University Of Portsmouth
BSc (Hons) Computer Science
First Year

Networks

M30231
September 2022 - May 2023
20 Credits

Thomas Boxall
up2108121@myport.ac.uk

Contents

S.1. Introduction To Module

📅 27-09-2022 🕘 09:00 🎓 Amanda 📍 Zoom

Module Overview

The module coordinator for this module is Amanda. Thanos also teaches on the module. Taiwo and Uchenna are practical tutors. Amanda and Thanos' offices can be found on the first floor of BK building. Taiwo and Uchenna can be found on the ground floor of BK building. In general, they all operate an open door policy.
The module runs through both teaching blocks.
The practical sessions are held in Portland 2.27. This is on the second floor, in the far right hand corner of the building. If you are going to this for the first time, its advised to allow extra time to find the room.
This module covers the fundamental building blocks of computer networks. It introduces computer networks, focusing on: data connections; current and legacy technologies; network protocols; computer network terminology.
There is a lot of terminology used in this module, some students have found it helpful to create a glossary.

Module Learning Outcomes

1. Recognize computer systems network terminology and use it appropriately. *(Terminology will be used in every lecture, the key to this outcome is the appropriate use of the terminology.)*

2. Define the fundamental principles of computer networking topologies and professional standards, utilizing simulation software. *(This will encompass the IEEE standard. This term, we will use simulation software to build networks and see how they work.)*

3. Describe the 7-layer OSI model and discuss its application.

4. Describe the fundamental operational aspects of Network Protocol Architecture. *(For the most part, networks are plug and play however they have lots of software and protocols that interface with different components to allow them to communicate with each other. Lots of this module is about the protocols and how they interface which makes things work. The end goal for networking is that the user has a seamless experience when using technology.)*

5. Examine the fundamental requirements of systems management. *(Management and maintenance of a network is often overlooked. Networks have to be seamless but also available 99.9% of the time, this limited downtime is the responsibility of the network administrators.)*

6. Identify network security and the impact of network vulnerabilities. *(Looking at how networks are secured, this is the fundamentals only.)*

Assessments

There are three components to the assessment for this module.

Exam 1

This will be a computer based, 45 minute exam held in the January 2023 exam period. It wil be closed book and have a variety of question styles. It will examine content taught in teaching block 1 and will be worth 30%. There will be revision sessions and revision questions made available closer to the time.

Coursework

This will be completed during teaching block 2 as part of a group. It will be in the area of Network Design and specification. The basic premise is that a group works together to cerate a company and deliver a pitch for a contract in a Dragons Den style presentation. This is worth 50%.

Exam 2

This will be a computer based, 60 minute exam held in the May/June 2023 exam period. It will be closed book and have a variety of question styles. As with exam 1, it will be worth 30% and revision questions and revision sessions will be made available closer to the time.

Hours

The lectures will be delivered online, most will be live with some pre-recorded. For live Zoom lectures, attendance is automatically recorded through Zoom.
The practical sessions will be held in Portland 2.27, in groups of about 20 people.
Outside of timetabled sessions, you should spend about 6 to 7 hours working on this module (university expects about 200 hours per 20 credit module). If you have lots of experience in this subject, then it may not need to be this much however if you are new to the subject, they you may require longer.
There will be quizzes provided throughout the year to test knowledge.

Resources

There are a number of options for the textbooks, each with varying degrees of detail.

- Stallings, W., 2013, Data and Computer Communications 10th Ed, Pearson Prentice-Hall (ISBN: 1292014385) - this covers all of the first year networking module and some of the second year networks module.

- Tanenbaum, A., 2010, Computer Networks 5th Ed, Upper Saddle River NJ, Prentice Hall (ISBN: 0132553171) - this covers all modules until the final year networking module, it can be hard to read.

- Kurose and Ross, 2011, 5thEd Computer Networking: A Top-Down Approach: International Edition (ISBN 978-0131365483) - this covers all modules until the final year module, it has a looser style making it easier to read than Tanenbaum.

- West, Dean and Andrews 2019, Network+ Guide to Networks - this covers the first year module only and is quite easy to read.

- Peterson and Davie, 2011, Computer Networks 5TH ED (ISBN: 0123851386) - this can be quite technical and covers quite a lot of the three years.

All the books listed above are available in the university library. It is recommended to have a look through them before purchasing so that you get the one which works for you.
If using Google to find information, be sure to use a reputable source.
We will be directed to internet resources when we need. If we are really keen, could do Linkedin Learning Courses. Any Cisco accreditation already completed are useful however there will be a difference in some terminology between Cisco and this course - we will be taught generic terms, Cisco uses Cisco-specific terms.

S.2. Practical 1

📅 30-09-22 🕑 14:00 🎓 Taiwo 📍 P2.27

This session will usually be taught by Amanda, it's being covered by Taiwo today.
This session is more of an introduction to practical sessions and a information gathering session than a taught session.
We were asked to answer the following questions about our experience of networks.

- Have you upgraded a computer previously?
- Have you built a wired network previously?
- Have you built a wireless network previously?
- What are you expecting to learn in this module?

The wireless access point (WAP) in the room is located behind the projector. WAPs are wired devices which broadcast wireless signals.
RJ-45 connectors are the common connectors on the end of a Cat 5/5e/6 cable.
RJ-11 connectors are the smaller version of RJ-45 which is commonly used for telephone cables.
We will learn lots oof concepts, which will be covered in exams.
We then completed a scenario based exercise thinking about delay, reliability and duplication of tasks on a network.

S.3. Computer Networks and Network Topologies

04-10-22 09:00 Amanda Zoom

Communications Network

Every time we communicate, we use a network of some description. Communications networks are vehicles for exchanging information, collaborating and sharing access to information.

Networks

Network

A group of two or more devices, connected through infrastructure that are able to communicate and exchange informaiton bexause they agree to use software that observes the same set of protocols.

