

EVAN Richards (223686)

 PRIFYSGOL CYMRU Y Drindod Dewi Sant UNIVERSITY OF WALES Trinity Saint David	LLEOLIAD - COLEG SIR GAR, LLANELLI
LOCATION - COLEG SIR GAR, LLANELLI	
LEVEL 4	LEVEL 4
EXAMINATION PERIOD MAY 2022	CYFNOD ARHOLIADAU MAY 2022

MODULE CODE: ACCA4024
NETWORKING & CYBER SECURITY ESSENTIALS

TIME: 2 HOURS

ANSWER ALL QUESTIONS

Equipment or materials required – None

The Candidates are not permitted to bring calculators, dictionaries; text books/case studies or any other reference materials into the exam room.

Show all your calculations in your final answers

ANSWER ALL FOUR QUESTIONS

QUESTION ONE

Attempt all of the following. Electronic Calculators are not permitted. Write down and show all your manual calculations in your exam book.

i) A consumer places his debit card close to a pay terminal at a shop and the shopping charge is successfully paid. Which type of wireless technology was used? (3 marks each)

- A. Bluetooth,
- B. RFID
- C. Wi-Fi
- D. 3G

Answer: B

✓ (3)

ii) The layer which describes how a device accesses and sends data over the network media in the TCP/IP model? (3 marks each)

- A. application
- B. internet
- C. transport
- D. network

Answer: D

✓ (3)

iii) What is the maximum size of a valid Ethernet frame? (3 marks each)

- A. 1522 bytes
- B. 1518 bytes
- C. 1400 bytes
- D. 2048 bytes

Answer: A

X

iv) A network design engineer has been asked to design the IP addressing scheme for a customer network which requires 255 hosts. The network design engineer decides to use IP addresses from the 192.168.10.0/24 network. Will this IP addressing scheme accommodate all the hosts in the customer network? (3 marks each)

- A. No, the network is not having required usable hosts
- B. Yes, the network is having the required usable hosts

Answer: B

v) DHCP is used to automatically assign IP address to hosts. (3 marks each)

- A. True
- B. False

Answer: A

vii) Private IP addresses are designed to be exclusively used for external networks and they can be used on the Internet (2 marks)

- A. True
- B. False

Answer: B

viii) The URL identifies the MAC address of the web server (3 marks)

- A. True
- B. False

Answer: B

ix) Hypertext Transfer Protocol is used by web servers to serve up a web page (2 marks)

- A. True
- B. False

Answer: A

x) Streaming audio and video applications require receipt of all packets regardless of delay. (3 marks)

- A. True

B. False

Answer: B

✓ (3)
Q1 - 21.

(25 marks total)

QUESTION TWO

You have a job interview for an advertised role of Network Support Technician in Coleg Sir Gar as part of the Interview process the IT manager has asked you to explain the OSI & TCP/IP models. He wants you to include the following information in your explanation.

- Purpose of the OSI & TCP networking models
- Give a definition and explain the purpose of the 7 layers of the OSI network model
- Give a definition and explain the purpose of the 5 layers of the TCP/IP network model
- Explain the differences between the OSI & TCP/IP models

Purpose of OSI and TCP/IP Networking models

The OSI model is a theoretical model that assists network engineers when trouble shooting. Then a fault is being diagnosed, a technician may refer to the issue as a "Layer 6" issue, which refers the Presentation layer of the OSI model. The OSI model is used as it includes 7 Layers, this breaks the encapsulation process down further than what the TCP/IP model does, hence why we use the OSI to diagnose faults.

The TCP/IP model, on the other hand, is not theoretical. This is the most accurate representation to demonstrate how data is encapsulated (sent) and decapsulated (received). The main difference between the OSI and TCP/IP models is the number of layers. In the TCP/IP model, the Application, Presentation and Session layer are all included within the Application layer.

OSI and TCP/IP Models –

OSI Model		TCP/IP Model	
Layer 7	Application	Layer 5	Application
Layer 6	Presentation	Layer 4	Transport
Layer 5	Session	Layer 3	Network
Layer 4	Transport	Layer 2	Data Link
Layer 3	Network	Layer 1	Physical
Layer 2	Data Link		
Layer 1	Physical		

Application Layer (OSI Model)

The application layer of the OSI Model only reverse to where the user interacts with the application, this layer is what produces the data that we would like to send over the network. Protocols that work at this layer may include: Telnet, SSH, FTP, HTTP and so on.

Presentation Layer (OSI Model)

This layer formats the data that was produced by the application layer. This is formatted so that the receiving application is able to process and interpret the data.

Session Layer (OSI Model)

Here, a session is initiated and terminated between a source and destination. This layer essentially controls the session between the communicating devices.

Application Layer (TCP/IP Model)

The application later of the TCP/IP Model differs from the OSI. This layer is a combination of the Application, Presentation and Session Layers of the OSI Model. The reasoning for this is that most modern computer programs are designed to: 1) Produce and format the data to be sent, and 2) manage sessions (which are sometimes encrypted) between the source and destination hosts.

