Hugh Baldwin
up2157117

Networks

M30231
TB1&2

University of Portsmouth
BSc Computer Science
1st Year

Contents

1 Lecture - Networks Introduction **2**

2 Lecture - Network Protocols **4**

3 Practical - Collisions **6**

4 Lecture - More Protocols **7**

5 Practical - Protocols **10**

6 Lecture - NICs and Ethernet **11**

7 Practical - Switches and Hubs **14**

8 Lecture - Standards and the OSI Model **15**

9 Practical - Riverbed Simulation Results **18**

10 Lecture - Communication Media **20**

11 Practical - Signals **22**
11.1 Key Terminology - Signals 22

12 Lecture - Communication Circuits **23**

13 Practical - Signals Cont.d **25**

14 Lecture - Wide Area Networks **26**

15 Practical - Excel Noise Simulation **29**

16 Lecture - Asynchronous Transfer Mode (ATM) **30**

17 Lecture - Interconnection Protocols **33**

18 Lecture - Network Security **36**

19 Lecture - Network Security Cont.d **38**

20 Lecture - Network Management **42**

21 Lecture - Application Support Protocols **46**

22 Lecture - Application Support Protocols Cont.d **49**

23 Lecture - Network Policies and Standards **52**

Lecture - Networks Introduction

09:00 04/10/22 Amanda Peart

What is a network?

- A network is a group of devices (PCs, Laptops, Mobile phones, etc) that are all able to communicate with each other to share data, files or programs
- Hardware - The physical connections between devices in the network, e.g. ethernet cables, fibre lines, wireless access points, etc
- Software - What enables ut to use the hardware for communication and exchanging information
- Networks should be ”Interoperable” - this means that different types of devices, using different operating systems, can all connect to the same network and communicate with each other to share information, as long as they can all communicate using the same network protocols

Network Topologies

- Star Topology:
  - All devices are directly connected to a central ”hub” - usually a switch
  - If one node fails the rest of the network will still function
  - More common in networks of today
  - Easy to add or remove nodes as they are needed
  - Number of nodes is limited to the number of ports that the central switch has
  - If the central ”hub” or switch fails, the entire network fails, and so there is a single point of failure
  - If the central ”hub” is slow, the entire network will be slow
- Bus Topology:
  - All devices are connected directly to the main cable known as the ”backbone”
  - Cannot cope with heavy traffic
  - Prone to collisions when two nodes try to communicate at the same time
  - Difficult to administer or troubleshoot as if the cable breaks the entire network stops functioning
  - Limited cable length, number of nodes is limited by the length of the cable
  - Performance degrades as additional devices are added
  - Not a popular design as it is very limiting
  - Should is really only be used for a small group of computers
- Token Ring Topology:

  - All nodes on the network are connected in a ”loop”
  - Nodes must wait until they have the ”token” before they can communicate on the network, making collisions impossible
  - All nodes get a chance to communicate on the network
  - Good ”quality of service”
  - If one of the nodes or cables goes down then the whole network may go down
  - Tokens may get lost or corrupted
  - Difficult to add or remove nodes from the ring

- Mesh Topology:
  - All nodes are connected directly to other nodes
  - Redundancy as if any node goes down the traffic can be re-routed
  - The network can be expanded without disruption
  - Requires more cabling than other topologies
  - Complicated to implement
  - Large amounts of cables that will only be used on occasion
  - A ”partial mesh” network can be constructed where each device is connected to a few others, but not all as that way there is still redundancy but less wasted cabling and less complexity

Lecture - Network Protocols

09:00 11/10/22 Amanda Peart

Protocols are the rules for communication. They define the rules that are used to communicate between devices, applications or components of an application

What if conditions:

- Networks protocols define the behavior for a ”what if” condition. e.g. missing packets, bit flips, receiver dropping packets due to limited processing power, etc
- This behavior could be anything from ignoring it and continuing, or resending the entire message, depending upon the protocol

An example

- Consider the problems that early telegraph operators would have faced
- 2 train stations have a telegraph line between them
- There are 10 telegraphs to send in the morning

The first problem:

- Should you just send a random telegram at any time?
- Should you send the shortest telegram first, or send them in a specific order?
- What if there’s no one at the other end? Should there be a special ”are you there” message before the actual telegram?

The second problem:

- Should you send the telegrams immediately after each other?
- Should you receive an acknowledgement from the other end after each?
- Should there be a break between telegrams?

The third problem:

- What if A is sending faster than B can receive?
- What if B has to stop receiving telegrams to do something else?
- What if you finish your shift but there are still telegrams to be sent or received?
- What if both A and B send at the same time?

These are all problems that are faced in a modern network, and are the reason that standardised protocols are so important

Connection-oriented protocols

- TCP is an example of a connection-oriented protocol
- A connection-oriented protocol is any protocol where there is a ”private network” that directly links the sender and receiver
  - They work similarly to a phone call as there is a ”virtual cable” directly connecting between the sender and receiver
  - Connection established
  - Data sent between devices
  - Connection closed

Connectionless protocols

- Less assurance that the message got to the receiver
- No connection established and therefore no disconnection
- IP is an example of a connectionless protocol

Tradeoffs of connectionless vs connection-oriented protocols:

- Connectionless protocols don’t need to establish or clear a connection
- Packets in connectionless protocols are more wasteful of bandwidth, as they need to have additional addressing information in the metadata of every packet, which adds up quickly, whereas a connection-oriented protocol only needs the virtual cable id added to each message
- Packets can be easily discarded if the network is too busy, whereas a virtual cable must be carefully managed

Why do we need TCP/IP?

- If we just sent out packets without the protocol, they would just get lost on the network
- For example, if we wanted to send a packet across the internet between LANs, each router along the ”journey” would read the desired IP address from the packet and relay the packet to the next router, getting closer to the receiver with each hop
- IP addressing is needed to route the packets across the internet
- TCP is needed to assure that the packets are all received, uncorrupted and in the correct order to ensure that all of the data is correct
- Every message sent across the internet uses at least these two protocols (TCP & IP) but usually also use other protocols within the message itself so the receiver knows how to interpret the message, for example an email may use SMTP or POP as well as TCP/IP

Practical - Collisions

12:00 12/10/22 Athanasios Paraskelidis

- By design, the one cable at the centre of a bus topology network is shared between all computers on the network, and therefore collisions are very likely
- A domain is a region of a network where all devices listen to any communication on the network, and a bus network only has one domain
- You can find the domain by looking at where there is shared medium (a physical connection shared between multiple devices, such as a bus)
- A collision occurs when multiple devices try to communicate in the same domain at the same time

Preventing Collisions

CSMA/CD (Carrier Sense Multiple Access / Collision Detection) algorithm:

1. Is the medium idle (no other messages being sent)?
   - Yes? Start transmitting
   - No? Go back to the start of the algorithm
2. Are there any collisions now?
   - Yes? Continue sending packets for the minimum packet time (minimum time for a packet to transfer across the medium) to ensure the other node has detected the collision
   - No? Finish transmission
3. Has the maximum number of transmission attempts been reached yet?
   - Yes? Abort the communication
   - No? Wait for a random length of time, then go back to the start of the algorithm (the node with the shortest time to wait will transmit first)

Lecture - More Protocols

09:00 18/10/22 Amanda Peart

- Rules for sending and receiving data across a network
- Provides addressing
- Management and verification of transmission
- Often used in conjunction with other protocols, such as TCP and IP

Connection Orientated

- Similar to phoning someone on a landline
- 3 phases
  - Connection setup
  - Open connection
  - (Send data)
  - Close connection
- Quality of Service
  - High quality of service
  - Low fixed delay between sender and receiver
  - Limited packet loss

Connectionless

- Similar to sending a letter in the post
- Each packet (letter) has an address attached before it is sent over the network (put in the post box)
- Once it is sent, you just have to assume that it was received
- Quality of Service
  - Variable delay between sender and receiver
  - Packets can and will be lost
  - Issues with packets arriving in the wrong order

