CS15210 Revision

Table of Contents

[Waves and Signals 2](#_Toc451792082)

[Basics 2](#_Toc451792083)

[Signals 2](#_Toc451792084)

[Damage 2](#_Toc451792085)

[Waves: Basic Anatomy 2](#_Toc451792086)

[Key Terms 2](#_Toc451792087)

[Polarisation 2](#_Toc451792088)

[More Waves and Signals 2](#_Toc451792089)

[Calculations 2](#_Toc451792090)

[Why Waves are Important 3](#_Toc451792091)

[Binary Signals 3](#_Toc451792092)

[Modes and Media 3](#_Toc451792093)

[Bits, Bytes, and ASCII 3](#_Toc451792094)

[Parity 3](#_Toc451792095)

[Transmission Modes 3](#_Toc451792096)

[More Modes and Media 4](#_Toc451792097)

[Choosing a Medium 4](#_Toc451792098)

[Types of Medium 4](#_Toc451792099)

[Data Transmission 5](#_Toc451792100)

[Equipment 5](#_Toc451792101)

[Modulation 5](#_Toc451792102)

[Nyquist’s Theorem and Logs 6](#_Toc451792103)

[The PTSN 6](#_Toc451792104)

[Bandwidth 6](#_Toc451792105)

[Multiplexors and Switching 7](#_Toc451792106)

[Networks 101 7](#_Toc451792107)

[Cellular Systems 7](#_Toc451792108)

[Multiplexors 7](#_Toc451792109)

[Data and Voice Networks 7](#_Toc451792110)

[Wiring the World 8](#_Toc451792111)

[History of Internet 8](#_Toc451792112)

[Internet vs. its Applications 8](#_Toc451792113)

[New Applications 8](#_Toc451792114)

[Implications 8](#_Toc451792115)

[Standards 8](#_Toc451792116)

[Definition and Types 8](#_Toc451792117)

[Enforcement 8](#_Toc451792118)

[Problems 8](#_Toc451792119)

[Protocol Models and Frameworks 9](#_Toc451792120)

[Introduction to TCP/IP Protocol Suite/Stack 9](#_Toc451792121)

[Ports and IP 9](#_Toc451792122)

[Dotted Decimal and IP Addresses 10](#_Toc451792123)

[Other Protocols, More Addresses 10](#_Toc451792124)

[More about TCP and UDP 11](#_Toc451792125)

[The Domain Name System 11](#_Toc451792126)

[Network Topologies 12](#_Toc451792127)

[Physical and Logical Topologies, Media Access 12](#_Toc451792128)

[Ethernet 13](#_Toc451792129)

[Standards and Protocols 13](#_Toc451792130)

[Components 13](#_Toc451792131)

[Media Access 13](#_Toc451792132)

[Types of Media 13](#_Toc451792133)

[Round Trip Time, Slot Time, Packet Sizes 13](#_Toc451792134)

[Packet Format 13](#_Toc451792135)

[User/Application level performance 14](#_Toc451792136)

[Bridges/Switches 14](#_Toc451792137)

[Packet Forwarding 14](#_Toc451792138)

[The JANET Network 15](#_Toc451792139)

[Origins and Coloured Books 15](#_Toc451792140)

[Upgrades 15](#_Toc451792141)

[LAN Deployment 15](#_Toc451792142)

[SUPERJANET’S ORIGIN STORY (As told by Marvel, and the JNT) 16](#_Toc451792143)

[International Connectivity 16](#_Toc451792144)

[SuperJANET Returns: The JANETing 16](#_Toc451792145)

[Wide Area Services 17](#_Toc451792146)

[Leased Lines 17](#_Toc451792147)

[Analogue 17](#_Toc451792148)

[Digital 17](#_Toc451792149)

[Short Haul Services 17](#_Toc451792150)

[Integrated Services Digital Network (ISDN) 18](#_Toc451792151)

[Services/Types of ISDN 18](#_Toc451792152)

[Digital Subscriber Lines 19](#_Toc451792153)

[Types of DSL 19](#_Toc451792154)

[New ADSL Services 19](#_Toc451792155)

# Waves and Signals

## Basics

In the 1840s, basic telegraphy was carried out using a switch, a power source, and a sensor. The switch would send data (0 and 1 encoded by switch open/close) to the sensor, which would read it. Current systems have evolved from this.

## Signals

Signals are sent as varying voltage over time, and can be analogue or digital. Analogue signals can have various, non-discrete values, and take any value within a given range, but digital signals can be discrete values, and usually only 1 or 0 (High/Low, Long/Short, A-Z etc.). Potentially, they can be 3 or more values, but usually just two. They have a discrete range of possibilities.

### Damage

They can be damaged in three ways:

Attenuation: When the amplitude of a wave degrades. The change in voltages (which define values) means they could be read incorrectly.

Dispersion: When a wave gets spread out over time, as the waves travel at different phase speeds. This is particularly bad for time-based reading.

Distortion: A mixture of the first two. The signal becomes unintelligible.

It takes a tiny amount of time to change voltage (E.g. From 0 to 5v), which causes minor distortion. The computer systems must have enough leeway to deal with this.

Data can be analogue (E.g. Sounds) or digital (E.g. text), and the data type is independent from the signal. Digital waves can send analogue data, and analogue waves can send digital data, via analogue-to-digital converters (ADCs) and digital-to-analogue converters (DACs).

## Waves: Basic Anatomy

### Key Terms

Waves have cycles. A cycle is defined as the time for one complete section of the wave (Getting from point A in direction A, to point A in direction B, back to point A in direction A. Frequency (Hz) is the number of complete cycles/second.

They also have crests and troughs. The maximum point in a cycle is a crest, the minimum point is a trough. Peak-to-Peak voltage/amplitude is the vertical distance between a crest and trough. Peak Amplitude is the vertical distance between a base value (0) and the peak value of a wave. Instantaneous Amplitude is the vertical distance between the base level and the crest **of a given instant.**

Wavelength (Lambda) is the cycle length in metres.

