Test 2: NET3011 – Advanced Switching

Winter 2014

Time: 50 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. (The only exception is ASL interpreters.)

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? ___________________________ Student Id? __________________

(Continued on next page)

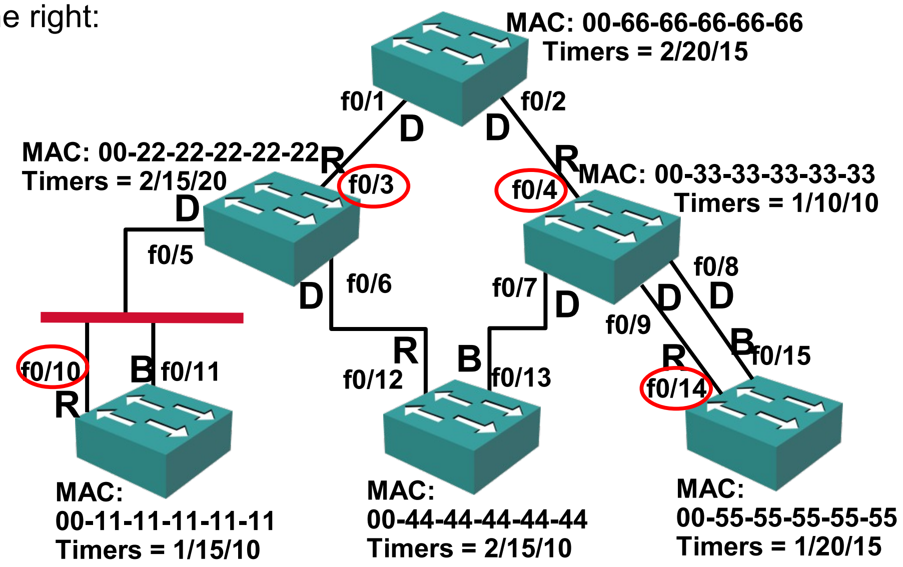
1. In the network topology on the right:
(anchor)

– Bridge priorities are set to different values, all of them higher than default

– Port costs are configured equal to the port # (ie. cost fa0/12 = 12)

– Port priorities are set to default values

– Timer values are set to all different values as shown.



A. [2 marks] Give a clear diagram of the BID field in the BPDU. Referring to the diagram, **clearly** explain why you *do* or *do not* have enough info to determine the root bridge.

Do **not** have enough info: Bridge Priority is the MOST significant 4 bits of the BID!

Priority (4**bits**)	Ext/Vlan (12**bits**)	MAC Address (6 **BYTES**)

B. [1 mark] Your must ensure the root bridge is the switch at the top. What command do you use (for Cisco switches)? [Must be mostly correct but spelling mistakes are allowed.]

```
spanning-tree vlan 1 root primary
```

C. [5 marks] Assume the top switch is the root bridge and clearly indicate the port state of all interfaces. **R** = Root, **D** = Designated, **B** = Blocking / Alternate

D. [2 marks] What cost would the bottom-left and bottom-right switches advertise to downstream switches?

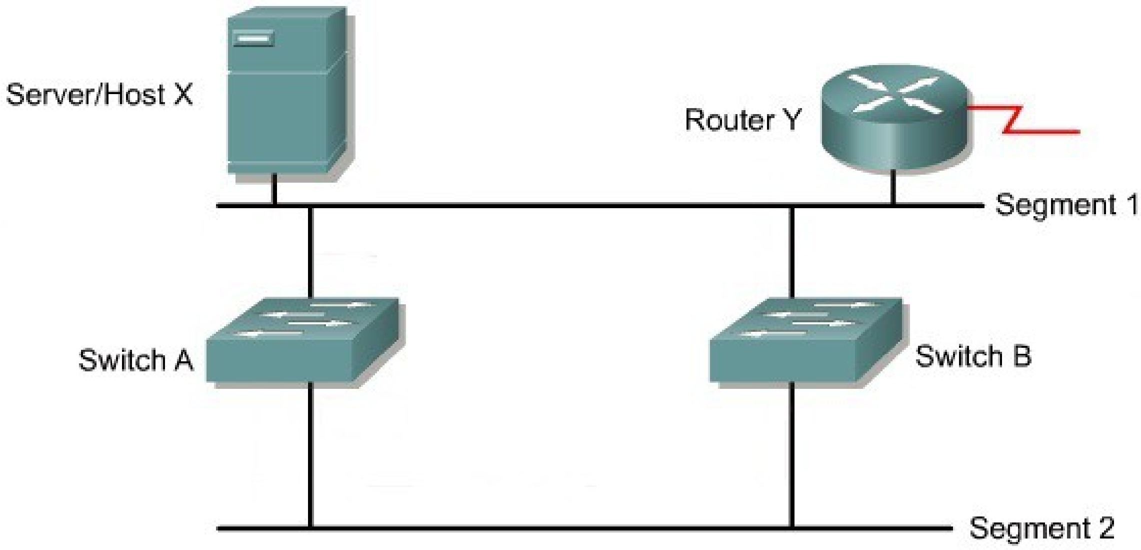
Bottom Left = 3 + 10 = 13; Bottom Right = 4 + 14 = 18

