Midterm Test: NET3011 – Advanced Switching

Winter 2017

Time: 110 minutes; Test scored out of: 68 Total Marks available: 76
(Allocation of marks is shown beside each question)

Instructions:

1. BEFORE answering any questions, please check that your copy of the test has all pages (as indicated in the footer at the bottom of each page). Please **read all instructions and all questions** carefully, then answer question 0 first!

2. This is a **closed book** test. No textbooks, notes, electronic devices, or any other aids are permitted.

3. If you need extra space, please continue your answer on the last page.

4. If you are uncertain what a question is asking, make reasonable assumptions, write those assumptions down on this test paper, and continue answering the question.

0. What is your:

NAME? Answers

(Continued on next page)

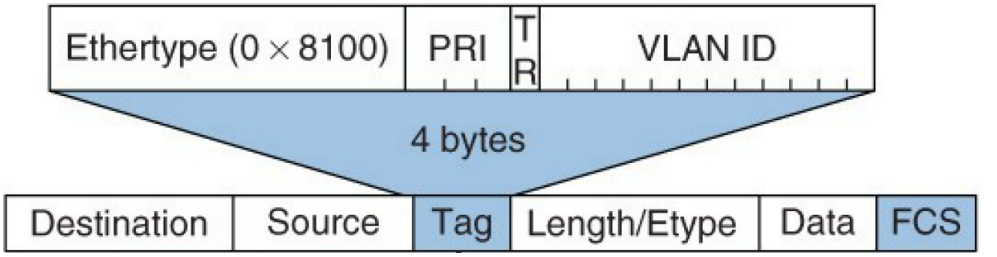
1. [2 marks] Explain in **clear** but simple terms, what is the fundamental difference in the way routers and switches forward traffic? (i.e. What are the two, or at most three, characteristics that distinguish routing from switching?)

   Groupings: Routers forward to *groups* of hosts based on *best* match;
   switches forward to *individual* hosts based on exact match
   Unknown destinations: Routers *drop* traffic to unknown destinations; switches *flood* it
   Partly relevant: routers learn destinations via protocols; switches learn via eavesdropping

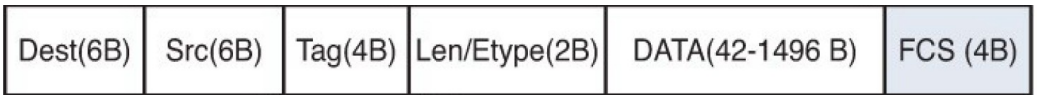
2. [1 mark] Explain **clearly** how a managed switch forwards traffic arriving on trunk interface for which neither the MAC address nor the VLAN has a matching entry?

   The switch (silently) drops the traffic
   The MAC address is irrelevant; without a matching VLAN, it's impossible to identify suitable egress interfaces.

3. [2 marks] **Clearly** and correctly identify (a) the **fields** and (b) their **length** in an Ethernet frame captured from a *trunk link*. You may give a list of the fields, or draw a correctly labeled diagram.



Ref: Fig 3-5, 3-7 FLG



802.1Q Tag Frame

4. [2 marks] Chapter 2 identified three generic methods for forwarding L3 packets. Clearly identify the method that is done (a) purely in software and (b) purely in hardware.

   Process switching is done purely in software
   Topology-based switching is done purely in hardware

5. **A**. [2 marks] What are the key VTP msg parameters for a switch to accept a VTP update?

   [1 mark/pair] version; domain name; password; revision number; MD5 hash

   B. [1 mark] One of the above parameters must **not** match the existing configuration on the switch. Which one is it and what are the requirements on it's value?

   revision number (in the received message): must be higher than switch's current value

6. [3 marks] Give **clear**, **full** explanations of at least 3 advantages of end-to-end VLAN design.

   Ref: FLG p. 46-49; slide deck for Ch 3, slide 10

   Choose from: grouping, virtualization, security,
   avoiding needless routing, specialized VLANs

   Must give a clear, full explanation for each

7. [3 marks] End-to-End design allows *many* VLANs to exist in a campus. Cisco switches have some significant limitations of support for large numbers of VLANs, either due to hardware limitations or protocol specifications. What are at least three (3) of these limitations? Tip: Different versions of some protocols reduce some of the limitations.

