Test 2: NET3011 – Advanced Switching

Winter 2015

Time: 60 minutes; Test scored out of: 43 Total Marks available: up to 46
(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 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. Make note of multi-part questions! Hints or answers *may* be available to assist you with later parts, but you will *not* get any credit for the parts where help is given.

4. Where there is ambiguity, assume that questions are referring to output, configuration, commands, and features on Cisco switches and routers.

5. 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. [1 mark] **Clearly** identify where STP is used within Cisco's 3-layer Hierarchical Network Model.
   Definitely within the Access layer, and reaching up into the Distribution layer.
   Usage in the core is unlikely except for small campuses. Check p. 31 & 33 for "layer 3".

2. [1 mark] What are the possible choices for the VTP mode when using pVLANs on 3560s?
   Only transparent

3. [1 mark] **Clearly** explain why a switch running MST in an all-Cisco environment is very likely to become the root bridge if all other switches are running RSTP.

   Bridge priority does **not** include VLAN ID, and thus is lower than RSTP priorities.

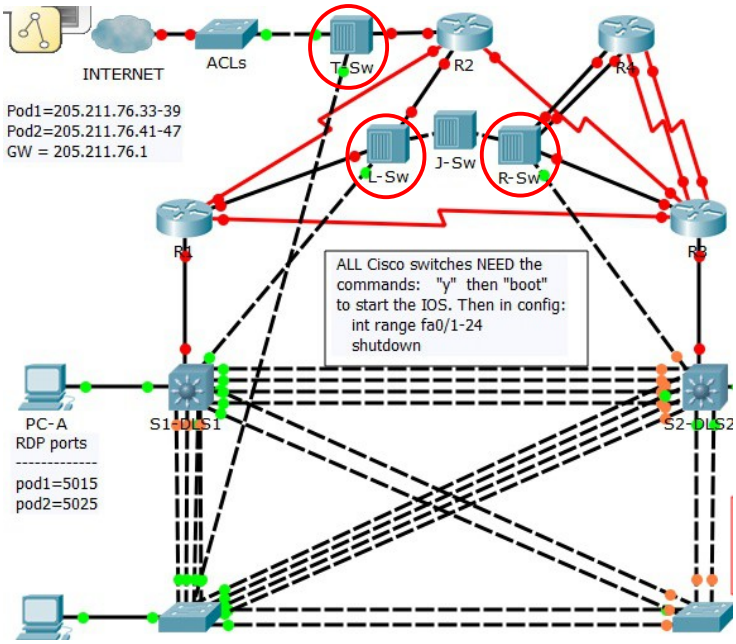
4. [1 mark] Use **clear**, concise wording to identify which VLAN carries traffic along the path to its destination in a pVLAN setup.

   "Traffic follows the source VLAN until the final egress interface."

5. [2 marks] NetLab is designed to be totally flexible, without imposing any restrictions on choice of IP addresses, VLANs, sub-interfaces, etc.

   For implementing NetLab, a set of cheap $10 switches is used to create extra connectivity (ie. "T-Sw", "L-Sw", "R-Sw" as circled). These switches are "dumb" and do nothing other than forward traffic based on destination MAC. They're used despite the availability of plenty of spare ports on the 2950 "ACLs" switch which could be used with 3 separate VLANs.

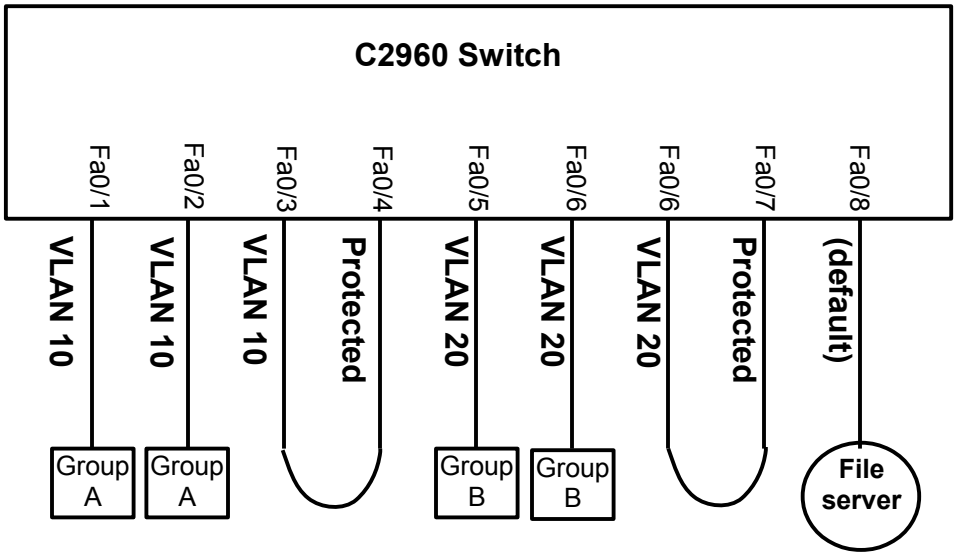
   Why was this choice **necessary**?