Within a network, the devices are connected via hardware and software. The hardware is what physically connects the devices together. For example, telephone lines, fibre-optic cables, routers and gateways and the computers themselves. Software is what enables us to use the hardware for communication and exchanging information. The software enables networks to follow a set of rules that are generally referred to as protocols.

Protocol

A pre-determined set of rules that govern how devices communicate with eachother, ensureing interoperability between different brands, categories and types of device.

Interoperability

Permitting devices follow the protocols, different types of computers, using different operating systems, can be connected, communicate with each other and share information as long as they follow the network protocols.

Network Topologies

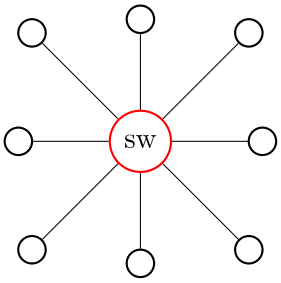
Toplogy

A toplogy is the arrangement of devices and connections within the network.

It is common for modern networks to have a full-ish mesh topology at the core with a star topology at the edges.
All of these topologies are in the context of LANs.
Key to shapes:
○ Node
○ Switch
■ Terminator
● Token

Star Topology

In the star topology, all devices are connected to a single central node. This central node is usually a switch or hub. This topology is more common in todays networks, especially due to the fact that multiple 'stars' can be interconnected.



Advantages

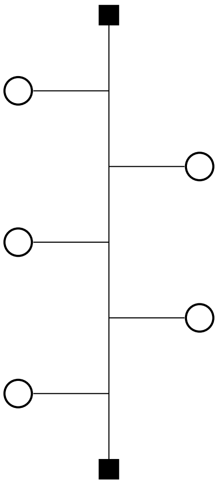
If one of the nodes fails, the network will still function; depending on the capacity of the central node, the network can accommodate heavy traffic; it is easy to add and remove nodes as necessary, the limit of numbers of nodes is the capacity of the central node.

Disadvantages

They are very reliant on the operations of the central node as it is a single point of failure (if the central node fails, the whole network won't functions); the effectiveness of the whole network is determined by how effective the central node is.

Bus Topology

In a bus topology, there is a central backbone cable which runs the entire length of the network. Linked into this backbone are the nodes. At the end of the backbone, there have to be special terminators. This design is limited to a very low number of computers. This topology is no longer a popular method due to the limitations of the design.



Advantages

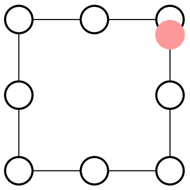
Allows relatively good rate of data transmission; it is simple to implement; it uses less cable than a star topology; it uses a lower grade of cable than star topology, hence it is cheaper.

Disadvantages

It doesn't cope well with heavy traffic; it is prone to collisions, where two nodes transmit at the same time; it is difficult to administer & troubleshoot, as a broken backbone can render the network useless; the backbone has a limited length, this limits the number of nodes which can be connected to it; the performance degrades as additional nodes are added.

Token Ring Topology

In this topology, all the nodes on the network connect together into a ring. Through software, a ‘token’ is created. This is passed from node-to-node; and when a node has the token, it is able to communicate. This is no longer a popular method for designing a network as the design is limited.



Advantages

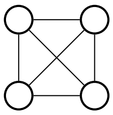
All nodes on the network have equal chances of transmitting data; there is a good quality of service; there are no collisions.

Disadvantages

If one of the nodes go down, the whole network may go down; as the token is virtual, it may get lost or corrupted; it is difficult to add or remove nodes from the ring.

Mesh Topology

In this topology, each node is connected to multiple other nodes directly. This required specialist software and hardware. Mesh topologies, can be either partially or fully meshed (meaning nodes only connect to some other nodes, or every node connects to every node directly). This topology is most commonly found in the core of networks, connecting switches together or meshing the routers together at an ISP level.



Advantages

It provides a redundant path between devices; networks can be expanded without disruption to the users; if nodes or cables fail, traffic can be re-routed easily.

Disadvantages

This requires more cables than the other topologies; there is a complicated implementation procedure; there are large amounts of redundancy through the network.

S.4. Introduction to Protocols

📅 11-10-22 🕘 09:00 🎓 Amanda 📍 Zoom

Networking Protocols

Networking protocols are the rules for communications, they define the rules for component-to-component communication. They are common sense rule/etiquette.
Protocols smooth the communications process between the sender and receiver or overwhelm the receiver. Protocol developers have to consider many potential problems.
Protocols are usually pieces of software that overcome problems raised by *what ifs*.

What If

Networking protocols control the *what if* conditions. What if a packet gets corrupt; the receiver can't keep up with the sender; the communications medium fails?

Connection-Oriented Protocol

1. Connection established
2. Exchange information
3. Disconnect

An example of the above would be a phone call, where the connection is established for the duration of the information exchange (phone call) and afterwards, the connection is 'torn down'.
This method makes use of virtual circuits. A virtual circuit is where the link between the sender and receiver is established and no other communications can use that transmission link for the duration of the transmission. After the sender and receiver finish communication, the virtual circuit is torn down and the transmission medium is available for another virtual circuit to claim. Virtual circuits give good quality of service when connected however they cost lots of money.
TCP is an example of a connection-oriented protocol.

Connectionless Protocol

This makes use of datagrams, where the two devices (sender and receiver) communicate over general use transmission mediums. This allows multiple different communications to be taking place simultaneously. However, using this protocol runs the risk of the packets not arriving at their destination. When we use this protocol, we hope that the packet will arrive at its destination.
IP is an example of a connectionless protocols.

Tradeoffs between VCs and Datagrams

With datagrams, no prior establishment or clearning is involved however with virtual circuits, this is required.
Datagrams require complete addressing information to be sent with each packet, whereas virtual circuits only require the circuit ID to be transmitted.
Packets sent via datagrams can all go different routes however packets sent through a virtual circuit all have to go the same route.
Datagrams are discarded if congestion occurs, whereas virtual circuits must take more elaborate precautions.

