



(see note 2 below)

SURNAME: Griffiths

FORENAME(S): DAIR SCOTT

12 Pages

Instructions to Candidates

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold over and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. **Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.**

1	Student Number	P146062.
2	Title of Examination Paper	wide area networks
3	Module Code	MGX1113
4	Date and Time of Examination	14/05/2018 15:00
5	Examination Venue	Gym
6	Seat Number	G046.
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
1	7Y2
3	16
4	4x2
Office Use	38

(Gweler yr ochr arall am y fersiwn Cymraeg)

51%

1A i Standard ACL and Extended ACL

Standard ACL are used when you are allowing or permitting or denying a packet using the source address. Only the source is taken care in a standard ACL. Destination, ports & protocols are not inspected.

Extended ACL are used when trying to filter traffic using source or destination address, ports or protocols. to permit or deny a packet. Extended ACL allow more filtering options for a packet.

1A ii IPv4 has two types of ACL and IPv6 ACL only has one type, it is similar to the IPv4 extended ACL.

~~IPv6 ACL can be applied to any protocol~~
 IPv6 ACL allow for only IP addresses to be used whereas IPv4 addresses allow ACL to be applied.

IPv6 ACL can be applied to MAC or IP addresses, IPv4 can only be applied to MAC addresses.

IPv6 ACL allow greater packet filtering options. It has three options whereas IPv4 only has permit or deny.

IPv6 ACL can filter packets by application type and IPv4 cannot.

IPv6 denies all packets that do not have an allowed statement automatically and IPv4 does not.

IPv6 rules take priority over IPv4 rules.

IPv4 uses wildcard addresses & IPv6 uses Subnet-

1A iii) if ALLIPSS

R1> enable

R1# Config Terminal

~~R1(Config)# Access-list 10 deny ip 0.0.0.0 0.0.0.0 255.255.255.255~~

R1(Config)# Access-list 10

R1(Config)# Access-list 10 deny ip 0.0.0.0 0.0.0.0 255.255.255.255

R1(Config-ACL)# Exit

R1(Config)# interface S0/0/0

R1(Config-if)# Access-list 10 inbound

R1(Config)# Access-list 20 permit tcp any any

R1(Config)# int S0/0/0

R1(Config-if)# Access-list 20 inbound

R1(Config)# int G0/0/1

R1(Config-if)# Access-list 10 inbound

R1(Config-if)# Access-list 20 inbound

R1(Config-if)# End

122.

1A iv) An access control list (ACL) controls whether a router will PERMIT or DENY packet traffic based on packet header criteria.

3- ACL are often used within routers between internal & external networks to provide a FIREWALL.

4- A router with three interfaces and two network protocols (IPv4 & IPv6) can have as many as TWELVE active ACLs.

5- For inbound ACL, incoming packets are processed AFTER routing has been performed.

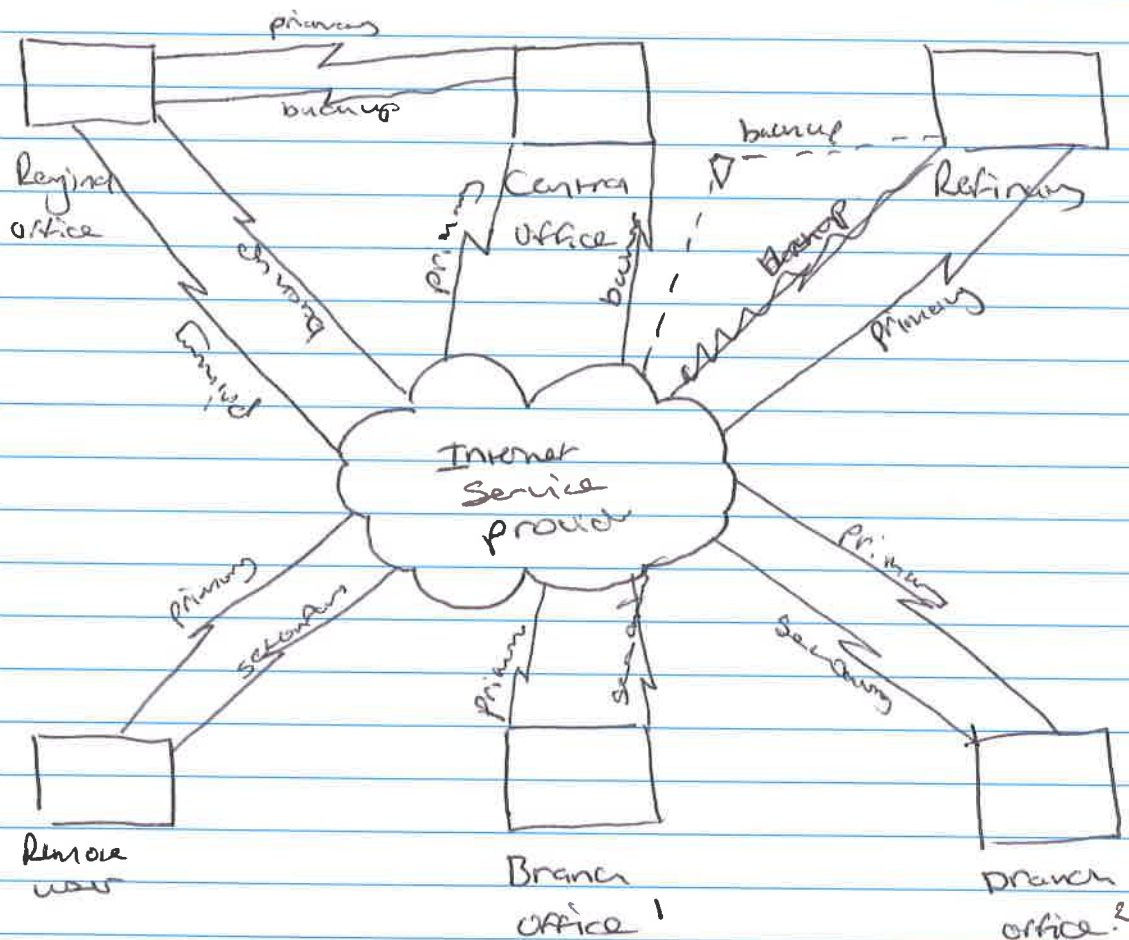
6- For outbound ACL, outgoing packets are processed BEFORE routing has been performed.

