

---

University Of Portsmouth  
BSc (Hons) Computer Science  
First Year

**Networks**

M30231

September 2022 - May 2023

20 Credits

Thomas Boxall  
up2108121@myport.ac.uk

---

# Contents

<b>1 LECTURE: Introduction To Module</b>	<b>2</b>
<b>2 PRACTICAL: Introduction to Practical Sessions</b>	<b>5</b>
<b>3 LECTURE: Computer Networks and Network Topologies</b>	<b>6</b>
<b>4 LECTURE: Introduction to Protocols</b>	<b>10</b>
<b>5 PRACTICAL: Collision Detection</b>	<b>12</b>
<b>6 LECTURE: Protocols Continued</b>	<b>13</b>
<b>7 PRACTICAL: TCP/IP &amp; UDP</b>	<b>15</b>
<b>8 LECTURE: Local Area Networks (LANs)</b>	<b>16</b>
<b>9 LECTURE: IP Addressing</b>	<b>22</b>
<b>10 LECTURE: OSI Reference Model</b>	<b>27</b>
<b>11 PRACTICAL: Network Capacity Calculations</b>	<b>30</b>
<b>12 LECTURE: Communication Circuits</b>	<b>31</b>
<b>13 LECTURE: Communication Circuit Options</b>	<b>34</b>
<b>14 LECTURE: Wide Area Networks</b>	<b>38</b>
<b>15 LECTURE: Wide Area Networks II</b>	<b>41</b>
<b>16 LECTURE: Interconnection Protocols</b>	<b>43</b>
<b>17 LECTURE: Security</b>	<b>46</b>
<b>18 LECTURE: Network Security</b>	<b>48</b>
<b>19 LECTURE: Intranet Systems Management</b>	<b>54</b>
<b>20 LECTURE: Application Support Protocols</b>	<b>58</b>

# Page 1

## LECTURE: 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 will 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 create 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.

## Page 2

# PRACTICAL: Introduction to Practical Sessions

📅 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.

## Page 3

# LECTURE: 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 information because 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 each other, ensuring 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

### Topology

A topology 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

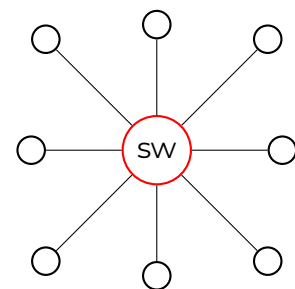
In the star topology, all devices are connected to a single central node. This central node is usually a switch or hub. This topology is more common in today's networks, especially due to the fact that multiple 'stars' can be interconnected.

### 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 function); the effectiveness of the whole network is determined by how effective the central node is.





## Bus Topology

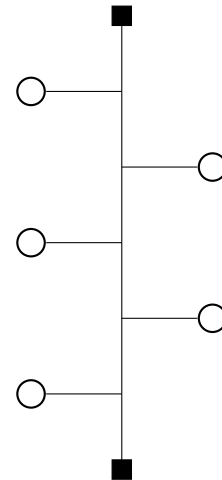
In a bus topology, there is a central backbone cable which runs the entire length of the network. Linked into this backbone are the nodes. At the end of the backbone, there have to be special terminators. This design is limited to a very low number of computers. This topology is no longer a popular method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

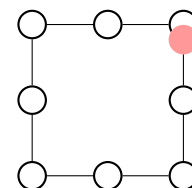
In this topology, all the nodes on the network connect together into a ring. Through software, a 'token' is created. This is passed from node-to-node; and when a node has the token, it is able to communicate. This is no longer a popular method for designing a network as the design is limited.

### 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.

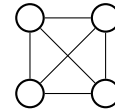


## Mesh Topology

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.

## Page 4

# LECTURE: 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?

## Types of Protocols

There are two main types of protocols. Each have a number of examples which will be explored in future lectures.

### Connection-Oriented Protocols

Connection-oriented protocols works as follows:

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

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, as part of this, they are able to have a high quality of service (QoS). This high QoS comes from extensive packet checking on receipt of a packet.

There are a number of downsides to using connection oriented protocols: they take time to setup and tear down; whilst in use, no other transmissions are able to use that communications link, which is an inefficient use of resources; and due to the packet checking on receipt of a packet, there are additional time delays.

TCP is an example of a connection-oriented protocol.

## Connectionless Protocols

reviewed  
2022-12-23

Connectionless protocols make use of general transmission mediums. This allows the sender to send the data into the network, and hope that it arrives at the receiver. The use of general transmission medium allows multiple transmissions to use the medium at once, with hardware redirecting traffic towards its destination. 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. The lack of a reserved transmission medium makes connectionless protocols much more efficient than connection-oriented. This makes connectionless protocols useful for situations in which data must be transmitted quickly, such as audio or video. There are a number of drawbacks to connectionless protocols. As all the packets can go via completely different routes, there is a variable amount of delay on each packet arriving at the recipient node. Packets may also get lost whilst in transmission, and the packets may not arrive in the correct order. The Transmission Control Protocol is used here to rectify some of these problems (see *next lecture*).

### How Connectionless Protocols Work

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. IP is an example of a connectionless protocols.

## Virtual Circuits

added  
2022-12-23

### Virtual Circuit

Where an exclusive connection between the sender and reciver is established through software. No other transmissions are able to use the transmission medium during this time. After transmission is complete, the connection is 'torn down' enabling other transmissions to claim that medium.

Virtual circuits give good quality of service when connected however they cost lots of money.

Virtual Circuits are able to be configured such that they use limited bandwidth, making them more efficient. Several virtual circuits are able to be assigned to a single length of cable, with a single virtual circuit 'claiming' the cable when it needs to transmit.

### Tradeoffs between VCs and Datagrams

With datagrams, no prior establishment or clearing 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.

## Page 5

# PRACTICAL: Collision Detection

📅 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.

## Page 6

# LECTURE: Protocols Continued

📅 18-10-22

🕒 09:00

👤 Amanda

📍 Zoom

*NB: Connection Type notes moved & merged with previous lecture (2022-10-11), for simplicity and clarity.*

## 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.

At a high level, TCP/IP protocols work together to break the data into small pieces that can be efficiently handled by the network; communicates the destination of the data to the network; acknowledges receipt of data; reconstructs the data into its original form; and checks that the data is not corrupt. These individual tasks are completed between the different protocols which make up the suite of protocols called TCP/IP.

## Transmission Control Protocol

TCP, a connection-oriented subprotocol, ensures reliable data delivery through sequencing a checksums as well as providing flow control to the transmission. 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 re-assemble 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.

## 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

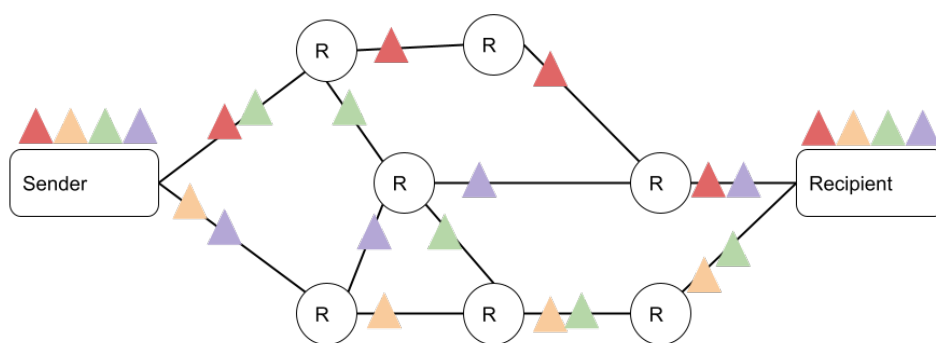
TCP sends the packets in sequence; ensures the integrity of the packets and where needed requests new packets to be sent if on receipt a packet is damaged; and acknowledges receipt of packets.

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 all packets have arrived undamaged.



Packet transmission across a network where packets travel from router to router

## Page 7

# PRACTICAL: TCP/IP & UDP

📅 21-10-22

🕒 14:00

👤 Amanda

📍 PO 2.27

*NB: These notes were written up during revision for the January exam in January 2023.*

## Three Way Handshake

A *three-way handshake* process is used to establish a TCP session. This has to be done before any computers communicate using TCP.