Transport Layer

This layer is responsible for how the data is sent over the network. Here, the data is broken down and given a header. This header can relate to either the TCP or UDP transfer protocol. TCP initiates a stable connection using a three-way hand shake (syn, syn-ack, and ack). The data is then given a header that includes an abundance of information relating to error correction. The receiver also sends acknowledgements after each packet. TCP is a great protocol for loading web pages, or file transfer. On the other hand, the Transport Layer could add a UDP header. This does not include error correction, however, similar to TCP it does include sequence numbers; So, the data can be correctly assembled on the receiving end.

The Transport Layer is also responsible for adding the source and destination port numbers. Once the Transport Layer has encapsulated the data, it becomes a segment.

Network Layer

The Network Layer is responsible for adding the source and destination IP Addresses. Once the Network Layer has encapsulated the segment, it becomes a packet.

Data Link Layer

The Data Link Layer is responsible for two things. Firstly, the source and destination MAC Addresses are added to the packet as a header. Secondly, a trailer is added to include error correction, such as a Parity Check. Once this layer has added the header and trailer, it becomes a frame. This can be seen in the diagram below.

Ethernet – Source and Destination MAC Addresses
Source and Destination IP Addresses

TCP/UDP Header & Source and Destination Port Numbers
Data
Ethernet - Error Correction

Physical Layer

The Physical Layer is where data is electronically transmitted over cables and other networking hardware.

The Difference between the OSI and TCP/IP

As mentioned previously, the OSI model is purely theoretical as it's only used to diagnose networking faults. The OSI model is a more detailed representation of how data is encapsulated and decapsulated. The TCP/IP model on the other hand is a more realistic representation. As I mentioned before, modern programmes process the data as per the Application, presentation and session layers of the OSI Model. This sometimes makes application, presentation and session layer faults harder to solve, as they're imbedded in the programme.

(25 marks total)

QUESTION THREE

Q2 - 21 marks

You were successfully in getting the Network Support Technician role in Coleg Sir Gar and the IT manager wants you to explain the purpose of IP addresses & Mac Addresses to the new IT apprentice. He wants you to include the following information in your explanation.

- Give a definition and purpose of IP addresses
- What OSI layer is responsible for IP addresses
- What is the difference between IP version 4 and version 6 IP addressing and what is the reason for developing IP version 6 addresses
- Give a definition for different IP address classes and their purpose
- What is the purpose of network address translation
- Give a definition and purpose of Mac addressed
- What is the length of a mac address in bytes
- What OSI layer is responsible for Mac addresses
- What are the 2 different types of mac addresses and what are their purpose

(20 marks total)

IP/Logical Addressing

An IP Address is assigned to a networked device in order for it to communicate with other hosts. There are 2 different formats of IP address – IPv4 and IPv6. IPv4 is a set of 4 'octets'. An octet is a number that's made up of 8 bits, IPv4 addresses follow the binary number system, however we represent them using the decimal number system for ease of understanding.

IPv4 Address example: 192.168.1.5

In regards to the OSI Model, the Network Layer (Layer 3) is responsible for adding both the source and destination IP Address.

The difference between IPv4 and IPv6 is that IPv6 follows the Hexadecimal. Here, numbers and letters can be used to identify a device. This method of addressing will allow for more devices to be added to the internet, as there are no more unassigned IPv4 addresses left.

Public IP Address Classes

Class	From	To	Subnet Mask
A	1.0.0.0	126.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	
E	240.0.0.0	255.255.255.255	

Class A – This range is commonly used by Internet Service Providers (ISP's) as the range allows for more hosts, and less networks.

Class B – This address space can also be used by ISP's to create more networks; however, they are all smaller than a class A.

Class C – This is used to create a smaller network again, consisting of 255 hosts.

Private IP Addressing

Class	From	To
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

The above IP Address ranges cannot be used on the internet, as they are strictly reserved to be used within a LAN.

Routers have a feature called Network Address Translation (NAT). This is where many devices, all using addresses from the private IP range, can communicating externally using the same external IP Address that's assigned to your router.

MAC/Physical Addressing

A MAC Address is a unique address that is permanently assigned to a Network Interface Card (NIC). This address is 6 bytes (48 bits) long. The first half of the address identifies the vendor/manufacturer of the NIC, and the second half identifies the NIC. On the OSI Model, the Data Link layer (layer 2) is responsible for adding the source and destination MAC Address as a header. MAC Addresses can be static and dynamic. A static address cannot be altered, where as a dynamic can.

QUESTION FOUR

It's the second week being employed as a Network Support Technician role in Coleg Sir Gar and the IT manager is off ill with Covid 19 so you are now responsible for all the network security of the college LAN and WAN. The principle is very worried about the potential risks of unauthorised access of the college network and he wants to better understand the ways to protect the network from unauthorised data access.