### Polarisation

Waves can oscillate at different orientations (Horizontal and Vertical), and waves travelling at certain orientations can be blocked by a polarisation filter, whilst still letting waves at other orientations through.

# More Waves and Signals

## Calculations

A kilohertz is 103 hertz. A megahertz is 106 and a gigahertz is 109.

A millisecond is 10-3 hertz. A microsecond is 10-6 and a nanosecond is 10-9.

Wavelength = distance = speed \* time.

Velocity = frequency \* wavelength

## Why Waves are Important

An analogue signal can be represented as a combination of waves of different frequencies and wavelengths. A Fourier analysis lets us break down a wave into a number of simpler waves.

Attenuation, dispersion, and distortion affect different frequencies/mediums to different degrees, in different ways. Every transmission medium has a range of frequencies it can transmit it with minimal signal damage, e.g. 2.4GHz and 5GHz for Wi-Fi. The most widely available network is the PSTN (Public Switched Telephone Network).

## Binary Signals

Binary Signals are digital signals with only two possible values (Usually 1 or 0, but can be any two contrasting values).

They may use a basic threshold, where anything above X is encoded as a one, and anything below X is encoded as a 0. E.g. X could be 2.5V, in a 0-5V range. However, using such strict boundaries can cause problems as a minor change in signal could send the wrong bit. We can mitigate this by using ranges. E.g. 0-2V is a 0, 2-3V is undefined, and 3-5V is a 1. This will let us see what bits need retransmission.

Binary Signals are widely used because they are easy to generate technically, and recognisable. Furthermore, any digital data can be encoded via them (As 1s and 0s), and any analogue data can be encoded as digital data.

# Modes and Media

## Bits, Bytes, and ASCII

ASCII assigns a **7-bit** code to every letter, digit, and punctuation character (Case-sensitive). There is also a parity bit used for error-checking, so each ASCII symbol is one byte (8-bit).

## Parity

Parity can detect one-bit errors (As long as the errors do not cancel out, e.g. A 0 changed to a 1 **and a separate 1 changed to a 0**), and has several different types:

* Vertical/Longitudinal Parity: Vertical is where every byte of characters has its parity checked, but it cannot find the incorrect bit, only indicate its existence.   
  Longitudinal or horizontal is where an extra byte of information is transmitted in each “block” of bytes, which indicates the parity for each corresponding bit (E.g. The first bit of every block has its parity indicated by the first parity bit of the extra byte). **By combining the two methods, we can find where the bit error is (Vertical shows us which byte has an error, horizontal shows us which bit in the given byte).**
* Odd/Even parity: The parity bit is set to 0 if the **number of 1s in a bit string is odd/even respectively**.
* We can use odd vertical parity and even horizontal parity (or vice versa) in the same block, they don’t have to match.

## Transmission Modes

There are several transmission modes:

* Simplex: Data can flow in only one direction. E.g. a PA system/intercom.
* Half-Duplex: Data can flow either way, but only one way at once. E.g. a walkie-talkie.
* Full-Duplex: Data can flow both ways, simultaneously. E.g. A conversation, a phone call.

It can also be Parallel (Every bit of data being transmitted has a separate “wire”/channel), or Serial (They share a wire/channel). Serial transmission can be synchronous or asynchronous.

Parallel is fast and convenient, but expensive, and mainly limited to very short (10m) distances because of “skewing” (Where a delay on the wire can send the wrong bit, so the wires become out of sync, causing a chain reaction). A short cable means there’s less chance of this occurring, and helps keep costs down.

Serial requires parallel-to-serial and serial-to-parallel converters, as senders/recievers usually deal with 8 bit blocks, which must be (dis)assembled at each end. Software is usually used to do this. It can be asynchronous, or synchronous.

* Asynchronous serial has a signal to define stopping/starting. These signals must be defined beforehand, and cannot be used in the bit stream. They also must be different. Having to send signals and gaps slows down communication, but it is cheap and effective (If speed is unimportant). It’s widely used for terminal-computer communication.
* Synchronous serial is time-based. Data is transmitted in blocks of bytes, with no signals or gaps within the block. The receiver then organises the bitstream into proper bytes. It must know the data transmission speed, and the two stations must be time-synced. This is faster than asynchronous, and the basis of modern communications devices.

# More Modes and Media

## Choosing a Medium

A transmission medium is the equipment transporting the signal from Tx to Rx. E.g. The air (wireless), copper wires, Twisted Pair, etc.

We choose a medium based on cost, efficiency, lifespan, robustness (against interference)/security (Wi-Fi is vulnerable) and speed (Depends on medium, distance, terminal equipment).

## Types of Medium

Mediums exist in several categroies:

