Unit 10, Assignment 1 – From End to End

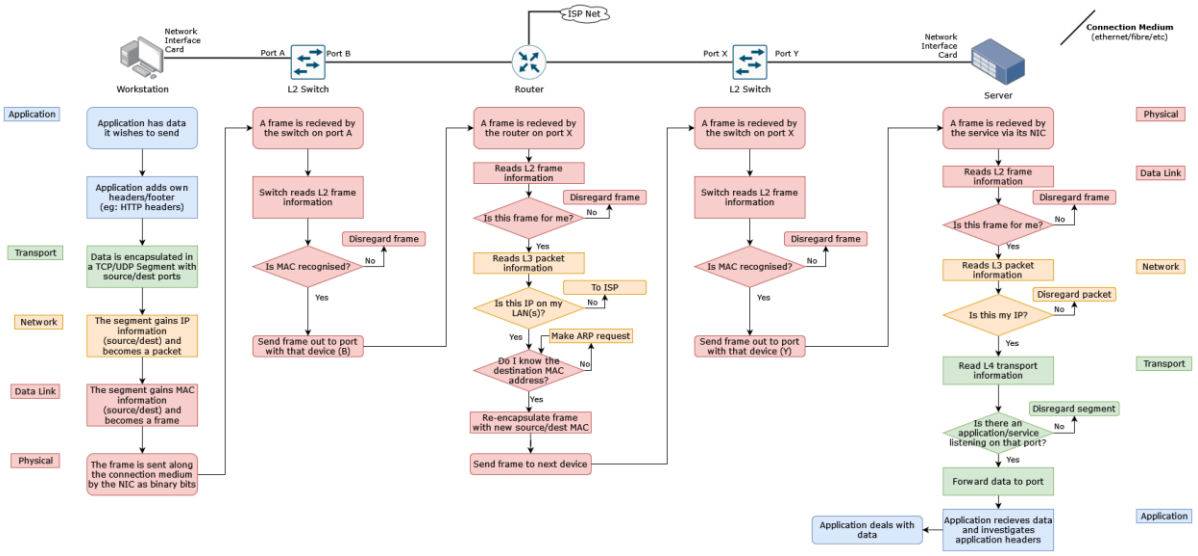
Thomas Robinson

SOLIHULL COLLEGE

Thomas Robinson

Task One (P1)

Diagram & Flowchart



U10A1 Task 1 Flowchart.drawio.png

Written

End Device Sends:

1. Application has data it wishes to send (Application Layer/7)
2. Data is encapsulated into a TCP or UDP **segment** with source/dest ports (Transport Layer/4)
3. The data is further encapsulated into an **IP Packet** with source/dest IP addresses (Network Layer/3)
4. The packet is encapsulated into a **frame** with source/dest MAC addresses (Data Link Layer/2)
   If the data is being sent outside of the network, the MAC address of the default gateway will be used as the destination here
5. The frame can now be sent over the connection medium

Switch Receives:

1. The switch receives the data on port X.
2. The switch reads the layer 2 frame information
3. The switch recognises the MAC address and sends the data onwards out of port Y where the device is.
4. If the MAC address is not recognised, the frame is dropped.

Router Receives:

1. Router checks the frame is for it (is this MAC address me?)

2. Router de-encapsulates the frame and reads the IP information
3. If the IP is on the local network, the router makes an ARP request for the MAC address of the destination device
4. The router re-encapsulates the IP packet into a frame with a new source/destination MAC address
5. The router sends the data to the switch

Switch Receives:

1. The switch receives the data on port X.
2. The switch reads the layer 2 frame information
3. The switch recognises the MAC address and sends the data onwards out of port Y where the device is.
4. If the MAC address is not recognised, the frame is dropped.

End Device Receives:

1. The device receives the frame
   If the MAC address is not that of the device, the frame is dropped
2. The device de-encapsulates the frame to read the IP information
   If the IP destination is not that of the device, the packet is dropped
3. The device further de-encapsulates the IP packet information to read the transport information
   If there is an application listening on the destination port, the device will forward the application data onto it

Task Two (P2, M1)

Standards

Wi-Fi (802.11)

Wi-Fi is a standard set of protocols for communicating data wirelessly using radio waves.

WPA & WPA2

Wi-Fi Protected Access 1, 2 and 3 are used to secure access to a Wi-Fi network through the use of TKIM (WPA) or AES (WPA2,3) encryption and a passphrase, RADIUS authentication server or WPS PIN.