Why do we need TCP/IP

To finish after practical on Friday.

S.5. Practical 3

📅 14-10-22 🕑 14:00 🎓 Amanda 📍 PO 2.27

Collision Detection

Within a network, we need a way to be able to detect if a collision occurs. For bus topologies, there is an algorithm which does this for us.

Carrier Sense Multi Access/ Collision Detection Algorithm

This algorithm starts when a node has a frame (packet of data) ready to transmit.
The node starts by listening to the medium (listens to the backbone for voltage, which if present, is packets being transmitted) and looks for quiet. If the medium is idle, transmission can begin. The node begins to transmit the packets, and listens to the medium while doing so; through this process, it can detect collisions on the network due to voltages. If no collisions are detected, the node finishes transmitting data until all data has been transmitted. However, if collisions are detected, transmission continues until minimum packet time has been reached to ensure the other node transmitting has also detected the collision. Then the original transmitting node checks to see if the maximum number of transmission attempts has been reached. If it has, then the transmission is aborted. If it hasn't, the node waits a random backoff (this is random to ensure both nodes don't both attempt to transmit again at the same time), then it starts this entire transmission process again.

S.6. Protocols Continued

📅 18-10-22 🕘 09:00 🎓 Amanda 📍 Zoom

Protocols Recap

Protocols are sets of rules which are used for sending and receiving data across networks. They can provide addressing as well as management and verification of transmission. Often protocols are used together to form a suite of protocols, for example TCP/IP.

TCP/IP

TCP/IP stands for Transmission Control Protocol/ Internet Protocols. It is a collection of protocols that govern the way that data travels from one machine to another across networks. Commonly it is found in the core of networks. In this term, networks could be a small LAN, enterprise environment networks, metropolitan networks or wide area networks. There are two major components of TCP/IP.

Transmission Control Protocol

At the sending device, TCP breaks up the data into packets which the network can handle effectively. During transmission TCP does nothing. At the recipient node, TCP ensures all the packets have arrived and are in a fit state; TCP then reports the condition of the packets back to the sender node so it knows if it needs to re-transmit any of them. TCP will then reassemble the data into its sequence.

Internet Protocol

IP is used to envelope the data, this provides a location for the sender and destination IP addresses to be added to the packet.

Connection Types

There are two types of connection, connection-oriented and connectionless.

Connection-Oriented

Connection oriented is where a dedicated connection is setup between the sender and receiver. This connection is setup for the duration of the transmission or a set amount of time, in the case of a lease line, then torn down and the infrastructure is available for other connections to use. There are five phases to connection oriented communications

1. Connection established
2. Open connection
3. Transmit data
4. Close connection
5. Tear down connection & make infrastructure available for other communications.

The connection oriented connection type is often compared to a landline telephone system where a dedicated connection is setup between the two phones.
As dedicated infrastructure is used, there is a high quality of service, low fixed delay and limited packet loss however this system isn't as efficient as other connection types because it requires time to setup and tear down the connection before and after the transmission. This connection type is also not an effective use of resources because only one connection can use that infrastructure at a time.

Connectionless

Connectionless connections are where the packets are sent any route which the infrastructure deems suitable. This provides a lower quality of service than that of connection-oriented however connectionless is more efficient as multiple different communications can use the same infrastructure.
Once a packet has left the sender node, it travels until it reaches the first switch/router. Here the recipient node's IP address (contained in the packets header) is looked at and the switch/router decides which he most efficient route to transmit the packet down is. The packet is transmitted down this route. Internet Protocol is used here to manage the IP addresses written in the packets.
Connectionless transmissions have a number of drawbacks, as all the packets can go via completely different routes, there is a variable amount of delay on the packets arriving at the recipient node. Packets may also get lost whilst in transmission, and the packets may not all arrive in the correct order. The Transmission Control Protocol is used here to help rectify some of these problems. (see TCP section above)
Connectionless connections are often compared to the postal system, whereby the post is sent from sorting office (switch/router) to sorting office until it arrives at the destination and we often don't think about which sorting offices the post will travel through.

Packets

A packet is a single unit of data that is sent across a network. Data to be transmitted is broken into a number of packets before it is transmitted across the internet. Packets have multiple parts, one part is the *header* in which, the sender and recipient IP addresses are stored as well as the code which is used to handle transmission errors and keep packets flowing.

Packet Routes

As the packet "hops" from node to node on its journey across the network, it across routers. These are devices which are dedicated to reading the header information and determining which route the packet should take to the next router. Packets move from router to router until they reach their final destination. All the packets going from one sender to one recipient may not all take the same route, there are a number of variables which influence this including the network traffic at that particular moment and the size of the packet being sent.

Packets and TCP/IP

TCP sends the packets in sequence; ensures the integrity of the packets and where needed requests new packets to be sent if on receipt a packet is damaged; and acknowledges receipt of packets.
IP breaks the data in to packets; places header information into packets; and determines how much data can fit into a single packet, this can include fragmenting the packet further if there is lots of congestion on the network.

Example Packet Transmission

The example below shows how an email message would be transmitted across a network.

1. The data that makes up an email message is split into packets by the IP portion of TCP/IP. IP also adds header information to each packet.

2. Using the header information in the packets, routers determine the best path for each packet to take to its final destination.

3. The TCP portion of TCP/IP reassembles the packets in the correct order and ensures that ll packets have arrived undamaged.