1. The sending device sends a packet to the recipient to see if it is ready. This packet is assigned a sequence number (unique to that instruction), acknowledgement value of 0 and flags set to `SYN`.
2. When this is received by the recipient node and it is ready to receive the full data, it responds with a new sequence id, the acknowledgement value set to the sequence of the previous packet incremented by 1 and the flags `ACK SYN`.
3. The sending node then responds to acknowledge the ready-ness of the server. This is done with a new sequence id, the acknowledgement value set to the sequence of the previous packets sequence id incremented by 1 and the flags `ACK`.
4. Payload transmission can begin
5. Once the payload has been sent, the `FIN` bit is set to 1 which indicates the end of the message.

If the recipient node isn't ready to receive data, then it just acknowledges the first packet and doesn't respond with a `SYN` flag then the third step doesn't happen. This whole process takes milliseconds.



## User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless transport service. This means that there is no guarantee that the packets will arrive in the correct sequence, or at all. UDP also provides no error checking or sequencing. This lack of features makes UDP much more efficient than TCP, which means it is much more suitable for applications in which speed of transmission is more important than integrity of transmission (for example, video calls). The UDP header is much shorter than the TCP header.



## Page 8

# LECTURE: 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.

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.

## Media Access Control Addresses

Media Access Control (MAC) addresses are written in hexadecimal and burnt into the read only memory (ROM). The manufacturer will assign a MAC address to a NIC. The MAC address is structured such that there is a manufacturer identifier part and a unique device identifier part.

## Ethernet LAN Access Devices

Client devices 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

Shared media LANs can only support a limited number of users and will generally be limited by their size. It shares its total bandwidth between all the devices connected.

#### 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.

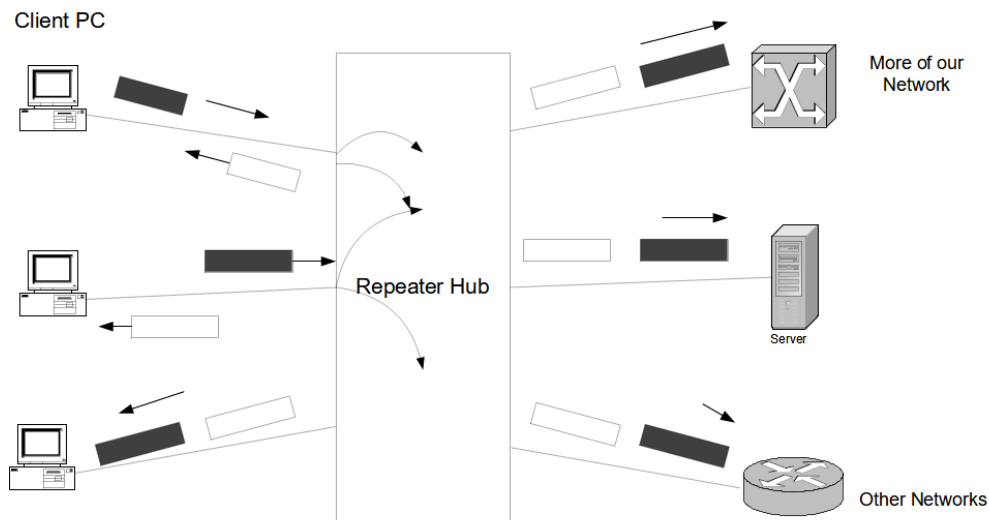


Diagram of packet transmission on a shared media LAN

## 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.

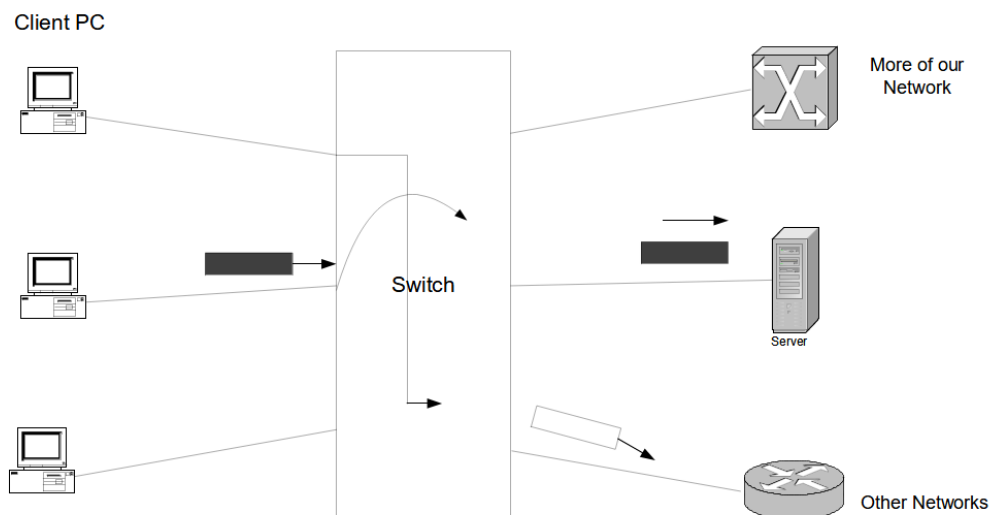


Diagram of packet transmission on a switched Ethernet LAN

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 out 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.

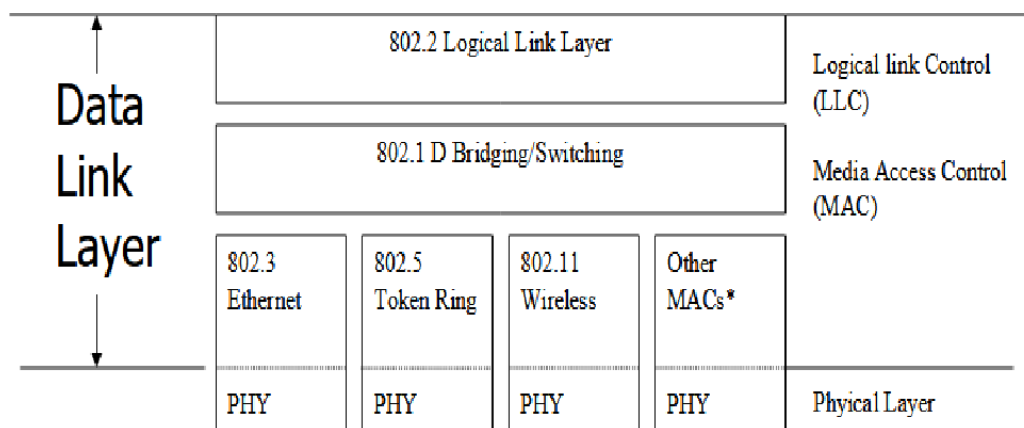


Diagram of the 802 LAN Standards

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 8.1: 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

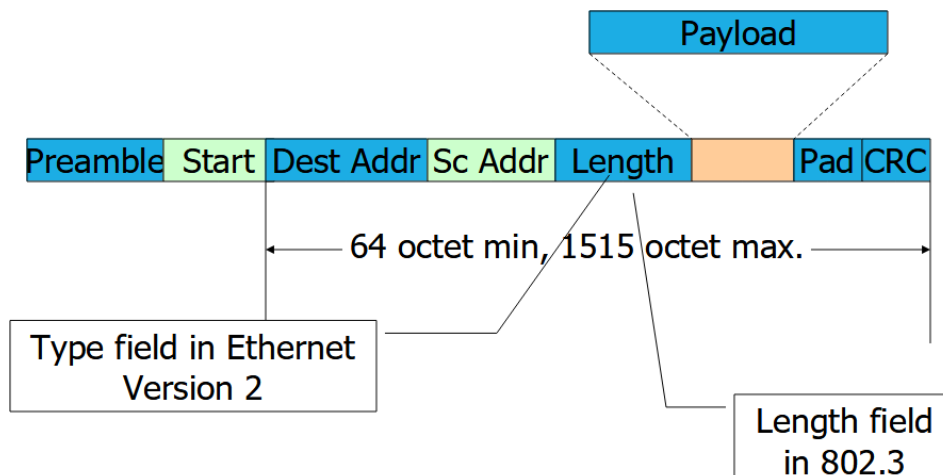
	ThickWire	ThinWire
Current Status	Legacy	Legacy
Specification	802.3	802.3
Data Rates	10 Mbit/s	10 Mbit/s
Topology	Bus	Bus
Cabling	Special coax	RG-58 coax
Connectors	Attachment Unit Interface	Bayonet connector
Max. Cable Length	500m	185m
Max repeaters	4	4

## Contemporary Ethernet

	<b>Ethernet</b>	<b>Fast Ether- net</b>	<b>Gigabit Ethernet</b>	<b>10G Ether- net</b>
Current Status	Mature	Mature	Current	Current
Specifica- tion	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	Star
Cabling	Cat 3 to 5e UTP	Cat 3 to 5e UTP	Fibre	Fibre
Connectors	RJ-45	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.