(Hint: Hopefully you paid attention during the pVLAN lab, where you joined two 3560 switches with a 29xx switch in the middle. What was needed for things work to?)

VLAN-aware switches drop traffic for VLANs they don't know. It's not possible to know what VLANs a person will choose, so traffic would inevitably be dropped.
(Also, switches have a limit <4094 for the number of VLANs that can be configured (eg. 255 for 2960's) so it's simply not possible to configure every single VLAN.)

6. [4 marks] Show your mastery of pVLAN concepts by implementing a simplified version of a pVLAN on a 2960 switch, using one or more protected ports. Draw on the diagram below and label ports to **clearly** indicate how to create the equivalent of two different communities which both access a file server.
(Answer on diagram)



[2 marks] If you've answered the question correctly, there may be a problem with the switch receiving unexpected or "conflicting" BPDUs. What command will completely eliminate BPDUs to solve this problem? **Give** the (kind of) command, and the required CLI context.

Apply BPDU filtering at the interface level, so **all** BPDUs are dropped/ignored.
(eg. Sw(config-if)# spanning-tree bpdufilter enable #But *global* config doesn't work!)
(Will also accept Sw(config)# no spanning-tree VLAN 10)

7. [3 marks] "Flexlinks" have at least one major advantage over all other redundancy technologies that we studied. They also have at least one distinct disadvantage. Finally, they have potential "danger" to the proper functioning of the network. **Clearly** explain each.

Advantage: fastest fail-over time: 50 msec; much lower than all STP variants
Dis-advantage: can not load-balance or make use of spare link, so more costly ($$$)
Danger: completely dis-ables STP, so Designer responsible for ensuring no loops!

8. [6 marks] You've hopefully memorized the steps in the STP port election process:

To elect the **root port**, the following criteria are used in order:

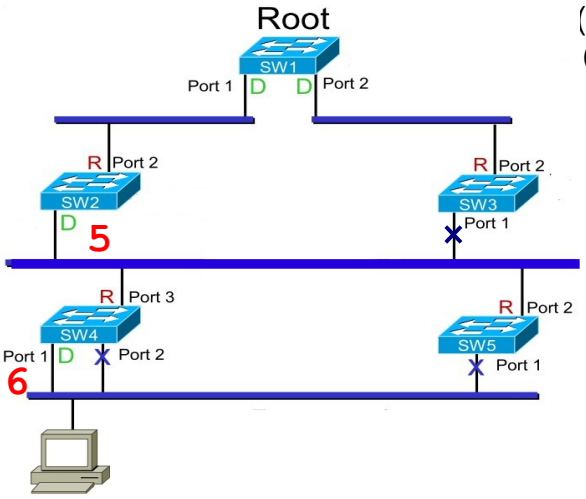
1. Accumulated Cost to Root bridge
2. Bridge ID
3. Port ID (of sender)
4. Port ID (of local switch)

