

APOLLO

A2 Networks

HL

Computer Science
First assessment 2027
2 questions | mark schemes

2. (a) *Award [1] max*

Router/Modem/Gateway

(b) *Award [2] max*

Award [1] for point, [1] for expansion

The network interface layer is responsible for the physical transmission of data;
...including the layout of bits into packets, frames, or other formats;

The network interface layer manages interactions between devices/hardware;
...and the network medium itself, such as Ethernet cable or Wi-Fi;

The network interface layer handles error notification;
...Identifying and reporting any issues or faults in the data transmission process (e.g. lost packets or a disconnected network cable);

The network interface layer determines the network topology (e.g., star, bus, ring, hybrid);
...which impacts network operations (e.g., scalability, fault-tolerance, and data transmission efficiency).

The network interface layer manages physical addressing;
...including assignment and identification of devices (e.g., MAC addresses).

(c) *Award [3] max*

Award [1] per point

Transmission speed/higher bandwidth;
Lower latency compared to twisted-pair cables;
Transmits signals over greater distances than twisted-pair cables;
Immune to electromagnetic interference (EMI) and radio-frequency interference (RFI);
Better security against unauthorized access or data tapping;
Better scalability as data transmission needs grow;
Generally more durable than twisted-pair cables;
Longer lifespan and lower maintenance requirements;

– 8 –

(d) *Award [4] max**Award [1] per point*

MAC address learning: A switch learns the device's MAC address (from the incoming packet's source address)/a switch maintains a MAC address table;
...and associates the MAC address with the physical port through which the packet entered;

Packet examination: destination MAC address is shown in the frame/packet;
...and compared with the switch's MAC address table to find the port;

Selective forwarding: The switch determines the appropriate port to forward the packet/frame based on its destination MAC address;
If the destination MAC address is unknown the switch broadcasts the packet (frame) to all ports;

Possible candidate response worth full marks

The switch saves the arrival port/sender mac address extracted from packet;
The destination MAC address is extracted from the packet;
And the port is looked up in a table based on the MAC address;
The switch then plots the path to the destination port.

Note: either frame or packet is acceptable for candidates' answers.(e) *Award [4] max**Award [1] for each point from the same section*

NAT translates private IP addresses of devices within a local network to a public IP address;
External entities see only the public IP address of the network;
NAT makes it more difficult for attackers to directly reach internal systems;
The extra layer of obscurity enhances the security of the network;

NAT and firewalls often work together;
Firewall inspects and filters incoming and outgoing traffic based on security rules;
NAT allows network administrators to control how traffic is routed;
NAT can be configured to forward specific types of traffic to specific internal devices;

Not only does NAT add an extra layer of security;
NAT enables multiple devices on a local network to share a single public IP address.
Useful given the limited availability of IPv4 addresses;
Enables the network to have more devices than they have IPv4 IP addresses;

5. (a) (i) *Award [1] per line up to [2] max*

Adware
Backdoor
Bots/botnet
Crypto-jacking
Drive-by download
Exploit kit
Fileless malware
Keylogger
Polymorphic malware
Spyware
Trojan horse
Virus
Worm
Zero-day exploit

Accept other examples of legitimate malware

(ii) *Award [2] max*

Award [1] for identifying issue and [1] for expansion

Reputational damage;
Clients may lose confidence in a company that has a breach of security;
For example, parents may withdraw their students from a school;

Financial fraud for patients;
Patients' credit card numbers/banking data/passwords may result in funds being removed;

Theft of data;
Patients' data is used unethically (e.g., insurance company refusing to insure patients with potential pre-existing medical conditions);

Identity theft;
Having your identity stolen can cause psychological damage; e.g., a person may steal a person's online profile and insult others, causing emotional distress;

Data loss causing disruption to hospital services;
Phishing attacks are often designed to steal sensitive data; e.g., doctors lose access to patients' records and can't treat them;

Legal consequences;
Company may be sued for leaking sensitive information by patients/companies/government/ombudsman and lose their license to practice medicine;

Additional malware installed;
Creates vulnerability for the additional malware to cause further disruption.