Packets

- A packet is a single unit of data that is sent across a network - The size of the packets is determined by the sender
- Data is broken down into packets before it is sent across the network
- Examples of data that is sent across the Internet using packets:
  - Emails - SMTP (Simple Mail Transfer Protocol) or POP3 (Post Office Protocol 3)
  - Files - FTP (File Transfer Protocol)
  - Web pages and images - HTTP (Hyper Text Transfer Protocol)
- Each packet also contains header information - This could be compared to the address written on the front of the envelope in the postal analogy
  - This includes the IP address of both the sender and receiver
  - It also includes information on how to handle transmission errors
  - Header information is used by routers and switches to determine where the packet should be sent next
- Routers are devices dedicated to reading header information and relaying packets to the next router
- Packets move from router to router until they reach their final destination - Similar to sorting offices in the postal analogy
- Each packet of a communication may not necessarily follow the same route to their destination
- The route is determined by the router, and which path is the fastest or least congested at the time, which can change between packets

TCP/IP

- TCP/IP is a connectionless protocol, which is actually made up of 2 protocols, and is used almost everywhere on the internet
- TCP = Transmission Control Protocol
  - Breaks up the data into packets that are easier for the network to handle
  - Verifies that all of the packets arrive at the destination
  - Re-orders the packets into the correct sequence to get the data back out again
  - If any packets are damaged, TCP will request them to be resent
  - It also acknowledges that all of the packets have been received successfully
- IP = Internet Protocol
  - Breaks the data into packets
  - Adds the header information into each packet
  - Determines how much data should be put into each packet

For example, sending an email:

- The data that makes up the email message is split up into packets by the IP (Internet Protocol)
  - Header data is also added to each packet

- Using the header information in each packet, the routers and switches that make up the Internet determine the best path for each packet to take to their final destination
- TCP (Transmission Control Protocol) then reassembles the packets into the correct order and ensures that all packets were received undamaged, then extracts the email message data from the packets

Practical - Protocols

12:00 19/10/22 Athanasios Paraskelidis

- In a packet, the information used to help deliver the packet is known as the header, and the actual data is known as the payload
- IP or Internet Protocol is responsible for addressing all devices on the internet, so that all other protocols know where the data needs to be sent

TCP

- 3 way hand shake
  - This is established before any packets of data are sent across the network
  - SYN is sent by the sender to receiver to request a connection
  - If the connection is to be accepted, the receiver sends SYN/ACK to confirm the connection
  - The sender then sends ACK to the receiver, to acknowledge the connection
  - Data is then sent across the connection - this may be either one small message or a large message broken down into smaller packets
  - When the payload has been sent, the last sent packet will have the ”FIN” bit set to 1, meaning that it is the final packet, and the connection can be closed
  - After each packet is received, the receiver sends back an ACK message to confirm that the packet was received intact. If the ACK message is not received by the sender, it will resend any packets that it did not receive an ACK message for
  - Once all of the packets are received intact, and a packet with the FIN bit set to 1, the connection is closed

UDP

- UDP (User Datagram Protocol) is another protocol commonly used on the internet
- There is no guarantee that the data has been received correctly
- No connection is established
- There is no handshake between sender and receiver
- There is no acknowledgement of received packets
- No error checking, sequencing or flow control
- It is faster and more efficient than TCP, but can not be used for all types of data. It is commonly used for streaming video over the internet as it does not matter if some packets are lost or received in the incorrect order, as this will result in dropped or frozen frames, but will not cause any issues such as corrupted data

Lecture - NICs and Ethernet

09:00 25/10/22 Amanda Peart

NICs (Network Interface Cards)

- There are many different types of aNICs, which are used to communicate using different mediums, e.g. WiFi, Ethernet, etc
- Each NIC has a 48-bit unique identifier known as a MAC address (Media Access Control address)
- The MAC address allows you to determine both which NIC communicated, but also which manufacturer made the card, and theoretically when the NIC was produced
- NICs read all broadcast addresses and
- All multicast messages with addresses it's been programmed to read
- The hardware will simply ignore all other messages

Ethernet LAN access devices

- Client devices have a cable between them and an interconnection device, usually in a network rack
- An "interconnection device" could be:
  - A hub (Legacy)
  - A Switch
  - A Router (To access a different network, such as the internet)

Access rules for ethernet hubs:

- Listen before sending
- Stop if multiple users start at the same time

Distribution rules for ethernet hubs:

- All traffic is sent everywhere
- One packet is sent at a time

Access and distribution rules for Ethernet LANs:

- Send whenever you want to
- No collisions
- Traffic is only sent where it needs to be
- Multiple packets can be flowing at the same time

Switched Ethernet

Characteristics of a switch:

- Automatically learns the addresses of all connected devices
- Forwards only to the destination
- Supports many ports per switch
- Supports full duplex on dedicated ports (Can send at full speed in both directions at the same time)
- Supports different data rates on different ports
- Ethernet switches usually operate in store-and-forward mode
  - Temporarily holds the packet while deciding which port the packet needs to be sent through
- Some switches may also support cut-through operation

Unicast vs Multicast

- Unicast sends a packet in one direction to a single node on the network
- Multicast sends a packet to multiple nodes on the network in a target group (not all nodes on the network)
- Broadcast sends a packet to all nodes on the network

The LAN networking model

- The data link layer is split into two sub-layers
  - LLC (Logical Link Control)
  - MAC (Media Access Control)
- Common aspects of LAN standards
  - All use the same MAC addresses
  - Supports broadcast and multicast addressing
  - All have 32-bit error checking
- Different aspects
  - Access methods (CSMA/CD vs Token)
  - Maximum frame size
  - Support for features such as priority
  - Specific data rates

Virtual LANs (VLANs)

- Software emulates a physical LAN
- The purpose of VLANs is to limit broadcast traffic to a set group
- The group is set by network management
- VLANs are enforced by
  - Selecting a set of ports on a switch
  - Selecting a set of MAC addresses
- VLANs are more convenient than re-wiring the entire network

Ethernet standards

- PoE (Power over Ethernet)
  - Provides power through the ethernet cabling, reducing the number of cables and ports needed for low power devices such as access points
  - Defined in 802.3af
- 10 Base5 (10mbps, 500m max)
- 10 Base2 (10mbps, 185m max)
- 10 Base-T (Unshielded twisted pair (UTP) 10mbps, 100m max)
- 10 Base-F (Fibre optic ethernet 10mbps, theoretically unlimited range)

Practical - Switches and Hubs

12:00 09/11/22 Athanasios Paraskelidis

Riverbed Simulation

- You can create multiple scenarios within one riverbed project
- You can then switch between them at any time
- Additionally, if you go to Manage Scenarios, you can simulate any scenario in the project easily to collect data
- If you then go into the DES menu, you can go to Results -> Compare Results, which allows you to easily compare the data from the two scenarios

Switches vs Hubs

- When using a Switch instead of a Hub, the average delay in the network is reduced drastically, in this simulation it decreases from 0.14 to 0.01
  - A hub broadcasts all incoming traffic to all interfaces, and therefor to every node connected to it
  - On the other hand, a switch reads the header in each packet and relays it only to the node that needs it
  - The result of this is that all devices connected to a hub are part of one ”collision domain”, and therefore only one node can communicate at a time, meaning that all other nodes have to wait until the network is not being used
  - This causes the greatly increased delay when using a hub rather than a switch
- Switches use a learning process to discover which nodes are connected to which interfaces (ports)
  - They have a register which relates the interfaces (ports)
  - Each time a node sends a packet, the switch reads the header and finds the IP address of the node that sent the packet, which it can then store in the register for future use
  - If the register does not contain the IP address the packet is destined for, it broadcasts the packet on all interfaces
  - Usually this learning process is quite fast, because any time a TCP transmission is sent, the receiving node will respond with a confirmation, which the switch can also use to learn the IP address of the node that responded
  - Once the learning process is complete, the nodes connected to a switch are each part of their own collision domain, containing only the switch and the node, making collisions essentially impossible

