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 Session - Collisions 6

4 Lecture - More Protocols 7

5 Practical Session - Protocols 10

6 Lecture - NICs and Ethernet 11

7 Practical Session - Switches and Hubs 14

8 Lecture - Standards and the OSI Model 15

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 Session - 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 anf 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 Session - 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 Session - 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