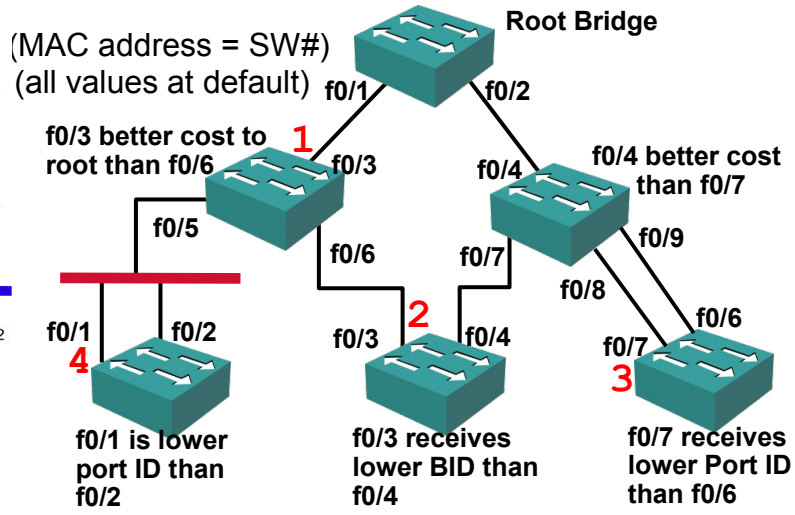
To elect the **designated port**, the following criteria are used in order:

Lowest cost to root

5. Bridge ID
6. Port ID

To prove your understanding of these elections, draw 1-2 (or more) small topology diagrams and **clearly** identify **where** in the topology each rule becomes the tie-breaker in the election process.





From STP-1, slide 34 From STP-1, slide 25 **AND** lecture notes!

ALL settings at default, unless otherwise noted

9. A. [2 marks] Ensuring and protecting the placement of the root bridge within a network topology is important from both the perspective of performance as well as security. **Clearly** explain the reasons why.

Performance: ensure it's centralized so traffic traverses fewest and highest-speed links
Security: to ensure that hackers don't siphon off traffic towards a spoofed root bridge, the root bridge should not be allowed at the network edge (ie. protected with root-guard!)

B. [1 mark] What STP command protects lower-level bridges from "over-throwing" the root bridge?

root guard

10. [8 Marks] While studying the main categories of L2 security attacks, we looked at five attacks that relied on spoofing of one type or another. Give the following information about **at least four** spoofing attacks: (1) name and briefly describe the type of attack; and (2) **clearly** explain how it can be prevented. You are encouraged to include specific Cisco command(s) in the second item. *Quality counts!!*

4 L2 Spoofing attacks: (A) Name & description; (B) Prevention method

~2 marks per type of attack, up to a max of 8 marks. I'm typically looking for correct info to **give** marks rather than looking for reasons to deduct marks.

1. MAC spoofing: spoof the MAC address of a valid host already known in switch MAC table; fix with DHCP snooping or port security

2. VLAN attack: spoof a switch to get traffic from extra VLANs; fix: static access/trunking

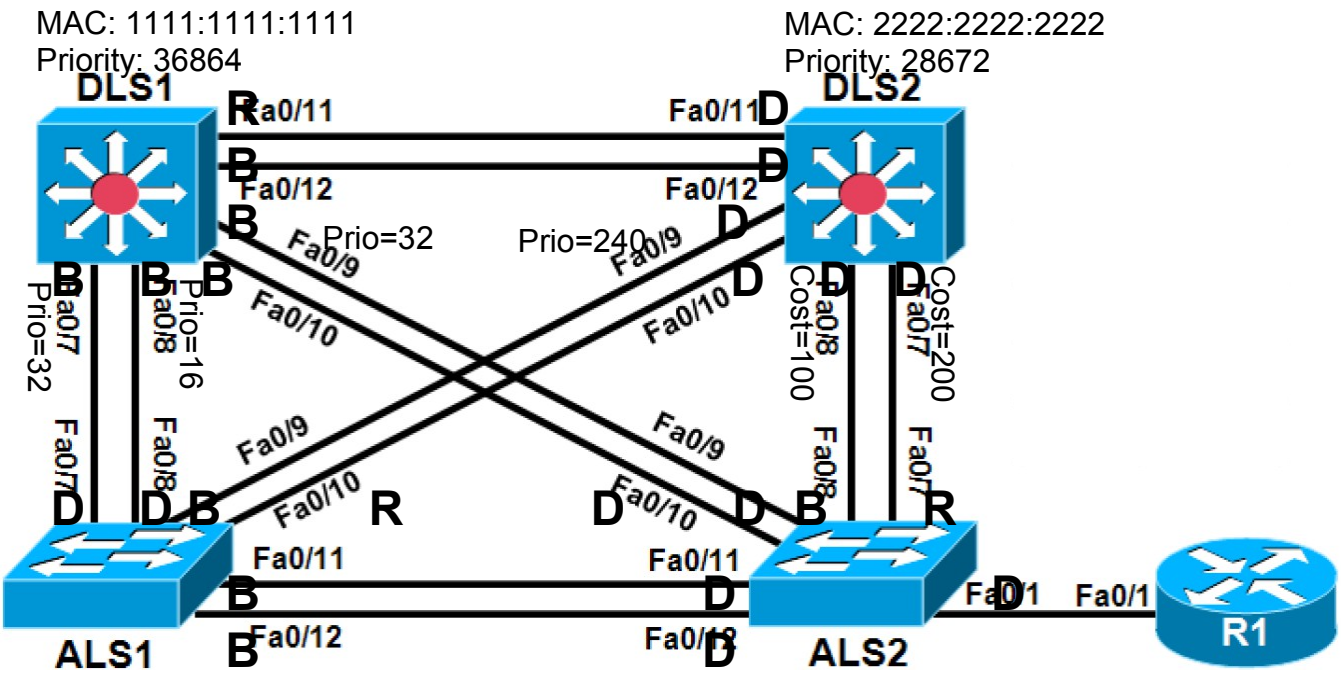
3. DHCP server spoofing; fix with DHCP snooping