Lecture - Standards and the OSI Model

09:00 15/11/22 Amanda Peart

- Development of the OSI model started in 1977, with a draft published in 1979 and finalised in 1984 as an international standard
- OSI stands for Open Systems Interconnection
- The OSI model provides common terminology as well as a framework for networking
- The standard is still used today, and is the standard model for inter-computer communication
- It describes how data is sent from an application, through a network medium, and into another application, on a different computer or network
- This data transmission is split into the 7 layers of the OSI model
- Each layer has a specific function that it performs before sending the data to the next layer
- The upper 3 layers provide services to the application, while the lower 4 deal with the actual transmission from one device to another
- There are 7 layers on the way down, and 7 on the way up

Layer	Name	Purpose
7	Application Layer	Provides support for email, file transfer and other protocols
6	Presentation Layer	Ensures that the data is in the correct format, and is where any encryption will occur
5	Session Layer	Maintains the connection and controls ports and sessions
4	Transport Layer	Transmits data using TCP and / or UDP
3	Network Layer	Provides IP addressing, routing and segmentation
2	Data link Layer	Defines how the data is formatted when it is sent over the network
1	Physical Layer	Adapts the data to be sent over the medium (Fibre transceivers, etc)

Layers in more detail

- Layer 1 - Physical Link
  - Deals with the physical communication over the medium
  - It defines the specification of communication between the physical link on the sender and receiver
  - Defines characteristics such as
    * Voltage levels
    * Timing of voltage changes
    * Physical data rates
    * Maximum transmission distance

        * Physical connectors (e.g. RJ45, TIA-232 aka RS-232)

- Layer 2 - Data Link
  - Deals with transmission across the medium
  - Provides the location of the intended destination on the network
  - Can provide reliable transmission using MAC (Media Access Control) addresses
  - Uses MAC addresses to differentiate between the different nodes connected to the same physical medium
  - This layer deals with network topology and access, error handling, ordered delivery of frames, and flow control
  - Standardised protocols such as Ethernet, Frame Relay and FDDI
- Layer 3 - Network
  - Defines the logical addressing
  - Sets how routing works and how routes are learned or discovered so that packets can be delivered
  - Also defines how packets could be split into smaller packets to be delivered more efficiently on different media
  - Routers operate on this layer
- Layer 4 - Transport
  - Regulates the flow of data to ensure end-to-end connectivity
  - Segments the data into packets on the sending host, and reassembles them on the receiving host
  - Protocols on this layer include TCP and UDP
- Layer 5 - Session
  - Defines how to start, control and end connections (or sessions) between applications
  - Uses ”dialogue control” for management of bi-directional communication
  - Synchronises dialogue between the presentation layers and manages their data exchange
  - Allows for efficient data transfer
- Layer 6 - Presentation
  - Ensures that the data sent by the application is readable by the application layer on the receiving device
  - Translates between different data formats using a common format
  - Provides encryption and compression of data
- Layer 7 - Application
  - This layer is closest to the user
  - Provides network services to the user’s applications
  - Does not provide services to any other OSI layer, only to applications
  - Checks if the receiver is available to receive data
  - Synchronises and agrees upon procedures or protocols for error handling and control of data integrity

Connection and connectionless transport

- Connection-oriented transport such as TCP is used when the data needs to arrive intact and in the right order
- Connectionless transport such as UDP is used when the application is capable of data integrity control
  - They can do this by repeating the request after a timeout
  - This can sometimes cause duplicate operations if the response was delayed or just not received
  - Common uses for UDP are Broadcasting and real-time VoIP applications

The importance of standards

- The use of open standards is fundamental to Open Systems
- Needed to maintain interoperability between devices made by different vendors
- Standards should be internationally recognised
- It's important to track new standards in order to know when it is "safe" to use a new standard
- However, the creation of standards can take many years, and by the time the standards are released, the device that would've used it would be obsolete
- 'Fast tracking' can be used to develop the devices and standards in parallel
- When using fast tracking, vendors often end up releasing products before the standards are released

Important standards organisations

- ISO - International Standardisation Organisation
- ETSI - European Telecommunications Standards Institute
- IETF - The TCP/IP Internet Engineering task force
- IEEE - Institute of Electrical and Electronics Engineers
- ANSI - American National Standards Institute

Practical - Riverbed Simulation Results

12:00 16/11/22 Athanasios Paraskelidis

Understanding the results

- The traffic sent was the same, regardless of whether a Switch or Hub was used
- The traffic received in the Hub scenario was less than in the Switch scenario
- This is known as packet loss (The data received is less than what was sent)
- The average delay in the Switch scenario was almost (but not quite) 0, whereas the delay in the Hub scenario was roughly 14 times higher

Traffic generation

- How much data is being generated by each node?
  - The Interarrival time is 0.02 seconds - so 50 packets are sent each second
  - The packet size is 1500 bytes
  - So each packet is 1500 * 8 = 12000 bits
  - At 50 packets per second, and each packet being 12000 bits, there is 50 * 12000 = 600000 bps
  - This is the same as 600000 / 1000 = 600 Kbps
- Therefore, with 16 nodes transmitting at 600 kbps, the total network traffic is 16 * 600 = 9600 Kbps
  - This is the same as 9600 / 1000 = 9.6 Mbps
- Clearly, this is too much traffic for the Hub to handle, but the Switch is able to handle it with ease
- The capacity of the network is usually limited by the medium being used to connect the devices on the network
  - e.g. Cat-5 has a capacity of 100 Mbps, Cat-5E or Cat-6 has a capacity of 1 Gbps
- The cabling used in networking can vary massively depending upon the requirements
- Ethernet standards are named as such:
  - 10BaseT
    - The 10 means 10 Mbps
    - Base means Baseband communication (This is outside the scope of the module)
    - T means twisted pair cabling, meaning that there are 8 conductors, twisted into 4 pairs
  - 100BaseT is the same concept, but 100 Mbps
  - 1000BaseT is the same again, but 1000 Mbps or 1 Gbps
  - 10GBaseT is the similar, but in this case it means 10000 Mbps or 10 Gbps

	Hub	Switch
How are packets sent to their intended destination?	The packets are broadcast to all nodes connected to the hub, and only the node that needed the packet responds to it	The packets are sent to only the node that needs it, all other nodes do not see the packet at all
Does the device support half or full-duplex?	Half-Duplex	Full-Duplex
What are the advantages of using it?		Each node has it's own collision domain that contains only itself and the switch, so collisions are very rare
What are the disadvantages of using it?	All of the nodes connected to the hub are in one single collision domain, so collisions effect all nodes	

Lecture - Communication Media

09:00 22/11/22 Amanda Peart

- Different types of media can all transmit the same data
- Cables are in layer 1 of the OSI model
- There are 3 main types of cabling:
  - Twisted-pair cabling
  - Coaxial cabling
  - Fibre-optic cabling
- In a wired network, there is usually a networking rack on each floor, that contains a patch panel or switch, which all of the network ports on that floor are connected to
- The network designer has to decide which sort of media to use for each connection, depending upon
  - The required bandwidth (including future growth)
  - The level of electrical interference
  - The maximum length of cabling that will be needed
  - Cost of the media
- Unshielded twisted-pair cables
  - The least expensive type of media
  - Can be used up to 100m
  - Data capacity defined by EIA/TIA 568
  - Cat3 supports up to 10Mbps
  - Cat4 20Mbps
  - Cat5 100Mbps
  - Cat5e, Cat6, Cat6a and above are used for 1000Mbps and above
  - A UTP cable consists of 8 conductors twisted into 4 pairs
  - They are terminated in an RJ-45 connector
- Multiplexing can be used to combine multiple signals to be sent across one physical medium
- This can be used to reduce the number of cables needed
- Cat6 cabling
  - The newest type of UTP cabling
  - There are few differences between Cat6 and Cat5e, mostly increasing the quality of signal
  - There are 2 forms of Cat6
    * UTP or ScTP (Screened Twisted Pair)
    * ScTP has an additional layer of metallic foil to improve its resilience to interference