   VTP ver 1,2 can only handle VLAN numbers up to ~1005
   Many Cisco switches can only handle up to 128 STP instances
   Cisco switches (e.g. intended for the access layer) can only handle 255 VLANs
   Private VLANs require VTP Transparent mode if using ver 1 or 2; so manual config!!!

8. [2 marks] **Clearly** identify (and/or describe if necessary for a clear answer) some key features which differ between VTP versions, as implemented on Cisco switches.

   Anything from p. 73-74 of the FLG is acceptable. Some differences seen in lab are:
   – ver 1-2 servers will learn a VTP domain name if none configured; ver 3 won't
   – ver 3 adds "primary" to the server mode, with only one Primary active at a time
   – ver 3 can propagate PVLANs; ver 1-2 can't (slide 7, PVLANs)

9. [2 marks] Does VTP pruning eliminate (prune) VLANs, loops, or traffic? Explain **clearly**.

   VTP pruning eliminates *flooded* traffic (e.g. broadcast) from nodes that have no ports in the VLAN.

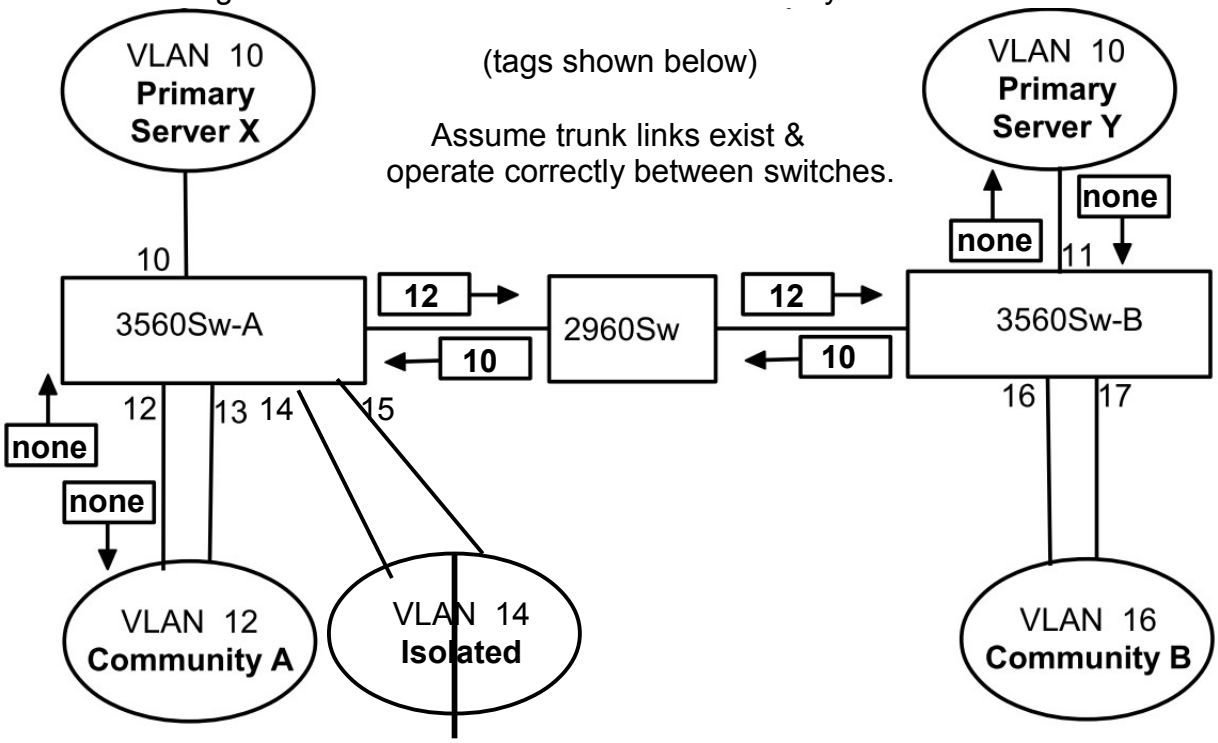
10. [2 marks; Bonus] A 2nd year student is wondering how many actual *types* of BPDU exist (ie have a different *message type*). Help her by **clearly** identifying all the different BPDU types. (Note: this question is **not** asking about different flags available within BPDUs!)

