clients: Internet Explorer, Netscape, Safari, Opera.
- Email Clients: Mail (Mac OS X), Eudora, Pine, Elm, Outlook Express
- FTP Clients: Fetch, Interarchie, MacSFTP, Transmit (Mac SFTP) Anarchie, xftp, Unix FTP.
- Telnet Clients: Terminal (Mac OS X), Unix Telnet, NCSA Telnet.
- News: NewsWatcher, News Xpress, Free Agent




Back
Close

Server Examples

A server is typically a powerful computer capable of handling information requests from many clients simultaneously.

How requests per minute do heavy web servers require?

- Google
- BBC News Web Page
- Cardiff University Web Server
- Your own web server?

Clearly different computer requirements in terms of power required to deliver an effective web service.




Sending Data over the Internet

How is data send over the Internet?

- **The same basic mechanism is used for all internet communication.**
- Governed by *Low Level* TCP/IP (Transmission Control Protocol and Internet Protocol)
- Large Data broken into smaller packets
- Packets sent to destination not necessarily all through same route.
- Packets need to sent securely
- Packets need to be assembled at client.




Packets

Need for Security?:

- Recall: Historical Origins of Internet was Military (1960 Cold War)
- Military Needed to protect against enemy interception.
- Security Strategy:
  - Break Data up in small packets — send packets via different routes
    So if parts of message intercepted hopefully not all message is understood
  - Encode via some cryptography each message/each packet
    Enemy need to break to code as well as gather enough packets?




Packets (Cont.)

Public Internet No Longer Used for Military Purposes

Need for Security Today?:

- These days we are more concerned with commercial and personal security
  - protect our online credit card/financial details
  - protect commercially sensitive information
  - protect personal private information




Back
Close

Basic Packet Sending

- The information coming from one computer is broken up into **packets** — Small portions of the whole data.
- Each Packet marked with:
  - Source and destination addresses
  - Packet length
  - Packet position in whole data
  - Time to live
- The packets of information travel along the links and are guided to their eventual destination by **routers** which looks at the destination address and decides the best route to send them.
- Packets collected at the other and reassembled.

More on packet structure later when we know more about networks




Computer Networks

The Internet is a Network of Computer Networks.

So Let us briefly study how Computer Networks are configured and how they work.

Classifying Networks

There are two basic ways in which we can classify networks:

- How they operate — **type of connection**.
- How they are configured — **Topology**




Network Connections

Switched Networks

There are two types of networks

- circuit switched
- packet switched




Circuit Switched Networks

- Dedicated connection is established between two stations
- Advantage: guaranteed capacity - once a circuit is established, no other network activity will decrease the capacity of the circuit
- Disadvantage: cost - circuit costs are fixed, independent of traffic
- An example is the Telephone System
- If you dial into to an internet provider then you have a dedicated circuit switched initial connection to the internet
- Some business (e.g. International Recording Studios) create dedicated ISDN/ADSL links so that performers can record either side of the Atlantic, for example.




Back
Close

Packet Switched Networks

- Network traffic is divided into small *packets*, usually a few hundred bytes in size
- Advantage: concurrent connections among computers can exist
- Disadvantage: as activity increases, a given pair of communicating computers receives a smaller share of network capacity
- Another advantage: Since multiple machines can share a network, fewer interconnections are required
- **Internet is comprised predominantly of packet switched networks**



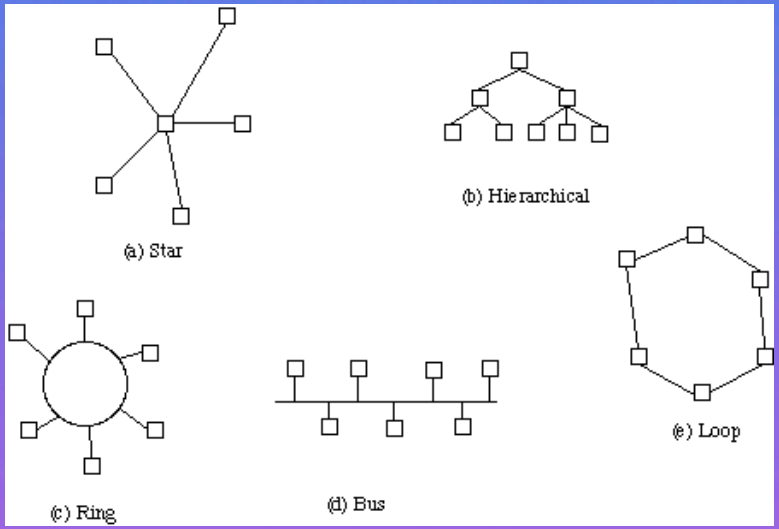

Back
Close

Network Topologies

Connecting two computers together is a straightforward task — Simple Point-toPoint

However, connecting several computers together is different.

