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

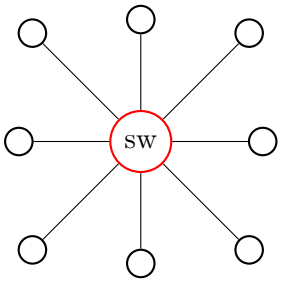
Toplogy

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

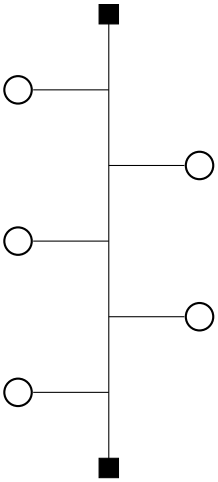
If one of the nodes fails, the network will still function; depending on the capacity of the central node, the network can accommodate heavy traffic; it is easy to add and remove nodes as necessary, the limit of numbers of nodes is the capacity of the central node.

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

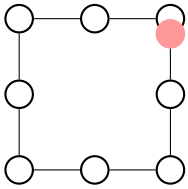
Allows relatively good rate of data transmission; it is simple to implement; it uses less cable than a star topology; it uses a lower grade of cable than star topology, hence it is cheaper.

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

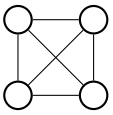
All nodes on the network have equal chances of transmitting data; there is a good quality of service; there are no collisions.

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.

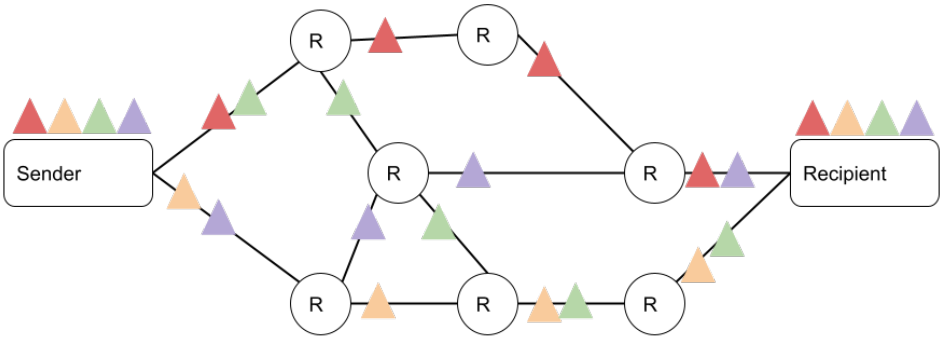


Figure 1: Packet transmission across a network where packets travel from router to router

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