Ethernet Frame Format according to IEEE 802.3

## Page 9

# LECTURE: 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 set 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 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	8 9 0 1	2 3 4 5	5 7 8 9	0 1 2 3	4 5 6 7	8
Version	IHL	Type of Service		Total Length			
Identification				Flags	Fragment 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 from 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.

## Page 10

# LECTURE: 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 scope.

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 mes-

sages. It synchronises dialogue between two hosts' presentation layers and manages their data exchange as 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.

## Page 11

# PRACTICAL: 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 lose 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, it's 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.

## Page 12

# LECTURE: Communication Circuits

📅 22-11-22

🕒 09:00

👤 Amanda

📍 Zoom

## Introduction

Communications media for Local Area Networks can either be wired or wireless.

### Wired

Wired approaches consist of: Twisted pair cabling; coaxial cable media; and fibre-optic cabling.

### Wireless

Wireless approaches consist of: satellite communication; radar; mobile telephone system; global positioning system; infrared communication; WLAN; and Bluetooth.

## Wired Approach

Modern wiring plans normally follow standard structured cabling methods. This quite often consists of a wired cabinet on each floor of a building with orderly cabling installation connecting each cabinet to other cabinets and computers. Cabling racks will often consist of patch panels, wiring distribution and network access devices

Some buildings are easy to install cables into; where walls are thin, they can easily be drilled through. However, some building are harder to install cables into; where walls are thick, it is harder to drill through a wall so alternative routing might be considered.

## Cabling Media Choices

The network designer has a number of alternative cabling media choices, discussed below. Whilst deciding what cabling to use, they must consider: the required data rate, and what this might grow to in the future; the level of electrical interference; the maximum cabling length; and finally the cost.

### Cable: Unshielded Twisted-Pair

Unshielded Twisted-Pair (UTP) is the standard family of cables which will be found in most installations today. They are the least expensive media and are capable of working for distances up to 100m.

The data capacity grades are defined by EIA/TIA 568 (ISO 11801) and are as follows

- Cat. 3 - to 10 Mbit/s or more
- Cat. 4 - to 20 Mbit/s or more
- Cat. 5 - to 100 Mbit/s or more
- Cat. 5e, 6 and 6A - to 1000 Mbit/s and above (these are used extensively today)



## Multiplexing

Multiplexing is where a number of signals are combined together to be transmitted through the same medium. This is possible with UTP as each twisted pair can carry a different signal.

### Cat. 6 Cabling

The latest form of UTP is Cat. 6. It adds additional quality to assurances beyond Cat. 5e. Cat. 6 comes in two forms: UTP; and Screened Twisted Pair (ScTP). ScTP has a layer of metallic foil to improve its interference rejection. It may use larger-diameter copper wires which help with PoE situations.

There are an additional two categories of cable, Cat. 7 and Cat. 8. These are either Screen Shielded Twisted Pair (SSTP) or Screened Foiled Twisted Pair (SFTP). Cat 7 & 8 have a specially designed connector, however they are compatible with standard RJ-45 connectors.

### Cable: Shielded Twisted-Pair

Shielded Twisted-Pair (STP) was primarily used by IBM and it should be better than UTP. This is because it has a shield which helps prevent interference from outside signals and also helps prevent interference to outside signals.

Token Ring Topologies will generally contain a mix of UTP and STP cabling.

### Cable: Coaxial Cable

Coaxial cable produces low amounts of noise, therefore has low bit-error rate. It is used in a variety of networking applications (for example, IBM Networks and in earlier Ethernet). The shielding may include multiple layers of foil and/or braid.

### Cable: Fibre-Optic Cable

Fibre-Optic cables have high data rates. In LAN environments, they can reach speeds of more than 100 Mbit/s. In Telephone company link environments, they can reach more than 10 times the LAN value.

They are typically deployed as two unidirectional links with one fibre transmitting in each direction. To transmit, the electrical signal has to be converted to light then back to electrical signals at the recipient end.

Physically, fibre-optic cables are thin. There are two key measurements to know, the internal and external. The external dimensions are often  $125\mu m$  in diameter. The internals of Single Mode (transmits a single signal at a time) may be as thin as  $9\mu m$ , while Multimode (transmits multiple signals in the same direction at the same time), may be either  $62.5\mu m$  for American sizes or  $50\mu m$  for European sizing. The relationship between the internal diameter (that of the glass) and the external diameter is expressed as follows: internal/external. For example, European multimode would be expressed as 50/125.

Whilst Multimode allows for multiple signals to be transmitted down the same fibre-optic strand at the same time, over longer distances the pulses spread out. This results in dispersion of the signals, ultimately resulting in corrupt data. Therefore, where the distance to cover is very long or the speed of transmission needs to be high, single mode fibre should be used.

At either end of the fibre strand, a connector is needed. These connectors are often the most expensive part of the fibre system.

The actual cable element costs approximately the same as a good quality Ethernet cable. Optical interferences are the most expensive component. The transmission is done by LEDs or Laser Diode. The receiver devices convert light pulses back into electrical pulses.

Fibre-Optic is the best available communications medium. It has excellent electrical noise immunity; is difficult to tap; is lightweight; and is smaller size.


A single fibre may support multiple light beams. This is one through Dense wave division multiplexing (DWDM); it can contain up to 25,000 or more simultaneous transmission. It is only used with single mode fibre. Media converters are required to convert between the different media types.


## **Wireless Communication Systems**

- Television and Radio Broadcasting
- Satellite Communications
- Radar
- Mobile Telephone Systems (Cellular Communications)
- Global Positioning System (GPS)
- Infrared Communications
- WLAN (Wi-Fi) IEEE 802.11
- Bluetooth
- Cordless Phones
- Radio Frequency Identification

## Page 13

# LECTURE: Communication Circuit Options

 29-11-22

 09:00

 Amanda

 Zoom

### Media Selection

This is the process through which you decide what media you will use in the communications circuit. There are a number of factors which must be considered when doing so:

- What maximum data rates can be supported?
- What is the maximum length of a single cable run?
- Is there any susceptibility to electrical interference?
- What are the major cost components associated with the medium?
- What are the infrastructure constraints?

Media Type	Data Rate	Distance	Interference	Cost Issues
Radio-based wireless LAN	Typically up to 11 Mbit/s	Up to 50m indoors and 205m outdoors	Some interference is possible	NIC plus WAP
UTP	Up to 1Gbps (high dist) or up to 10 Gbps (low dist)	Up to 100m for low speed or 37.5m for high speed	Some interference is possible	Labour required
Multimode fibre	Up to 1 Gbit/s	Up to 2km at 100 Mbit/s and 500m at 1 Gbit/s	No interference problems	Labour costs plus expensive electro-optical adapters
Single Mode Fibre	Up to 10 Gbps	Up to 40km	No interference problems	Labour costs plus expensive electro-optical adapter and high power laser
Shielded	>25 Gbps	100m	Minimal Interference Problems	Labour costs

## Analogue Transmission

Analogue Transmission is done through systems based on technology developed in the 1800s. 42% of businesses (2.4 million) are still reliant on analogue transmission; and 33% of larger companies also still use ISDN or PSTN. BT plans to switch off analogue services in 2025 however not all providers will follow.

## Dial-Up Telephone Links

Dial-up telephone links are still available in two forms: analogue and digital. Analogue telephone links require a digital-to-analogue modem card, where the PC provides a digital signal which can be converted to analogue. Digital links require a digital-to-digital adapter card, where the digital signal from the PC is converted to an alternative digital form.

## Modulation

Modulation converts a digital signal into an analogue signal which can then be sent across the analogue line. Demodulation converts the signal back to digital. This will be done by a modem (MOdulation-DEModulation).

Modems are standardised by ITU-T, V-series recommendations. Typical modems include

- V.34 at 28.8kbit/s and 33.6kbit/s
- V.90 at somewhat less than 56kbit/s

- V.92 for higher-speed uplink, faster connection time, and the ability to accept an incoming call

The data rate may fall back to lower rates. The modem will operate at the highest available dial-up line data accepted on an incoming call.

The modem may perform V.42 error correction; V.42bis (4:1) or V.44 (6:1) data compression; V.54 loopback testing; V.250 command set.