- They can be connected in a variety of ways:



- Many of these topologies exist on Internet.


Advantages/disadvantages of each method of connection

- Star, Hierarchical and Loop configurations are all **point-to-point** topologies:
  - Each computer communicates directly with its neighbour.
  - Relies on Neighbour to rely data around network.
  - Problems if on computer fails.
  - Star extreme example as a central computer is present. If this fails ....
- Bus and Ring configurations are called **broadcast** topologies.
  - A message is placed on the bus or ring containing the name of the intended receiving computer.
  - All computers listen constantly.
  - If name identified by listener, message is captured.
  - Only one node can broadcast at a time: Needs a Protocol.
  - Bus and Ring Topologies very common.

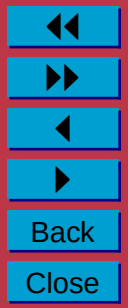



Data Transmission

Having "wired" up our networks — How does data get sent down the "wires"

What considerations/implications of transmission medium?

- Interference — Electro-Magnetic Noise, Radio/Satellite Transmission
- Physical Limitation — Speed of Transmission through Wires, Optical Cables, Radio/Satellite
  - Governs Amount/size of Packets that can be send in given time
  - Governs amount of data that can be sent PERIOD — **Bandwidth** Limitation.



The Physical Design Layer — Wire, Optic Transmission

Using wire to transmit signals has been around since the telegram.

However, there are problems with this medium.

- A signal pair of wires can carry (send and receive) telephone conversation for some distance but suffer from
  - Electromagnetic interference (EMI) — noise *etc*
  - Crosstalk — interference of the two signals.
- Twisted pairs —- Twist wires together
  - reduces EMI and Crosstalk.
  - Used in telephones.
  - Can carry several simultaneous telephone conversations (100 voice channels).




- Coaxial cables — Place one wire inside another conductor separated by an insulator.
  - Superior rejection of EMI and Crosstalk.
  - Can support 10,000 analog voice channels
- Fibre-optic cables — one or more very thin (human hair thickness) glass rods.
  - Very little outside interference.
  - Can carry very large amounts of data (several gigahertz)
  - For example, laser light modulation carries data at 140 million bits per second. Best telephone rates 56,000 bits per second.

Bandwidth

As we shall see later in the course, the modern forms of media (digital audio and video, as well as fancy graphics) place a huge burden on the amount of data needed to be transmitted around the Internet (esp. World Wide Web).

Bandwidth is the amount of information or data that can be transmitted from one end of the medium to the other in a given time.

Clearly the design of the physical layer plays a fundamental role in the amount and hence speed of data transmission.

We will look at implications of this much later in the course.




Back
Close

Larger Networks of Computers

Local Area (LAN) and Wide Area (WAN) Networks

When we connect computers together they reside and communicate over some physical location(s).

- Many times a lab or office will be locally networked together
  - perhaps a single **gateway** to the outside Internet.
- Many times computers will connected together on a single network over a larger area.
  - For example the Cardiff University Campus Wide Network
  - Still a single **gateway** to the outside Internet.
- Clearly range and medium of connectivity affect Network Charateristics.