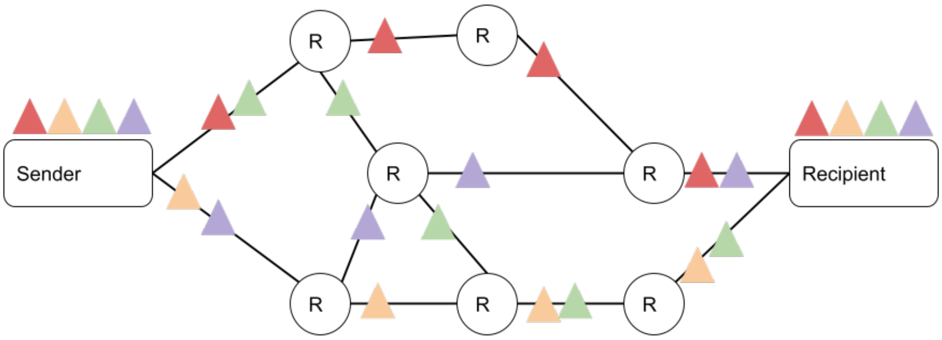


Figure 1: Packet transmission across a network where packets travel from router to router

NB: Notes from practical session on 21-10-22 also included in this lectures notes as no new content covered.

S.7. Local Area Networks (LANs)

📅 25-10-22 🕘 09:00 🎓 Amanda 📍 Zoom

Network Interface Cards

Any transmission from a Network Interface Card (NIC) will reach every other NIC. Each NIC has a unique LAN address, this is a 48-bit globally unique identifier called a Media Access Control (MAC) Address. MAC addresses are written in hexadecimal and they are burnt into the ROM chip of the NIC. A MAC address is assigned partly by global identifiers and partly by the manufactures.
NICs read all broadcast messages and all multicast messages with addresses that they have been programmed to read. The hardware of the NIC will ignore all other addresses.

Ethernet LAN Access Devices

Client deices can have a cable between their PC and an interconnection device in a network rack. These interconnection devices could be: a hub; a switch; or a router.

Access and Distribution Rules

Shared Media LANs

Access Rules for Ethernet Hubs

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

Distribution Rules for Ethernet Hubs

- All traffic goes everywhere (NICs on receiving devices will pick out which packets are for it)
- One packet at a time

There can still be collisions.

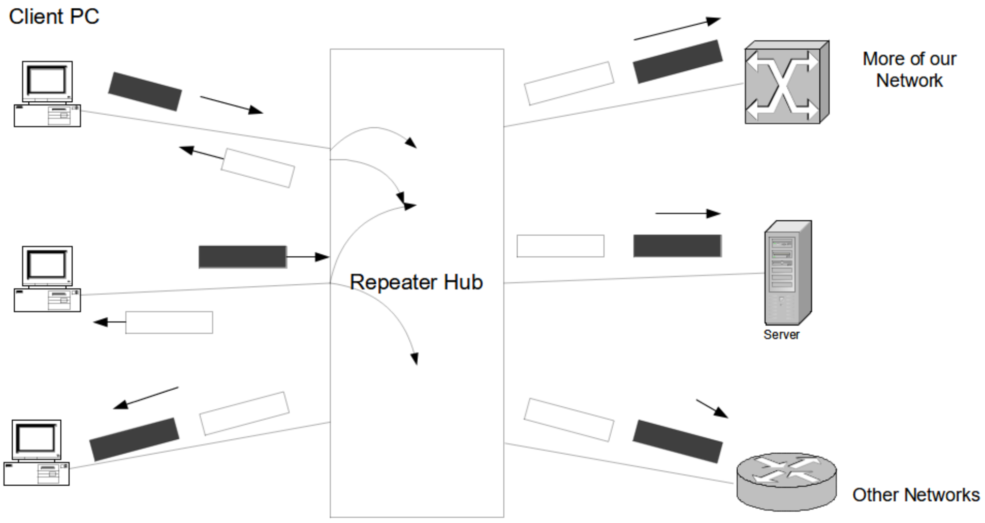


Figure 2: Diagram of packet transmission on a shared media LAN

Switched Ethernet LANs

Access Rules for switched Ethernet

- Send whenever you want
- No collisions

Distribution Rules for switched Ethernet

- Traffic only goes where it needs to go
- Multiple Ethernet frames can be flowing

This LAN works by the packet arriving at the switch, it looking at the header of the packet and determining which route the packet should take to reach its destination. The switch sends the packet to the correct destination only. If the packet needs to go to multiple destinations, multicast has to be used.

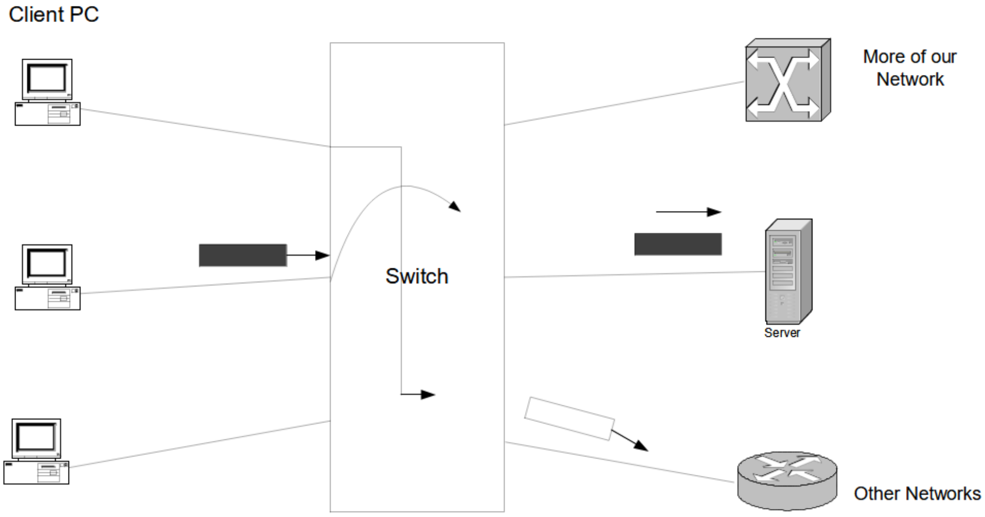


Figure 3: Diagram of packet transmission on a switched Ethernet LAN

Switched Ethernet is a hardware implementation of bridging. Switched Ethernet automatically learns address; forwards selectively to the destination; supports many ports per switch; supports full duplex on dedicated ports.
Switches can support different data rates on each port. Ethernet switches will generally operate in *store and forward* mode, this is where they temporarily hold the frame whilst making the forwarding decisions. Some Ethernet switches may also support *cut-through operation*, which is where they start to forward after receiving the destination address part of the frame; this can only happen if the output port id is free and of the same data rate. Cut-through reduces the delay of the packet getting through the switch.