4. IP address spoofing; fix with IP Source guard **added to** DHCP snooping

5. ARP spoofing; fix with Dynamic ARP Inspection (DAI) **added to** DHCP snooping

Also accepted: MAC flooding: spoofing the existence of many, many devices; fix with port-security

11. Study the topology diagram below carefully. All parameters are at default unless indicated.
(anchor for hidden text)



A. [1 mark] ALS2 uses all default settings except that Fa0/1 is set as portfast. Does R1 receive BPDUs?

Yes, otherwise there would be no need for BPDUfilter on an interface!

ref: slide 48; http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10586-65.html

B. [2 marks; 1 per **pair**] Identify the STP role for every device and port in the topology:
1. Circle the root bridge. 2. Draw the letter R(oot), D(esignated), or B(lock)

DLS2 = root bridge; all other ports as shown in diagram.

C. [2 marks] I do not want any odd numbered ports as Root ports. What change(s) can satisfy this requirement (other than shutting down the port!)

Change costs of local ports: OR Change priority of upstream ports:

decrease local cost of even ports OR decrease port priority of upstream even ports
OR increase local cost of odd ports OR increase port priority of upstream odd ports

12. A. [1 mark] What is the primary technical reason for using portfast?

    To allow DHCP messages to get through immediately upon connection.

    B. [2 marks] There are four different combinations / variations for deploying of portfast. **Clearly** identify the four, **and** identify the response upon receiving a BPDU.

    Portfast only: goes to Blocking mode (bounce port or wait for a timeout interval)
    Portfast with BPDU guard: goes to error disable mode (bounce port to release)
    Portfast with BPDU filter - applied globally: port reverts to normal non-portfast operation
    Portfast with BPDU filter - applied to interface: "nothing"; BPDUs are completely ignored!

13. [3 marks] STP has three port roles: blocking, designated, root. RSTP adds two more port roles. **Name** the new roles, and then **clearly** define or explain each one. [Hint available]

    STP, slide 71
    [1 mark] Alternate and Backup
    Backup is a non-designated port on the same segment as the designated bridge.
    Alternate is a non-designated port on a different switch than the designated bridge.

    B. [1 mark] The two new RSTP port roles don't exist in 802.1D. In what state would these same ports be if 802.1D is running instead of RSTP?

    Blocking

14. [2 marks] If you've studied properly for this test, there must surely be a question you were expecting that has not been asked. **Clearly** state a **security-related question** and the correct answer. The question must be worth (at least) two marks, and must not be a repeat from a previous test this semester.

    Any question that is clearly stated and followed with a clear & correct answer is eligible for marks. One mark will be given for each substantial item in the answer. Note that only a single question may be used, and must be security-related as specified above.

    Examples include: port states for 802.1x; response modes for port-security (in order!); other questions relating to 802.1x; etc.

Additional work, notes, or rough work