        * Cat7 and Cat8 are SSTP (Screen Shielded Twisted Pair) or SFTP (Screened Foiled Twisted Pair)

- Coaxial cabling
  - Low noise (low error rate)
  - Used to be used in a variety of applications
    * In IBM networks
    * In early ethernet (limited to 10Mbps)
  - The shielding may include multiple layers of foil or braid
- Fibre-Optic cabling
  - Used for extremely high bandwidths
    * Up to multiple Terabits per second, if using high-grade fibre
    * Many times more bandwidth than typical twisted-pair cabling
  - Typically formed of two individual fibres, each of which transmits only in one direction
  - They need to convert the electrical signals to optical signals and back
  - Not susceptible to electromagnetic interference as signals are sent as light, not electrical signals
  - Very thin glass strands
    * Multimode fibre is on the order of 50 microns
    * Singlemode fibre is on the order of 10 microns
  - The actual fibre cabling costs roughly the same as high-grade twisted pair cabling, but the connectors needed on either end are rather expensive, depending upon the type of connector, and the device it's connecting to
  - Media converters are needed on each end of the fibre cable, and depending upon the device it's connecting to, and the bandwidth needed, they can be rather expensive
- Additionally, wireless communication may be used, such as
  - Television and Radio
  - Satellite Comms
  - Radar
  - Mobile Telephone System (Cellular Communication)
  - GPS (Global Positioning System)
  - Infrared Communication (needs line of sight and has low bandwidth)
  - WLAN (Wi-Fi) - IEEE 802.11
  - Bluetooth
  - Cordless landline phones
  - RFID (Radio Frequency Identification)
  - NFC (Near Field Communication)

Practical - Signals

12:00 23/11/22 Athanasios Paraskelidis

- When using a switch in the network the ethernet delay drops over time, as opposed to when using a hub, in which the delay increases over time
  - This is because, at the start of the simulation, the switch does not know the IP Address of any of the nodes
  - Over time the delay decreases, as the switch learns the IP addresses of the nodes connected to it, meaning it can use the lookup table to send to a specific node rather than broadcasting

11.1 Key Terminology - Signals

- Periodic signal
  - A signal that repeats (every x seconds, minutes or hours)
- Non-periodic signal
  - A signal that does not repeat (it instantly disappears)
- Amplitude (A)
  - The strength of the signal (Decibels, dB)
- Frequency (f)
  - The number of times the signal repeats every second (Hertz, Hz)
  - $f = \frac{1}{T}$
- Period (T)
- The time for one cycle to be completed (Seconds, s)
  - $T = \frac{1}{f}$
- Bandwidth
  - The range of frequencies that are used to communicate, the distance between the maximum and minimum frequency
  - The higher the bandwidth, the greater the communication speed that can be used (Higher bps)

Lecture - Communication Circuits

09:00 29/11/22 Amanda Peart

Things to consider when designing a network:

- What is the maximum data rate needed?
- What is the maximum length a single run of cable is required to be?
- Could there be an issue with electrical interference?
- What constraints are there with the cable runs? e.g.
  - Listed buildings
  - Client requirements
  - etc
- What are the major costs associated with the selected medium?
- What medium is the external connection? e.g.
  - Broadband
  - Fibre
  - Dial-up
  - Satellite

Types of communication circuit

- Dial-up
  - Dial-up is available in two forms
    - Analogue (Mostly legacy, not everywhere)
    - Digital
  - Analogue links require a digital-to-analogue modem - this converts the digital signals from your computer to analogue signals
  - Digital links require a digital-to-digital modem - this converts the digital signals from your computer to a different digital signal to be sent over the phone line
- Modulation
  - Modulation converts a digital signal into an analogue signal, which can be sent across an analogue connection
  - Demodulation converts the analogue signal back into a digital signal, which can be used by a computer
  - Modem stands for **Mo**dulation **dem**odulation
  - Standard modem speeds are as such:
    - V.34 at 28.8 or 33.6 kbps

        * V.90 at 56 kbps
        * V.92 allows higher-speed connections and the ability to accept an incoming call

- Reasons to switch to digital
    - Computers are inherently digital, so easier to convert to a digital communication standard
    - Higher data rates are available
    - Easier to switch
    - Better (lower) error rate
        * Noise is not amplified along the line
- Digital telephone communication channels are available
    - Each channel communicates at either 56 or 64 kbps
    - These channels are then multiplexed (combined together) to create higher data rate connections
- Problems with E1/T1 and T3/E3 systems
    - T1 is used in the US and Japan but is incompatible with E1 which is used in Europe and the rest of the world
    - It is complicated to add or remove a channel to convert between the two
    - There is a need for higher bandwidth
    - A new standard is needed
- SONET/SDH
    - Synchronous Optical Network (SONET) is a North American standard
        * Works in multiples of 51.84 Mbps
        * STS-3 supports triple the bandwidth (155.52 Mbps)
        * Multiples of 4 up to 40 Gbps
    - Synchronous Digital Hierarchy (SDH) is an international standard
        * Works in multiples of 155 Mbps
        * A very resilient form of SONET and SDH is the dual ring, where there is a ring in both directions
    - If a cable is cut or goes down, the nodes at the ends reroute the data back along the ring in the other direction
    - This recovery happens in 50 milliseconds

Practical - Signals Cont.d

12:00 30/11/22 Athanasios Paraskelidis

- If you have the following equation, $s(t) = 10.5\sin(100\pi t) + 8.25\sin(200\pi t) + 6.5\sin(300\pi t)$, you can get the following information just by reading the components:
  - The amplitude of the signal is the greatest multiple, in this case, $A = 10.5$
  - The frequency of each component is derived by dividing the value in the brackets by 2π, e.g. $f_1 = \frac{100\pi}{2\pi} = 50\text{Hz}$
  - The period of each component is $T = \frac{1}{f}$, using the previously calculated value for f
  - The bandwidth is the difference between the highest and lowest frequency, e.g. $Bandwidth = f_{min} - f_{max}$
  - Attenuation can be calculated using $10^{\frac{db}{20}}$ where db is the power attenuation

Lecture - Wide Area Networks

09:00 06/12/22 Amanda Peart

- Unlimited distance (Interconnections provided by ISPs (Internet Service Providers))
- High speed
- Relatively expensive given the complex design
- Only the interface to the WAN and services hosted on it are of concern to the user (The actual design is irrelevant)
- ”Value added” WANs add more uses for dedicated point-to-point links
- Transparent LAN Services (TLS) hide the complexities of the WAN from the network administrator

Packet / Frame / Cell-Switched WAN links

- Individual units of data may be called:
  - Packets
  - Frames
  - Cells
- The difference between the 3 is that Packets and Frames can be of variable length
  - This allows the network to be more efficient but requires more processing in software on either end
  - The speed of processing in software limits the speed of communication over the link
- Cells are of fixed length
  - 5 bytes of header data and 48 bytes of payload data
  - Because they are all the same length they can be processed in hardware, which is usually much faster
  - This allows for much higher data rates

Switched and Permanent Virtual Circuits

- Some alternatives to packets, frames or cells can come in one of two forms:
  - Switched Virtual Circuits (SVC)
  - Permanent Virtual Circuits (PVC)
- SVC is like a dial-up connection
- PVC connections are always connected and leased out
- Not all WAN technologies support both SVCs and PVCs

  - X.25 Virtual Circuits (VCs) are usually SVCs
  - Frame Relay VCs are usually PVCs
  - ATM VCs can be either SVCs or PVCs
  - TLS is like a ”best effort” service

Services provided by WANs

- Provide a route across the network, between the source and destination
- Divide and reassemble data as required to be sent across the network
- Limit the network traffic to a level that can be effectively handled (congestion control)