* Guided (Wired)
  + Twisted Pair: Pair of insulated copper wires twisted together, twists reduce noise. Standard and colour-coded pairs, each pair has a pair-number. They can be shielded (Overall, individual, or both) or unshielded.
    - Category One/Two standards are basic and only good for voice telephony/very low speed data
    - Category Three needs at least three twists/foot and can transmit 10Mbps. Standard for most telephones.
    - Category 5/5e need 5+ twists/foot, 100Mbps (5e is better protected against crosstalk (wires picking up signals from each other))
    - Category 6 has 6+ twists/foot, 1Gbps.
    - TP suffers from high attenuation so is limited to <100m, and is easy to tap.
  + Coaxial: Copper wire surrounded by insulator, metallic shield, and plastic jacket. Similar cost to shielded TP, 1Mbps-1Gbps, moderate susceptibility to attenuation/noise so can be used 1-2km. Easy to tap.
    - Graded as RG-6, RG-7 etc. with variance in number of shield layers, core/insulation thickness, and ratio of voltage/current amplitude.
  + Fibre: Silica fibre with cladding and an outer jacket, light is reflected down the core. Light carries signal instead of electricity, much less susceptible to noise, very fast (1.48Tbps recorded). Difficult to tap, expensive, fragile and difficult to install. Most long distance voice/data transmission and inter-continental traffic use it.
* Unguided (EM Spectrum, wireless)
  + Focused
    - * Microwaves are limited to line of sight.
    - Microwaves (Satellite)
      * Greater distance reduces their focus, so they’re easier to tap. Mostly used for TV broadcasting, some satellite phone purposes. Expensive, but huge capacity so using a small bit is cheap. Must orbit at 35863km, so high propagation delay (affects speech quality). Largely replaced by fibre for voice, but heavily used for data communications.
    - Microwaves (Terrestrial)
      * Repeaters can be used to achieve greater distances, and channels are simplex. Atmospheric conditions can cause interference. High capital cost, but cheaper than fibre. Hard and expensive to tap.
      * Still used for voice telephony, but fibre has replaced them for data.
  + Unfocused
    - * Broadcast makes it inherently unsecure, subject to attenuation etc.
      * Roughly line of sight at very high frequencies.
      * Reflection can cause problem of multiple paths.
    - Wireless (Wi-Fi, radio)
      * Covers larger areas than IR, can penetrate. Doesn’t need line of sight usually, fast transmission (54Mbps).
      * Hard to shield (penetrating), generates/subject to interference, licenses needed outside very limited frequency range.
    - Infrared
      * Simple and cheap, no licenses needed. Easy to shield, fairly secure, no interference from electrical devices.
      * Cannot penetrate walls, low bandwidth, needs line of sight.
    - Free Space Optics
      * Line of sight, but can pass through windows. 2.5GBps on distances up to 3km, used for “last mile” and linking LAN sections. No licensing.

# Data Transmission

## Equipment

Data Terminal Equipment is the source/destination of **digital** data, e.g. Software or network cards.

Data Circuit-Terminating Equipment is any device that transmits/receives data as an **analogue/digital** signal over a channel, e.g. modems.

A modem modulates and demodulates signals. Modulation converts digital to analogue, and demodulation converts analogue to digital. A method must be agreed beforehand.

## Modulation

Digital signals are prone to distortion, as their values are quite strict. We can avoid this by using it to **modulate** a carrier wave, which is then transmitted. Carrier waves can be adjusted based on the data type. We use Amplitude/Frequency/Phase-Shift Keying for Amplitude/FrequencyPhase modulation. They change the carrier wave’s amplitude/frequency/phase respectively.

Amplitude-Shift KKeying is much more noise-susceptible than FSK or PSK, and FSK needs to use two frequencies so requires more bandwidth for the same amount of data.

PSK can carry more information than either other method. It can represent data in two ways: By using a basic phase change to indicate change in value, or by indicating value by how **much** we shift it. E.g. If we split the cycle into quarters, we can indicate four different values via shifting. This is known as 4-PSK.

As there are four possible values, we can indicate two bits per cycle: 00, 01, 10, and 11. 8-PSK would let us send 4 bits per cycle, etc.

Bit rate refers to bits/second, baud rate refers to signalling events/second (Bd). E.g. 4-PSK might have a bit rate of 2kb/s, and a baud rate of 1kBd. The bit rate is greater than the baud rate when each signal sends more than one bit.

## Nyquist’s Theorem and Logs

Ignoring noise, maximum channel capacity (With bandwidth B and M possible signalling levels) is

2*B*log2*M* bits/sec

# The PTSN

The PTSN was designed for voice telephony, not data, so it has a limited range of frequencies (Like the human voice). This deliberately limits the bandwidth. To use it for data, we need modems, and channel capacity is limited and the signal/noise ratio is poor.

However, it’s everywhere and so is frequently used for data transmission. Better equipment (Broadband, Fibre etc.) has improved signal quality and it is now much more digitally-oriented.

Setting up a connection between two stations is called **switching**, and units that do it are called **switches**. Telephone exchanges are good examples of switches.

Consumers connect to local exchanges via cables like TP or Fibre etc., and this is managed by BT. Local exchanges connect to trunk exchanges (Which only connect to other exchanges via trunk lines (usually fibre, could be terrestrial microwave)), and these connect to international connections (Usually Fibre, could be Satellite microwave).

## Bandwidth

A **link’s** bandwidth is the range of frequencies it can transmit properly (Depends on medium, equipment, and link length).

A **signal’s** bandwidth is the range needed to transmit it properly.

Channel capacity is bits/sec, and depends on bandwidth, modulation technique, and signal=to-noise ratio.

A normal telephone circuit can transmit from 300Hz to 3300 Hz, and can transmit data in the range of 600-3000Hz. However, modern circuits have greater bandwidth.

Signal/Noise ratio is calculated as 10log10(signal power/noise power) dB.

The **Shannon-Hartley theorem** describes maximum channel capacity (Regardless of signalling levels) as *B*log2(1+10(r/10)) bits/sec, where r is the signal/noise ratio.

# Multiplexors and Switching

## Networks 101

Any node on a network can be categorised as a switch, client (E.g. A PC, software like browsers), or a server (Provides services, like web pages, a database, file store etc.)

A Local Area Network (LAN) covers one site or several very close sites, e.g. Aber’s network. They are usually privately owned by a single organisation, I.e. the Uni.

A Wide Area Network (WAN) connects sites further away from each other (From a few miles to globally), and physical infrastructure (Wires, links etc.) are usually provided by a separate provider. E.g. The UK’s Janet network.

## Cellular Systems

In a cellular system, the coverage area is divided into cells, each of which contains a base station. A base station has a ratio Tx and Rx to communicate to mobile phones, and are all connected to each other (Usually by fibre).

When a mobile phone calls someone, they communicate via radio with a base station, and the station routes the call (via fibre) to the appropriate base station for the target mobile phone, or to the PTSN via a gateway if they are calling a landline.

## Multiplexors

Multiplexing allows for several channels to be transmitted via a single physical channel (E.g. cable). A single microwave channel can typically multiplex 600 voice channel and 100x8Mbps data channels.