– 15 –

(b) *Award [4] max*

Award [1] for identifying strategy and [1] for expansion

Implement **device authentication** protocols;
Registering devices, require complex passwords, two-factor authentication, certificate authentication, or biometric data to access the network;

Implement **access control** protocols;
Restricting the user access based on their role;

Use **device management software**/mobile device management (MDM);
Allows IT to manage, monitor, and secure employees' mobile devices;

Require **security updates**/patches be installed;
Devices without the updates/patches will trigger an alert to IT admin;

Install **anti-malware software** on all devices;
Ensure it is kept up to date/push updates to the users' devices;

Remote wipe software;
Install software to delete company data on lost devices remotely;
End-user technical agreement agreeing to device use;
Employee signs as part of their contract;

User training on cybersecurity;
To reduce the risk of cybersecurity breaches;

Mark as [2] + [2]

(c) *Award [4] max*

Award [1] for advantage, and [1] for expansion

Cost efficiency: Reduces initial costs on purchasing hardware;
Maintenance, repair, and replacement costs shifts to employ;

Familiarity: Users are more familiar with their own devices;
Leading to increased productivity/satisfaction and reduced training needs;

Personal choice: Employees are empowered to choose their own devices;
Gives them autonomy/sense of ownership/enables remote working;

Mark as [2] + [2]

(d) **Award [12] max**

Candidates should discuss prevention and response, expressing their opinions on the effectiveness of the strategies. The best responses will demonstrate research and cite real-world related events and/or experts in the field.

Prevention

Implementing robust security protocols: TaylorMade Healthcare can establish stringent security protocols, including firewalls, encryption, email filtering, and regular software updates. These measures can prevent many common attacks, but candidates should be aware that security measures quickly become outdated.

Access control and authentication: Implement strict access control policies, ensuring employees have access only to the data necessary for their role. Use strong authentication methods like two-factor authentication.

User awareness training: Educating staff about potential threats, such as phishing scams and ransomware attacks, can prevent many attacks. Candidates should be aware that human error remains a significant challenge. TaylorMade Healthcare should have clearly defined procedures and protocols for new staff and departing staff. No matter how much training is provided, it is virtually impossible to eliminate all human errors that might lead to a security breach.

Network segmentation and access control: This strategy can limit the damage if a breach does occur by preventing hackers from accessing the entire network. Candidates should be aware that this strategy may not prevent the initial breach and can be complex to implement and manage.

Update and patch management: Ensure all software, including operating systems and applications, are kept up to date with the latest security patches.

Regular security audits and assessments: Conduct regular security audits and risk assessments to identify and address vulnerabilities.

Monitoring and logging: Continuously monitor network activity and maintain logs to detect and investigate suspicious activities.

Physical security: Enhance physical security measures to prevent unauthorized access to servers and other critical IT infrastructure.

Vendor risk management: Assess and manage the cybersecurity risks associated with third-party vendors and service providers.

Cybersecurity insurance: Consider purchasing cybersecurity insurance to mitigate financial risks associated with data breaches.

Collaboration with law enforcement and cybersecurity agencies: Work with law enforcement and cybersecurity agencies for threat intelligence sharing and guidance on emerging threats and best practices.

Response

Data backup and disaster recovery plans to limit the damage caused by an attack and ensure that services can quickly resume after a breach. Candidates should be aware that implementing these measures requires significant resources and that recovering from a breach can still be a lengthy and expensive process.

Third-party services: Cybersecurity consultants and managed security service providers can help respond to breaches quickly and effectively. Candidates may consider whether TaylorMade Healthcare can afford this approach because these services can be expensive.

Failover systems: These systems ensure that critical services remain available even if the primary system fails. However, failover systems require significant investment and ongoing maintenance.

Conclusion

A reasoned conclusion that expresses an opinion supported by evidence.

Marks	Level descriptor
No marks	- No knowledge or understanding of the relevant issues and concepts. - No use of appropriate terminology.
Basic 1–3 marks	- Minimal knowledge and understanding of the relevant issues or concepts. - Minimal use of appropriate terminology. - The answer may be little more than a list. - No reference is made to the information in the case study or independent research.
Adequate 4–6 marks	- A descriptive response with limited knowledge and/or understanding of the relevant issues or concepts. - A limited use of appropriate terminology. - There is limited evidence of analysis. - There is evidence that limited research has been undertaken.
Competent 7–9 marks	- A response with knowledge and understanding of the related issues and/or concepts. - A response that uses terminology appropriately in places. - There is some evidence of analysis. - There is evidence that research has been undertaken.
Proficient 10–12 marks	- A response with a detailed knowledge and clear understanding of computer science. - A response that uses terminology appropriately throughout. - There is competent and balanced analysis. - Conclusions are drawn that are linked to the analysis. - There is clear evidence that extensive research has been undertaken.