Classification of Transmission

Unicast - single destination addressing. This specifies a single node on the network to transmit to.
Multicast - multiple but not all destinations addressing. This transmits packets to all nodes in a target group. Not all destinations. The same packet is duplicated by the switch to go our on multiple ports.
Broadcast - all destinations. This transmits packets to all nodes on a network. Hubs will broadcast to all devices connected. Switches can broadcast to all devices connected if the address says it can.

The LAN Networking Model

LANs operate at the *data link* layer of the Reference Model. IEEE has divided the data link layer into two sub-layers: Logical Link Control (LLC); and Media Access Control (MAC).
Quality Of Service lives in the MAC sub-layer.

IEEE 802

As seen in the diagram below, there are a number of different LAN standards. They all come under the IEEE 802 standards.

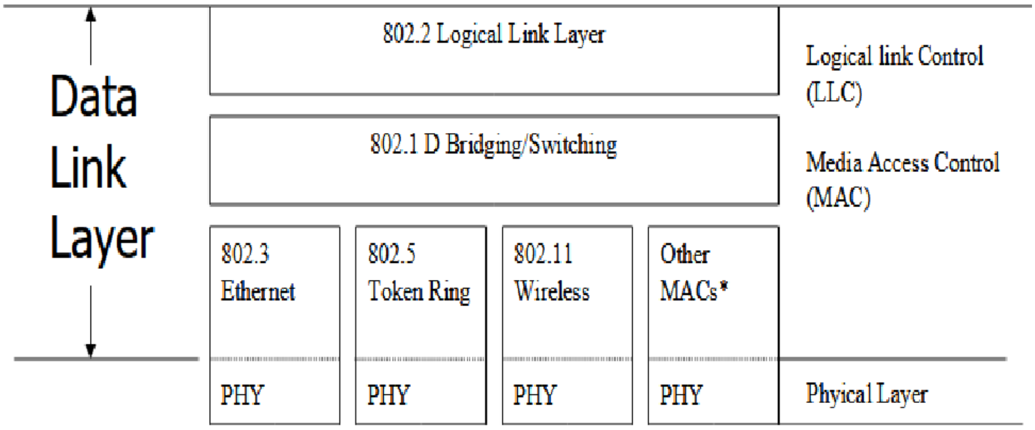


Figure 4: Diagram of the 802 LAN Standards

802 is often pronounced ”eighty-two”.

Common Aspects of the LAN standards

All standards use the same MAC address length (48 bits); support broadcast and multicast addressing; and all have good (32-bit) error checking.

Different Aspects of the LAN standards

There are a number of differences between some of the LAN standards: access methods (some use CSMA/CD while some use token passing); maximum frame size; support for features (for example priority) is only available in some standards; and specific data rate values.

Virtual LANs

Virtual LANs (VLANs) are pieces of software which give an appearance of a physical connection. Their purpose is to limit broadcast traffic to a defined group (workgroup). The workgroup is defined by network management. Membership is setup by selecting a set of ports on a switch; selecting a set of MAC addresses; or Layer 3 protocol type (for example IP or IPX). The network administrator configures the VLAN membership, this is much better than re-cabling. Multiple VLANs can be configured and one VLAN can connect to another VLAN.

Power over Ethernet

Power over Ethernet (PoE) utilizes the Ethernet cabling to deliver power to some Ethernet attached devices, for example: ethernet telephones; or wireless access points. PoE is defined in standard 802.3af. The advantages of PoE are that power outlets may not be near and backup power may not be available in everyone’s offices.

Ethernet Standards

Standard	Properties
10 BASE5 (thickWire Ethernet)	10mbit/s, baseband, 500m maximum
10 BASE2 (thinWire Ethernet)	10mbit/s, baseband, 185m maximum
10 BASE-T	10mbit/s, baseband, 100m maximum. Uses unsheilded twisted pair (UTP)
10 BASE-F	Fibre optic Ethernet (10mbit/s)
10 BASE-T and 100 BASE-F	10mbit/s, baseband

Table 1: Variations of IEEE 802.3

There are a number of 1Gigabit/s Ethernet standards aswell: 10GBASE-T UTP (Gigabit Ethernet, GbE); 10GBASE-x Fibre; 40GBBASE-X Fibre; and 100GBASE-X Fibre.

10 BASE-T

This is a multiport repeater. It can support up to four hubs (four repeater sets) along a data path. It can carry 10 mbit/s over two-pair Category 3 or better cabling. It supports up to 100m of cable length from the hub.

100 BASE-T

This is a direct extension of 10 BASE-T. It can carry 100Mbit/s over two-pair category 5e UTP (fast Ethernet). It can support up to 100m of cable length from the hub and two 100BASE-T switches can be interconnected.

Gigabit Ethernet

There are a number of different gigabit Ethernet standards.