There are two main types:

* Time-Based
  + Time Division Multiplexing (TDM): All the bandwidth is given to a single channel for a single slot of time, then to another, and so on. Every slot is of equal fixed length, similar to Round-Robin scheduling. They switch fast enough to appear simultaneous.
    - Statistical TDM (STDM): Similar to TDM, but each time slot has a variable length based on how much traffic each channel has. More data being sent over a channel gives it a bigger slot, along with other factors such as signal priority, amount needed to transmit to end etc.)
* Frequency-Based
  + Frequency Division Multiplexing: Available bandwidth is split between channels (E.g. If the bandwidth is 1800Hz, two channels might each have 900Hz to transmit on) and they transmit **genuinely** simultaneously.

## Data and Voice Networks

In contrast to networks like the PTSN (although less so, recently), data networks are **specifically** designed to carry data. They have a higher bandwidth, and better signal-to-noise ratio which gives them a higher channel capacity and less need for modems (Less noise means we can just send signals digitally), and they can use “baseband” (digital) signalling.

Data transmission sends data in bursts (separated by varying gaps), whereas telephone signals are uniform and continuous. Because of this, the networks work differently: A constant data connection between terminals would be wasteful, and voice telephony would be difficult if a connection was established and dropped every time someone spoke.

Voice telephony uses circuit switching, where a temporary but dedicated physical connection is made during the call.

Data networks use packet switching, where data is sent in discrete packets (Of variable, limited length). Long messages may be split into several packets. Every packet has a control header. Every packet is sent independently, with each node choosing the next. Packets may take different routes and appear in the wrong order, or not at all, requiring retransmission.

If the packets must appear in the right order (E.g. for VoIP) without being reordered at the other end, we can use virtual circuits. A single route is chosen initially, and all packets follow it. This preserves the order, and reduces processing overhead, but at the cost of not having redundancy.

A Switched Virtual Circuit (SVC) is similar to dialup: A constant connection for a single session’s duration.  
A Permanent Virtual Circuit (PVC) is permanently set up (Until a contract ends).

# Wiring the World

## History of Internet

Created during cold war, 1969.

Initial use for universities and government research, decentralised against risk of nukes.

Shifted to IPv4 between 1982 and Jan 1st 1983.

## Internet vs. its Applications

Early internet applications were data transfer, email, and remote access.

Modern applications allowed for voice/video calling, remote access to huge multimedia databases.

Undersea fibre optic cables are vital for the internet’s running, as they connect international exchanges and servers.

## New Applications

The internet can be used by businesses, to find clients/consumers, market to them, gather market research, and provide e-Commerce.

Websites now host live access to audio/video, on demand access, easy remote access, various user tools, cloud storage, interactive conferencing etc.

## Implications

Internet TV predicted 1998 by BBC, social media boom, auto-tweeting.

Cloud based computation

# Standards

## Definition and Types

A standard means that a common protocol is agreed upon and used by manufacturers of something, so that devices and/or software share compatibility with one another. Web standards are governed by the W3C.

Standards help to ensure compatibility, keep things safe (E.g. Limiting how much power something can draw to stop overloading), and potentially encourage competition to become the new standard.

**De Jure** standards are recognised and laid down by a formal body, **De Facto** standards are accepted/complied with generally, but have no formal authority.

Full International Standards (Base standards) do not rely on other standards to work. This might allow too many different options, so the marketplace becomes saturated. Countries/Regions/Sectors may interpret these base standards in specific ways, to create **functional standards**.

## Enforcement

No general mechanism exists to specifically enforce standards, but non-compliant products can be sued by both consumers and sometimes the relevant standards-body. Some sectors (Telecommunications, pharmaceuticals, aviation etc.) have their own regulatory bodies (These are NOT standards-making bodies).

Standards are made by (inter)national organisations (British Standards Institute, International Organisation for Standardisation), professional bodies (IEEE), manufacturers (Sun/Oracle, with regards to Java), and major customers.

The ISO usually is membered by national bodies, and adopts their proposals. Their standards are reviewed every five years.

## Problems

De Jure standards take a long time to produce, so they may become outdated. They also must cover all areas, and so can become too general. Furthermore, the IP rights of the product/standard is left in question, and it can preserve old mistakes by forcing people to keep using them.

Until the early 1980s, standards were proprietary and so certain manufacturers dominated. **Open Standards** help to liberate users, as they have no copyright. E.g. UNIX, SQL, etc.

# Protocol Models and Frameworks

In the mid-70s, there were no general, overall structure to communication protocols, and no formal standard. Things used proprietary architectures/protocols. In 1970, the ISO (International Standards Organisation) established a sub-committee to handle this.

CCITT (Various telecommunication bodies, e.g. Post Office) was a liaison member of ISO, and they had a lot of common delegates. They agreed to word their documents identically, and began holding meetings in the same room, with the same people, at the same time (Basically joint meetings in all but name).

Out of this came the OSI Reference Model, which provided a basic framework to communication protocols. It provided layers to reduce complexity, and each layer (E.g. TCP/UDP, IP) handled one group of problems.

The layers were designed to work with a minimum of interactivity, be self-contained to stop internal changes affecting other layers, and only have interfaces to directly surrounding layers (E.g. TCP/UDP could contact IP layer, not Data Link layer). **The Seven Layers were Application, Presentation, Session, Transport, Network, Data Link, and Physical.**

# Introduction to TCP/IP Protocol Suite/Stack

Back in 1982-3, the internet shifted to Ipv4, and the Internet Protocol Transition Workbook was published to help people change.

The CATENET Model for Internetworking described the overall concept, and almost every technology (Pigeons!) is used. A **Catenet Gateway** allows different networks to connect and communicate, with multiple paths (No single point of failure). Within a network are sub-networks with hosts, connected by **Hidden Gateways**.

CATENET Gateways are now called **Routers**, and **Local Gateways** are now Interfaces.