2G, 3G, 4G, 5G

Are standard protocols for mobile telecommunications, used by cellular mobile devices, such as phones, tablets and laptops. Each new generation offers increased bandwidth and capacity.

IrDA

The **IrDA** is the Infrared Data Association who are a consortium that create and maintain standards for use with infrared data networking. Primarily, they authored the IrDA Control and IrDA Data standards for use in this area.

WAP

Wireless Application Protocol is a standard for information access using mobile networks. The protocol suite covered everything from the browser environment to the wireless datagram protocol. WAP pages (written in WML) were a simpler alternative to HTML-based webpages that were specifically designed for small, low-resolution and low-colour feature phone displays.

Ethernet

Ethernet is collection of standards for wired networking technologies, including data transfer specifications, cable specifications and connector specifications.

Protocols

TCP/IP

The **Transmission Control Protocol/Internet Protocol** stack is a collection of protocols that govern how data should be split into packets, routed, sent and received.

DNS

The **Domain Name System** is a way of associating IP addresses with human-readable names. In the context of the internet, a DNS server acts like a phonebook: translating a domain name (solihull.ac.uk) to an IP address (78.109.173.187). DNS servers use port 53.

DHCP

The **Dynamic Host Configuration Protocol** is a method of assigning information and configuration to devices on a network. Most commonly, it is used to assign IP addresses on a LAN or WAN. DHCP servers make use of port 67 which communicates with port 68 of a client.

HTTP

Hypertext Transfer Protocol is designed for transmitting 'hypermedia' (websites and associated data/documents), though it can be used for other purposes. Port 80 is used for plaintext traffic and the secure variant (HTTPS) uses port 443 for encrypted communications.

FTP

File Transfer Protocol was introduced in 1971 used for—as the name implies—transferring files between a server and a client. It issues textual commands to a server to manipulate files. Port 21 is used for issuing commands and control and port 20 is used for data transfer.

SMTP

Introduced in 1981, the **Simple Mail Transfer Protocol** is a standard for sending and receiving email (though it is often only used for sending). Standard ports include 25 for unencrypted communication and 587 for encrypted.

TCP/IP	OSI	Protocols
Application	Application	DNS, FTP, SSH, SMTP, HTTP, DHCP
	Presentation	AFP, NCP, X.25
	Session	NetBIOS, PPTP, SOCKS
Transport	Transport	TCP, UDP
Internet	Network	IPv4, IPv6, IPsec, ICMP/IGMP
Link	Data Link	ARP, CDP, MPLS, Ethernet, Wi-Fi
	Physical	OTN, IRDA, DSL, ISDN, Bluetooth, IrDA Physical Ethernet Physical Layer, Wi-Fi Physical Layer

Why are standards important? (M1)

Standards and protocols are important since they dictate how computers, servers and applications can talk to each other and work together. Without a set of common standards, interoperability between devices would be near-impossible since nothing would be able to communicate without being able to speak every possible 'language'.

Task Three (D1) – OSI & TCP/IP

The OSI and TCP/IP are both models that abstract the technologies and protocols used for transferring data and information across a network or group of networks.

The OSI model was created in the late-1970s by the Open Systems Interconnection group at the ISO. In contrast, the Internet Protocol Suite (as it is officially known) was devised in the mid-1970s by the Defense Advanced Research Projects Agency at the US DoD. Henceforth the IP Suite will be referred to by its more common—though technically incorrect—designation: the "TCP/IP model."

The primary difference between the two models is the number of layers and their purposes. The OSI model is split into seven layers: Physical, Data Link, Network, Transport, Session, Presentation and Application, with the former three being "Media Layers" that take place independent of a host device. The TCP/IP model—in comparison—is simpler, traditionally containing only four separate layers: Application, Transport, Internet and Link. The TCP/IP model provides descriptions of scopes that are used by the Internet, rather than prescriptions that can be used across all networks.

Application

In both the TCP/IP stack and the OSI model, the topmost layer is the Application Layer. This is the layer in which an application (or 'process') wishes to send data, for example, a web browser wishing to make a web request.

Both models employ the concept of data encapsulation, with the original piece of data being appended and/or prepended with additional information at each subsequent layer. In the Application Layer, the data that wishes to be sent is encapsulated by application-specific headers and/or footers. In the example of a web request, these are HTTP headers.

Other protocols that sit at the Application Layer include: SMTP and IMAP—for sending and receiving emails, respectively; DNS for hostname lookups; FTP, SFTP and SMB for file transfer; Telnet and SSH for remote shell connections, among many others—both proprietary and open in nature.