IEEE	**Designation**	**Data Rate**	**Media Type**	**Max segment length**
802.3z	1000BASE-SX 850nm	1000 mbit/s	50 micron MMF	500m
	1000BASE-SX 850nm	1000 mbit/s	62.5 micron MMF	275m
	1000BASE-LX 1300nm	1000 mbit/s	Single Mode Fibre	5000m
802.3ab	1000BASE-T	1000 mbit/s	Cat 5e UTP	100m
802.3an	10GBASE-T	10000 mbit/s	UTP	100m
802.3ae	10GBASE-X	10Gbps	SMF or MMF	40km
802.3ba	40GBASE-X	40Gbps	MMF or SMF	40km
802.3ba	100GBASE-X	100Gbps	MMF or SMF	40km

802/3ae

There is a never ending demand for higher-data-rate communications. Despite the higher-data-rate capabilities, some things never change: 802.3/ Ethernet frame format; same minimum and maximum frame sizes; and same structured cabling topologies all stay the same. However, there are some things which do change (for 1 and 10Gbit/s), there is no CSMA/CD and it only uses full duplex communication. 10Gbit/s will be used in MANs, large networks and SANs; it is a replacement for SONET/ SDH networks.

Legacy Ethernet

	ThickWire	**ThinWire**
Current Status	Legacy	Legacy
Specification	802.3	802.3
Data Rates	10 Mbit/s	10 Mbit/s
Topology	Bus	Bus
Cabling	Special coax	RG-58 coax
Connectors	Attachment Unit Interface	BayoNet connector
Max. Cable Length	500m	185m
Max repeaters	4	4

Contemporary Ethernet

	Ethernet	**Fast Ethernet**	**Gigabit Ethernet**	**10G Ethernet**
Current Status	Mature	Mature	Current	Current
Specification	802.3	802.3u	802.3z, 802.3ab	802.3ae
Data Rate	10 Mbit/s	100 Mbit/s	1000 Mbit/s	10 Gbit/s
Topology	Star/ Tree	Star	Star	Stat
Cabling	Cat 3 to 5e UTP	Cat 3 to 5e UTP	Fibre	Fubre
Connectors	RJ-54	RJ-45	SC, MT-RJ or RJ-45	Fibre Optic Connectors
Max. Cable Length	100m	100m	Varies	Varies
Max. hubs	4	2	N/A	N/A

Ethernet Frame Format

The diagram below shows the Ethernet Frame Format.

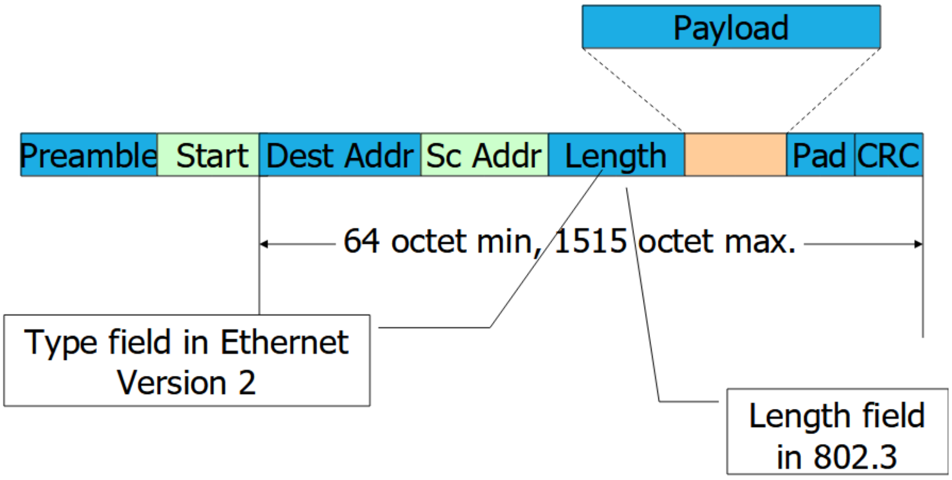


Figure 5: Ethernet Frame Format according to IEEE 802.3

S.8. IP Addressing

📅 08-11-22 🕘 09:00 🎓 Amanda 📍 Zoom

Introduction to Internet Protocol

The Internet Protocol (IP) is a connectionless protocol with best effort delivery. It has no built in data recovery capabilities. IP uses the IP addressing system which is a hierarchical, logical system which is highly scalable. The IP address is the address that sends data to specific computers in the form of packets and it can either be used in the form of static IP addresses or dynamic IP addresses (which get allocated by the Dynamic Host Configuration Protocol, DHCP).

Review of Functions of Internet Protocol

IP has rules of communication; creates packets; aids the movement of packets across the network; performs one st of tasks when transmitting data and another set of tasks when receiving data.

IP Addresses

IP addresses are always known outside of the domain which the device is within, this is different to MAC addresses which are generally only known within the domain which the device is on. IP is more commonly used to identify where the packet is going. MAC addresses are burnt into the Network Interface Card of a device whereas a IP address is assigned to a device and can change.
Similar to postal addressing, there are two areas of IP addressing. The network ID is similar to a street name and the host ID is similar to a house number.

Fields of IP Addresses

IP addresses have three key fields.

Unique x bit address

In IPv4, this is 32 bit and in IPv6, this is 128 bit. This address is unique to each node on the network. Originally IPv4 had enough possible permutations for every device which was internet connected. Now there are too many devices so IPv6 was introduced. This gives many more potential addresses, in theory enough for every internet connected device.

Subnet Mask

This is a 32-bit pattern used to identify the network and host addresses. Each device does not have a unique subnet mask.

Default Gateway

This is optional. It identifies the address of the router used to access another network outside of your own network, over the internet.

IP Data Transmission

Sending Data

This section assumes IP has already broken the data to be transmitted down into a packet.
The first step of sending data is to establish if the destination is on the same network or a remote network. This is achieved using Addressing Resolution Protocol (ARP), which will use a broadcast to

determine if the address is on the same domain at layer three of the reference model. ARP will then translate the IP address of the recipient into its MAC address to aid communication at the data link layer.