The TCP/IP Protocol Stack is four layers, sitting on top of the actual program:

* Application: Many different options, standard ones like telnet, ftp, http etc. and also user defined ones.
* Transport: Well-defined protocols for transferring information (Transmission Content Protocol/User Datagram Protocol). TCP is reliable, uses ports, flow control (Consumer controls connection speed) and connections. UDP is unreliable, uses ports but no connections.
* Network: The networks being used, intercommunication (IP)
* Link: Wiring and such moving the actual data. (Ethernet, LAN, CSMA etc.)

## Ports and IP

Ports are an extra address used together with IP address. The IP Address identifies the host connection, the port number identifies the program targeted (Process numbers change/OS Dependent, but applications can reference ports and some have permanently assigned ones).

IP is connectionless, and every network connection has an IP address as well as a hardware-specific MAC address. Datagrams are independently routed, and it is unreliable. No flow control, order control, or error recovery at all. IP supports broadcasting and multicasting, and data fragmentation. Only the header is checked for errors (And trashed).

IP Datagrams are made of many different sections:

* 4bit Version, 4bit Header **length,** 7bit Type of Service (Precedence, delay, high-throughput Boolean etc.)
* 15bit Total **Length**
* 15bit Identifier
* 4bit Flags (Control fragmentation: Can/not be fragmented, last/not last fragment) , 11bit Fragment Offset (Every fragment has an identical header, where this fragment’s position was in the original packet)
* 7bit TTL (Time to Live, how many router hops to go for before being trashed), 8bit Protocol (256 options, what protocol is above IP (Usually TCP (Dec 6) or UDP (Dec 17), with about 40 **defined** options).
* 15bit Header Checksum
* 15bit Source Address: Usually dotted decimal notation, mapped to/from names via DNS. Different classes.
* 15bit Destination Address
* 15bit Options/Padding

## Dotted Decimal and IP Addresses

32bit numbers aren’t very human readable, so they are split into four 8bit groups and each group is treated as decimal. The decimal numbers are then put together, with dots between them. E.g. 10100101010010001111010101100101 becomes 10100101 01001000 11110101 01100101 becomes 165.72.245.101

IP Addresses don’t identify a host or device directly, they identify a network connection point (E.g. Router). There are four classes, all of which are 32 bit. The first bits (Marker) always end in 0, and identify the class:

* Class A: Marker bit is a 0, then a 7bit Network Address, then a 24bit Local Address. Only 128 (27) exist, but each can hold a huge amount of hosts.
* Class B: Marker bits are 10, then 14bit NA, then 16bit LA. A good balance between network quantity existing and hosts each can hold. Aber has one.
* Class C: Marker bits are 110, 21bit NA, 8bit LA. (Fairly small but fairly common too)
* Class D (Multicast): Marker is 1110, only has a 28bit Multicast address (A group of hosts subscribed to this certain address all receive the data).

A router updates its network map every couple minutes, and routes IP packets as fast as possible. It knows how to get to directly-attached-network machines immediately, and usually knows the optimal route to some small, specific networks (with other routers). Most routers have a “default” router gateway which is used if no better route exists.

**Netmask** is a better and more flexible system. Netmasks don’t have specific partition sizes for NA and LA, writes bits as 1 if they part of NA, as 0 if LA. Routers/Machines attached to networks that use netmasks must be told about them. E.g. A Class A’s netmask would be 11111111 000…0, or written as 255.0.0.0 and this allows for smaller network address sizes, so that individual networks don’t all need to take every address (E.g. 128 in a Class A) that a class allocates.

Netmasks allow us to split large networks into smaller ones (using Subnet Masks), or combine networks into larger ones (using Supernet Masks). This is done by allocating X amount of bits away from NA or LA, into LA or NA to reduce addresses one section can have, to increase them in the other section.

## Other Protocols, More Addresses

Two other protocols are the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). Both of these are part of the IP layer.

A MAC Address is interface-unique and usually burnt into the hardware, it is 48bits in Ethernet. If the interface card fails, it is replaced and the MAC address changes. This means that if we routed via it, everything would need updating. To get around this, we route via the IP address and MAC addresses are only known within their own network (up to router).

ARP and RARP are protocols to map IP Addresses to Media/Physical Addresses.

## More about TCP and UDP

TCP maintains reliability by sending first a certain-sized “window” and getting an acknowledgment from Rx, then sending more bits, until the window is full. The receiver can change the size of the packet window (flow control) by including a new value in the header of returning datagrams. The window uses **bytes, not packets**.

TCP doesn’t have an explicit command to request retransmission, it happens automatically if acknowledgement is not received in time. However, the Round Trip Time (RTT, which is key to setting this value) can vary over transmission.

UDP is connectionless, and has no error recovery, flow control, or delivery confirmation. It is faster than TCP, and adds multiplexing (via ports), but has no real advantages beyond that.

The UDP packet contains a source/destination port, length, and checksum (optional), and then just data.

# The Domain Name System

DNS maps hostnames to IP addresses, and vice versa. It’s a distributed database of info, and runs on a client-server basis. No single site manages the whole name space, Network Information Centres maintain different top level domains (E.g. the “.uk” domain) and delegate authority for zones (subtrees, like ac.uk) to other institutions.

A Number to Name Lookup requires separate DNS servers to hold the mappings.

The organisation in charge of a zone must provide multiple Name Servers for the zone, and Name Servers have authority for one or more zones. Primary and Secondary NS exist. An NS can serve info from its own zone, and cached info from other zones, or query other NSs for up-to-date info.

DNS Messages have:

* ID and Flags
* Number of Questions, Number of answer RRs
* Number of Authority RRs, Number of additional RRs,
* Questions
* Answers
* Authority
* Additional Info

DNS has ports for both TCP and UDP, but predominantly uses UDP except for two special cases:

* If we try to query a previously-unknown ftp server’s IP address, we use a TCP connection.
* Trying to query another ftp domain (Far away) for its IP address.
* It tends to be used for large file transfers.