    Only two types of message: Config BPDU (0x00); TCN BPDU (0x80)

11. Examine the following configuration commands deployed identically across a pair of 3560 switches which are joined by trunk links to a 2960 switch.

```
3560Sw(config)# vlan 12
3560Sw(config-vlan)# private-vlan community
3560Sw(config-vlan)# vlan 14
3560Sw(config-vlan)# private-vlan isolated
3560Sw(config-vlan)# vlan 16
3560Sw(config-vlan)# private-vlan community
3560Sw(config-vlan)# vlan 10
3560Sw(config-vlan)# private-vlan primary
3560Sw(config-vlan)# private-vlan association 12,14,16

3560Sw(config-vlan)# interface fastethernet 0/10
3560Sw(config-if)# switchport mode private-vlan promiscuous
3560Sw(config-if)# switchport private-vlan mapping 10 12,14

3560Sw(config-if)# interface fastethernet 0/11
3560Sw(config-if)# switchport mode private-vlan promiscuous
3560Sw(config-if)# switchport private-vlan mapping 10 12,16

3560Sw(config-if)# interface range fastethernet 0/12 - 13
3560Sw(config-if)# switchport mode private-vlan host
3560Sw(config-if)# switchport private-vlan host-association 10 12

3560Sw(config-if)# interface range fastethernet 0/14 - 15
3560Sw(config-if)# switchport mode private-vlan host
3560Sw(config-if)# switchport private-vlan host-association 10 14

3560Sw(config-if)# interface range fastethernet 0/16 - 17
3560Sw(config-if)# switchport mode private-vlan host
3560Sw(config-if)# switchport private-vlan host-association 10 16
```

A. [2 marks] Complete the diagram by filling in the value of the VLAN tags appearing on the frame at each stage of communication between a Community A client and server Y.



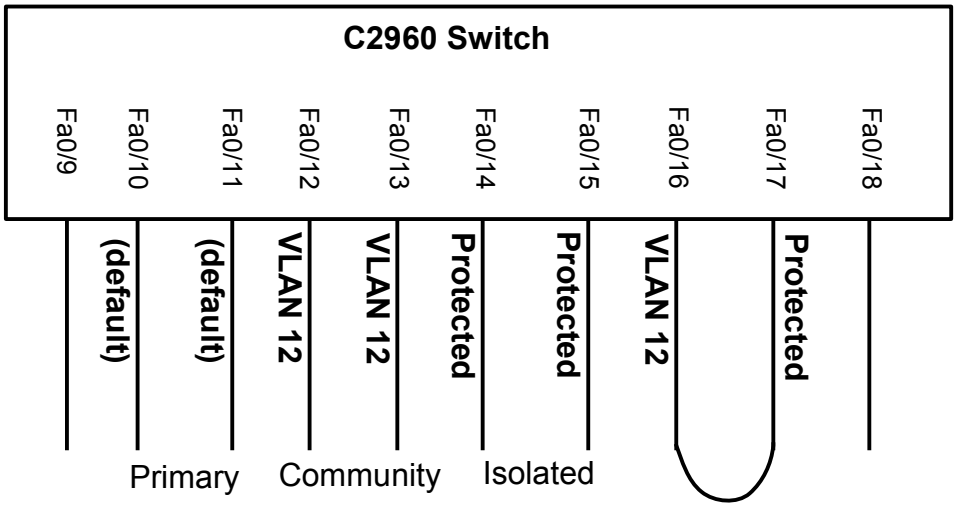
B. [1 mark] There's one critical item missing from the 3560 configuration above in order for Private VLANs to work. What is that missing item? Hint: Think about your lab work.

VTP mode transparent on both 3560 switches, when using VTP ver 1 or 2

C. [2 marks] Identify all possible combinations of DTP modes which would result in successful trunk links between the 2960 switch ports and the 3560 switches.

