



SURNAME: Phillips

FORENAME(S): Tordan

12 Pages

1. Please give the information requested in the boxes.
2. Enter your name in the space provided to the invigilator and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can read your answers in any 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.**

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)

Rhestrwch ffau'r cwestiynau a ymgelisiwyd gennyh	
At Ddiibenion y Swyddfa	

(See the other side for English version)



Prifysgol Cyfmr
y Drindod Dewi Sant
University of Wales
Trinity Saint David



Cyfarwyddiadau i Ymgeiswyr

1. Rhwch yr holl wybodaeth y gofynnir amdani yn y blychau isod.
2. Rhwch eich enw yn y lle a ddarparwyd ar y dde, plynwch et a'i selio i lawr (gan ddefnyddio'r label a ddarparwyd) i guddio'ch enw.

1. Rhaid i'r atebion fod mewn llawysgriften ddarllenadwy. Gall yr Arholwyr naill ai anwybyddu sgript annarllenadwy, neu drefnu iddi gael ei theipio a chael yr ymgeisydd i dalu.
2. Ysgrifennwch eich atebion mewn inc.
3. Dechreuwch bob ateb ar dudalen newydd. Gwnewch unrhyw fras nodiadau yn y llyfr atebion a thynnu llinell drwyddynt.
4. Ni ddylid rhwngo unrhyw ran o'r llyfr hwn; rhaid ei gyflwyno yn gyfan.
5. Os defnyddir mwy nag un llyfr, rhwymwch hwy gyda'i gilydd gan ddefnyddio'r tagiau sydd ar gael oddi wrth y gwyllwyr/gwylwyr.
6. Rhaid dychwelyd pob llyfr. Ni chaniateir mynd â llyfrau atebion, wedi eu defnyddio neu heb eu defnyddio, allan o'r lleoliad arholi o dan unrhyw amgylchiadau.

Llenwch, plynwch a selwch
(gweler nodyn 2 isod)

CYFENW:

ENW(AU) CYNTAF:

- ① a) i) Redundant topologies possess a number of problems such as broadcast storms, ~~where~~ switches receive a packet and forward it through all ports. ~~The~~ In redundant topologies there are multiple connections between switches, meaning a switch could send a packet ~~to~~ back to the sender switch.

Other problems include ~~some~~ recursive lookups, which has problems with multiple connections between devices, ~~adds~~ additional cost in network design, ~~and~~ other looping of packets and additional routers can be unutilised. These topologies ~~also~~ have the issue of not utilising each device to their full potential.

- ii) Solutions to problems caused by redundant topologies include utilising spanning tree protocol. This protocol ensures that there is only one path to traverse the network. All redundant paths are deactivated but ~~can~~ ~~be~~ still exist and are reactivated should the primary link fail.

EtherChannels are a solution to unused bandwidth. This process bundles multiple ~~links~~ physical links into one logical link, improving the bandwidth on this link.

First hop redundancy protocol (FHRP) is used as a solution and redundancy technique to multiple router devices. This method ~~provides~~ ~~or~~ combines multiple routers so

Not required
explain more
about STP.

They appear as one logical default gateway. This method utilises all routers as one IP gateway, therefore ~~sw~~ switching and routing tables require less entries and all participating routers accomplish the same goal. If one router fails, the others ~~are~~ able to take over in the task.

b) To set up EtherChannel, a number of steps must be taken:

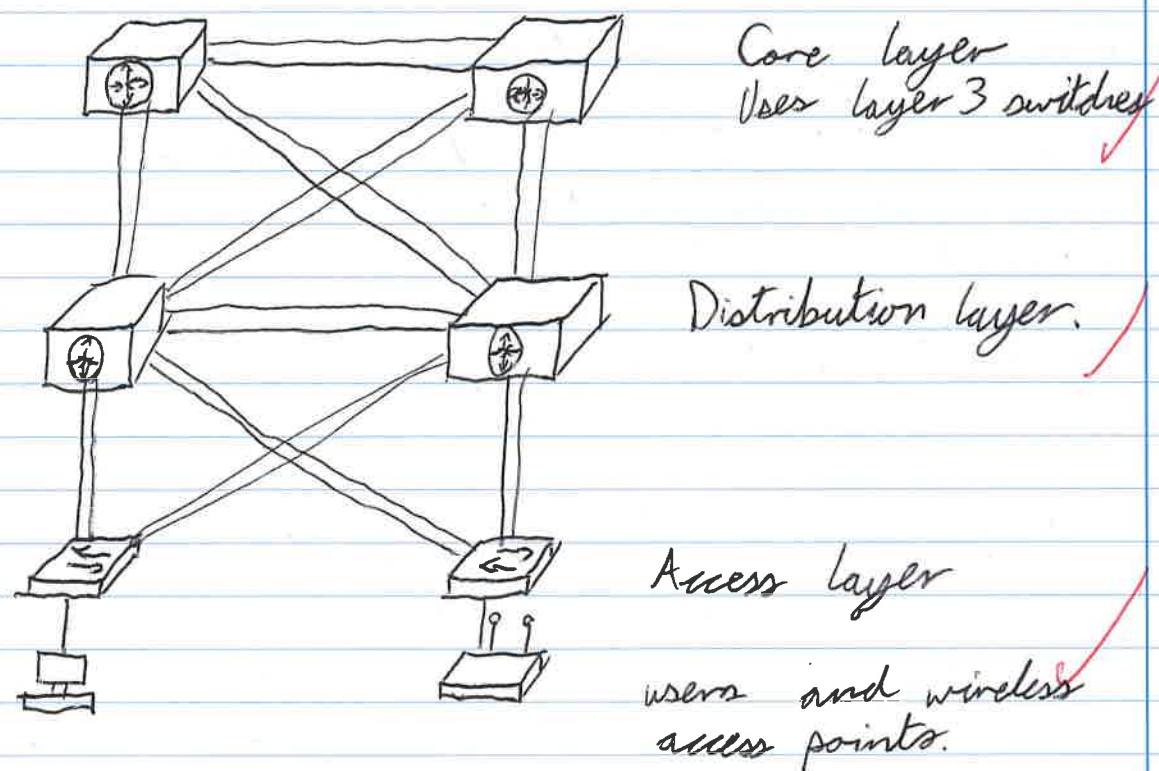
- Define the interface range participating within the EtherChannel.
- Group the interfaces into a single, logical connection.
- ~~Defi~~ Define the new EtherChannel ID so ~~that~~ that it is identical on both ends and unique within the network.