# Network Topologies

The three traditional types of topology are:

* Star: Equipment connected centrally, central machine routes all traffic intelligently. Single point of failure, but can also be faster as routes between nodes require less jumps. However, can survive failure of single nodes. Other nodes will find it difficult to intercept traffic, but access to the central node gives access to all traffic.
* Ring: Equipment connected in a ring, traffic travels around ring until hitting the destination. No single point of failure, but may take longer than Star. More damaged by single nodes failing, but can survive one node failure or a break in the ring by having a counter-rotating ring as well. A single exploited node will have access to all traffic.
* Bus: Equipment connected to one shared medium in a linear fashion, data is broadcast on medium to reach destination. A break in the line will cause any nodes past it to divide into subnetworks. Furthermore, a signal will “rebound” when it abruptly hits the end of the cable, which can cause problems with corrupt duplicate data. Also, any compromised node can easily spy on data. However, it can survive any nodes being lost.

## Physical and Logical Topologies, Media Access

Physical and Logical topologies may not always be the same. For instance, all nodes may **appear** to connect to a central hub, but actually just connect to other nodes directly from it, by linking wires to each other with no central point.

In a LAN, users share common links in the network, so right of way must be established. One way of doing this is **Carrier Sense Media Access (CSMA)**: Continuously check to see if the link is in use, transmit info when it’s free, return to step one.

You can also add Collision Detection to this, for CSMA/CD: When transmitting, we check for a collision, and transmit JAM if there was one. It then delays for a random bounded amount of time, and goes back to checking for a free link.

A different method is Token Passing: In a Ring network, all equipment is linked to the link. A token is passed around, and kept by a device that wants to transmit, until it finishes transmitting and releases the token. If the token is kept too long, a duplicate one is made, which can cause issues. Issues also are caused if the token-holder goes offline, and there is then no token.

Slotted Systems also exist, which initialise the Ring to have a fixed amount of bits. The network is then split into slots of a fixed amount of bits, and each piece of equipment can wait for an empty slot to fill with data needing to be transmitted. Cambridge Ring is a variant of this, where receivers take a **copy** of the data and add an acknowledgement token to the slot.

# Ethernet

## Standards and Protocols

Derivative of work from Xerox, Intel, and Digital Equipment Corp.

Produced Ethernet Blue Book in 1980.

802.3 Revision in 1982 by IEEE, 1984 Revision 8802/3 by ISO.

## Components

An Ethernet uses Coaxial cable (For the bus), MAUs to link devices to the bus, repeaters to clean up/amplify signals before connecting them to a bigger bus, terminators to stop signals from reflecting, bridges to selectively forward between **similar** networks, routers to IP-level forward between different network types etc.

## Media Access

Uses CSMA/CD, no priority.

## Types of Media

The original Ethernet (10BASE5) delivered 10Mbps using a baseband coaxial cable in 500m segments. Each segment could be tapped 100 times, with a maximum of four repeaters between any pair of stations (E.g. Host computer).

10BASE2 (1985) allowed for a thinner coaxial cable, and segment length of 185m with a maximum of 30 taps per segment.

Other options for the medium were:

* 10BASE-T: Unshielded Twisted Pair, 10Mbps.
* 100BASE-TX: Twisted Pair, 100Mbit/s.
* 1000BASE-T: Twisted Pair, 1Gbit/s Ethernet
* 10Gbit/s Ethernet for point-to-point only, with various media options.
* Fibre variants

## Round Trip Time, Slot Time, Packet Sizes

All stations attached to Ethernet **must** be aware of any collisions involving packets that they send. This means that packet length must be of a size that transmit time is greater than twice the transmission delay of the longest route, so that every station has time to notice corruption.

For the biggest network allowed (2.5km) at a speed of 10Mbit/s, the slot time is 51.2 microseconds so we have >512 bit packets.

## Packet Format

* Preamble: 7 octets. (Used to calibrate timings at each end)
* Start of Frame Delimiter: 1 octet.
* Destination Address: 6 octets.
* Source Address: 6 octets.
* Length in 802.3/packet type in original Ethernet: 2 octets. (Usage depends on format, almost always packet type)
* Data and Padding: 46-1500 octets.
* Frame Check Sequence: 4 octets.

## User/Application level performance

Because we have to send so much information that isn’t data, and have a minimum packet size of 512 bits in a 2.5km network, “raw” speed is very inaccurate, and much slower (When sending small chunks of data, much less noticeable with large chunks of data).

When using CSMA/CD with an 802.3 LAN, it is not guaranteed that the media will ever be free, and collisions can be indefinite for very busy networks. If you transmit JAM, the random delay window then increases in size, so you have more **distinct** values to choose from. Every time doubles the amount of options to choose from.

This means that it’s not necessarily good for Real Time Use, but this depends on the function. Time-sensitive, or critical things aren’t good options for it, but most other things are.

## Bridges/Switches

Bridges and Switches partition a LAN, which segregates the load, and add reliability and security. Remote LAN segments can then be combined into a single logical network, and separately developed/controlled whilst still able to communicate easily. If a packet doesn’t come from a whitelisted node, it can’t pass through the bridge, in some cases where security has been added.

A Bridge monitors all traffic, and forwards a copy of any data that needs to move inter-network to the right network. Whilst waiting for an open line on the second network, the copy is held at the bridge. Forwarding is based on the packet’s header info. A switch is very similar to a bridge, and practically identical at this level.

All traffic enters the bridge (as a copy), but is discarded unless it needs forwarding.

IEEE 802 LANs often use these. Bridges usually contain a repeater, and are sometimes known as a MAC level relay.

## Packet Forwarding

* If the packet’s destination is in the same LAN, it is discarded.
* If the destination is in a different LAN, it is forwarded.
* If the destination address is unknown, the packet is forwarded to all non-source LANs in a flood.

Bridges update their forwarding database (What addresses are in what LANs) when packets arrive from a certain port/LAN, as the source address must be in that source port. This works well if there are no alternative routes, but not if there are loops in the network. Unfortunately, loops are useful to maintain resilience (No single point of failure).