Auto-Desirable, Desirable-Desirable, Trunk-Auto, Trunk-Desirable, Trunk-Trunk

D. [4 marks] Draw a **clearly** labeled diagram showing how you could use a 2960 switch (which only supports Protected ports) to implement just the portion of the Private VLAN functionality that exists on 3560Sw-A. Be sure to indicate the VLANs and specify the default or any non-default configuration on the ports.



E. [2 marks] From our study of STP, it is clear that BPDUs will need to be completely eliminated from any looped interfaces above.
– What is the command that eliminates all BPDU processing? (format need **not** be exact)
– What is the config context where that command must be applied?

– BPDU filter
– Must be applied to the interface; global mode won't work for this situation

F. [1 mark] The above command only works if a port is in a certain mode. What is that mode?

Portfast

File server

12. [2 marks] We've now encountered multiple examples where *describing* a desired configuration is separate from the command which actually *activates* the configuration. Give one example and **clearly** identify the command which *activates* the configuration.

    port-security: activate with "switchport port-security"
    STP: activate with "spanning-tree mode {pvst | rstp | mst }"
    trunking: activate with "switchport mode trunk"
    access port: activate with "switchport mode access"
    - also accepted: VLAN editing mode and activate with "exit"
    - also accepted: sdm prefer {template} and activate with "reload"

13. **A**. [3 marks] **Clearly** identify the different fields that can potentially be used to load-balance traffic across a single LAG. Be specific.

    [1 mark] single MAC address field: src-mac, dst-mac
    [1 mark] single IP address field: src-ip, dst-ip
    [1 mark] combo address fields: src-dst-mac, src-dst-ip
    Do **not** confuse the load-balance *field* with the load-balancing *algorithm* (XOR, hash)

    B. [2 marks] Pick one of the load-balancing options you listed above and **clearly** describe one of more scenarios where that options would (hopefully) provide good balancing.

    Several scenarios exist; simplest is many hosts accessing a common network resource

    (multiple hosts) → (balance with src-addr)
    going to common resource →
    ← coming from resource
    (balance with dst-addr) ← common resource

14. [1 mark] Identify in a list all the differences between configuring Cisco L2 and L3 LAGs.

    Config is very, very similar: links must all be configured the same (speed, duplex, etc)
    So essential difference is that L3 ports have "no switchport" applied
    - also accepted: L3 LAG has an IP address assigned to it

15. **A**. [0 marks] Which performs "better": a switch with *many* fast ethernet ports connected as a LAG or a switch with just a few gigabit ethernet ports (but which can't be put in a LAG)?
    B. [3 marks] Explain your reasoning, with reference to specific attributes or limits on each system.
    For full marks, must identify at least 3 points, e.g. speed, STP, redundancy, load-balance

    Speed: max speed for a LAG is 8x (i.e. 8x100Mbps), so a GigE is faster
    BUTcan match with *multiple* LAGs (though this requires *lots* of ports!!)
    STP: using LAG may allow the elimination of STP in the case of a single "link"
    Redundancy: LAG potentially offers much better redundancy (and graceful degradation)
    Load-balancing: both a blessing & a curse:
    – if balancing method is poor, may obtain no better than single link speed from LAG!
    – if trunking, can reach GigE speed with multiple LAGs which load-balance per VLAN

16. [5 marks] Carefully read the article from this past weekend about a new, *real problem* and then answer the questions.

An attacker compromised over 5,000 IoT devices on a campus network -- including vending machines and light sensors -- and then used them to attack that same network. "In this instance, all of the DNS requests were attempting to look up seafood restaurants," reports ZDNet, though the attack was eventually blocked by cybersecurity professionals. Verizon's [manager of investigations] blames the problem on devices configured using default credentials -- and says it's only going to get worse. "There's going to be so many of these things used by people with very limited understanding of what they are... There's going to be endless amounts of technology out there that people are going to easily be able to get access to."