OSI's further abstraction

In the OSI model, there are several layers underneath the Application Layer that do not exist in the TCP/IP model. These are the Presentation

Layer and the Session Layer. These two layers are considered a part of the Application Layer in the TCP/IP model.

The Presentation Layer is responsible for ensuring that the data is interoperable and can be read by both the sending device and the receiving device. The sending device is responsible for converting the data to a standard format and the receiving device is responsible for converting the data back, ready to be read by the application. An example of a technology at the Presentation Layer is MIME, which is used to enable emails to embed multimedia content and non-ASCII text.

Below the Presentation Layer in the OSI model is the Session Layer. This is responsible for managing sessions between applications and their creation and termination. Protocols at this layer include NetBIOS, PPTP, RPC and SOCKS. A connection from process-to-process made in this way is known as a socket, even if the processes are not on the same end device.

Transport

The transport layer exists in both the TCP/IP and the OSI model. Protocols at this layer are responsible for delivering data to the correct process on a host device. The two most popular transport protocols—TCP and UDP—both use "ports" for this purpose. An application can open a port (or multiple) to send and receive data on, similar to a letterbox on a house. In the TCP/IP stack, only TCP and UDP are used.

At this layer, the data is further encapsulated into a "segment." In the case of TCP or UDP, the headers appended will contain source and destination port information.

Internet/Network

At the Internet Layer, the data leaves the host device and is first received in a network. In the OSI model, it is referred to as the "Network" layer, whereas the TCP/IP stack uses the term "Internet." It is at this layer where IP addressing is used, and a transport-layer "segment" is encapsulated into a "packet" that will contain a source and destination address. The TCP/IP stack enforces the use of IP addresses, whereas the OSI model does not dictate the use of any specific protocol or standard.

This layers' purpose is to route traffic between intermediate routers to ensure it arrives at the correct network. Protocols used at this layer include: IPv4 and IPv6 for IP addressing; ICMP and IGMP for sending diagnostic ping requests and ARP for translating an IP address into the devices' MAC address.

Other than routers, modems also sit at this layer.

Since the TCP/IP model refers only to the protocols used by the Internet, the definitions as to what protocols fall into this category differ between the two models.

Data Link & Physical

The bottommost layers in both models, TCP/IP groups these two layers together into a single “link” layer.

At these layers, the connection between devices in a single network is concerned. Devices have their own individual MAC address which identifies them and facilitates the switching of frames to the correct device. An IP packet is encapsulated with a source and destination MAC (physical) address which is read by a switch and then sent on.

Switches and bridges sit at layer 2.

The Physical Layer refers to devices that have no “smarts”, including cabling and hubs.

Conclusion

Both the TCP/IP stack and the OSI model are capable of illustrating the fundamentals of data encapsulation and the various stages data takes in a network. The TCP/IP stack, being more simplified, is not as capable at demonstrating every step.

Task Four (P3) – DTE & DCE

DTE (Data Terminal Equipment)

A DTE device is a source or destination of binary data within a network. It includes routers, switches and end devices that generates or consumes data.

DCE (Data Circuit Terminating Equipment)

A DCE device is usually responsible for bridging a LAN and WAN and converting from one format to another. An example is a modem that converts the binary signal into audio to be sent down an analogue phone line. A DCE device is responsible for creating a clock signal to facilitate this.

A device that works at layer 3 of the OSI model and can communicate between networks using IP addresses.

DTE - Router

A layer 1 device that broadcasts all signals it receives.

DCE - Hub

An end user device that can be connected to a network wired or wirelessly and can be carried around.

DTE - Laptop

A handheld device that is used for voice and data using 4G, 5G and wireless networks.

DTE – Mobile Phone

A network device that converts digital signals to analogue and back.

DCE - Modem

An end user device that can be connected to a network and usually sits on a desk.