## Reason for going Digital

Computer data is inherently digital (you are able to adapt it more easily using digital transmission); higher data rates available; easier to switch; and there is a better error rate (noise is not cumulative as repeaters can reject induced noise however amplifiers also amplify the noise).

## Digital Telephone Channels

Digital telephone communications channels are also available. These operate at 56 or 64 kbps per channel (or a multiple of them) or at 1.544 mbit/s or 2.048 mbit/s (in the US, Canada and Japan) channels.

### DSU/CSU

Instead of modems, Data Services Unit/Channel Services Unit (DSU/CSU) adapter devices may be needed. These are placed at either end of the communications link, attached to the communications device. The DSU adapts the digital signal (transmit and receive voltages, and timing). The CSU normalises voltage levels, provides maintenance capabilities, and protects the public network.

A different interface, the V.35 interface, is often used for higher speed DSU/CSU's. The V.35 has two-wire circuits, which gives balanced lines for data and timing. This is different to the RS 232 interface which is unbalanced. A significant problem with the V.35 interface is that it can be plugged in the wrong way around, unlike the RS 232 which can only be inserted one way.

## Other Interfaces

We have already looked at the RS 232 and V.35 interface. There are a number of other interfaces which are important.

### X.21 & Serial I/O interfaces

X.21 is a popular serial I/O interface. It is European.

Its connector has a reduced number of pins (15 pins) and has a transmit & receive pairs (for data and encoded commands). It has input and output control pairs (to indicate whether the transmit and receive are currently handling data or control). It has a timing signal pair. Networking devices typically support many different serial I/O standards. Usually they do this with a common connector on the I/O module and a separate adapter cable for each different type of serial I/O standard (for example, RS 232, RS 449, V.24 or X.21).

### T1/E1 and T3/E3

There are several problems with traditional T1/E1 systems. T1 (North America and Japan) and the E1 (the rest of the world) are not compatible. It is very complicated to add or drop

a 64 kbit/s channel. There is little problem isolation information in these systems. There is a need for higher bandwidth. A new system is needed, this is SONET/SDH.

Fractional T1/E1 links are multiples of 64 kbit/s. A common example is 348 kbit/s ( $6 \times 64$  kbit/s). This is commonly used with video conferencing. Fractional T1 may also be in multiples of 56 kbit/s.

Full T1/E1 is one of the most common types of WAN links. T1 operates at 1.544 mbit/s (24 slots at 364 kbit/s plus 1-bit framing). E1 operates at 2.048 mbit/s (32 slots at 364 kbit/s including framing).

Sharing a communication circuit in this manner is called time-division multiplexing (TDM). A T3 channel is 28 T1 channels multiplexed together (T3 is approximately 45 Mbit/s). An E3 channel is 16 T1 channels multiplexed together (E3 is approximately 34 Mbit/s). An E4 channel is 64 T1 channels multiplexed together (E4 is approximately 144 Mbps).

## High-Speed Synchronous optical Networking Standards

Two different forms have been developed.

### SOTNET

Synchronous Optical Network (SOTNET) is a North American standard. It operates at multiples of 51.84 Mbit/s. STS-3 supports triple the bandwidth at 155.52 Mbps. Multiples of 4 upto 40 Gbps.

### SDH

Synchronous Digital Hierarchy (SDH) is an international standard. It operates at multiples of 155 Mbit/s.

### STM

STM-1 operates at 155 mbps, STM-4 operates at 622 Mbps, STM-64 operates at 10Gps.

### SOTNET/SDH Ring

SOTNET/SDH can be combined into a resilient form, which is a dual ring. It automatically wraps to use both rings when one is cut; recovery time of this is within 50msec.

## Page 14

# LECTURE: Wide Area Networks

📅 06-12-22

🕒 0900

👤 Amanda

📍 Zoom

## Characteristics of Value-Added WANs

These will be able to operate at any distance as interconnection is by means of public carriers such as ISP. A WAN is high speed, relatively expensive and complex in design. Only the interface and network services are of concern to the user. The internals of the 'network cloud' are not an issue. Value-added WANs add features beyond those of dedicated point-to-point links. Transparent LAN services (TLS) hide the complexities of the WAN from the LAN administrator.

## Packet/ Frame/ Cell Switched WAN-Links

Individual data units may be called: packets, frames or cells.

The principal distinction is that packets and frames are of variable length. This means they usually require software processing, which limits the data processing rate. These are used in X.25, frame relay and TLS for example.

In contrast, cells are fixed length. They contain a 5-byte header and 48-bytes of data content. They can be processed in hardware which results in much higher data rates. However, if you want to use Cells and do not have 48-bytes of data to transmit, then you will have to pad out the payload to fill out all 48-bytes. This isn't used in core networks as it is not cost effective.

## Switched & Permanent Virtual Circuits

Some packet/ frame/ cell WAN alternates may be available in one or each of two forms: switched virtual circuits (SVC) or Permanent virtual circuit (PVC). SVC are switched to the needs of the data that is going through them, like dial-up links. Permanent circuits are always connected, meaning dedicated circuits are in place, similar to lease lines. Nowadays, for connections in the modern networks, switched virtual circuits are most commonly used.

Not all WAN technologies support both. Some have a preferred approach in terms of use. X.25 virtual circuits are usually secure virtual secures. Frame-relay virtual circuits are normally private virtual circuits. ATM virtual circuits can be either. TLS is more like a 'best effort' service.

## Objectives and Services for Value-Added WANs

- To provide an appropriate topology
- To provide a path (route) across a network
- To divide (segment data as required then to reassemble the segment)

- To limit the network traffic to that which can be handled effectively (congestion control)

## X.25 Interface

X.25 is a WAN interface ITU-T standard. It is a legacy system which is being phased out however it is still in use in some places, It is connected to public packet-switching network; with physical, data link and network layer from the OSI reference model. It uses an element of IP addresses and was last used in the WAN in 2015 by financial card companies. These companies have now upgraded to newer specifications. X.25 is still used by the aviation industry.

## Frame Relay (an alternative to X.25)

This is a connection oriented public switched service provided by the telecommunications company. It works at layer 2 defined by the ITU-T and ANSI in 1984.

Frame Relay is more ideal for modern day applications (streaming, VOIP) and it is needed for applications such as graphics and image transfers, especially for LAN-to-LAN communications in which high throughput is required.

Frame relay provides higher throughput by means of: larger frame size (1500+ bytes); higher interface data rates; reduced processing requirements.

Frame relay is a variation of High-Level Data Link Control (HDLC). It detects and discards frames with error, it doesn't retransmit them. With frame relay you would need to run another protocol, for example TCP.

Frame relay builds on highly reliable fibre-optic infrastructure. It is a good alternative to T and E carriers.

### Levels of Traffic

Frame relay supports two levels of traffic. Committed Information Rate (CIR), traffic up to this rate will be accepted and Excess Information Rate (EIR), where traffic between the CIR and EIR may be accepted however is marked as being 'eligible for discard' with a reduction in cost. Frame relay traffic conveys congestion information, frame relay users are expected to exert flow control.

Ultimately, frame relay is just sending packets which are usable at the other end, discarding unusable packets.

### Advantages of Frame Relay

It is a stable protocol, and is an international standard.

It is available in many (but not all) countries and all vendors offer this protocol.

It takes advantage of modern fibre-optic infrastructure, makes use of LAN-to-LAN support, minimising congestion and corrupt packets. It has the same throughput capabilities of T and E carriers and is less expensive than a fully meshed T1/E1 for bursty traffic.

### Disadvantages of Frame Relay

There is little support for Switched Virtual Circuits. It does not provide improvised fault tolerance, it requires other protocols to manage errors. It is not suitable for sending delay sensitive data, such as: real time, time voice or video, or teleconferencing. This is due to the fault tolerance not due to its speed, where it is good enough.

It involves some data overhead and processes this overhead with every packet.

It is more expensive compared to the internet service.