The article suggests "ensuring that IoT devices _____[omitted]_____ " But it ends by warning that "until IoT manufacturers bother to properly secure their devices -- and the organizations which deploy them learn to properly manage them -- DDoS attacks by IoT botnets are going to remain a huge threat."
https://mobile.slashdot.org/story/17/02/11/2250218/college-network-attacked-with-its-own-insecure-iot-devices

A. In what layer of the network heirarchy do the IoT devices reside?

[1 mark] They reside in the *access* layer

B. Would any STP features be helpful in preventing this type of problem? If yes, give clear details of which feature(s) would help and why/how.

[1 mark] Not really; STP prevents loops but does **not** block connectivity

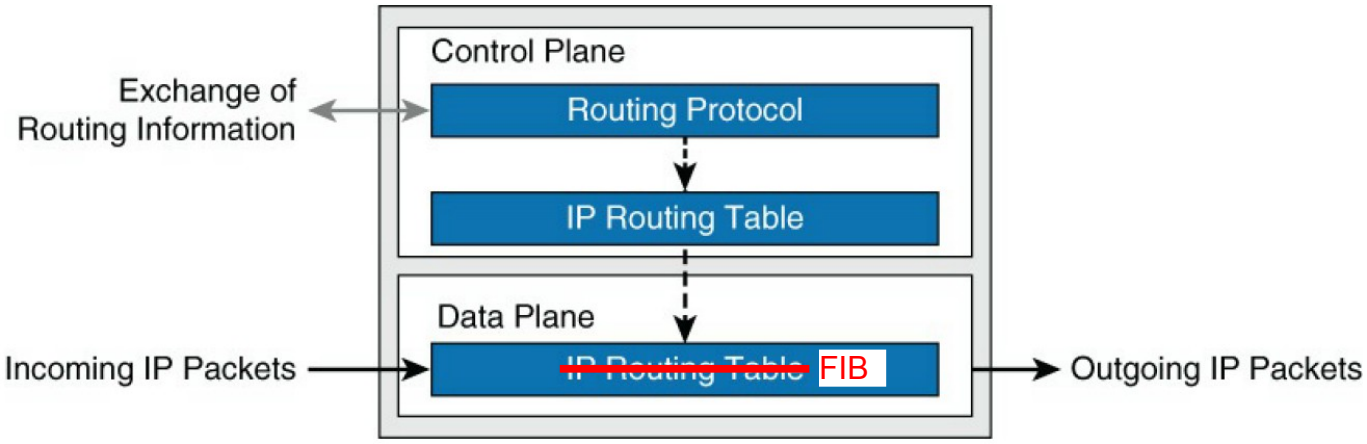
C. The original article suggested how to prevent this problem; it was removed for the purposes of this test. **Clearly** describe two techniques or methods (from the material that we've covered so far in the course), that might help prevent the IoT devices from interfering with the rest of the network?

omitted text: IoT devices *are on a completely different network* to the rest of the IT estate
1 mark per correct option; max 2 marks
– an ordinary VLAN: the IoT VLAN (yet another one to add to our VLAN list)
– Private VLANs: all IoT devices could be *isolated* hosts
– "protected" ports achieve same result as PVLAN isolated hosts

D. From your knowledge of the definitions for each layer in the network hierarchy, what layer would be responsible for enforcing additional security to prevent interference from IoT devices?

[1 mark] *Access layer* is generally where (security) policy relevant to this kind of device is implemented & enforced;
e.g. it would contain ACLs (and/or rate limiting) to define (restrict) allowed behaviour
Ref: FLG p. 13; Ch 2 slide deck, slide 8

17. [1 mark] The diagram below is an exact copy of Fig 2-16 from p. 29 of the FLG, showing details of a Cisco L3 Switch. Examine it carefully. From your knowledge of L3 switches, **clearly** identify and correct the mistake in the diagram.



Cisco L3 switches have a **FIB** in the Data Plane, not a routing table!

