



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.**

SURNAME: THOMAS

FORENAME(S): IVAN.

List the numbers of the questions you have attempted	Office Use
2	12
3	10%
4	10
Office Use	39%

(2.a)

(b. ~~Link control protocols~~ it begins the negotiation
 pap password authentication protocol.
 It ~~comp~~ checks for a password on the link
 and establishes a ~~some~~ connection if both passwords
 match. The password is sent in clear ~~text~~ across
 the links.

Chap (Challenge handshake authentication protocol)
 matches the username + password between both links.
 If both links have the same ~~username~~ & each link
 asks for the others username + password + checks
 against it's config. If it matches then the link
 comes up. the password is encrypted between
 transmissions.

(c. Lcp ✓
 Ncp ✓
 Lcp ✓
 Lcp ✓
 Ncp ✓
 Lcp ✓
 Lcp ✓

(Q4: The internet of things refers to connecting the previously unconnected to the internet. They consist of sensors, applications, computers, ~~and~~ appliances.

Cloud computing refers to providing a customer or business with a service. ^{through the internet} There are 3 types of clouds. private clouds. i.e. government organisations. who public i.e. ~~amazon web services~~ one drive, google drive, Dropbox. + Hybrid clouds who do both. Amazon web services for example; They provide cloud services to ^{end} users, organisations. ~~to google~~

Virtualisation. ~~Removing~~ utilising the power of ~~Software~~ from the limitations of hardware.

Virtualisation is the term given to stacking multiple Applications + operating Systems onto ~~one~~ one piece of hardware or ~~to~~ software. by removing Hardware limitations, we ~~are~~ boost computational resources + power.

Type 1 refers to directly installing multiple operating systems + services onto a piece of hardware.

Type 2 virtualisation is used by running a OS or + its services on an already established operating system. examples include virtual box or virtual pc. These are good for testing or sandboxing unknown software you may not trust.

(Q4): Software defined networking refers to the virtualisation of networking equipment. For ease of management, configuration, monitoring + cost. Layer 2 + 3 switching is separated from other tasks to speed up the process. Once the data is passed from one plane to another the secondary plane runs the routes calculated in the previous plane. This separation gives the administrator full control over network performance, security + health. This multiple virtual switches + routers can all be controlled through a single GUI. SDN saves the administrator money through virtualisation, running multiple switches on one physical hardware.

This reduces purchasing costs, cooling + configuration. A script could run to monitor multiple devices.

(Q3): The refinery is connected to the ISP through a packet switched WAN technology. MPLS to be exact. The provider will negotiate, provide a translation device so the refinery edge router can connect to the ISP customer edge router. On this link will be layer 2 + PPP chap authentication between central + refinery. + a layer 3 IPsec VPN over GRE tunnels.

Branch offices are connected through site to site VPNs. Again a GRE Tunnel will be used so all traffic between the two sites is seen as a singular hop. Both IPv4 + IPv6 can transition across this link, providing scalability for IPv6 enabled devices.

IPsec encrypts all data between branch + Central. Therefore only interception is unreadable + the ~~business~~ business is protected.
 A Secure Intranet will be accessible to users who wish to work from home. However the firewall require a VPN connection + a 3 step authentication before access is permitted. All these connections will be monitored by the firewall + only HTTPS is allowed.

The remote user will either use a cable or DSL connection. For the intranet likely provided to their home. For the example they are using a cable connection + will use a ~~VPN~~ VPN to work from home. to login credentials + HTTPS traffic requirements must be met for the user to remote into our network.

Regional office will have a packet switched connection to the internet. The Highspeed line between central + regional will be for back up's ~~for backup~~ + as it is likely a leased line with all available bandwidth allocated to the international oil company. Utilizing this with backups provides control + the best value for money as the bandwidth will always be used.

The ISP will once again provide a translation device if required, to connect to their network. Speed will be less than a leased but cheaper + more than adequate for our traffic.

explained no diagram

X

Q4. Justifications.

Site to site vpn's for protection of all sensitive data between branch + central. GRE will ~~keep it~~ logically provide a tunnel through the Isp for more control of our data. Ipsec or similar will be configured to encrypt + chap will keep links open as long as nothing is tampered with. ~~If charges rise~~ ^{AOEN}

Highspeed — backups over a leased line. Will utilize the best speeds + costs through consecutive replications.

Remote user to cable + browser vpn. ~~cable~~ cable connection provided by their home Isp providing it's close enough to the exchange. Otherwise we will use DSL. A vpn on their pc will be a requirement to access ~~networking~~ resources by the firewall in the C-EO. This keeps data inbetween safe.

All others are on mpls packet switching as this is largely the technology used by Isp's + providers. The ~~fastest~~ fastest shared option of data through a Isp. Sometimes ~~it~~ described as residing on the 2.5 layer of the OSI model due to its routing + switching technologies based on labels.