You need to include the following in your discussion:

- Definition and purpose of both hardware and software firewalls and explain how they can prevent unauthorised access of data.
- Definition and purpose of network ports on firewalls and discuss which ports do you always need to be open on the firewall and discuss common ports which can often be closed.
- What is the purpose and benefits of having a 'Demilitarized' zone established as one of the security techniques to try to prevent unauthorised access to data.
- Definition and purpose of different types of 'Intrusion Detection systems' which can be employed to prevent unauthorised access of data.

Firewalls

A firewall can come as either a piece of hardware or software. This tool will allow network traffic to be blocked, accepted or even filtered depending on the associated port number. This tool works on the Transport Layer (Layer 4) of the OSI Model, and can provide enhanced security by closing, opening or filtering traffic on specific ports. These rules are set by the network administrator. There are two main types of port filtering. Firstly, there's packet filtering, which only analyses data on the lower layers of the OSI model. Secondly, there's application layer filtering. As per its name, this method of filtering analyses data all the way up to the application layer, for a more thorough check.

✓ (3)

Network Ports

There are 65535 ports that can be used in networking. A port number is essentially a virtual door within the network. Open ports can easily be exploited by cyber criminals, that's why it's important that we close the ones we don't use. The first 1023 ports are referred to as the commonly known ports. These include services like HTTP (port 80), HTTPS (port 443) and RTSP (port 554). Ports should be opened depending on what services you'd like to be available to computers in your network. For example, for internet browsing, ports 80 and 443 should be open.

✓ (2)

Demilitarized Zones

A Demilitarised zone is where multiple Firewalls are implemented at different places in a network. This can be an essential tool to enhance the security of an organisations network. For example, Coleg Sir Gar could implement a Firewall to protect the web server of the college's public website. This firewall will have a number of open ports to allow all the required services. However, the college could then implement a second Firewall to stand between their public resources, and tools like the Active Directory Domain Controller (ADDC), and computer systems used by the students. On the second Firewall, there will be a stricter set of rules applied by the administrator to allow for increased security. (2)

Intrusion Detection Systems

An Intrusion Detection System (IDS) is a hardware/software tool that can be implemented within a network to analyse network traffic. This tool does not prevent cyber security attacks; however, it does have the ability to send emails/notifications to administrators to inform them of any unusual traffic. An IDS has the ability to learn what is considered as normal network traffic, and to detect signatures of known cyber security attacks. (2)

Q4A - 9 marks
(10 marks)

Explain the purpose within a network of the following networking hardware devices Modem, Routers, Switches, Hubs in your explanation discuss if these devices are intelligent or not and also include which network layer they are located.

Modem

A Modem is a layer 2 (Data Link) device that is used to convert analogue and digital signals. Here, a signal is inputted to a modem. This could be in the form of Fibre, DSL and so on... After the signal has been converted, it is sent into the network. However, when data is sent from the network, this process is reversed. A Modem is also responsible for maintaining a connection to your Internet Service Provider (ISP). A Modem is not considered as intelligent. (2)

Routers

When data enters a network, a Router comes after the Modem. The main purpose of a router is to route network traffic, this allows an internet connection to be shared between multiple devices. A Router uses Network Address Translation (NAT) to use multiple private IP Addresses within the LAN. Routers work on the Network Layer (layer 3) and are considered as intelligent. (2)

Switches

A Switch is a layer 2 (Data Link) device that has multiple ethernet inputs. These can be used to connect multiple computers and other networking devices together. A switch functions by mapping the MAC addresses of all connected devices. This allows data to be transmitted around the network only using the source and destination MAC addresses. Switches are considered as intelligent. (3)

Hubs

A Hub is a networking device that works on layer 1 (the Physical Layer) of the OSI Model. Similar to a switch, multiple devices can be connected by ethernet. The main difference is that a Hub has no address mapping capability. Whenever data is received from one device, it's then sent on to every other device connected. A hub is not considered as intelligent. (3) ✓

(10 marks)

(20 marks total)

QUESTION FIVE

Q4 part B = 10.

i) While configuring Wireless access points/ wireless routers, which type of device filtering technique is used to enhance the security? (2 marks)

- A. Authentication
- B. Encryption
- C. IP Address
- D. MAC Address

Answer: C and D (1) ✓

ii) In Wireless networks, which wireless security initiative helps to secure sensitive information during data transit? (2 marks)

- A. Authentication
- B. Encryption
- C. IP Address filtering
- D. MAC Address filtering

Answer: B (2) ✓

iii) The function that provides secure remote access to servers? (2 marks)

- A. DNS
- B. DHCP
- C. SSH

D. Telnet

Answer: C

✓ (2)

iv) One of the below command communicates with the name server for details about the destination domain is (2 marks)

- A. Ping
- B. Tracert
- C. nslookup
- D. netstat

✓ (2)

Answer: C

v) The Ping command is used to (2 marks)

- A. test the end to end connectivity between hosts
- B. display the network connections
- C. display the route information from source to destination
- D. none of the above

✓ (2)

Answer: A

(10 marks total)

Q5-9.