E. [1 mark] **Clearly** explain how the STP timer values are selected during the election(s).

STP timer values are simply copied from the root bridge, ie. 2/20/15 for this question

2. [1 mark] Every switch running STP has:
(a) at most one root port **correct**; the root bridge has no root ports (all Designated)
(b) exactly one root port
(c) at least one root port
(d) always more than one root port
(e) None of the above

3. A. [1 mark] The network below does **not** have any form of STP enabled. **Clearly** illustrate a broadcast storm by tracing the path of a frame as it travels through the network. Ref STP-1, slide 7



A broadcast frame sent from Host X would form loop(s), ie. counter clockwise through switch A, then B, then A, … and clockwise through switch B, then A, then B, ...

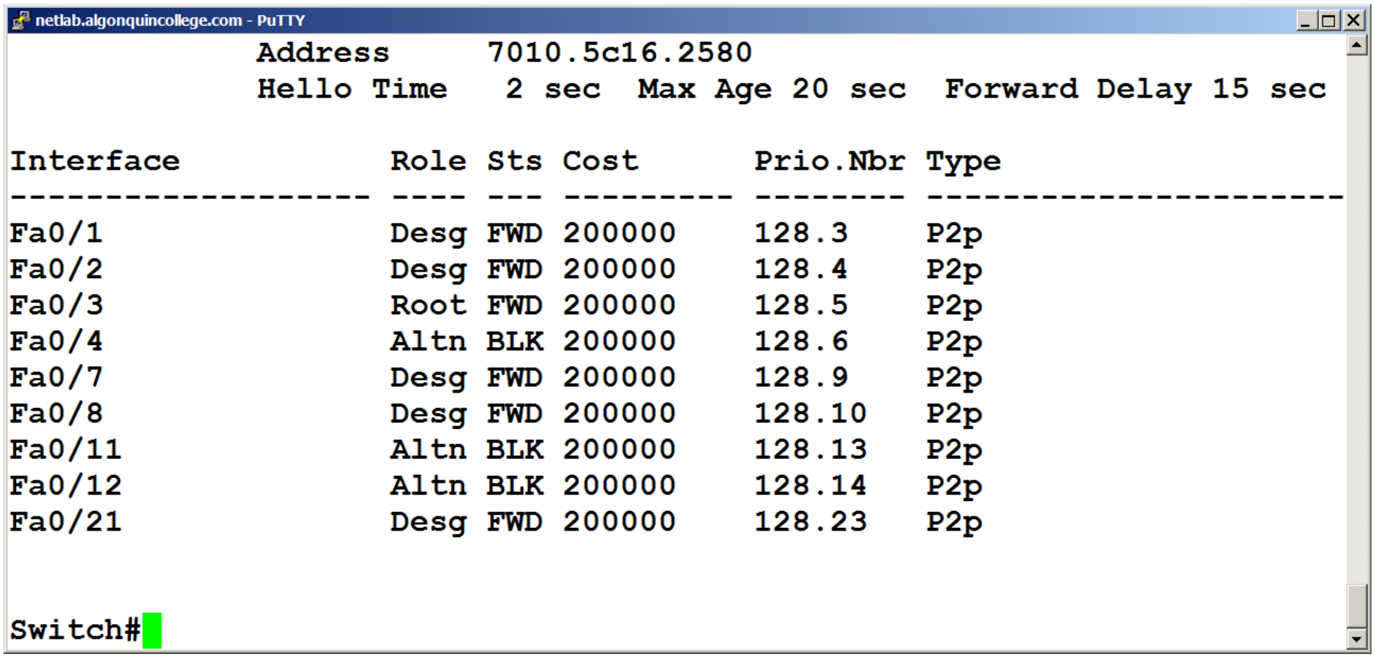
B. [1 mark] Give specifics about the actual (type of) frame that could cause such a broadcast storm.

