



12 Pages

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.**

(see note 2 below)

SURNAME: Ridd

FORENAME(S): Ethan

1	Student Number	P144 898
2	Title of Examination Paper	Wide area networks.
3	Module Code	M6A113
4	Date and Time of Examination	14/05/18
5	Examination Venue	G7M
6	Seat Number	G054
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
1	19
2	23½
3	17
Office Use	59.5

Q1

i/ Standard Acl — blocks or allows a specific address and must be placed as close to the destination as possible

Extended Acl — can block packets based on a number of criteria such as source IP, destination IP, source port/udp, destination port/udp, port numbers and protocols. It must be placed as close to the source as possible to prevent the packet from travelling the whole network.

ii/ IPv6 acls can only be named Acls unlike IPv4 acls can be named and numbered. IPv6 does not require a wildcard mask as the IPv6 prefix is . /64 is used.

```

iii # IPv6 Access-list PC3-DENY
# IPv6 Access deny 2001:DB8:CAFE:30::/64 ANY
    ANY pub ANY

# IPv6 Access allow ANY ANY icmp ND-NS
    NA-NS

# int S0/0/0
# traffic-filter PC3-DENY
  
```

- iv/ 1 point ✓
 2 deneg ✓
 3 firewall ✓
 4 ~~32K~~ frame ✓
 5 before ✓
 6 after ✓
 7 discarded ✓
 8 interface ✓
 9 protocol ✓

9

19

Q2

a) Flag - marks the beginning of a frame ✓

address - contains the broadcast address in bits ✓

|||||, |||||, |||||, |||||

Control -

data - the data stored within the frame ✓

protocol - the protocols used by the frame ✓

FCS - frame check sequence ^{provides} the FCS on the other end of the link if incorrect the packet is dropped.

flag - marks the end of the frame.

b) Challenge handshake authentication protocol is a authentication protocol that requires both a username and password, it needs to be configured on each end of the link. and is more secure due to encryption. each router must know the username and password of its neighbor to connect. ✓

password authentication protocol is the default and is less secure as it doesn't support encryption and operates with the use of a shared password.

c)