18. [2 marks] **Clearly** explain as much as you can about the command "*switchport host*". Refs: FLG p. 57, STP enhancements slide deck; Lab 5.1

[1 mark] It's a macro, so you will never see "switchport host" in the running config
[1 mark; require at least 2] It sets port to: access mode, portfast, disables LAG

19. [2 marks] The FLG says on p 194: "Do not use Loop Guard in combination with BPDU Guard." Perhaps this is another error in the textbook, and should instead say something like "Loop Guard is best used in combination with BPDU Guard." Indicate which is the correct statement and **clearly** explain **why**.

The original statement is correct:
Loop Guard *requires* receiving BPDUs to operate properly, whereas
BPDU Guard will error disable (shutdown) a port if a BPDU is ever received
(i.e. there should normally *never* be any BPDUs received).
As a result, they require exactly opposite conditions for the port to operate normally.

20. **A**. [1 mark] **Clearly** explain the effect of the command "switchport" or "no switchport".

Command simply changes the port to operate in Layer 2 mode ("switchport" – switched) or Layer 3 mode ("no switchport" – routed).

B. [4 marks] Give a complete list of steps that will be performed on a frame received on an interface configured with "no switchport". Tip: You can have the answer to part A, but you will forfeit the associated marks. Ref: Ch 2 slide deck, FLG p. 28

[1 mark per correct phase, as shown below: ingress, IP header, routing, egress]

ingress
1. Check CRC (if bad, drop, done); check dest MAC addr (if not me, drop, done); strip L2 framing
2. Check for VLAN tags and strip them (there may possibly be some processing) L3 Packet modified / re-written

IP header
3. Check IP header details: verify checksum and if okay then check destination IP if dest IP is me, punt up to Control Plane, done; else continue forwarding!
4. Decrement TTL count by 1; if now 0, punt up to Control Plane for ICMP msg L3 Packet modified / re-written
5. Recalculate Checksum in IP header L3 Packet modified / re-written

route
6. Check routing table for best longest(!) match to destination IP

egress
7. Determine encap required for egress interface: Dest MAC, Src MAC, (VLAN ?) L2 frame modified / re-written
8. Compute CRC and add to egress frame L2 frame modified / re-written

21. [3 marks] Page 1 of the CCNPv7 Lab 4-2 states: "Cisco switches like those used in these labs allow only a limited number of PVST instances – usually 128."
A. **Clearly** explain the impact on this factor on the choice of VLAN design in a campus.

This can limit the total # of VLANs possible in end-to-end OR
increase the cost of the network (need more expensive switches!)

B. **Clearly** and fully describe at least one other **disadvantage** associated with a campus VLAN design having the large number of VLANs.

Ref: FLG p. 46-49; slide deck for Ch 3, slide 10
Choose from: more complicated management; more extensive broadcast propagation; more difficult to troubleshoot

C. What method(s) exist(s) to avoid the PVST limitation given above?

Use MST to group VLANs and stay within the 128 instance limit
(Assuming **all** campus switches are capable of MST!)

22. [2 marks] A second year student is confused and struggling with MST in the new CCNA curriculum. He's been told to use VTP to ensure all switches are synchronized to the same parameters. It is **not** working, so he checks the configuration:

```
DLS1# show span mst config
Name      [CCNA]
Revision  1              Instances configured 2
Instance  Vlans mapped
--------  ---------------------------------------
0         1-98,101-4094
1         99-100
-------------------------------------------------
```

He uses "**`show vtp status`**" on the other switches and finds that the revision number is higher than 1. Is the student heading down the right path? Explain **clearly** why or why not.