X.25 Interface

- X.25 is a WAN interface ITU-T (International Telecommunication Union Telecommunication Standardization Sector) standard
- Connected to a public packet-switching network
- Covers the physical, data-link and network layers from the OSI reference model
- Last used over ”the WAN” in 2015 by financial and debit/credit card companies
- Still used in the Aviation industry

Frame Relay

- Connection-oriented, public switched service
- A Layer 2 protocol defined in 1984 by the ITU-T and ANSI
- A much higher performance alternative to X.25
  - Needed for high-performance applications, such as graphics and image transfers
  - Very useful for LAN-to-LAN communications which need high throughput
- It provides higher throughput by using
  - Larger frame sizes (1500+ bytes)
  - Higher interface data rates
  - Reduced processing requirements
- A variation of High-Level Data Link Control (HDLC)
  - Detects and discards frames with errors, and does not retransmit them
  - You must use another protocol on top of Frame Relay, e.g. TCP
- Builds on the fibre-optic network
- A good alternative to E and T carriers
- Supports two levels of traffic
  - Committed Information Rate (CIR)
    - Traffic up to this rate will be accepted, anything above will be rejected
  - Excess Information Rate (EIR)

    * Traffic between the CIR and EIR can still be sent but will be marked as "Eligible for Discard", so they can be discarded if congestion is too great

- It conveys congestion information, which can be controlled by users
- Advantages:
  - International protocol
  - Available in many (but not all) countries
  - Available from all major vendors
  - Takes advantage of modern fibre-optic infrastructure
  - Good LAN-to-LAN support
  - T and E carrier throughput capabilities
  - Less expensive than fully meshed E1/T1 lines for bursty traffic
- Disadvantages:
  - Poor support for SVCs
  - Does not provide any built-in fault tolerance, other protocols such as TCP are needed for error handling
  - Not suitable for latency-sensitive data such as real-time audio or video conferencing
  - Data overhead and processing overhead for every packet sent
  - More expensive compared to internet service

X.25 vs Frame Relay

	X.25	Frame Relay
Development Date	Mid 70s-Early 80s	Late 80s-Mid 90s
Underlying Infrastructure	Low data rate, error prone copper circuits	High-speed, highly reliable fibre-optics
Original Design Objectives	Support terminal to host	Support LAN-to-LAN
Design Approach	3 layers of the OSI model (Network, Data link, Physical)	2 layers (Data link, Physical)
Typical Data Rate	9.6-64 kbps	Fractional or full T1/E1
Error Recovery	Error detection and transmission	Error detection with discard, no recovery other than when using TCP
Max Packet/Frame Size	128-4096 bytes	1500 bytes (Full ethernet frame)
Processing per Packet/Frame	Two dozen processing steps	Half-dozen processing steps
Availability	Worldwide	Only in countries with fibre infrastructure
Applications	Good for terminal-to-host but not for LAN-to-LAN, used for credit/debit card verification	Good for LAN-to-LAN, could be used for credit/debit card verification

Practical - Excel Noise Simulation

12:00 07/12/22 Athanasios Paraskelidis

- To enter a periodic in Excel, you put `=Cell+MinAmplitude/10` e.g. `=A2+0.007/10` the first cell must be 0
- To enter the equation, you put `=A*SIN(f*PI()*t)` e.g. `=10.5*SIN(100*PI()*A2)`
- Then when you limit the equation to the bandwidth, you remove any terms that have a frequency higher than the bandwidth
- To add in the attenuation, you multiply the entire equation by the previously calculated attenuation
- To add noise, we need to use the rand function. In this case, we want noise that varies from 2.5 to -2.5
  - To get this, we add `+(RAND() * (max - min) + min)` in this case, `+(RAND() * (2.5 - -2.5) - 2.5)`

Lecture - Asynchronous Transfer Mode (ATM)

09:00 31/01/23 Amanda Peart

- Telecommunications standard defined by ANSI and ITU-T
- ATM is a data link layer
- Used in WANs
- Supports the transfer of data using a wide range of QoS assurance methods
- Core protocol used in SONET & SDH
- A form of ”cell relay”
- Relatively large packets which are segmented into 48-octet chunks for transmission (with 5-octet headers)
- These packets are switched across the network and than reassembled at the destination
- There is an unpredictable amount of time between the arrival of packets
- The cells are multiplexed with others when transmitted through the system
- Designed to provide virtual circuits across highly reliable media
- Optimised for the connectionless style of IP

Traffic Engineering / QoS

- QoS can be configured for every ATM interface
- Constant Bit Rate (CBR)
  - Can transmit at a Peak Cell Rate (PCR) for a maximum interval before it becomes problematic and throttles back to the CBR
- Variable Bit Rate (VBR)
  - Can transmit at a Peak Cell Rate (PCR) for a certain time until it has to drop back to the Sustainable Cell Rate (SCR)
- Available Bit Rate (ABR)
  - A minimum bit rate is guaranteed
- Unspecified Bit Rate (UBR)
  - Traffic is allocated until the maximum bitrate is reached, any further cells have to find another route or wait for bandwidth

Uses of ATM

- ATM is usually limited to the backbone of Wide Area Networks as it is not cost effective to run to edge nodes (e.g. homes or businesses)
- Since it has built in support for voice and video data, it is good for high-speed backbones
- It's QoS is very good, making it a good choice for high-speed backbones

Advantages

- Meets international and industry standards
- In use in most high-speed WANs
- Has built in support for voice and video, providing good QoS for these uses
- Cost competitive in the core of the network

Disadvantages

- Complex operation and configuration
- Somewhat inefficient (roughly 10% overhead due to header data)
- Not cost competitive to the edges of networks

Transparent LAN Services (TLS)

- Transparent meaning that you don't have to deal with it manually
  - No need to worry about the WAN
  - No provision needed for frame relays, ATM, leased lines, etc
- TLS bridges geographically separated LANs
  - This makes them appear as one big LAN
  - Decreases the need to manage WANs
- Often use ATM circuits
- Supplies ATM access to Ethernet circuits
  - Often known as "Metro Ethernet" or "Ethernet Transport"
  - Available at all Ethernet data rates

Overview of Wired WAN Technologies

OSI Layer 1	OSI Layer 2	Medium
Dial-up over PSTN	PPP	Copper
ISDN	PPP or Frame Relay	Copper
DSL	PPP, Ethernet or ATM	Copper or Fibre
Cable Broadband	Cable Broadband, Ethernet	Copper and Fibre
T/E-Carrier	PPP, Frame Relay or ATM	Copper or Fibre
SONET/SDH	PPP, Frame Relay, ATM, MPLS	Fibre

- PPP = Point-to-Point Protocol
- MPLS = Multiprotocol Label Switching

Lecture - Interconnection Protocols

09:00 07/02/23 Amanda Peart

Voice over Internet Protocol (VoIP)

- Originally, the motivations were to reduce the number of emails that need to be sent, and with VoIP phones you only need one network
- Current motivations are:
  - Reduction of cost
  - Single network
  - More capable than typical phones
  - Avoid delays
  - Provide good QoS
- Downsides are:
  - The quality of the connection may not be great, depending upon the gateway between IP phones and legacy networks
  - Wireless devices may drop connection temporarily when moving between access points

Session Initiation Protocol (SIP)

- Application layer protocol
- Signalling protocol for real-time sessions
- Provides infrastructure for voice, video, instant messaging
- 5 Categories
  - User Location - Realtime local discovery
  - User Availability - Is the user available to communicate (online, engaged, etc)
  - User Capability - Choice of media and encoding
  - Session set-up - Establishing the session
  - Session management - Transferring sessions, modifying parameters
- SIP is ”similar” to HTTP, as it’s a request-response connection

The Internet and Network Access Points (NAPs)