If the destination is local, the node can initiate direct communication. Otherwise, the communication must be via a gateway (router). Once the packet is prepared, it is passed to the Network Access Layer which transmits the packet to the connection media where the packet can begin its journey to the destination.

Receiving Data

When the packet arrives at the Network Access Layer of the receiving node, the datagram is checked for corruption and the that the address is correct. If all is okay, then the Network Access Layer extracts the data and passes it to the designated protocol.

The IP address gets checked for corruption, this is done by comparing the IP addresses and it ensures that the packet has been delivered to the correct destination.

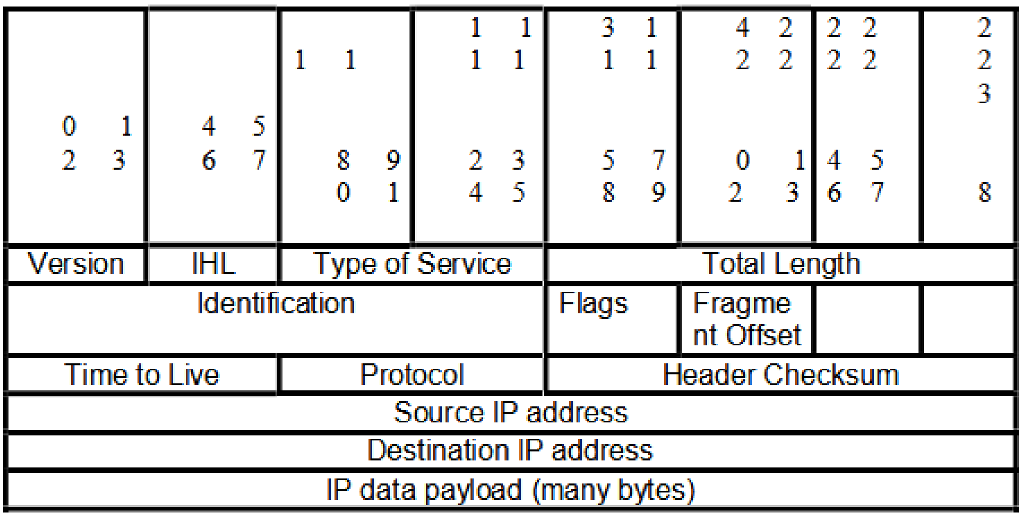
The instruction set is then checked to determine the next action. This could be to deliver the data to the next layer (TCP or UDP).

IP Header

Each packet contains a header as well as the actual data. The header is constructed on the sending computer and it contains information that is used by the protocols and layers. A header has several distinct units of information known as fields.

The IP Header contains, the IP address of the sending computer; the IP address of the destination computer and a set of instructions. As the packet travels through the switches/ routers, the header is examined and updated.

Detailed Contents of the Header



0 1 2 3	4 5 6 7	1 1 8 9 0 1	1 1 1 1 2 3 4 5	3 1 1 1 5 7 8 9	4 2 2 2 0 1 2 3	2 2 2 2 4 5 6 7	2 2 3 8
Version	IHL	Type of Service		Total Length			
Identification				Flags	Fragme nt Offset		
Time to Live		Protocol		Header Checksum			
Source IP address							
Destination IP address							
IP data payload (many bytes)							

Headers are at least 20 bytes.

Versions

This identifies the IP version used by this packet (e.g. IPv4 or IPv6).

Internet Header Length

IHL shows the length of the IP header in 32 bit words.

Type Of Service

This gives special routing information requirements. For example

- Low or Normal delay
- Normal or High throughput
- Normal or High readability

Total Length

This identifies the length of the packet in octets. The length includes the IP header and the data.

Identification

This gives each packet a unique identifier, in the form of an incrementing sequenced number.

Flags

This indicates fragmentation possibilities of the packet. DF indicates Don't Fragment and MF indicates More Fragments, 0 indicates no more fragments or there was no fragments.

Fragment Offset

This is a numeric value assigned to each fragment, which is used to reassemble the fragments.

Time To Live (TTL)

This is the time in seconds or router hops that the datagram can survive. Routers decrement this field by one as the packet passes through them or by the number of seconds that the datagram is delayed. When the field reaches nought, the datagram is discarded.

Protocol

This holds the protocol address where the IP should deliver the data.

Header Checksum

This holds a 16-bit calculated value to verify the validity of the header.

Source IP address

This is the address of the sending device which is used by the destination IP to verify delivery.

IP Data Payload

This is the data to be delivered. Its size is variable.

IDs

Every computer has a unique IP address. This is guided by the public and private addressing rules. Every computer on a LAN has the same *network ID*. Within that network, each computer will have a unique *host ID*. When these two are combined, they create the IP address.

Servers

Servers can have multiple IP addresses, this is due to the fact that they can have multiple NICs. Each individual network adapter is a point of contact and therefore known as a node. Therefore each Host ID corresponds to each individual node.

IP Address Structure

This section only looks at IPv4
An IP address uses 32 bits, this is hard to remember. The IP address is then broken down into 4 groupings known as octets. Each octet contains 8 binary bits converted into a decimal (this will be a number between 0 and 255).

IP Address Classes

A 32 bit binary number has 4 billion different permutations, this means there are 4 billion different IPv4 addresses.
A 128 bit binary number has 340282366920938463463374607431768211456 different permutations, this means there are 340 duodecillion IPv6 addresses.
TCP/IP does not support quite that number. The addresses have been broken down into smaller groups known as classes. These refer to different types of network IDs.
IP addresses are assigned based on the needs of the organisation. They are based on a classes A - C public IP addresses. There are two other classes, D and E however these have different uses.

Class A

This contains 8 network ID bits and 24 host ID bits. Class A can support 16,777,216 computers.
The leftmost bit is always 0, The leftmost 8 bits comprise the network ID. The rightmost 24 bits contain the host ID.

```
NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH
255.0.0.0
```

A subnet is used to differentiate the network ID form the host ID. This is assigned to networks that support large numbers of hosts.