Issue	X.25	Frame Relay
Development Date	Mid 70s - early 80s	Late 80s - mid 90s
Underlying infrastructure	Low data rate, error prone, copper data circuits	High-speed, highly reliable fibre-optic links
Original design considerations	Support terminal to host	Support LAN to LAN
Design approach	3 layers (network, data link and physical)	2 layers (data link and physical)
Typical physical link rate	9600 bit/s to 64 kbit/s	Fractional or full T1/E1 Fibre cable
Error recovery	Error detection and transmission (at the data link) layer	Error detection with discard. No recovery (need TCP for this)
Maximum packet/frame size	Varies from 128 bytes (octet) to 4096+	Full ethernet frame 1500 bytes
Amount of processing per frame/ packet	Two dozen basic processing steps per packet (network and data link)	Half-dozen processing steps frame (only data link)
Availability	Worldwide	Only in countries with fibre-optic infrastructure
Conclusions	Good for terminal-to-host, but not for LAN-to-LAN, used for credit card verification	Good for LAN-to-LAN, as well as credit card verification
Application of this technology	For limited applications and countries where frame relay is not available	Good alternative to dedicated T1/E1 mesh

## Page 15

# LECTURE: Wide Area Networks II

📅 2023-01-31

🕒 09:00

👤 Amanda

📍 Zoom

## Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a telecommunications standard defined by ANSI and ITU-T which operates at the data-link layer. It is used within Wide Area Networks (WANs), never seen in LANs and supports the transfer of data within a range of guarantees for quality of service. It is a core protocol used in the SONET/SDH backbone where it utilises fibre optic protocols.

ATM provides integrated voice, video and data transmissions, all at high data rates. ATM was developed to move on from just transferring text from one device to another.

## ATM as a Form of Cell Relay

Data to be transmitted using ATM is segmented into 53-octet cells. These 53-octets comprise of 48-octets for transmission and 5-octet headers. If the data to be transmitted is not 48-octets in length, the data will be padded out to fill 48-octets.

The cells are then relayed across the network and reassembled at the destination. There is an unpredictable amount of time between the arrival of the individual cells, as ATM works in connectionless environments.

ATM cells get multiplexed with other cells during transmission.

## ATM Architecture

ATM has a layered architecture. Each different usage of ATM has its own ATM Adaptation Layer (AAL), these break down as follows. Layer 1 is for voice and video (where there is a constant bit rate); layer 2 is for compressed voice and video (where there is a variable bit rate); layers 3 and 4 are for general user data; and layer 5 is for TCP/IP etc. Layers 3, 4 and 5 have an unspecified bit rate.

## Traffic Engineering or Quality of Service

Quality of Service (QoS) can be configured at each ATM interface. This allows us to set a Constant Bit Rate (CBR) which has a Peak Cell Rate (PCR) that can be sustained for a maximum interval before being problematic.

Alternatively, a Variable Bit Rate (VBR) can be used which has a Sustainable Cell Rate (SCR) that can peak at a certain level.

The Available Bit Rate (ABR) specifies a minimum guaranteed bit-rate.

The Unspecific Bit Rate (UBR) will allocate traffic to all remaining transmission capacity.

## Uses of ATM

ATM technology is generally not brought out to the desktop or other "edge" parts of the network as it is not cost effective. ATM resides in the high-speed core portion of the network; supporting voice, compressed video; and data transmission. A major feature of ATM is its built-in QoS.

## Advantages of ATM

ATM meets international an industry standards and it operates over most current high-speed WAN circuits. It directly supports QoS for multimedia transmission needs. It is cost competitive within the core of the network.

## Disadvantages of ATM

There is a complex operation and configuration which must be undertaken before it can be used. It is somewhat inefficient (as it has a 'cell tax' - cells *must* be 53-octet in size). ATM is not currently cost competitive at the 'edges' of the network.

## Design Choices

ATM was designed to provide virtual circuit services across highly reliable media, with no error checks and re-transmissions of the data. It optimises the connectionless generality of IP.

## Transparent LAN Services

The *transparent* in Transparent LAN Services (TLS) means you don't see or have to deal with it. This means you don't have to deal with the WAN or provision for frame relay, ATM, leased lines etc. With TLS, a carrier bridges between your geographically separated LAN segments. This makes them all appear to be one big LAN and decreasing subscriber WAN management burdens.

Carrier bridges are often ATM Circuits, which is a good example of the heavy reliance on ATM by carriers.

Ethernet access to carrier's ATM networks is called "Metro Ethernet" or "Ethernet Transport" and it is available in all Ethernet data rates.

## Overview of Wired WAN Technologies

PPP: Point-to-Point Protocol

MPLS: Multiprotocol Label Switching

Functions at OSI layer 1	Functions at OSI layer 2	Primary Media
Dial-up over PSTN	PPP	Copper
ISDN	PPP or Frame Relay	Copper
DSL	PPP, Ethernet or ATM	Copper or Fibre Optic
Cable Broadband	Cable broadband, Ethernet	Copper and fibre Optic
T/E-Carrier	PPP, Frame Relay or ATM	Copper or Fibre Optic
SONET/ SDH	PPP, Frame Relay, ATM, MPLS	Fibre Optic

Overview of wired WAN technology

## Page 16

# LECTURE: Interconnection Protocols

📅 2023-02-07

🕒 09:00

👤 Amanda

📍 Zoom

## Voice Over Internet Protocol

*Voice over Internet Protocol* (VoIP) was originally created to reduce the need to pay to send to email. However this raises the question, why pay for digitalised voice traffic?

VoIP is commonplace now and will be found in many businesses, the University, for example uses VoIP in place of traditional phones in many locations.

The current motivation behind using VoIP is: to reduce the cost; only need to maintain a single piece of infrastructure (the network, rather than a computer network and telecommunications network); to gain extended capabilities; avoid excess delivery delay; and provide a good QoS. However there are a number of downsides: the quality of the connection may not be great, this depends on the "gateway" between the VoIP phones and legacy telephone networks; and wireless devices may drop connection temporarily when moving between access points.

## Session Initiation Protocol

*Session Initiation Protocol* (SIP) is an application layer protocol which provides a single infrastructure for voice, video and instant messaging communications to be transmitted through. SIP started as a way establish a connection, modify a connection and terminate a connection used for calling. SIP is a signalling protocol for real-time sessions.

There are five categories.

- User Location - real time local discovery
- User availability - is user able to communicate?
- User capability - choice of media and coding scheme
- Session setup - establishing the session
- Session Management - transferring sessions; modifying parameters

SIP is similar to HTTP in that SIP and HTTP are both request-response connections.

## The Internet and NAPs

The internet consists of a hierarchy of *Internet Service Providers* (ISPs) of various sizes

- Tier 1 - International ISPs
- Tier 2 - National ISPs
- Tier 3 - Regional ISPs
- Tier 4 - Local ISPs

*Network Access Points (NAPs)* are *Internet Exchange Points (IXPs)*. They interconnect public peering ISPs to exchange traffic and they exchange routing information using BGP-4. BGP-4 works on service level agreements to allow other companies to use their infrastructure (generally the amount the borrowing company can use is quite high and will have a cost associated if they go over their quota), the SLAs get updated quite frequently. Selective Private Peering with direct inter-ISP links. The private aspect of this may be dedicated for some businesses or for ISP use.

NAPs are layer 2 switches, which typically use ATM switching and have support for ISO-provided routers. NAPs are interconnected by high-speed backbones.

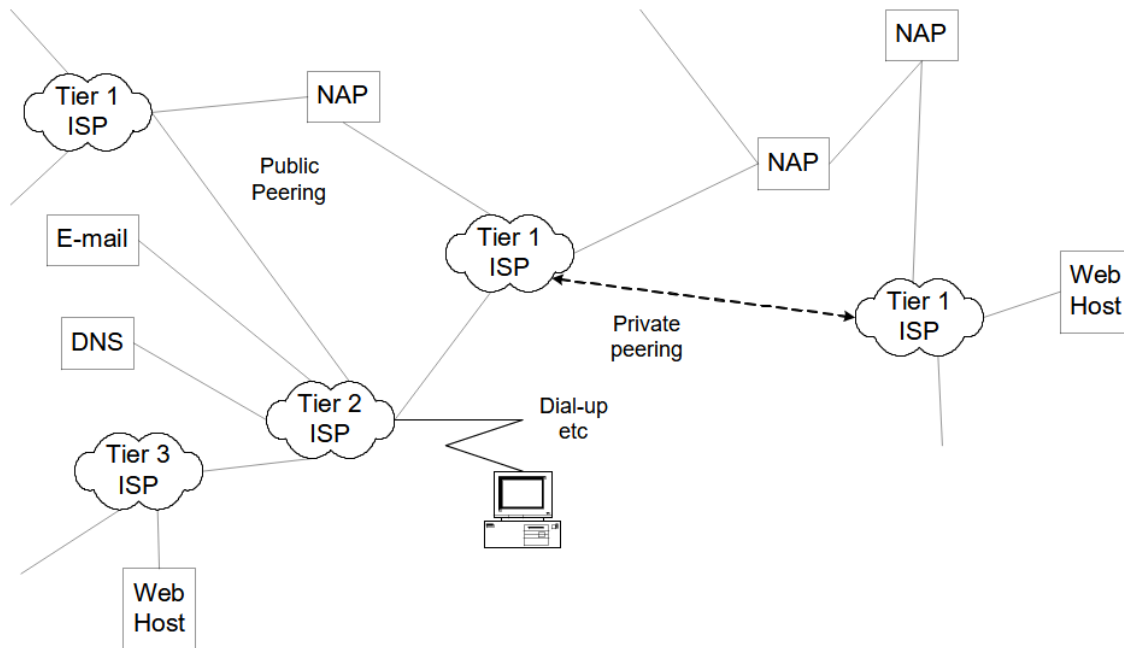


Diagram of the relationship between NAPs and the internet

## Router Capabilities

There are several different types of routers.