- The internet consists of many ISPs which operate on different levels:
  - Tier 1: International
  - Tier 2: National
  - Tier 3: Regional
  - Tier 4: Local
- Network Access Points (NAPs) are a type of Internet Exchange Point (IXP)
  - They connect between public ISPs to exchange traffic
  - Routing information is exchanged using BGP-4
- Selective peering may be done with direct links to other ISPs
- NAPs are layer 2 switches
  - Typically use ATM switching
  - Support for ISO-provided routers
- NAPs are connected by high-speed backbones

Router Capabilities

- Routers may be of several types:
  - Access Routers - Edge of the internet
  - Enterprise Routers - Organisation networks
  - Core Routers - Handle heavy data flow
- Routers may also have Layer 2 switching
- May have hardware or software routing capabilities
- Routers may be table top or rack-mount
- Modern ”Routers” may be embedded into other multi-feature devices, such as
  - Wireless Access Points
  - Small (e.g. 4 or 5 port) ethernet switch
  - Firewall

Multi-Protocol Label Switching (MPLS)

- ”Route at the edges, switch in the core”
- Provides the best parts of Layer 3 routing, and Layer 2 switching
- Intended for use in the core of the Internet or Intranets
  - Useful for carriers, ISPs and enterprise WAN networks
  - MPLS router in the core of the network is known as a label-switching router (LSR)
- Why use MPLS?

  - Specifications allow many options
  - The first packet between two networks is routed, so that the Layer 2 switched connection can be setup
  - Subsequent packets are handled at Layer 2, swapping the label at each LSR
- Benefits:
  - Traffic engineering capabilities (paths can be explicitly set without routing)
  - MPLS-based VPNs can be setup with simpler provisioning of network infrastructure and bandwidth
  - Good QoS
  - Improved performance as compared to routing at each hop
  - Much greater scalability
  - Also has many of the benefits of connection-oriented networking

QoS with IP

- QoS usually refers to providing support for time-sensitive delivery, such as voice or compressed video
- Efforts include
  - Various forms of IP switching
  - Differentiation between services (e.g. prioritise VoIP or Video packets over emails or web browsing)
  - Multi-Protocol Label Switching (MPLS)

Lecture - Network Security

09:00 14/02/23 Amanda Peart

Key Elements

- Security Attack - Any action that compromises the security of information
- Security Mechanism - A mechanism that is designed to detect, prevent or recover from an attack
- Security Service - A service that enhances the security of data processing systems and information transfers, usually making use of more than one security mechanism

Security Goals

- Confidentiality - Keeping the information private
- Integrity - Preventing the information from changing
- Authentication - Ensuring the information is from a known source

Security Attacks

- Interruption - Data does not flow to the destination
- Interception - Data flows to the destination, as well as a 3rd party
- Modification - Data is intercepted and changed before reaching it's destination
- Fabrication - Data is fabricated and sent to the destination, without any interaction from the source

Passive Threats

- Passive attacks are listening in on transmissions
- The goal of the attacker is to obtain information that is being transmitted

Active Threats

- Attempt to actively cause harm, often through system faults or errors, or using brute force attacks
- May attempt to overload victim's computers to the point of unusability or crashes (known as Denial of Service (DoS) attacks)

Security Services

- Access control
  - Levels of access
  - Some people may need write access, others may not
- Availability
  - Denial of Service Attacks
  - Viruses that delete files

Methods of Defence

- Encryption
  - Transforming the data in such a way that only people who have been given a piece of information are able to read it
- Software Controls
  - Access control used to limit user access to a database
  - Operating system controls used to limit user access to other users and their information
- Hardware Controls
  - Smartcards used to access data
  - Biometrics such as finger prints or retinal scans required to access data
- Policies and Procedures
  - Frequent password changes
  - Strong password requirements
- Physical Controls
  - Limit physical access to computers that can access information, or the servers the information is stored on

Security Vulnerabilities

- Securing network communication has always been a problem
- It is hard to secure the initial requests
- The data needs to be protected at all times when it is in transit
- Users need to be trusted before they are given access

Lecture - Network Security Cont.d

09:00 21/02/23 Amanda Peart

Vulnerabilities

- Remote attacks
- Software developed with ”back doors”
- Insecure configuration
- Internal attacks (Disgruntled employees)
- Access control
- Connecting compromised personal devices to secure networks

Security Management

- Control and Distribution
  - Control who can and cannot access files
  - Control where files can be downloaded to (e.g. not personal devices or storage)
- Event Logging
- Monitoring
- Parameter Management

Security Services

- Denial of Service prevention
  - Have a device outside of the network that is capable of absorbing the traffic of a DoS attack
- Access Control
- User Authentication
  - Multi-Factor
  - 2FA
- Data Confidentiality
- Accountability

Security Mechanisms

- Encryption and Decryption
- Message Authentication
- Password Policy
- Digital Signatures
- Access Control

Secure Communications over Insecure Networks

- Use encryption to ensure that even if a man-in-the-middle attack takes place, the message remains unreadable for the attacker
- Asymmetric encryption is less secure than symmetric encryption, but it is usually necessary to use both for better security
- One issue with this is that it's impossible to determine who sent the encrypted message(s), so another method of security must be used to certify authenticity
- To do this, we can combine cryptography and digital signatures to ensure that the message is from a trusted source, and that no one else is able to read the message

Secure Sockets Layer / Transport Layer Security (SSL / TLS)

- These protocols are used when communicating securely using HTTPS
- The encryption key may be anywhere from 40 to 128 bits
  - 40 bit keys are obviously less secure than 128 bit keys, but both are susceptible to issues with key generations, such as poor Random Number Generation on specific platforms
  - 256 bit keys can be used for applications needing higher security, but this is not a standard feature
- Trusted certificates contain the owner's public key and is cryptographically signed by a trusted certificate agency
- Types of Encryption
  - The Data Encryption Standard (DES) dates all the way back to the 70s, and uses a 56-bit key, which could be broken in a matter of hours on a modern computer
  - Triple DES has a much longer effective key length but is still inadequate for our current needs
  - The more recent Advanced Encryption Standard (AES) is much more secure, as it uses keys between 128 and 256 bits and a specifically designed algorithm

Virtual Private Networks (VPNs)

- A private network that uses a public network (usually the Internet) to connect remote sites or users together
- Rather than using dedicated or rented physical lines, it uses a virtual connection
- While it is often touted that they're secure, the security is not inherent to the VPN's operation
  - VPNs may use encryption to send all traffic, but this is not a given

  - The encrypted packets are sent in ”Routable IP Packets”
- An outsider may be able to intercept packets in-flight, but if they’re encrypted it is practically impossible for them to read or modify the packets
- VPNs give no QoS assurance, and so packets are delivered on a best-effort basis

Remote Authentication Dial-In User Service (RADIUS)

- Provides Authentication, Authorisation Checking and Accounting
- Uses a Point-to-Point protocol
- Operates on port 1812
- Commonly used to facilitate roaming
- Authentication and Authorisation Flow
  - Client sends Access-Request to the Server
  - Server responds with one of the following, depending upon if the user is authorised
    * Access-Accept
    * Access-Reject
    * Access-Challenge

Uncontrolled Connections to the Internet

- It is very easy to connect to the Internet
  - All you need is a router and approval
- However, this is often not a good idea as it would make it very easy to steal data sent over the Internet
- There are dangers present if uncontrolled connections to the Internet are allowed
- There are a few ways of preventing this, but the most common one is Firewalls

Firewalls

- Routers which connect to the Internet typically have a firewall
- Firewalls filter out requests which are unwanted
- This may consist of adult content filters, or might filter what can be connected on the network, e.g. preventing VPN connections
- There can also be firewalls on individual devices
- These are known as Host-Based firewalls, and are useful for devices exposed to the Internet, as it allows them to block unwanted connections
- Host-Based firewalls are typically more secure, but are more expensive to setup and maintain
- Dedicated Firewall devices may have other functions such as
  - Intrusion Detection (Signature verification, etc)
  - Network Address Translation (NAT)
  - URL and Content filtering