Negotiate and set up control options for the link
- LCP

manage packets from several network layer protocols - NCP

Establish, configure and test the data link connection
- LCP

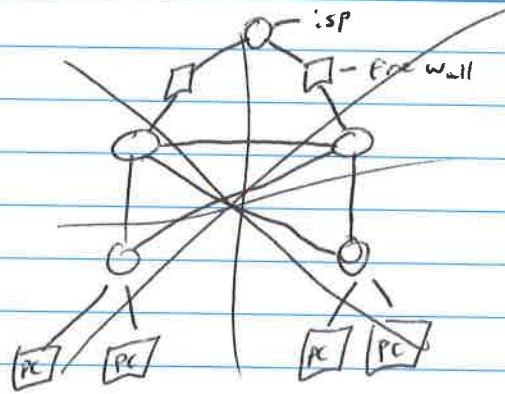
Terminate the link - LCP

Bring network layer protocols up and down - NCP

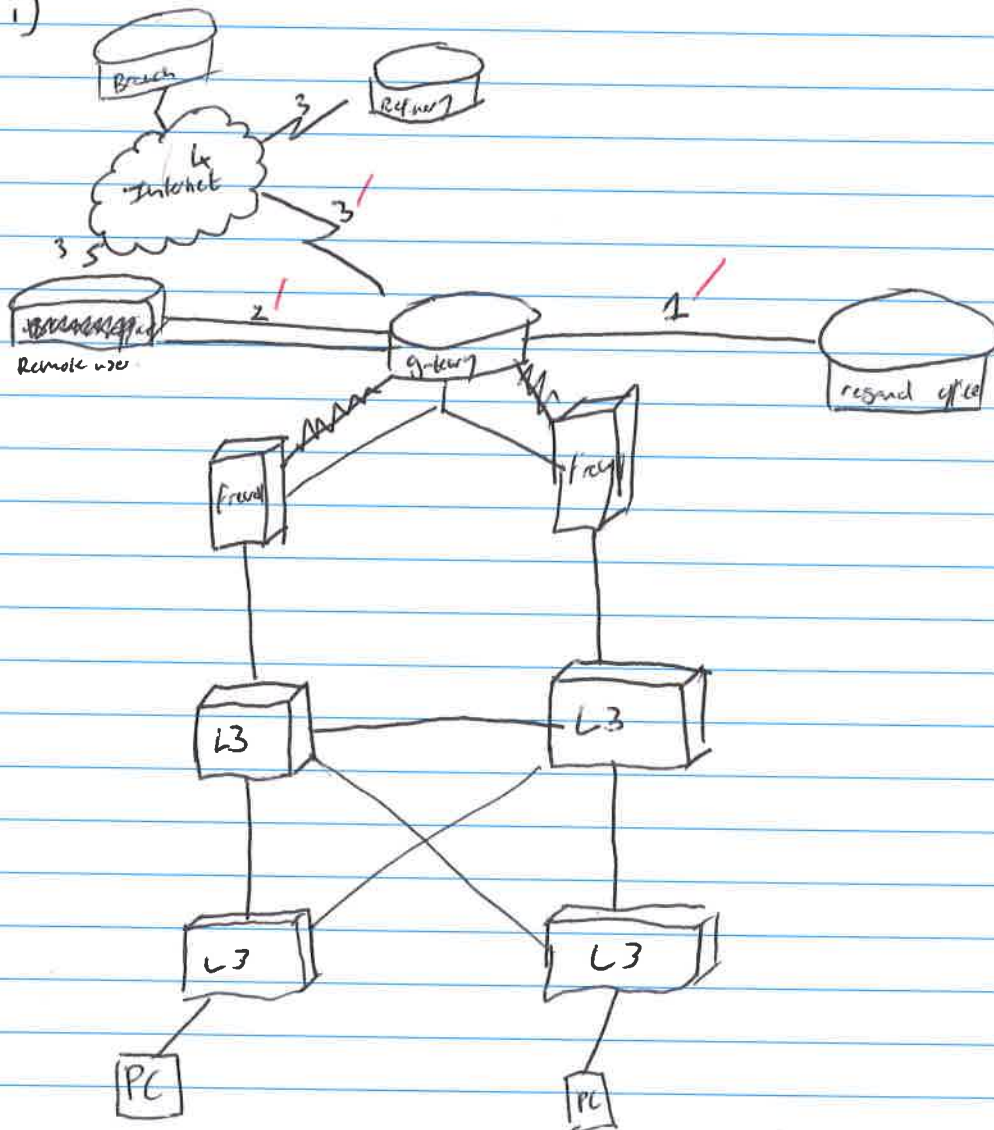
Determine whether the link is functioning properly - LCP

encapsulate and negotiate options for ipv4, ipv6 and ipx - NCP

Q3



i)



1 - on L1 dedicated connection point to point high speed and high availability.

2 - tunnel for remote accessing using IPsec and GRE

3 - access to the internet using high speed fibre

4 - all routing performed using BGP.

ii) The structure used is a standard collapsed core hierarchy to allow connectivity to the local hosts. firewalls placed between the core and gateway routers to act as a DMZ for security and to act out ACL policies. dual links for gateway redundancy using a hub and spoke topology. a remote access tunnel between remote wing branches and central office created using ipsec. Our goal is provide encryption through the tunnel. a dedicated T1 line between regional and central offices provide high speed and the infrastructure would already be in place. As the offices are connected to the internet using high speed fibre. benefits of the network is plenty of security and redundancy with encryption and encryption. Limiting if the gateway goes down then access to the central office goes down. The dedicated line utilizes chap authentication and PPP encapsulation.

✓

17