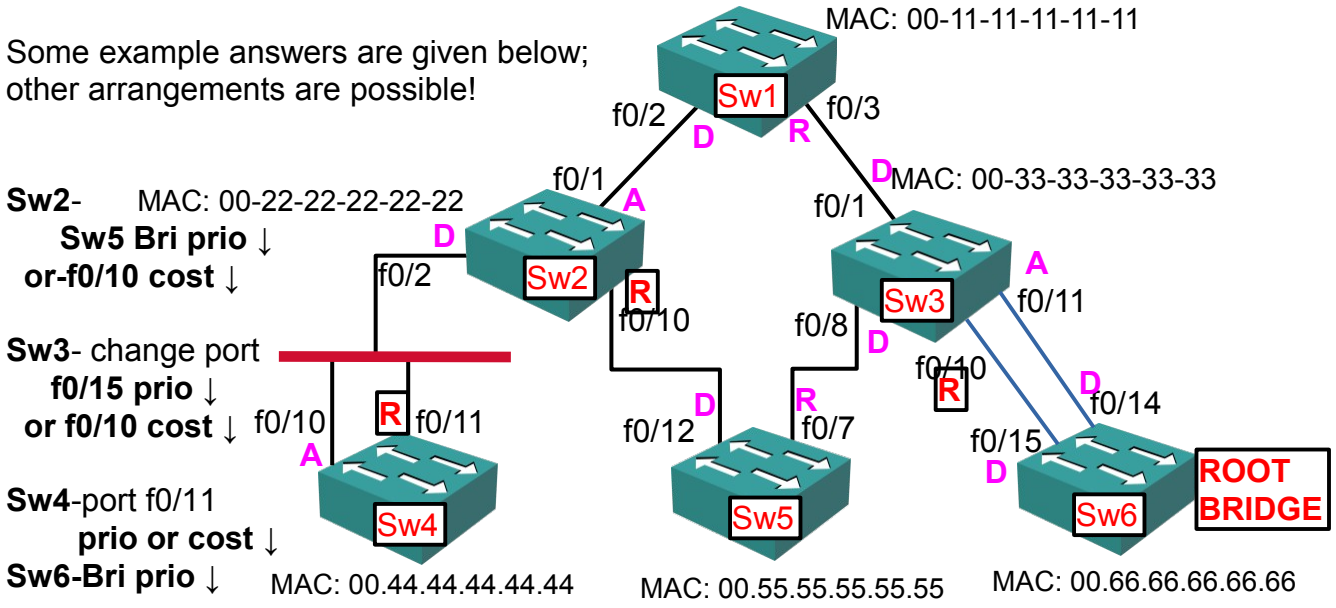
No, he's not. *The two "revision" numbers have nothing to do with each other*.
In MST, it is a static admin-configured value; in VTP it counts the number of changes.

23. [1 marks] The second year student is still struggling with MST. Unfortunately he's never had Mr. Anderson as a Prof. He's busy typing all kinds of MST config and does a "do show run" from time to time, but *nothing* ever changes in the displayed config. Please, suggest something helpful so the student can *get the correct results* as required in the lab.

MST config is an editing mode, just like VLANs; you must *exit* for it to take effect!
Alternatively, use *show pending* from the MST config context
Note that some config is *never* stored in the running or saved config;
as you have hopefully noticed, this can be especially true for VLAN config & info.

24. **A**. [4 marks] Carefully examine the Cisco network topology below. All values are at default. Label the diagram with the (fewest possible) changes to priorities and costs to achieve the four (4) indicated bridge and port roles.

Some example answers are given below; other arrangements are possible!



B. [2 marks; Bonus] Now review your changes carefully! Let's add one more requirement: fa0/2 on Sw1 must be Designated. Modify your changes, if/as necessary, to achieve this while preserving all other conditions. If no changes are necessary, write "no change" below.

With rare exceptions, *no change* is required since Sw1 is a full layer closer to root bridge

C. [2 marks] Write the RST port roles for all ports where it is not already indicated.

As shown above

D. [2 marks] What is the Root Path Cost that is advertised out port fa0/2 of Switch 2?

Cost to root is *cumulative*: with unaltered costs: 19 (Sw6→Sw3) + 19 (Sw3→Sw5) + 19 (Sw5→Sw2) = 57

25. [2 marks] You've surely studied very hard for this test. It's equally certain that there's an area or topic for which you studied that's been completely omitted from this test. At your option, you can **clearly** state both a question and the correct answer and receive full credit (maximum 2 marks). Remember: it must be a topic or area **not** covered at all in this test!

[1 mark per item]

Generally, any question from NET3011 course material is acceptable, with the proviso that T/F questions, or answers providing only 2-3 words are worth at most 1 mark. Remember that your question must actually be *answered* (indeed, some students don't actually answer what their question asks).

Extra Work