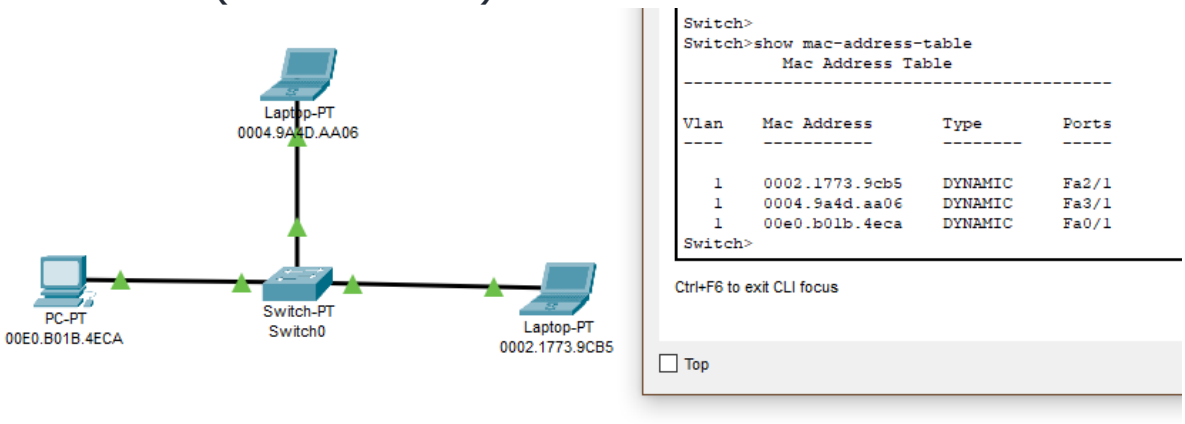
DTE – Desktop Computer

A component that allows a device to connect to a network through a WAP.

DCE – Wireless NIC

Task Five (P4) – Data Elements

Addresses (MAC and IP)

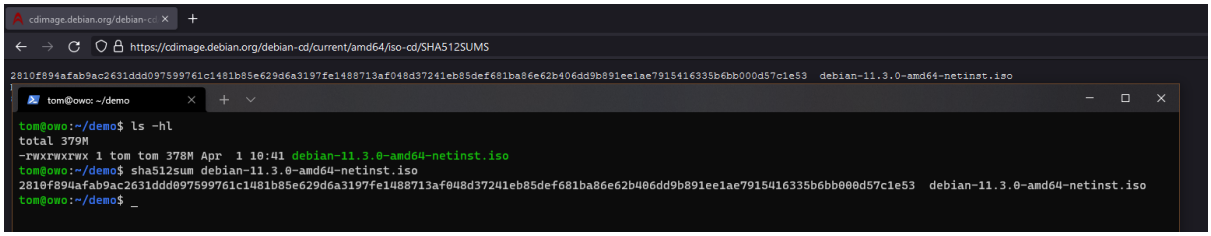


MAC Addresses are used to identify devices at Layer 2 of the OSI model. This facilitates communication within a LAN.

IP Addresses are used to identify devices at Layer 3 of the OSI model. This facilitates communication between multiple networks.

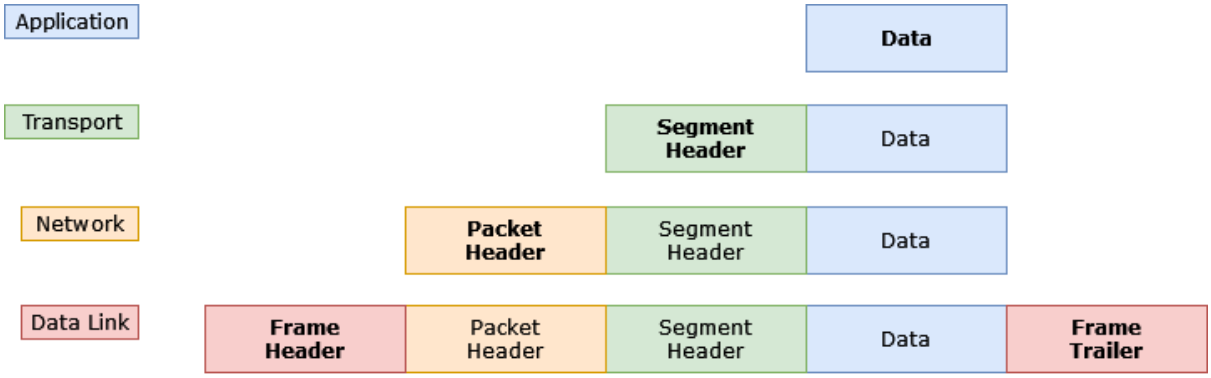
Both forms of address are important to ensure that data arrives at the correct device.

Checksum



A checksum is a way of representing a set of data in a uniform number of characters. Changing a single part of the data will completely change its checksum They are used to ensure data integrity and to check whether two files are different without checking all of the data.

Encapsulation



Encapsulation is the process of enclosing data in a new format with additional information appended and/or prepended to it. It is a key concept of the TCP/IP and OSI models.

Sequence Numbers

Are used to ensure data is read in the correct order in case it is received in a different number. They are used to keep track of each byte sent by a device. Each packet, the sequence number increases by the number of bytes of the packet. So if one packet is 1250 bytes in length, the sequence number is increased by 1250.