- Access Routers - edges of the network (this is the usual type of the domestic router)
- Enterprise Routers - Organisation network
- Core Routers - Handling heavy data flow

Routers may also have layer 2 switching capabilities and they may have hardware or software routing capabilities. Routers can either be table top or chassis based (these can contain multiple plug-in router modules).

## Modern Router Capabilities

Routers may be embedded into other multi-feature network devices, which also can include

- Wireless Access Point (WAP)
- A small (for example, 4-port) wired switch
- Firewall (usually a standalone hardware device)

## Multi Protocol Layer Switching

*Multi Protocol Layer Switching* MPLS's philosophy is "route at the edges, switch in the core". It provides the best parts of both layer 3 routing control and layer 2 switching. Layer 3 is the "multi-protocol" part of MPLS, since the switch is done at layer 2.

MPLS is intended for use in the core portion of intranets/ the internet. It is useful for carriers, ISPs and enterprise WAN networks. MPLS router in the core is called a *label-switching router* (LSR).

MPLS specifications allow many variations (options). Route the first packet when an MPLS label path doesn't exist to the destination network, as the first packet is processed at each LSR- the layer 2 switched connections is setup between those LSRs. Subsequent packets are handled by switching at layer 2 (eg ATM), swapping the label at each LSR, and label switching is also label swapping.

### A Specific MPLS Approach

Benefits of MPLS include

- Traffic engineering capabilities (explicit path other than that selected by routing)
- MPLS-based VPNs with simpler provisioning
- Service differentiation (QoS)
- Improved performance (switching instead of routing at each hop)
- Scalability

MPLS brings forward many of the benefits of connection-oriented forwarding to connectionless intranets and their routing protocols.

## QoS with IP

QoS usually refers to providing support for time-sensitive delivery, such as voice or compressed video.

Much of the work in this areas is now showing up in products, usually involving prioritisation of traffic based on the type of data being carried.

Effort includes: various forms of IP switching; differentiation services (using the IP TOS byte); multi protocol label switching MPLS

## Page 17

# LECTURE: Security

📅 2023-02-14

🕒 09:00

🎓 Amanda

📍 Zoom

### Security Attack

Any action that compromises the security of information

### Security Mechanism

A mechanism that is designed to detect, prevent, or recover from a security attack (eg antivirus software)

### Security Service

A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms

## Security Goals

We want to achieve a mix of confidentiality (transmission privacy), integrity (data hasn't been altered), and authentication (knowing who created or sent the data).

## Security Attacks

A security attack is where the data to be transmitted leaves the information source and gets altered/ stopped before it reaches the information destination.

- Interruption - this is an attack on availability
- Interception - this is an attack on confidentiality
- Modification - this is an attack on integrity
- Fabrication - this is an attack on authenticity

## Wire Taps

There are a number of different types of wire tap which can be used for ethernet cables. Fibre optic cables are more difficult to tap as they do not give off EM signals therefore they have to be spliced which is very hard to do.

- 10BASE5
- LAN
- Passive Spliced

## Security Threats

There are two different main types of security threat.

### Passive Threats

Passive attacks are eavesdropping on, or monitoring of transmissions. The goal of the attacker is to obtain the information which is being transmitted. The threat here is the release of message content and the analysis of traffic.

### Active Threats

Active threats attempt to cause harm typically through system faults or brute force attacks. They attempt to overload the victims computer to the point that it either slows to an unusable crawl, hangs or completely crashes. The threats here are that someone could masquerade as someone else, transmissions can be replayed, message content is modified and service is denied.

## Security Services

*Non-repudiation* (the order is final) provides the assurance that someone cannot deny something. Digital signatures ensure that a message has been electronically signed by the originator.

*Access Control* (prevent misuse of resources) allows different levels of access to be given to different people, it also allows people to be assigned either read or write permissions.

*Availability* (permanence, non-erasure) prevents denial of service attacks and viruses that delete files.

## Methods of Defence

- Encryption - altering the original data so only those it is intended for can read it.
- Software Controls - access limitations in a database, operating system protects each user from other users
- Hardware Controls - smart card access to data, biometrics, fingerprints, iris scans
- Policies and procedures - for example, frequent changes of passwords
- Physical controls - controlled access

## Security Vulnerabilities

Securing communications over networks have always been a dilemma. There needs to be a secure way to initiate such communication. The data needs to be protected at all times. Users need to be trusted.

Security policies are brought in to help solve the vulnerabilities, these are based on organisational requirements. They can include: prevent/ detect security violations; disaster recovery; security risk policies; and legal requirements (such as Data Protection).



## Page 18

# LECTURE: Network Security

📅 2023-02-21

🕒 09:00

🎓 Amanda

📍 Zoom

"Security isn't a happy accident"

- Amanda

## Security Problems

There are a number of areas of concerns when it comes to security.

**Remote Attacks** People try to find vulnerabilities in systems for fun, or just trying to improve their hacking skills.

**Backdoors** When software is developed, software developers can intentionally (or unintentionally) leave 'backdoors' in the software which allows access to it.

**Insecure Configuration** When servers/ systems are not configured correctly, this can expose vulnerabilities.

**Internal Attacks** These are attacks which originate from within the organisation. The perpetrator of such an attack would probably be a disgruntled employee, who knows what physical cables to pull, where to release the virus. This is a big threat within organisations.

**Access Controls** Within organisations, as employees move from role to role, they should have their access permissions updated accordingly. Not only what they can access, also the level of access (read, write, etc) should also be considered.

**Personal Devices** Within organisations, it is a security risk to allow employees to attach personal devices to work networks. USB devices are included in this.

## Security Management

There are a number of strategies which can be used to manage security risks.

**Control & Distribution** Ensure appropriate controls (eg Access Controls) are put in place to restrict users access and prevent editable copies of files from being downloaded.

**Event Logging** This is a good tool when investigating an issue with the network (both security issues and general network issues). The logs show when anything was done to the system, what time it happened, who did it and what they did.

**Monitoring** This is generally done by software now. It includes reviewing things like ports to see if any have been left open for an extended period of time.

**Parameter Management** Reviewing normal parameters and live data, to see if anything is out of the ordinary.

## Security Services

**Denial of Service Prevention** Nowadays, these attacks are more likely to be DDOS. It is hard to work out where a DDOS is coming from as it is multiple pings at the same time to bring down a server or service.

**Access Controls** Making sure that the access the users have is role based.

**User Authentication** At a basic level, this will probably just be a password. For increased security, Multi-Factor Authentication should be used.

**Data Confidentiality** How the data is kept secure, for example not allowing downloading of data.

**Accountability** This is the process of working out who has access to what systems, who is responsible for what systems and who is responsible for the 3rd party systems' security.

## Security Mechanisms

- Encryption / Decryption
- Message Authentication
- Password Policy
- Digital Signatures
- Access Controls

Security Mechanism	Confidentiality & Privacy	Integrity & Protection	Access Controls & Availability	Non-Repudiation & Accountability	Authentication
Access Control Mechanism	Y		Y		Y
Digital Signature		Y		Y	Y
Encryption Mech.	Y	Y		Y	Y
One-Way Hash (OWH)		Y			
Certification			Y	Y	Y
Password Techniques	Y	Y		Y	Y
MAC	Y	Y		Y	Y
Key Exchange/Generation	Y	Y			Y

## Secure Communication over Insecure Networks

When we communicate over insecure networks, we need to communicate in a secure way to protect the *confidentiality* and *integrity* of the data we are transmitting. Encryption can help prevent man in the middle attacks, in that if someone listens to the transmission then they will not be able to understand it.