Back
Close

Recall this Picture

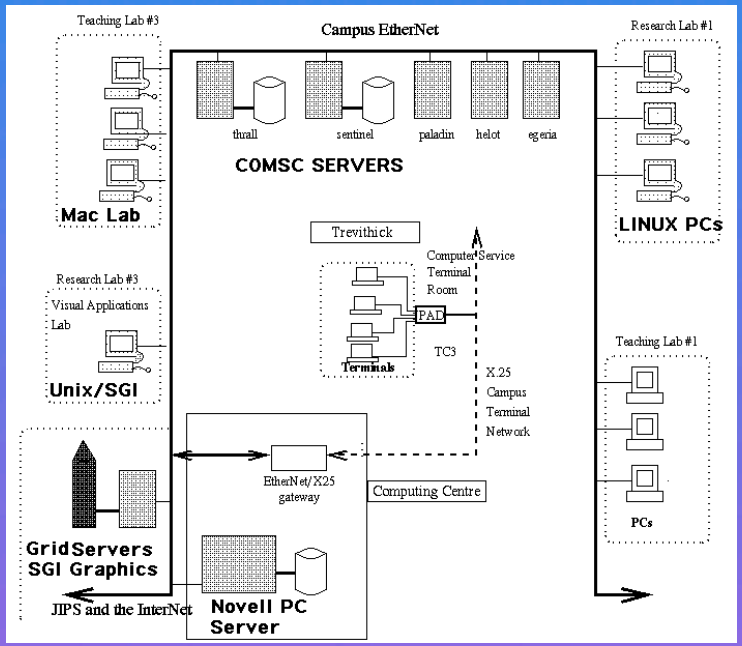


Figure 3: Department Local Networks and Internet Connectivity




Local Area Networks — LANs

- LANs can link several computers in a single building.
- The LAN can then itself be linked to other LAN's.
- The Internet is made up of thousands of LAN's.
- Provide the highest speed connections among computers
- Cannot span large distances
- Typical LAN spans small building and operates between 4 Mbps and 2 Gbps
- Usually bus based (Ethernet) networks.



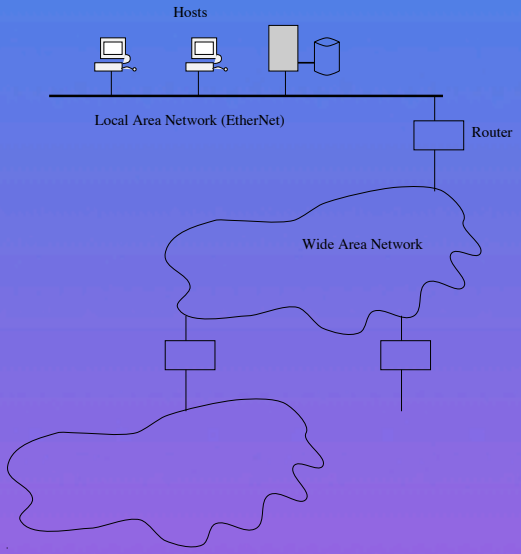



Figure 4: Local Area Connect to Wide Area Networks

Wide Area Networks — WANs

- Sometimes called long haul networks
- Allow endpoints arbitrarily far apart
- Intended for use over large distances
- Operate at speeds from 9.6 Kbps and 45 Mbps




A more formal look a Network protocols

A Model for all Protocols?

As we will shortly see there very many Networked and Internet Protocols:

- Each client application/server needs to communicate in a slightly different way.
- However, the basic transmission mechanism is same for all:
  - prepare data for transmission — encode, packetise etc.
  - send data — set destination and route to it
  - Server/Client recieves data and reassembles and prepares for viewing

Conceptualise these processes into a MODEL for all Network Communications




The OSI 7 Layer Model for Network Protocol

As we have pointed out already:

- There is a real need for a communication protocol to established for any process.
- There is clearly a need for a *standardised* protocol in the global context on networking — otherwise the Internet could not exist in its current form.

Therefore:

Networking protocols need to be established from the low level computer communication all the way up to how application programs communicate.

- There clearly several process or steps from low level computer communication to application programs
- Each step in this protocol is called a layer.




The OSI 7 Layer Model for Network Protocol (CONT.)

The International Standards Organisation (ISO) defines a 7 layer model for network communication protocol.

The model is more formally called the Open Systems Interconnection (OSI) model.

All Network Protocols should adhere to the Model:

- Not all levels always need to be supported
- depends on nature/level of application




Advantages of the 7 Layer Model Design Approach?

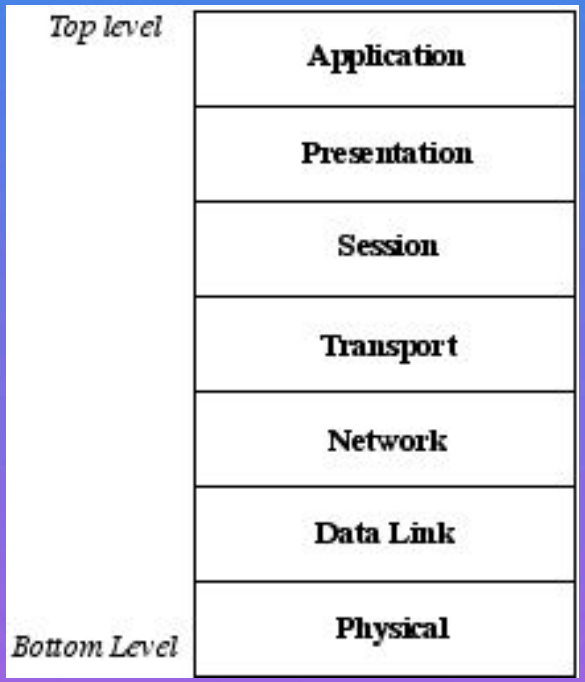
The advantage of breaking down the protocol into layers is twofold:

- Each layer can be regarded as a *black box*.
  - Well defined inputs and outputs exist, **but**
  - The Inner workings of the layer can be regarded as being independent
  - **Thus**, New versions, updates or better methods can be written without affecting the whole system.
  - Network is *Future Proofed* to a great extent.
  - Benefits passed on to whole network.
- Communication need only take place at the layer appropriate for the task.