If there are loops in the network, this doesn’t work because the bridges receive the same packet multiple times, from apparently different sources, and so overwrite values with incorrect ones. We can solve this using a spanning tree (no loops) by representing a LAN with a node, and a bridge as an edge:

1. Every bridge is numbered
2. Broadcast numbers periodically
3. One bridge becomes the root bride
4. Every bridge discovers route to the root bridge via the root port.
5. Each LAN gets a **designated** (minimum weight) bridge to the root bridge, determined by minimum weight path-holder.
6. Only designated bridge can forward to/from LAN.
7. Communicate with each other by sending a Bridge Protocol Data Unit: Originating Bridge number, root bridge number, root path cost.
8. Initially all bridges think they are root, and broadcast their BPDU accordingly. If a superior bridge’s BPDU is found, that bridge then is assigned to be root port/path cost.
9. If a BPDU with a shorter root path is found, the bridge releases claim of being a designated bridge.
10. This means the lowest numbered bridge becomes root, and each LAN has one designated bridge.
11. Other bridges are blocked.

A Local Bridge connects two+ adjacent LANs, with high throughput. There is likely minimal degradation of speed caused by waiting for packets to be acknowledged/transferred.

A Remote Bridge connects two+ widely-separated LANs, and consists of two “half bridges” connected by a WAN link. The link between the half bridges is usually slow, 64Kbps or 2Mbps.

Bridges are often available in a managed form, and able to be loaded with forwarding tables. They can filter for packet type, or for host, and often provide feedback like traffic reports, forwarding issues, network errors etc.

A Bridge to the management station is required.

# The JANET Network

## Origins and Coloured Books

Original team (Joint Network Team- JNT) created in 1979, with six staff. Large variety of networks, control, management, and technologies so hard to keep everything compatible.

The X.25 network was a CCITT standard, and in use for UK HE. It was adopted by the Post Office for a packet switching system (PSS, the Packet Switching Service). It had diverse Upper Layer Protocols.

X.25 was slow because it’s error-checking (at IP layer), integrating with it slows down other technologies.

Coloured Books started to be produced by JNT to define standards and protocols for different fields and technologies. The **Yellow Book** defined Transport Protocols to unify various technologies.

Coloured Book protocols were made mandatory in Computer Board funded procurements, and HE became early large scale users of PSS.

## Upgrades

In September 1980, JNT proposed that HE built a dedicated network using X.25, and this was completed in April 1984. It was X.25 based, with 9.6kbit/s link speeds and about 50 sites. (Legality of this was controversial as telecoms were heavily regulated)

LANs appeared in the early 1980s.

In the mid-80s, it was upgraded to 64kbit/s links and a 2Mbit/s trunk connection. It was upgraded again in the early 90s to 2Mbit/s links, and became the highest performance X.25 network globally.

In the late 1980s, it was funded to support polytechnics and colleges, which allowed research/HE from outside universities to join the network. It was now serving 200+ sites, and the JNT team totalled about 12 staff.

The JNT team had to decide whether to use X.25 or Cambridge Ring networks for their LANs.

The Orange Book was designed to define protocols for transport over Cambridge Ring, but dragged down Cambridge Ring to be an X/25 equivalent. This book led to ISO 8802-7.

Meanwhile, the world adopted Ethernet, unlike the UK who developed the Pink Book to make Ethernet essentially another X.25 network.

The JNT Packet Assembler Disassembler (PAD) allowed terminals to connect to X.25/Ethernet Networks.

## LAN Deployment

Ethernet started to be deployed at 10Mbit/s, and in the early 1990s some FDDI (Fibre links) at 100Mbit/s.

Asynchronous Transfer Mode LAN program in 1994

Coloured Books were planned to be transitioned to ISO protocols like the rest of the world, and the White Book was produced to help with this.

X.500 was used for Directory Services, X.400 for Email Services.

## SUPERJANET’S ORIGIN STORY (As told by Marvel, and the JNT)

In 1991, the JANET IP Service was introduced on a shoestring budget, sharing X.25 bandwidth and carried over X.25 tunnels.

In 1987, there was at 64Kbit/s (Total) link between JANET and NFSNET (US Science/Research network), upgraded to a 2Mbit/s Atlantic link in 1994.

JNT proposed SuperJANET in 1989, and BT got an £18million contract to build it in November 1992. This became a 34Mbit/s SMDS network and 34Mbit/s ATM network, with upgrades planned for 155Mbit/s. JNT staff reached 22.

In 1994, JANET was taken over by the JNT Association (Created 1993, later known as UKERNA).

SuperJanet II procured Metropolitan Area Networks (MANs, e.g. South Wales MAN) and created new links to 27 institutions, either SMDS (4Mbit/s) or leased lines 8Mbit/s. 8Mbit/s Aber-Cardiff link. Also MANs at Edinburgh, Glasgow, etc.

## International Connectivity

By June 1997, there was a 45Mbit/s TeleGlobe link. Connectivity growing over the years.

May 1998: two 45Mbit/s links, 34Mbit/s link to Europe.

UK ISPs providing 100Mbit/s links.

US declares tariffs on TransAtlantic links in Nov 1998, 2p/MB because line is too saturated. 1am till 6am free.

## SuperJANET Returns: The JANETing

SuperJANET IV meant to be built for growth, gigabit capacity. Planned to link all HE MANs.

Initially 2.5Gbit/s link, later upgraded to 20Gbit/s link. Harnesses new technology and broadens user base, uses multiple light frequencies down fibre for multiple channels. Installed around 2001.

SuperJANET V planned to minimise single points of failure, more flexible. Two links to major network points to increase reliability.

SJ5 completed in 2008, some 40Gbit/s links.

Janet6 planned in 2009, Janet4G project launched.

# Wide Area Services

There are various modern services available for the public to receive and send data.