Additionally, switches participating in EtherChannels ~~must~~ ^{must} be full duplex, have the same ~~band~~ bandwidth and speed on both ends of the connection.

- c) Layer 2 vulnerabilities include ~~data~~ broadcast storms and recursive lookups, where switches receive packet from one interface and forward them through all others, ~~potentially~~ potentially returning to the original device creating a constant stream that ~~degrades~~ degrades network performance.

MAC layer attacks
VLAN attacks
Spanning attacks

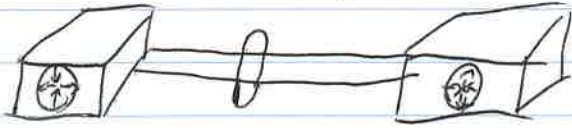
② a) i)



- ii) Core layer is the high speed backbone that connects the distribution layer to other networks and campuses. The core layer is where all traffic enters and exits the network and is constantly active. This layer requires high transfer speeds to process inbound and outbound traffic.

The Distribution layer connects multiple access points to other network resources and the core layer on a policy based system. This layer typically terminates any VLAN traffic before leaving for the core layer, and switches between multiple VLANs. Speeds at this layer are lower than core but higher than access. Both Core and Distribution have high redundancies to ensure no single point of failure.

- c) VSS creates a virtual switching stack by combining multiple physical switches using EtherChannels.



VSS has the benefits of combining the switching power of multiple switches which enhances their performance and efficiency.

Access layer is the final layer where users are able to access the network from end devices. This layer also connects wireless access points to the network.

SSH should be used on all layers for secure remote access.

- iii) Access layer is the layer where users gain access to the network and its resources. This layer is capable of switching traffic to the upper layers based on users and traffic type.

This layer is capable of supporting multiple VLANs on different ports, but must use the distribution layer to allow different VLANs to communicate.

Access layers are also able to extend the network using IP phones and wireless access points.

High availability
convergence
an other point.

b)

- b) Best practices for network management with SNMP include utilising SSH for remote access, as the connection is encrypted. Management should be isolated within its own VLAN to separate traffic from other users. Managers should limit user access to network resources based on user permissions. SNMP managers should also be able to access all of the network to monitor and manage areas.

③ a) A VLAN trunk is a connection between devices, such as switches, that allow for multiple ~~VLANs~~ ~~as~~ different VLANs to ~~to~~ send packets over a single link.

The capability of a single link carrying multiple VLANs worth of traffic eliminates the need for a single link per VLAN.

This allows switches to transmit packets to a destination that can switch between different VLANs, such as layer 3 switches or routers configured for router-on-a-stick.

A trunk link must ~~must~~ define which VLANs are allowed to use the link.

Trunking configuration must be identical on both ends. This includes which VLANs are allowed over, ~~encapsulation~~ encapsulation used, speed and duplex.

b) Dynamic trunking protocol is an ~~old~~ method that allows switches to negotiate trunking methods.

Access is utilised to disable trunking on a link. Switches with switchport access mode will attempt to prevent trunk mode. Access on both ends prevents trunk mode entirely.

Trunk mode is used to enable trunking on a link. If switchport mode is set to trunk on both ends, a trunking link is created.

Nonegotiate prevents switches from negotiating trunking protocols.

Dynamic Desirable will attempt to convert the link to a trunk link but only if the other end has been configured with Trunk, dynamic desirable or dynamic auto. It does not forcefully convert the link like switchport mode trunk.

Dynamic Auto will base the decision of converting to trunk link or not depending on what the other end switch is configured to.

Trunk links are created using a combination of Trunk / Trunk, Trunk / dynamic desirable, desirable / desirable, Trunk / dynamic auto and desirable / auto.

Auto / Auto, Access / Access and Access / Auto result in no trunk connection.

Trunk / Access give limited connection.