



SURNAME: Blunt

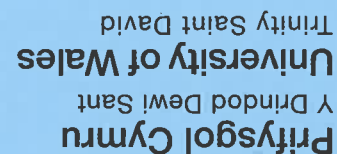
FORENAME(S): Liam Joseph Mark

12 Pages

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold the flap over the flap label, and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners cannot 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.**

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)



12 Tudalen

Cyfarwyddiadau i Ymgeiswyr

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

1. Rhaid i'r atebion fod mewn llawysgriften ddarllenadwy. Gall yr Arholiwr naill ai anwybyddu sgrïp 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 rhwgo 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/gwylywyr.
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 amgylchriad.

(See the other side for English version)

1	Rhif Myfyriwr	
2	Tell y Papur Arholiad	
3	Cod y Modwl	
4	Dyddiad ac Amser yr Archoliad	
5	Lleoliad yr Arholiad	
6	Rhif Sedd	
7	Nifer y Llyfrau Atebion a gyflwynwyd	

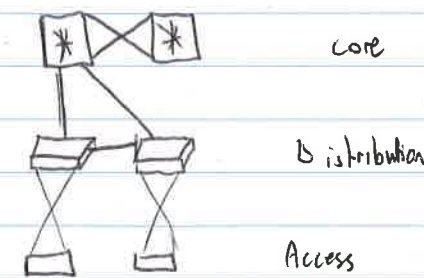
[illegible]

Llenwch, plygwch a seliwch
(gweler nodyn 2 isod)

CYFENN:

ENW(AU) CYNTAF:

D a)



The 3-tier hierarchical network design is made up of the core layer, distribution layer and Access layer, as shown by the albeit crudely drawn diagram above.

The core layer is the backbone of the network and consists of advanced switches and data transfer methods such as fibre. The main purpose of this layer is the fast delivery of information around the network, which is why there will be advanced QoS features present, to prioritise certain information. No packet manipulation is done here.

The ~~core~~ Distribution or ~~workgroup~~ ^{packet} layer is the layer that does what most would consider networking such as packet distribution and manipulation. This layer prioritises reliability over speed, but to a certain degree. While there are QoS features present, they are not to the level of the core layer, but nonetheless. It is here where policies and security methods are implemented such as ACL, DHCP and NAT.

The Access layer is made up of level 2 switches and devices, prioritising the connectivity and reliable communication to send user/end devices. It is here where security features are implemented such as VLANs and therefore trunking (should the network require it).

b) The ACL inbound and outbound filters can be filtered via source, destination or communication means/port (such as SSH, TFTP). The inbound filter as you may guess blocks any packet coming into the router within its guidelines before processing the entire packet. Outbound filter as you may guess blocks/drops those in its criteria after processing it for forwarding. Using these you can block unwanted traffic in the network. For example were either one of these filters blocking the IP range of a pc trying to ping said router, the ping will always fail as a ping requires a return, of which an outbound will block, and an inbound will block even beforehand.

- c) Store forwarding - The entire packet is received and CRC or error checked before forwarding. Between the two methods in the question this is the more reliable but slower and more CPU intensive of the two.

2

Cut-through - Only the frame is read until it has the ^{required} information for forwarding such as source and destination, ~~before the first 64b~~ the router will start forwarding. This is the faster but more unreliable method, as well as less CPU intensive. ~~A compromise between the two would be Cisco express forwarding.~~

1

2) a)

- i) Inside local address - the IP of a device from the inside of the NAT boundary router. The type to normally see in a network design.

2

- ii) Inside global address - The IP of an outside the NAT boundary from the perspective of an ^{outside} device. For example before translation the device may be 192.168.0.15 becomes 209.165.27.1 via NAT translation.

1

- iii) Outside local address - The address of a device on the other side of the network once it has been de-translated by NAT. Like the inside ^{local} but from the opposite perspective, ~~from the~~ where the inside may see 209.165.1.7, the local is 192.168.7.2.

1

- iv) Outside global address - The opposite perspective of inside global, before being de-translated by NAT, of which could be 204.165.2.19.

1

* See diag diag diagram on page 4.

- b) Process switching - Process switching will process the entire ~~frame~~ ^{packet}, performing CRC checks and such before "switching" the packet. Although it is slower, it is more reliable as it performs error checks.