* PTSN: Slow, not designed for data, but infrastructure available everywhere.
* High Speed Short Haul Services
* Integrated Services Digital Network: Fully digitally dial-up network
* DSL: Digital Subscriber Line, e.g. ADSL.

WASs are designed to have a greater broadband, tuneable lines for better signal/noise ratio, and may use fibre or more than one wire pair. They also have very different tariff principles.

## Leased Lines

* Available 24/7 with a fixed annual charge.
* Analogue and Digital available
* Single exchange area, long distance both available
* Some unavailable for new supply post-Oct 2016

PTSN costs tend to be around 3.4p/minute to 6.7p/minute for local/national (Consumer), 20p/minute for businesses, and cost a significant deposit to install the phone line, or to rent it annually

### Analogue

* For the cost of installing and annually renting an analogue Leased Line, you get only 220 PTSN hours/annually, or 100 hours/annually for the cost just renting it for a year, for lines within the same town.
* For lines between nearby towns (Several miles), installation costs the same as 170 PTSN hours, and then 300 PTSN hours annual rent.
* For long distance (Couple hundred kilometres), 740 PTSN hours to install and rent for one year, 565 PTSN hours to rent for one year.

### Digital

* For long distance (Couple hundred kilometres), 640 PTSN hours to install and rent for one year.

(KiloStream: 2.5Kb/s – 64Kb/s services, 128Kbps/1024Kbps premium service).

## Short Haul Services

Provided via either LAN/Ethernet Extension Services (LES/EES, mostly deprecated. Still one 10Gbit/s link available) or SHDS Connect (Short distance <45km point-to-point communication carrying Ethernet between sites, nationally available. 10/100/1000Mbit/s Ethernet LANs)

# Integrated Services Digital Network (ISDN)

ISDN was the first time that dial-up digital communications reached customer locations. It also introduced important features like Caller ID in a standardised manner, and provided a channel for the first flexible video conferencing.

It’s still very much used today, e.g. to bring in telephone service.

ISDN provides more services to end users, which were previously not available outside of things like leased lines.

New services for it are designed to be compatible with 64Kbit/s switched connections, and the network is intelligent to provide management and maintenance functions.

## Services/Types of ISDN

* Bearer service: Provides only connectivity, no knowledge of data or protocol.
* Tele Services: Interprets protocols, provides extra services, cross-compatible with PTSN customers.
* Supplementary services: Additional extras, such as Caller ID, Call Forwarding, Caller ID Hiding, closed user groups etc.
* Basic Rate Access:
  + Can have up to eight devices between the three channels, old equipment (Analogue telephones, X.25) used Terminal Adapters to connect.
  + 2B Channels: 64kbit/s each
    - Voice
    - Fax
    - Slow video
    - Data
  + 1D Channel: 16kbit/s
    - Signalling (Can signal without interrupting phone calls)
    - Telemetry
    - Low speed data
* Primary Rate Access:
  + UK/Europe: 2Mbps
    - 30B Channels 64 Kbit/s
    - 1D Channel 64Kbit/s
  + US, Canada, Japan
    - 23B Channels 64Kbit/s
    - 1D Channel 64Kbit/s

It costs about £370 installation, and £145 monthly rent. Call charges are equal to PTSN, and bit cost are less for data. Generally cost-effective against leased line if you only need connectivity for a few hours a day.

A clever variant of this was BT Home and Business Highway. They offered an ISDN2e service, with two analogue sockets as well. Essentially just two inbuilt TAs for analogue equipment, still only two B channels and one D channel.

# Digital Subscriber Lines

A lot of companies offer DSL services, and almost all provide IP services/internet, but almost all only resell the underlying (BT/Kingston owned) infrastructure for connecting users. However, they usually own their own equipment.

Some resell “Local Loop Unbundling” services provided via BT’s Metallic Path Facility. This means that multiple telecoms can be connected to the same end-user connection.

One rare example of a company using its own infrastructure is Virgin Media, and some other cable TV companies.

## Types of DSL

* ISDN: Integrated services Digital Network
* ADSL: Asynchronous Digital Subscriber Line
  + Most people use this.
  + Single copper wire pair of TP wires.
  + Download speed is faster than upload.
  + Link shared with normal phone service, performance based on distance from exchange, cable quality, and contention ratio (How many users you’re sharing connection with, usually 50:1 standard for home products, but could be better as not everybody downloads at once. Can also be affected by ISP’s connection to network, or their equipment’s internet connection).
  + Signal is split into ATM cells, carrying IP packets. Uses BT’s IPStream service.
  + Uses ADSL splitters to keep ADSL signals away from phones, modems etc.
  + Can use an ADSL modem (configurable for ATM transport) or a Router (connect to multiple computers, may have modem integrated or separate)
* SHDSL: Symmetric/Single-pair High bit-rate DSL
  + BT SHDSL takes whole line, can’t share with voice/other services.
  + Uses dedicated MPF
  + Being phased out in favour of Broadband Connect
* MPF: Metallic Path Facility
  + Not really DSL, direct access to end-user wire connections. Services depend on what the LLU Operator connects, can now access poles/ducts.
  + Symmetric
* BTnet Leased Line
  + Variety of symmetric internet access links
  + Varies from 512Kbps to 10Gbps
* Cable TV Services
  + Virgin Media owns their own infrastructure, offers speeds from 50Mbps (£19 monthly) to 200Mbps (£32 monthly) plus £18 phone rental.

## New ADSL Services

New ADSL services (E.g. IPStream Max (Premium)) handle contention differently, more dependent on the way IP connects to the BT network.

Quality of Service facilities now exist to allow ISPs to prioritise traffic to some customers, stop their rates dropping (Premium).

Easynet’s LLUStream uses BT’s MTF, uses SHDSL, ADSL etc. and offers 8Mbps ADSL, 2Mbps SHDSL. Higher speeds with other technologies.

Eclipse Internet allow you to increase bandwidth on demand. Some providers offer mail boxes, web space, IP addresses etc.