### Approaches of Encryption

There are two different approaches to encryption, *symmetric key encryption* and *public key encryption*.

	Symmetric Key	Public Key
Encrypt and decrypt key values	The same values	Different values
Secrecy of keys	Must be kept secret	One key is kept secret (private key) and the other is made public (public key)
Confidentiality	Provided	Encryption in a public key provides confidentiality
Crypto signature	Not provided	Encryption in a private key provides a signature.

A message which has been encrypted in a private key can be ready by anyone (using the public key). There is a certain amount of trust in who you give your public key to. The fact that the cyphertext is properly formatted with a message with a reasonable content provides a digital signature by the sender.

## Secure Sockets Layer/ Transport Layer Security

Secure Socket Layer (SSL) and Transport Layer Security (TLS) operation are the basics for how security is achieved. The mechanisms are utilised whenever a web access screen indicates that you are going into secure operation.

### How SSL & TLS is used

This example uses both symmetric and private key encryption.

1. Alice contacts her brokers website and clicks 'login'.
2. The broker send s a trusted copy of its public key
3. Alice's PC generates a random (secret) working key
4. Alice's PC sends the key to the broker encrypted in its (the broker's) public key
5. Both now have the (otherwise secret) working keys and can communicate.

The encryption used may vary from 40-bits to 128-bits. The 40-bit approach is very weak; the 128-bit approach can be much stronger, however that depends on other factors as well (including how random the key generation really is). 256-bits are used for a stronger cypher.

## Trusted Certificates

Trusted certificates contain the owner's public key. They are trusted because they are cryptographically signed by a trusted agency.

## Types of Cypher

### Data Encryption Standard

Data Encryption Standard (DES) dates back to the mid-1970s. It has a 56-bit key length, which in the modern world is inadequate, and can be broken in less than 24 hours (in reality, within a few hours).

### Triple Data Encryption Standard

The Triple Data Encryption Standard has a much longer, more effective key length.

### Advanced Encryption Standard

The Advanced Encryption Standard (AES) is more recent and provides greater security (has 128-256-bit length). AES is an internationally developed algorithm (from Belgium).

## Virtual Private Network

### Virtual Private Network

A private network that uses a public network to connect remote sites or users together. It uses virtual connections.

Virtual Private Networks (VPN)s appear to be private. However they are not, the 'privacy' occurs due to the encryption, then encapsulation is in 'routable IP packets'

Outsiders may be able to intercept the packets, but they cannot: read them; modify them without detection; or impersonate expensive T1/E1 leased lines.

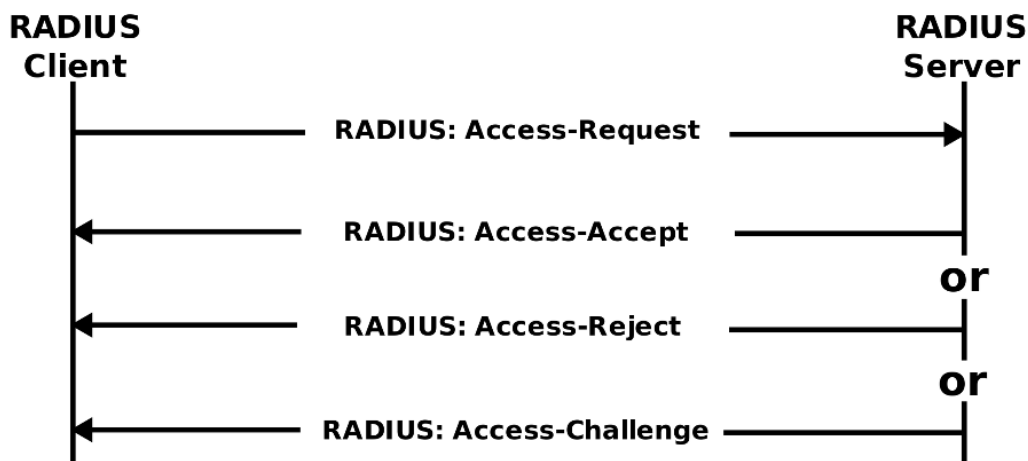
A typical use of a VPN is to replace the expensive T1/E1 lease lines. If an organisation chose to do this, removing the T1/E1 lines would require the use of the organisations intranet or internet instead.

However, replacing T1/E1 lease lines with VPN does not provide any assurances or timeliness of delivery (it gets the usual best-efforts delivery of the intranet/ internet).

## Use of Radius Protocol

Remote Authentication Dial-In User Service (RADIUS) protocol provides

- Authentication, Authorization, checking and accounting
- Uses Point-to-Point Protocol (PPP)
- Operates on port 1812
- Commonly used to facilitate roaming
- Can provide customisable login prompts



Authentication and Authorisation flow

## Internet Access

It is easy to connect to the internet - all it takes is a router. However, just using a router is not a good idea. There are real dangers in uncontrolled interconnection into the internet, this is a network manager's worst nightmare.

## Firewalls

The solution to uncontrolled connection to the internet is usually something called a 'fire-wall'.

The router we use for interconnection to the internet may include filters, which can filter out undesired traffic (for example, external TELNET or FTP request) or allow only some things in (for example e-mail).

## Router-Based Firewalls

The firewall may be a screening router. This means that the router is setup to filter connection requests, these are not considered to be very strong security measures. This is a low budget approach.

## Host-Based Firewalls

Alternatively, a host-based firewall can be used. This controls inbound and outbound internet traffic and may include an e-mail gateway, FTP server or Web server.

## Firewall Data Sheet Parameters

The firewall may be router or host based; router based filtering is less expensive however host-based is more secure.

Firewall must be configurable to support your security policy, and allows you to determine what connections you will permit and usually deny all others.

Firewall should be capable of filtering unauthorized connection attempts. There are known vulnerabilities in many approaches to this. Considerable care must be taken in configuring the firewall.

The firewall should be capable of detecting all known internet security attacks.

Firewalls may also include other network security capabilities, including: intrusion detection (known attack 'signature' and anomalies); Network Address Translation (NAT); and URL and content filtering.

## Evaluated Products

There is an internationally accepted security rating system called 'Common Criteria Evaluated Products' with an Evaluated Assurance Level (EAL) range of 1 to 7.

Many government and commercial procurements are requiring an EAL rating for security-related hardware/ software. These products include firewalls, intrusion detection, down-grade guards, etc.

**EAL 2** is the minimally accepted assurance level

**EAL 4** is the highest level obtainable for a retrofit product

**EAL 5 to 7** are extremely expensive to obtain (typically limited to government/ military applications)

## Page 19

# LECTURE: Intranet Systems Management

📅 2023-02-28

🕒 09:00

👤 Amanda

📍 Zoom

## Motivation for Network Management

Computer networks are mission-critical to organisations. Any downtime in these systems can cause big problems for organisations, as such we aim for 99.9% uptime. When systems go down, there can be *catastrophic* impacts - see current Royal Mail issues or Blackberry issues historically.

## Goals for Network Management

Network management has to be responsive. End users need to be able to report issues and which need to be able to be dealt with quickly, this may include isolating them. Often the *Help Desk* will be the first place users go to get support, this will often involve a list of pre-defined questions and they will have the ability to remote-in to troubleshoot further. The next line of support are the *Network Support Technicians*, these people will attempt remote support before attempting on-site support as this is a much more efficient use of their time.

The final line of support are the *Network Systems Management* who monitor the network (whats happening, where traffic is coming from, are there any bottlenecks, etc). They diagnose problems as they happen, control the network and attempt to resolve issues before system outages.

## Network Systems Management

Network Systems Management is software which runs on simple workstations. The software:

- monitors the network - to make sure everything is running as it should do, there are no problems, and there are no additional pings (as this can be early warning of a DDOS)
- displays the current status - often through a traffic light system
- notifies the existence of problems as they arise - this can be done through exception reports
- identifies causes - this is the most important thing to find out when something goes wrong
- supports remote diagnostics
- has intelligent network management

- supports self healing networks - which is another piece of software that sits on the network and knows about the trigger points, and can resolve issues before they become a problem. This doesn't eliminate the need for network support technicians

## TCP/ IP Network Management

Network management involves three distinct needs.

**Protocol** Reads & Writes critical network management (for example event reports).

**Database** Contains specific parameters (for example, queue length, throughput, transmission speed, delay in the system, jitter). Database produces the exception report (which can be done daily, hourly, etc depending on how mission critical the system is).