Common Criteria Evaluation Assurance Levels (EAL)

- An internationally recognised method of comparing security of different network-enabled devices
- These levels range from 1 to 7
- EAL 2 is the minimum level to be accepted
- EAL 4 is the highest attainable level for a retrofitted product
- EALs 5-7 are extremely expensive to obtain and are typically limited to applications such as Governments, Militaries and Healthcare

Lecture - Network Management

09:00 28/02/23 Amanda Peart

- Computer networks have become mission critical for many businesses
- Network downtime causes problems for communication and individual work

Goals for Network Management

- Responsive network management is needed, for example
  - Help desk
  - Network support technicians
  - Network system management
    * Monitor the network
    * Have the ability to diagnose and control the network

Network Systems Management

- Monitors the network
- Displays the current status of the network, often using a ”traffic light” system
  - Red = Active outage
  - Amber = Problems that may cause an outage
  - Green = No problems detected
- Provides notifications as problems arise

TCP/IP Network Management

- Network management involves 3 distinct needs
  - A protocol for creating network management data, such as event reports
  - A database of information, that contains data about queue length, throughput, etc over time
  - A computer that is able to run independently of the network so that if the network goes down, the data is not compromised
- These needs are met by
  - SNMP - Simple Network Management Protocols
    * Read/Write between network management devices and network client devices
  - MIB - Management Information Bases
    * The database of information pertaining to the network
  - SMI - Structure of Management Information
    * Device independent notation of device information

Simple Network Management Protocol (SNMP)

- The manager needs to be able to monitor and control the devices on the network
- It needs to be able to
  - Read the value of parameters (SNMP Get)
  - Read sequences of table entries (SNMP Get_Next)
  - Write into parameter values (SNMP Set)
  - Receive unsolicited event reports (SNMP Trap)

Remote MONitor (RMON)

- SNMP Management Information Bases (MIB) include remote monitoring capabilities
- RMON can be implemented in different ways
  - As an independent probe device attached to each LAN segment
  - Integrated into network devices, such as switches or routers
- RMON is available in two forms
  - RMON 1 monitors OSI layers 1 and 2, collecting collision and error statistics
  - RMON 2 monitors higher levels of the OSI model, collecting information about application traffic
- Can be cost effective, and control network traffic
- Increases the effectiveness of network management personnel, as they can remotely diagnose and fix issues

Network Management Areas

The OSI identifies five areas on network management:

- Configuration
- Fault management
- Performance management
- Accounting management
- Security management

Configuration

- A wide range of issues can fall under configuration issues
  - Faulty IP address assignment
  - Hardware or Software updates to switches, routers, etc
  - Software license control
- There are several parameters that fall under configuration
  - Configure switches and routers to filter out certain traffic
  - Multi-protocol routers can be configured to run selected protocols
  - Configuration of bit rate, parity, etc

Fault Management

- Provides identification and isolation of detected faults
- Tools and techniques include
  - Bit-Error Rate Tests (BERT)
  - Time Domain Reflectometer (TDR)
  - Optical TDR (OTDR)
  - Protocol Analyser (for data links and LANs)
  - Loopback Tests
  - Ping Tests
  - Artificial Traffic Generation (Usually done out-of-hours to avoid creating further issues for the network)

Fault Isolation (LANs)

- Limiting faults is possible by isolating the fault using switches and router configuration
- All traffic across the LAN can be monitored
- All exceptional conditions can be detected, e.g. collisions, viruses infecting computers across the network, etc
- Devices called LAN analysers or LAN protocol analysers can be attached to the network
  - These devices record selective information about packets that may be of interest
  - May be set up to filter based on address, protocol, or other fields of interest

Performance Management

- Network Performance Management
  - Concerned mainly with statistical data
  - Round trip delays
  - Throughput
- May require prioritisation of traffic
  - May include QoS capabilities
- Tuning of performance (eliminating bottlenecks)
  - Buffer size adjustment
  - Setting timer values
- Establish a baseline
  - Set a minimum level of performance that is needed for the business
- Performance management also involves finding bottlenecks
  - WAN links between remote switches and routers
  - Access to server resources, e.g. storage
  - Parts of the network which are near or at capacity
- Many fault-management tools are useful for performance management

Accounting Management

- Can be the billing for network usage
- Accounting Parameters usually include
  - Number of connections made
  - Duration of each connection
  - Number of email packets sent and received
  - Number of packets generally sent and received
  - Systems that are accessed across the network
  - Internet usage
- Accounting management may be broadened to include other network attached resources
  - Server usage (connection times and storage used)
  - Traffic using expensive dedicated WAN circuits
  - Data storage
- Accounting management may also be used to cap the use of network resources or storage space

Security Management

- Confidentiality
- Integrity
- Authentication
- Access Control
- Nonrepudiation
- Vulnerabilities
  - Wiretaps placed on cables
  - Third parties intercepting remote logins
  - Viruses and other Malware
- Protection Mechanisms Include
  - Encryption
  - Physical Access Control
  - Access-Control lists
  - Audit Data Collection

Lecture - Application Support Protocols

09:00 14/03/23 Amanda Peart

TCP vs UDP

- User Datagram Protocol
  - No guarantees of delivery
  - Acts as an interface to IP-Level for the Application layer
  - Just sends data directly, without checking if the receiver actually exists or that a path exists
  - Packets that are lost are just lost
  - There is no checking of dropped, corrupted or incorrectly ordered packets
  - As it's unreliable, there are only a few applications that it should be used for, e.g. voice or video streaming
    - Low delay is essential in these applications
    - The lost data is most likely irrelevant, so does not need to be re-requested
- Transmission Control Protocol
  - Reliable data transmission
  - Performs integrity checking, retransmission of dropped packets, reordering of packets, etc
  - Connection oriented - a connection must be established before data can be sent to verify that a path exists and that the receiver is willing to receive the data
  - The connections are setup as a virtual channel between the sender and receiver
  - The 3-way handshake is made before the connection is established
  - TCP should be used almost anywhere else, such as file transfers, webpages, email, etc
    - Delay is not as sensitive
    - Any data that may be lost needs to be recovered, otherwise the data would become corrupted and useless

TCP/UDP Multiplexing

- Since multiple applications on a computer may be using TCP or UDP at once, there must be a way of differentiating the incoming transmissions
- This is done using **ports** which are like a virtual connection to the computer
- Each device has 65535 ports
- Each application uses it's own port, and some have their own specific port, such as HTTP which uses port 80, HTTPS on 443 or SSH on 21
- The incoming packets enter the transport layer, where they are split up and sent into the application layer of the application using that port

Layer 6 - Presentation

- This layer interprets the data before the application receives it
- Where the Secure Sockets Layer (SSL) resides
- Not always used in protocols
- Data abstraction
  - All protocols have their own format for the data they're sending
  - The application does not need to see this data directly, just what is encoded in that data
  - This could be something such as translating between different character sets, e.g. between ASCII and UTF-8

Secure Sockets Layer (SSL)

- A socket is a method of making connections
- You can open a socket to connect to a remote host, or you can open a local socket to listen to a port on the computer
- SSL
  - Provides end-to-end encryption
  - Provides the same abstraction as other protocols and can usually be used as a slot-in replacement for traditional sockets
- When is SSL used?
  - Almost any time that secure transmission is needed
  - HTTPS (Banking websites, most websites at this point... 2006 powerpoint smh)
  - SFTP (Secure File Transfer Protocol)
  - SSL Email (More secure emails)

Layer 7 - Application

- Client - Server model
  - The server is usually a more powerful computer which responds to many clients at the same time
  - This is good as it reduces the number of machines needed, but it reduces the resilience of the application as there is a single point of failure
- Peer-to-Peer
  - Each peer acts as both a client and server
  - Broadcast searches for services
  - Each peer has a smaller internet connection, so multiple peers are used at the same time to increase speeds
  - Disadvantage of this is that other people are responsible for hosting the data, and could modify the data