Fast switching - Processes only the header and does no error checks, "switching" as soon as possible before or even the first 64b are processed, it will ~~start~~ start switching the packet.

Cisco express forwarding - Similar to both, it will do so as fast switching, but with ~~no~~ error checks the first 64b before forwarding, as this is the most likely place

where errors occur. As you may guess it is a Cisco proprietary concept/method.

- c) Three primary uses of static route

- Default route / Gateway of last resort
- Manual, ^{fixed} secure, line (Manual or static routes are harder to "hack" with ^{unethical} means)
- Backup route should dynamic routing fail for ~~or~~ whatever reason

2

- d) The command is that of a ~~default~~ ^{floating static route} route directed towards 192.168.1.1, that should a packet not find their destination route on the immediate network, it will forward it to 192.168.1.1. Cases such as this are often used to direct from stub networks to larger the larger section of the network or it to work as an internet connection ~~in the same way~~ as is often in the case in home networks.

- 4) a) i) Benefits of VLANs

- Improved security - can limit what users can access via their VLAN
- Improved manageability - As opposed to managing a singular huge network, you can manage multiple smaller networks of which each can have their own permissions, and ACL and security implementations.
- Reduced cost - Instead of buying multiple smaller networks and sectioning them off physically, you can section them off digitally, achieving near enough the same ends.
- Improved performance - If sectioning off the network, the strain put on the network as a whole in peak times will be reduced, as with less avenues of approach, there are less errors and the strain on the network will be corrd into partial ~~seet~~ sections/VLAN environments.

4

- ii) Default VLAN - the VLAN of which ports are attributed automatically is no VLAN is specified. By default VLAN 1 is in Cisco routers.

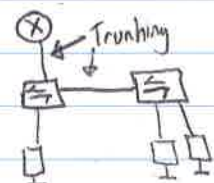
1

Data VLAN - An ordinary VLAN that offers no QoS such as a Voice VLAN would. These are the most common of the VLANs used, at least in most cases. Although

Management ~~VLAN~~ VLAN - The VLAN of which is in control of management functions such as certain SSH or other communications to other parts of said VLAN. Management VLANs tend to have higher priority than the rest as the others ~~cannot~~ cannot function properly should the management VLAN fail one way or another. Management VLAN is often used to communicate VLAN updates should a VLAN be changed or deleted or other misc management-related functions.

2

111)



2

In traditional VLAN routing 1 VLAN = 1 physical port, whereas in router on a stick it is the same except 1 VLAN = 1 virtual port, allowing for multiple VLANs on a singular physical port. Saving both space and money at the cost of reliability. This is due to the fact that the more VLANs you put on a singular port, the larger point of failure it becomes, which is why it's uncommon on large enterprise networks. This method exists due to trunking and virtual sub-interfaces of which will be expanded ^{you} in the next question. In the above diagram the trunk connection to the router must have the appropriate sub-int configured.

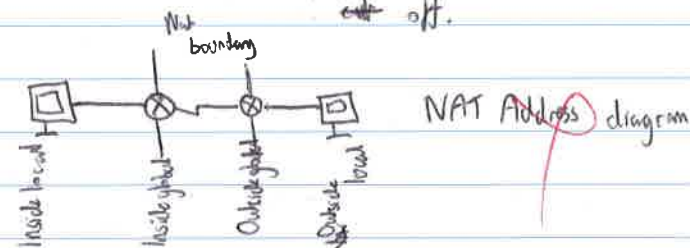
P

2

iv) A VLAN trunk is a connection of which allows multiple VLANs via a single port, something that isn't possible without trunking. Each VLAN acts as a branch on a tree, giving its name, multiple branches diverge from the trunk. As mentioned before this comes at the cost of being a larger point of failure to the network. When setting up a trunk, both sides/ports of the connection must be configured for the trunking process to work. ^{All} VLANs don't use trunking if using a router on a stick method must have a sub-interface configured to the appropriate VLAN. Trunking also allows in ~~for~~ certain configurations, communication between the VLANs, so it isn't completely cut off.

2

2a)



Question No.

Examiner Only

Rhif y Cwestiwn

Arholwyr yn unig