**Computer** This PC should be independent of the network so that if the network goes down then there is one PC that doesn't.

## Simple Network Management Protocol

The *Simple Network Management Protocol* (SNMP) reads & writes between managers and network devices. It provides the services too

- Read the value of the individual parameters (SNMP GET)
- Read sequences of table entries (SNMP GET\_NEXT)
- Write into parameter values (SNMP SET)
- Receive unsolicited event reports (SNMP TRAP)

These events and parameters are the *MIBs* which are documented using *SMI* notation.

## Remote MONitor

The *Remote MONitor* (RMON) protocol can do some things, including pinging machines/ checking it isn't user error and removes the need for network technicians to travel on-to site.. SNMP MIBs include some remote monitoring capabilities. RMON is implemented as an independent probe device (software) attached to each LAN segment and can be integrated into networking devices, however this has a performance impact.

RMON is available in two different forms: RMON 1 monitors OSI layer 1 and 2 including collision statistics and error statistics; RMON 2 includes monitoring of higher levels, including hosts and what application causes the most traffic etc. It can be cost effective to deploy as it can help control traffic throughput. RMON can increase the effectiveness of network management protocols as it can identify where the problems are for troubleshooting, and deal with a large amount of what the helpdesk deals with.

## Network Management Areas

OSI identifies five areas of network management.



## Configuration Management

This includes a wide range of issues, including address and name assignment of network devices (subnet, public/ private IP); hardware/ software updates to switches and routers (some OS can be updated easily, some are legacy systems which can't be upgraded easily); software license control (which is a legal requirement, some organisations have been taken to court over using illegal software); and setting up parameters (configuring switches and routers to filter out certain types of traffic, multi protocol routers can be configured to run selected protocols, configuration of bit rate etc).

## Fault Management

Fault Management provides identification and isolation of faults detected. Tools and techniques used include

- Bit-Error Rate Test (BERT) - how much data goes through the network
- Time Domain Reflector (TDR) - time it takes for data to go through the network
- Optical TDR (OTDR)
- Protocol analyser - for data links and LANs, used for troubleshooting all protocol layers - looks at protocols and bottlenecking
- Loopback tests - when a packet doesn't make it to its destination and is sent back to the sender, this causes more network traffic and should be eliminated
- Ping - allows you to see if different devices are 'up' or on the network, this can be the first troubleshooting step
- Artificial Traffic Generation - can test how robust the network is and should only be done out of hours or on an isolate parts of the network as generally tests are run until the network crashes.

## Fault Isolation

Limiting faults is possible by isolating the fault using switches and router configuration. All traffic across the LAN can be monitored, as well as all exception conditions (collisions, lost token etc) can be detected. Devices called *LAN analysers* (or LAN protocol analysers) can be attached to the network, which selectively record information about the packets of interest or may be setup to filter based on address, protocol or other fields of interest.

## Performance Management

A slow network results in money lots, customers lost and man hours lots. Performance management is concerned with statistical data (round trip delays and throughput of data), may require prioritisation of certain traffic (including other quality of service capabilities), tuning of performance (eliminating bottlenecks by adjusting buffer size or setting timer values) and can establish a baseline (which is the adequate minimum system performance required). Performance management is also concerned with finding bottlenecks, which commonly are: wide area links between remote switches and routers, access to server resources for example data storage, and parts of the network that are nearing overload.

Many fault-management tools are useful in performance management.

## Accounting Management

This can be billing for network usage.

Network managements generally will spend their time doing accounting unless there is a fault. Parameters include

- Number of connections made
- Duration of each connection - is the current Service Level Agreement enough, do we need more capacity
- Number of email messages sent & received - are they all necessary, do we need a new procedure to reduce the number of emails
- Number of packets sent and received - is there too much transmission on one part of the network?
- Systems that are accessed across the network - including cloud storage, is there sufficient capacity within these services, do we need to change it
- Internet usage - is the internet being abused, do we need misuse protocols?
- Server usage - probably will be cloud based rather than on-prem, have we got enough internet capacity to access these?
- Data storage - have we got enough space, are we storing data because we need it or are we storing data because its data.

## Security Management

Security Management includes: confidentiality, integrity, authentication, access control, nonrepudiation.

Vulnerabilities can include: wire-taps placed on cables, outsiders intercepting remote login attempts from across the network (can be done through a delay), introduction of a virus.

Security protection mechanisms include: encryption, physical protection, access-control lists, and audit data collection.

## Page 20

# LECTURE: Application Support Protocols

📅 2023-03-14

🕒 09:00

👤 Amanda

📍 Zoom

*NB: This lecture was cut short due to Amanda needing to get to the other side of the Uni for a meeting. To be continued in next weeks lecture*

## 20.1 UDP or TCP

### 20.1.1 User Datagram Protocol

User Datagram Protocol (UDP) is jokingly known as *Unreliable Datagram Protocol*. This is due to the fact that there is no guarantee of delivery of the packets. UDP will treat packets a bit like a hot potato, in that it passes it onto the next node without performing any checks on the contents of the packet. This can result in undetected corruption of data (which could manifest as pixelation of media or drop in quality of streamed content etc). UDP passes the packet down to the IP layer and sends it onto the next node, with a slight modification. It doesn't care if the next node doesn't exist or if it does exist but isn't running the service request, the packet will still be sent. UDP will not request packets to be re-transmitted if they get lost and it will discard packets if they arrive late.

### 20.1.2 Transmission Control Protocol

Transmission Control Protocol (TCP) provides reliable data communication. TCP performs integrity checking, retransmission of lost data, reordering of lost packets, etc. This means when the application receives the data, it is all correct, in the right order and not corrupt. TCP is connection oriented, which means before transmission can begin a connection must first be established which is generally done using a three-way handshake. TCP uses this connection to not only receive the data but also to notify the sender of every packet received and its status (good, corrupt, missing, etc). This allows the sender to know if re-transmission is required or not.

If TCP receives a later packet before an earlier packet, it waits to have them in the right order before passing them up the layers. TCP uses virtual channels.

### 20.1.3 When To Use Which?

UDP is the best to use for voice/ video applications as it has low delay (the only delay is the time it takes for the packets to cross the network, no delay is injected from error checking etc). TCP would re-transmit lost data which causes delay, despite a better QoS being achieved, there would be lots of delay for the end user.

For the majority of other transmissions (transferring files, web pages, MSN, etc) TCP is the better to use as it has a higher QoS.

## 20.2 Multiplexing in TCP/ UDP

Each packet is tagged with a different data type. This allows a PC to determine between web traffic and video conference data.

### 20.2.1 Ports

Every computer has 65535 ports and each TCP or UDP packet stores the port we're using as part of its headers. Applications have ports assigned to them (for example port 80 is assigned to HTTP, port 21 assigned to FTP etc). Ports work a bit like virtual channels, in that traffic on one port is independent of traffic on another port - there is no interference between them.

As packets come into the PC the transport layer will inspect each packet and determine which port the packet needs to enter the computer on.

## 20.3 Layer 6: Presentation

The presentation layer is concerned with interpreting data before the application gets it. It uses a number of techniques to achieve this.

### 20.3.1 Data Abstraction

This is concerned with taking the raw data (0s and 1s) that come into the machine and interpreting it. For example, decoding binary to ASCII characters.

Data abstraction also converts between character sets, which can be defined in application protocols.

### 20.3.2 Secure Socket Layer

#### Socket

An abstraction, a means of making connections. Opens a socket to a remote host or open a socket to listen on a local port

Secure Socket Layer (SSL) encrypts data between two ends. It provides the same abstraction and can mostly slot in-between traditional sockets and the application. SSL doesn't have its own transmission medium, it uses the same as non-SSL packets.

If a SSL packet is "picked up" then it cannot be interrogated without the encryption key. It is used anytime we want to send anything secure over the internet or outside our network and offers encryption and digital signatures (provides confidentiality of who we are sending to).

## 20.4 Application Layer

### 20.4.1 Client-Server Model

The clients take inputs from the users and send instructions to the server. The server processes the requests and produces data to send back to the client.

### 20.4.2 Peer to Peer

Peers have information which they are willing to share with other peers and private information which they do not want to share. This makes the peers both clients and servers.

## 20.5 Domain Name Systems

DNS is a directory of all IP addresses.

Port 53 is used by UDP for queries and TCP for transfers.

There are several types of records in a DNS

- A - maps `www` to an IP address
- MX - IP address of a mail server
- PTR - reverse lookups
- Lots more.