7.- For every acl, there is an implied deny statement. if a packet does not match any of the ACL criteria, it will be DISCARDED.

8.- ACLs can filter data traffic per protocol, per direction per INTERFACE.

9.- ACLs can filter traffic based on Source/Destination address, PROTOCOL, and port numbers.

Q3 Ai



Regional office - Central office

- o Primary link LEASE LINE
- o Secondary link ETHERNET WAN

Regional office - ISP

- o Primary link LEASE LINE
- o Secondary link ETHERNET WAN

Central office - ISP.

- o Primary link LEASE LINE
- o Secondary link ATM.

Regional - ISP.

- o Primary link Digital Subscriber line (DSL)
- o Secondary link Satellite

Remote user - ISP.

- o Primary link Fibreoptic
- o Secondary link DSL.

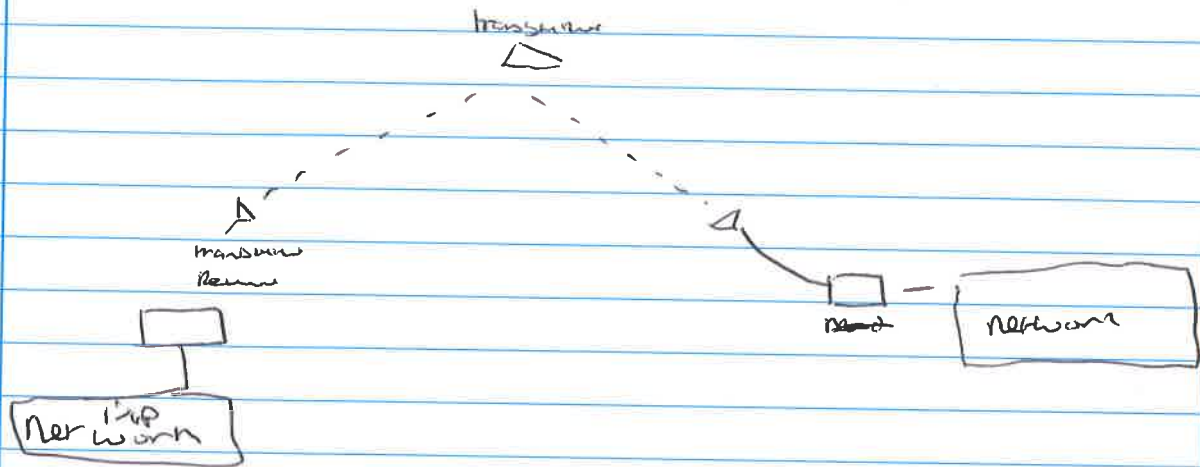
Branch office 1 & 2

- o Primary link LEASED Line
- o Secondary link ATM.