The 7 Layer s of the OSI Model

The 7 layers must be organised in the specified order:



The Bottom 3 Layers

The function of each layer (from bottom to top) is:

Physical — The interface between the medium and the device.
The layer transmits bits (ones and zeros) and defines how the data is transmitted over the network, what control signals are used and the mechanical properties of the network (Cable size and connector for example.)

Data Link — Provides low-level error detection and correction.
For example if a packet is corrupted this layer is responsible for retransmitting the packet.

Network — Responsible for routing packets of data across the network.
For example, a large email file will be divided up into packets, each packet addressed and sent out at this layer.




The Top 4 Layers

Transport — An intermediate layer that higher layers use to communicate to the network layer.
This layer hides the complexities of low-level networking communication from the higher levels.

Session — The User's (transparent) interface into the network.
The layer manages the "current" connection (or session) to the network. Note: In packet-switched network a full-time network connection does exist, even though it may seem so. The Session layer keeps the communication flowing.

Presentation — Ensures computers speak the same language.
They convert text to ASCII or EBCDIC form and also encode or decode binary data for transport.

Application — The programs you use directly may need to communicate.
E.g a file transfer, email program or web browser




Some Example (Local) Network Protocols

Token ring — low level network message passing protocol.

Media Access Control (MAC) — A protocol that defines the way workstations gain access to transmission media, most widely used in reference to LANs. For most LANs, the MAC layer is the lower sublayer of the data link layer protocol (Layer 2).

Carrier sense multiple access/collision detection (CSMA/CD) — In this protocol, stations listen to the bus and only transmit when the bus is free. If a collision occurs, the packet is retransmitted after a random time-out. CSMA/CD is used in Ethernet.

Network File System (NFS), External Data Representation (XDR) and **Remote Procedure Call (RPC)** — Work together to enable transparent access to remote network resources

X Windows — Serves as a distributed windowing and graphics system used for communication between X terminals and UNIX workstations (Sun, Dec, Linus, Mac OS X ..). Works across any network (incl. Internet).




Some More Example Network Protocols

Finger — Obtains information about a user from their profile.

Whois — Obtains information about domain registration.

Daytime - Network Time Protocol — The daytime protocol retrieves the current day and time.

Simple Network-Management Protocol (SNMP) —- Primarily reports anomalous network conditions and sets network threshold values




Some Example Low Level Internet Protocols

Transmission Control Protocol/Internet Protocol (TCP/IP) — The low level protocol: Basis of all Internet data transfer

Internet Control Message Protocol (ICMP) — a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source.

Common Gateway Interface (CGI) — How web forms and other means of web input communicate with special programs that process data on Web Servers.

Interior Gateway Protocols (IGPs) — How networks communicate with wider WWW.

Border Gateway Protocol (BGP) —How networks communicate with wider WWW.




Back
Close

Some More Example Low Level Internet Protocols

Internet Router-Discovery Protocol (IDRP) — Router Govern how packets will get delivered across the web

Point-to-Point Protocol (PPP) — Governs how "dial-up" connections communicate with WWW.

Serial Line IP (SLIP) — Older "dial-up" Protocol.

User Datagram Protocol (UDP) — Alternative to TCP.




Some Example Internet Protocols Application Layer Protocols

Telnet — Serves as a terminal emulation protocol

Domain Name System (DNS) — Translates the names of network nodes into network addresses

File Transfer Protocol (FTP) — Moves files between devices

Secure File Transfer Protocol (SFTP) — encrypted file data transfer

Simple Mail Transfer Protocol (SMTP)

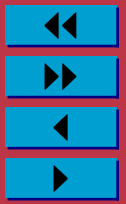
Post-Office Protocol version 3 (POP3), IMAP — email protocols

Network News (Groups) Transfer Protocol (NNTP) — Govern how news group data is distributed.

Hypertext Transfer Protocol (HTTP) — Basis of Nearly all WWW Comms

HTTPS — encrypted Hypertext Transfer Protocol. Should used for all commercial and other secure Web transactions of data.

NOTE: We will meet and study many of these protocols in coming lectures



Summary: OSI Model and Internet Protocols