An ARP or DHCP frame are just two examples of common broadcast frames in a LAN

4. [2 marks] A root bridge has a 10Mbps, two 100Mbps, three 1Gbps interfaces running STP. What is the cost *advertised by the root* in the BPDUs sent out each of these interfaces? If the answer depends on the type of STP running, explain whether the answer changes. Ref: STP-1 slide 26

The root always sends out BPDUs with an advertised cost of 0 (regardless of i/f speed)
The advertised cost always means "Once you reach (this bridge), the additional cost to get to the root is [advertised cost]."

5. [2 marks] Below is a screen shot of "show spanning-tree" output. Unfortunately the window size was so small that many lines scrolled off the top. Using your experience from lab work, what kind of STP is running? Give the common name as well as the official IEEE standard!



```
             Address     7010.5c16.2580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Fa0/1               Desg FWD 200000    128.3    P2p
Fa0/2               Desg FWD 200000    128.4    P2p
Fa0/3               Root FWD 200000    128.5    P2p
Fa0/4               Altn BLK 200000    128.6    P2p
Fa0/7               Desg FWD 200000    128.9    P2p
Fa0/8               Desg FWD 200000    128.10   P2p
Fa0/11              Altn BLK 200000    128.13   P2p
Fa0/12              Altn BLK 200000    128.14   P2p
Fa0/21              Desg FWD 200000    128.23   P2p


Switch#
```

MSTP = IEEE 802.1s; on Cisco switches, it's the only version with BIG costs

B. [2 marks] In the output that scrolled off the top of the window, there were **two** other indicators for the type of STP running on a Cisco switch. What are the other indicators?

At least two indicators (three actually): the spanning tree instance is "**MST**00"
"Spanning tree enabled protocol **mstp**"
"Bridge ID Priority 32768 (priority 32768 sys-id-ext **0**)" – **0** only occurs for MSTP

6. [2 marks] The textbook and slide deck identified the best practice of disabling telnet in order to prevent switch attacks, but the chief Network Architect of your organization insists that telnet is required for other reasons. What are two methods are available for providing a measure of security for telnet sessions?

Use management VLAN, use VACLs
Also acceptable: use ACLs on the vty line(s)

7. [2 marks] Two students are studying for a test in NET3011. One is explaining to the other that the only purpose of STP is to create an optimal path for frames through a redundant layer 2 network. He's mistaken. **Clearly** explain two reasons why! Ref: STP-1, slide 14

1. Not necessarily optimal to destination; only optimal to root!
2. Main purpose of STP is to provide loop free topology
3. Network need not be redundant to obtain protection from STP: will protect against broadcast storms if two edge ports are accidentally connected together!

8. Consider the following configuration commands:

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

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

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

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

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

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

A. [5 marks] For each of the interfaces 12-17, **clearly** identify which other interfaces they may communicate with. Hint: drawing a diagram will likely help in finding the answers.

(anchor)

F0/12: F0/10, F0/11, F0/13

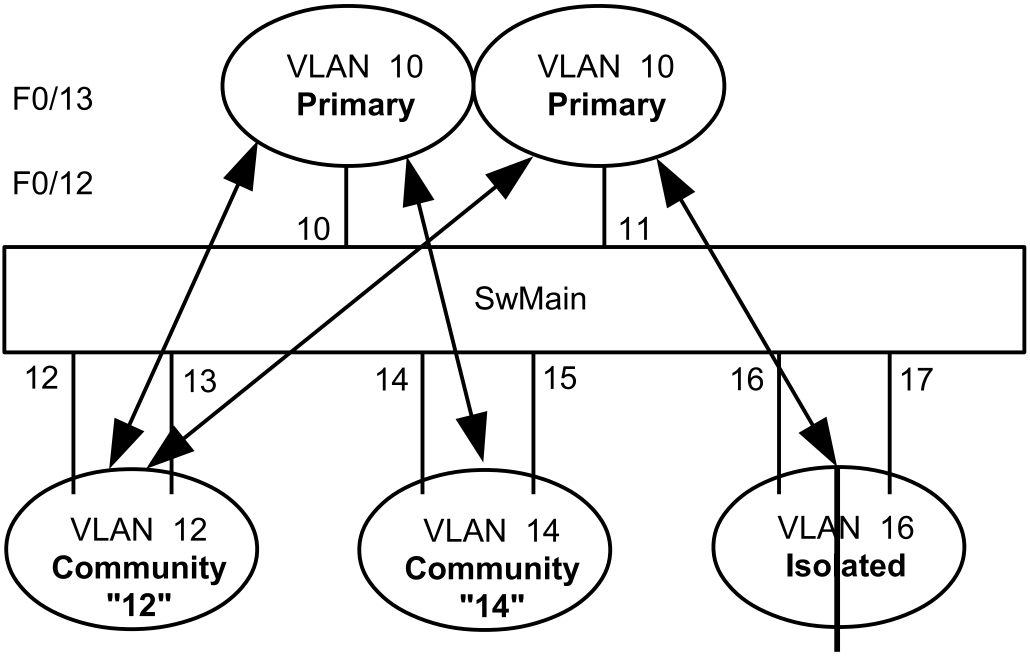
F0/13: F0/10, F0/11, F0/12

F0/14: F0/10, F0/15

F0/15: F0/10, F0/14

F0/16: F0/11

F0/17: F0/11



B: [1 marks] Name (or **clearly** describe) the specific type of attack for which pVLANs provide protection. Ref: Ch 6 slides 9, 46