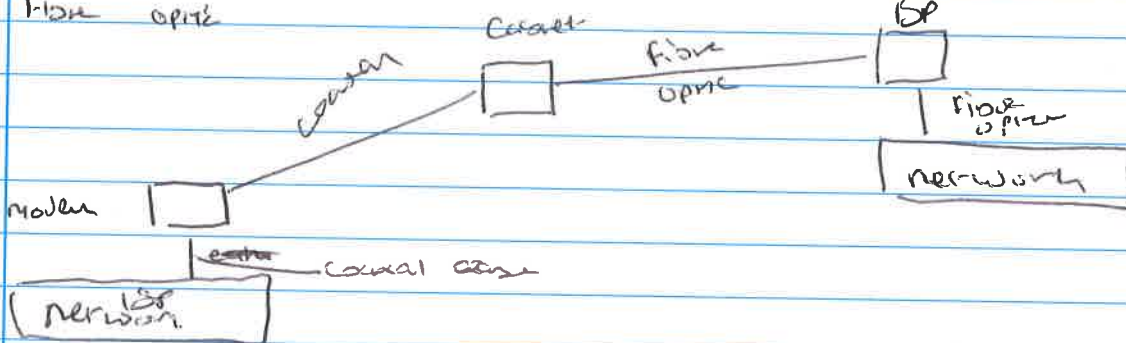
Security implementations.

- o Each Location has a fire wall ✓
- o All devices have ~~security~~ Anti-Virus ✓
- o All Extranet WAN have a L2TP/IPsec VPN with an ~~ipsec~~ openvpn as a backup.
- o ATM connections use L2TP/IPsec VPN and openvpn as backup.
- o DSL used an L2TP/IPsec VPN with a ipsec VPN.
- o Satellite connection have an L2TP/IPsec VPN and a backup ipsec VPN.
- o Access control lists are applied in each location.
- o Virtual Local area network are implemented within each location.

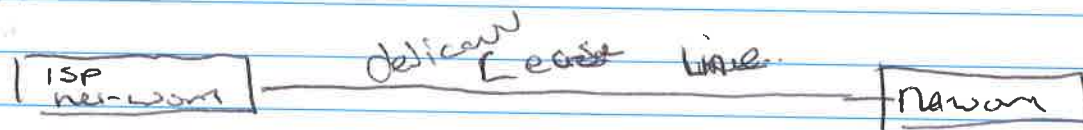
Satellite Connection



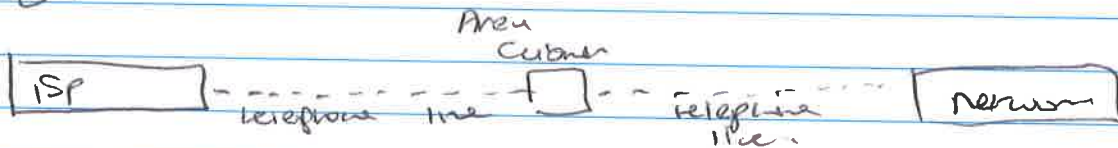
Fibre optic



LEASE Line



DSL



Ethernet WAN



~~Quizzes~~

10

3Aii Lease lines were preferred in the scenario as they are secure, if tapped into the signal is lost. Reliable, lease lines have an uptime % rating of or over 99%. Lease lines are ^{fast} secure up to 10gb/s. ✓

Extranet WAN was chosen as it is fast not as fast as a lease line but is a good lower cost option. Reliable, not as reliable as a lease line but still very reliable. Secure as either can be used from it is again very secure as if tapped it loses connection. ✓

ATM was chosen as it is fast and prioritises voice, video over data to reduce delay. It is not the most secure so VPN has been added to ensure it is secure. ATM is very reliable. Speeds of 600+mb/s. ✓

DSL was chosen as it was the best option available. Easy to install everywhere so many telephony lines are used. DSL is not the best for security, so an L2TP IPsec VPN was implemented. DSL is not the most reliable however in remote locations it can be the only option. DSL can have speeds up to ~~100~~ ⁷⁰ mb/s. So it is only used as a backup. ✓

Satellite was only used for the refinery that is in ~~the middle of the desert~~ a remote location. Satellite is not very fast but it is able to provide good coverage. Not secure so VPN is used. ✓

Fibre optic was used as it is fast & commonly used within home networks. Fibre optic is not secure as the links are shared with others. This is why a VPN was used to ensure data is kept safe. Fibre optic is very reliable.

Every server has a primary & backup link to ensure reliability is as high as possible.

4# Internet of Things

The internet of things is connecting devices to the internet so they can be controlled.

- Devices are not generally well secured due to poor manufacture.
- Although smart devices seem like a good idea, if hackers get into them they could make serious privacy & security issues.

Cloud Computing

- Made to reduce company's running costs.
- Saves small companies managing a network.
- Only pay for what is used.
- Very reliable.
- Data stored securely.

Virtualization

There are two types, type 1 & 2. Type 1 virtualisation is done on physical hardware. Type 2 is run on top of another OS. Very popular as server utilisation can be achieved.

Software defined networking is becoming more popular as more and more better technology is launched. It allows software to run & manage & ^{configure} ~~create~~ networks.

✓✓

✓✓
(✓)