Domain Name System

- A register of which Domain Names point to which IP addresses
  - e.g. `google.com` is currently linked to `142.250.187.206`
- There are multiple layers in a DNS, starting at the root server for the TLD of the domain
- DNS typically uses port 53
- Uses UDP for queries and TCP for transfers
- There are multiple types of records
  - A record (Maps subdomain to an IPv4 address)
  - AAAA record (Maps a subdomain to an IPv6 address)
  - MX record (Maps to the IP address of a mail server)
  - PTR records (Reverse lookups)

Lecture - Application Support Protocols Cont.d

09:00 21/03/23 Amanda Peart

Hyper Text Transfer Protocol (HTTP)

- Standard protocol used on the world wide web
- Requests one file at a time, typically starting with an HTML web page
- The web page may point to other files that need to be loaded
- Mainly consist of ‘GET‘ and ‘POST‘ requests
- Typically uses port 80
- Some websites are interactive, and as such the HTML changes
- Some of these websites use server-side rendered HTML to keep the website faster for low performance clients
- How do we send data for an interactive web page?
  - Using a GET request
    - GET `http://{website}/{file}?information={data} HTTP/1.1`
  - Using POST
    - POST `http://{website}/{file} HTTP/1.1 {data}`
  - Why do the two different methods exist?
    - GET exists to allow links to dynamically generated content
    - POST keeps data out of the URL, which is useful for information such as passwords

Email (SMTP, POP3, etc)

- Before we can send an email, we need to find out the IP address of the mail server
- To do this, the application requests the MX record for the domain in question, e.g. ‘port.ac.uk‘ if trying to send an email to ‘amanda.peart@port.ac.uk‘
- Once we know the IP address, we use SMTP (Simple Mail Transfer Protocol) on port 25
- Anti-Spam measures
  - Standard practice is to use closed relays
    - Only accept mail destined for that mail server
    - Only send mail out from the mail server when the client requesting mail to be sent has an IP within a certain range, or is authenticated with a certificate or password
  - Real-time blackhole lists (RBL)
    - Automatically blocks reported email addresses which are then blocked

        * Can be annoying for people who have been inadvertently placed in the list
    - Content scanners can be employed to block spam messages, however these are often seen as a breach of privacy

- Can we impersonate someone else?
    - You can replace the sender and recipient addresses in the SMTP messages to be whatever you wish
    - However, there are multiple mechanisms that block this
        * Anti-spam measures often block these emails anyway
        * Most mail servers reject messages sent from an IP address other than the one specified in the MX record for the domain
        * e.g. you change the sender to ‘boris@gov.uk‘, most recipients will block the message as your IP address does not match that belonging to the MX record of ‘gov.uk‘

How do we get our emails? (POP3)

- To get our messages from the mail server, we need another protocol known as POP3 or Post Office Protocol v3
- Mail delivered by SMTP is stored on the mail server
- Our email client then requests the mail from the server using POP3
- POP3 is another simple text-based protocol
    - Authenticate with the server using a username and password
    - Request the number of messages waiting on the server
    - If more than 0, request each email one by one
    - Optionally: delete the messages from the server after they’ve been downloaded

The real world

- How would a company set up their internal intranet with a website and internal mail server?
    - Typically one or more internal DNS server on the network which handles an internal domain, or subdomain
    - HTTP server (Apache, IIS, Nginx, etc)
    - Mail server (Exchange, sendmail, etc)
- In a smaller business, all of these services could be running on one machine, but it is often better to split them up to improve
    - Redundancy
    - Security
    - Performance
    - Network bandwidth

HTTP over SSL (HTTPS)

- Used for the vast majority of the world wide web at this point
  - Originally only used for high security applications such as banking
- Server certificates are used to verify the authenticity of the server
- There are a few problems with HTTPS
  - Server certificates (used) to be expensive
  - It is possible to impersonate servers if they forget to renew their certificates, or use self-signed certificates

Lecture - Network Policies and Standards

09:00 28/03/23 Amanda Peart

The Internet Society

- Aims to oversee the standardisation of protocols, improving global interoperability
- Coordinates Internet
  - Design
  - Engineering
  - Management
- The society has 3 main sections
  - Internet Architecture Board (IAB)
    - Defines the architecture of the internet
  - Internet Engineering Task Force (IETF)
    - Defines the protocols of the internet, based upon the architecture given by the IAB
  - Internet Engineering Steering Group (IESG)
    - Technical management
    - Defines the ”internet standard”
- Working groups investigate the actual details of any and all proposed standards and protocols
  - Draft version is created
  - Given out for consultation
  - The IESG gives final approval
  - Published as a Request for Comments (RFC)
    - If the draft hasn’t progressed in 6 months, it is withdrawn
- The criteria for all standards
  - Be clear
  - Be technically competent
  - Have multiple independent but interoperable implementations
  - Gain significant public support (both users and manufacturers)
  - Be useful
- The process
  - Draft made of the standard
  - The standard is proposed, and left open for 6 months for comments
  - If the standard is relevant and correct, it becomes a draft standard and left open for 4 months

  - If the standard is still relevant and no errors are found, it becomes an internet standard
  - When the standard becomes irrelevant, it becomes a historical standard
- For a standard to be ratified, it needs to have two independently developed implementations that are fully interoperable
  - Once it is ratified, it is given a STD number and RFC number

International Standards Organisation (ISO)

- The ISO aims to promote standardisation and related activities to facilitate international exchange of information and services
  - Provides standards for all sorts of things, including networks and other electronics
- 6 step development process
  - Proposal Stage
    - A new proposal is assigned to a working group, who create a proposal for the standard
  - Prepatory Stage
    - A working group creates the draft of the standard
    - Once created, it is passed to the committee for the public consensus phase
  - Committee Stage
    - Registered at the ISO central Secretariat
    - Distributed for balloting and comments
    - Once a census is achieved, it becomes a Draft International Standard (DIS)
  - Enquiry Stage
    - DIS is sent to all ISO bodies
    - Time limit of 5 months for voting and approval
    - It becomes a Final Draft International Standard
    - If not approved it is returned to the working group to be reworked
  - Approval Stage
    - Redistributed for final acceptance
    - 2 month time limit
    - Technical comments are no longer considered
    - If not approved it is returned to the working group to be reworked
  - Final Stage
    - Once approved, it becomes an International Standard
    - Some minor editorial changes are allowed before final publication

Telecommunications Standardisation Sector (ITU)

- UN specialised agency
- Members are governments
- Responsible for broadband standards based upon ATM technology
- Processes
  - Works in 4 year cycles
  - Meetings of world telecommunication standardisation conference

  - Work program for the next cycle established
  - Study groups are created and abolished
  - There is an accelerated procedure allowing recommendations to be approved when they are ready
- Ballot Process
  - Wide participation by Governments, Users and Industrial representatives
  - This causes significant delays
  - Because of this, it is now being streamlined by majority rule ballot

Institute of Electrical and Electronic Engineers (IEEE)

- Initiating a project
  - Sponsors input to create a collaborative group
  - A Project Authorisation Request (PAR) is produced
- Once a PAR is approved,
  - A working group is created
  - They work to write standards
  - Anyone can be included in the group
- Drafting the standard
  - The first draft is written
  - The Mandatory Editorial Coordinator checks the draft
  - Then it goes to ballot
- Balloting process
  - Once the standard is stable
  - The sponsor creates balloting groups
    - Anyone is able to comment upon the standard
  - Balloting group consists of
    - Producers
    - Users
    - Government
    - General internet users
  - Balloting lasts 30-60 days
  - Decisions
    - Approval
    - Disapproval
    - Abstain
    - Consensus is 75% respondents with 75% group approval
- Gaining approval
  - The IEEE-SA board approves or denies the final standard
  - The board's decision is based upon recommendations by the committee
  - Standards are valid for 5 years, after which they can be
    - Reaffirmed
    - Revised
    - Withdrawn