pVLANs can help mitigate both: attacks between devices on a common VLAN, and VLAN Hopping attacks on trunk links

C. [2 marks] Could VACLs be configured to provide equivalent protection as the pVLAN configuration given above? Comment (briefly) about the feasibility of doing so.

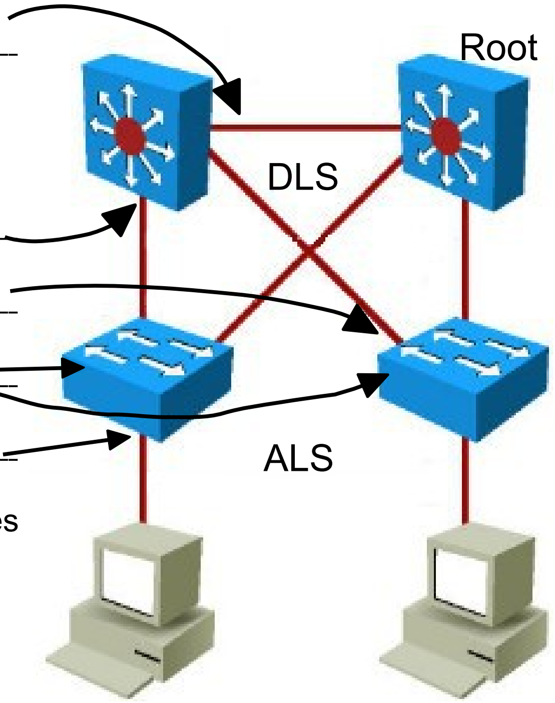
pVLANs are configured based on switch ports, without reference to MAC or IP address. VACLs are configured based on MAC and/or IP address, and apply to an **entire** VLAN, without reference to specific ports. Based on that, the two are *very* different.
Only in a scenario where the host equipment was essentially fixed (ie. not mobile hosts) could VACLs approximate pVLANs. This would, however, be much more challenging to configure and verify for accuracy, and certainly more tedious to update if/when ever equipment changed.

9. A. [7 marks] Pictured below is the portion of a network at the distribution and access layer. From the chapters on STP and Security, name all* the **options** and **features** that should be applied to the interfaces, or switch, to maximize network security and stability.

(1) Loop Guard or UDLD-aggressive
(Backbone-fast no use since no higher-level Sw)

(2) Root guard, UDLD-aggressive (L.G. no good!)
(Backbone-fast no use since no higher-level Sw)
(2) Loop Guard or UDLD-aggressive; Uplink-fast;
DHCP snoop trust; DAI trust
(1) DHCP snooping; DAI; possibly VACLs also

(5) access, Portfast, BPDU or Root guard, port sec;
IP source guard; 802.1x; [3 marks]



* The leading number indicates the number of features that should be applied. If you think there's more, explain why (for bonus marks).

More *are* possible, as above plus others

B. [2 marks] In the network shown, is there some way to completely disable STP while still preserving redundancy between the Access and Distribution layers? If yes, how? If not, why not? Be **clear** and specific.

Yes. A flexlink pair would be configured for each of the access switches.
Note that using flexlinks has the disadvantage of eliminating any possibility of load balancing over the two uplinks on each access switch.

10. [3 marks] **Clearly** define and distinguish the three response modes for port security.

Protect: Simply disallow (by discarding) any frames from the extra MAC addresses

Restrict: disallow (by discarding) any frames from the extra MAC addresses **and** report the violation via syslog and by sending an SNMP trap

Shutdown: enforce the configured limit on MAC addresses by putting the interface into the **errdisable** state, thereby dropping **all** frames from all hosts.
The violation is reported in syslog and by sending an SNMP trap.

11. [2 marks] If you've studied properly for this test, there must surely be a question you were expecting that hasn't been asked. **Clearly** state both a security-related question and the correct answer. The question must be worth (at least) two marks, and must not be a repeat from either of the two tests 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.

Additional work, notes, or rough work