Class B

This contains 16 network ID bits and 16 host ID bits. It supports 65,536 computers.
The leftmost bit is always 1 and the next bit is always 0.
It is assigned to medium sized networks and a subnet mask is used to differentiate the network ID and host ID.

```
NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH
255.255.0.0
```

Class C

This contains 24 network ID bits and 8 host ID bits. It supports 256 computers.
The leftmost two bits are 1 and the third bit is 0.
It is assigned to small networks and a subnet mask is used to differentiate between the network ID and host ID.

```
NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
255.255.255.0
```

Class D

The four left most bits start with 1110. This is used for multicasting.

Class E

This is an experimental class.
The five leftmost bits start with the pattern 11110.

S.9. OSI Reference Model

📅 15-11-22 ⏲ 09:00 🎓 Amanda 📍 Zoom

Standardisation

In the past, networks were built using many different hardware and software implementations, as a result the different networks were incompatible and it became difficult to effectively communicate between different networks. Effective networks devices must be able compatible and able to communicate with one another.
The International Organisation for Standardisation (ISO) researched different network schemes to resolve this issue, through doing this they established the need to create a global Network Model; and thus the OSI Reference Model was formed.

Importance of Networking Standards

Standards are fundamental to Open Systems. This provides independence from vendor proprietary approaches, allows open procurement and interoperability. Standards should be international in score. New standards should be tracked, so that we know when it is *safe* to use a new standard.

Network Standards Organisations

- International Standardisation Organisation (ISO)
- European Telecommunications Standards Institute (ETSI)
- The TCP/IP Internet Engineering Task Force (IETF)
- Publishes Request For Comments (RFC)
- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)

Fast Track For New Standards

The standardisation process is used to follow the successful development of some capability, this process can take 5 or 6 years. At the end of which, some products may be obsolete.
It is possible that standards can be 'Fast Tracked', which is a process where products and standards are developed in parallel. This can result in vendors releasing products before the standard is complete.

History of the OSI Model

The Open Systems Interconnection (OSI) reference model was ratified in 1984 as an international standard. It provides common terminology and a framework for networking, which has become the primary architectural model for inter-computer communications. OSI is still widely used today.
The OSI reference model describes how data makes its way from the application program, through the network medium to another application program on another device. It divides this problem of transmission of data into seven smaller, more manageable problems, called layers.

Layers of the OSI Reference Model

Each of the seven layers of the OSI model have a specific function/ task to complete and through the use of layers, the complexity is reduced. Each layer provides a service to the layer above.
The lower four layers are concerned with the flow of data from end to end and the upper three layers are focused more towards services to the application.
It is very common to refer to the layer by its number or name.
At the different layers, different protocols are added to the 'envelope' which contains the data.

LAYER 1: Physical

This layer deals with the physical characteristics of the transmission medium (the hardware). It defines the specifications for communication between the physical link and recipient node. The physical layer deals with characteristics such as: voltage levels; timing of voltage changes; physical data rates; maximum transmission distances; and physical connectors.

LAYER 2: Data Link

This provides access to the networking media and physical layer. It deals with transmission across the media, to the intended destination on a network. The Data Link Layer can provide reliable transit of data across a physical link by using MAC addresses, through using MAC addresses, multiple stations can share the same medium and still uniquely identify each other. This layer is concerned with: network topology; network access; error notification; ordered delivery of frames; and flow control. This includes Ethernet, Frame Relay and FDDI.

LAYER 3: Network

This layer is concerned with the end-to-end delivery of packets. It defines logical addressing and how routing works, as well as how routes are learned so that the packets can be delivered. It also defines how to fragment a packet into smaller packets to accommodate different media. Routers operate at this layer.

LAYER 4: Transport

This layer regulates information flow to ensure end-to-end connectivity between host applications is reliable and accurate. It segments data from the sending host's system and reassembles the data into a data stream on the receiving host's system. The transport layer includes TCP and UDP.

LAYER 5: Session

This layer defines how to start, control and end conversations (called sessions) between applications. It uses dialogue control for management of multiple bi-directional messages. It synchronises dialogue between two hosts' presentation layers and manages their data exchange sa well as offering provisions for efficient data transfer.

LAYER 6: Presentation

This layer ensures that the information the application layer of one system sends out is readable by the application layer of another system. It translates between multiple data formats by using a common format and provides encryption & compression of data.

LAYER 7: Application

This layer is closest to the user. It provides network services to the user's applications however it doesn't provide services to any other OSI layer. It checks the availability of intended communication partners and synchronises & establishes agreement on procedures for error recovery & control of data integrity.

S.10. Network Capacity Calculations

📅 19-11-22 🕑 14:00 🎓 Amanda 📍 PO 2.27

This practical continues on from the previous weeks practical where we used OpNet to simulate a 16 node star topology network with a switch as the central node.

To calculate the amount of data sent per second from a single node, use the formula

$$\frac{1}{\text{time interval of packet being sent}} \times \text{packet size} = \text{bytes per second}$$

To get the bits per second, we divide the bytes per second by 8.

To get the kilobits per second, divide the bits per second by 1000.

To get the total amount of traffic in a single second for the whole network, multiply the number of nodes by the amount of traffic per second for a single node. This is a really useful piece of information to have as it allows us to work out if the network is at capacity or not and so that we know if the network is able to cope with that amount of data or not. This is crucial to know as if the network cannot cope then in a business setting, this is really bad as the network will slow down productivity of employees therefore loose the business money.

A solution to an over-capacity network is to add a second switch which takes some of the load off the original switch. In the example used of the previous weeks simulation, a second identical switch would take 8 of the connections. However, when doing this, its important to ensure that the original switch can cope with the speed of the new switch, so to not create a bottleneck. Provided the two switches can cope with each other, adding a second switch removes a single point of failure and adds some load balancing.