Test 2: NET3011 – Advanced Switching

Winter 2013

Time: 50 minutes; Test scored out of: 45 Total Marks available: up to 48
(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. 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. [1 mark] Which of the following is **not** a valid load balancing criterion?
   (a) dst-ip
   (b) dst-mac
   (c) src-dst-ip
   (d) src-dst-mac
   (e) all of the above are valid criteria **correct**

2. [2 marks] Give at least two **clear** reasons why 802.1Q is the preferred standard for VLAN trunking.

   There's lots of possible answers:
   – Open (IEEE) standard not proprietary
   – Better support for QoS
   – Less overhead (ISL adds 30 bytes; 802.1Q adds only 4 bytes)
   – ISL is deprecated and not supported on all Cisco equipment

3. [2 marks] One day, Anderson and Smith are working together in T108. Anderson connects a pair of 2960 switches and immediately gets a trunk link. Smith connects his pair of 3560 switches but does **not** get a trunk link. **All** switches are completely in their default state. **Clearly** explain the reason for these results.

   Some switches (eg. Anderson's) have default values "dynamic desirable" for trunking. Other switches (eg. Smith's) have default values "dynamic auto", which won't trunk if they're the only switches at both ends of the link.
   Also accepted (but not the main thrust of the question): 3560's support both 802.1Q and ISL, so encap type may need to be set before trunking will succeed.

4. [2 marks] What is a typical re-convergence time for MST? **Justify** your answer (… or else you get 0 marks).

   MST converges exactly as fast as RST (ie. typically a *few seconds*) because it *uses* RST. It therefore converges *much faster* than CST (ie. the original 802.1D).

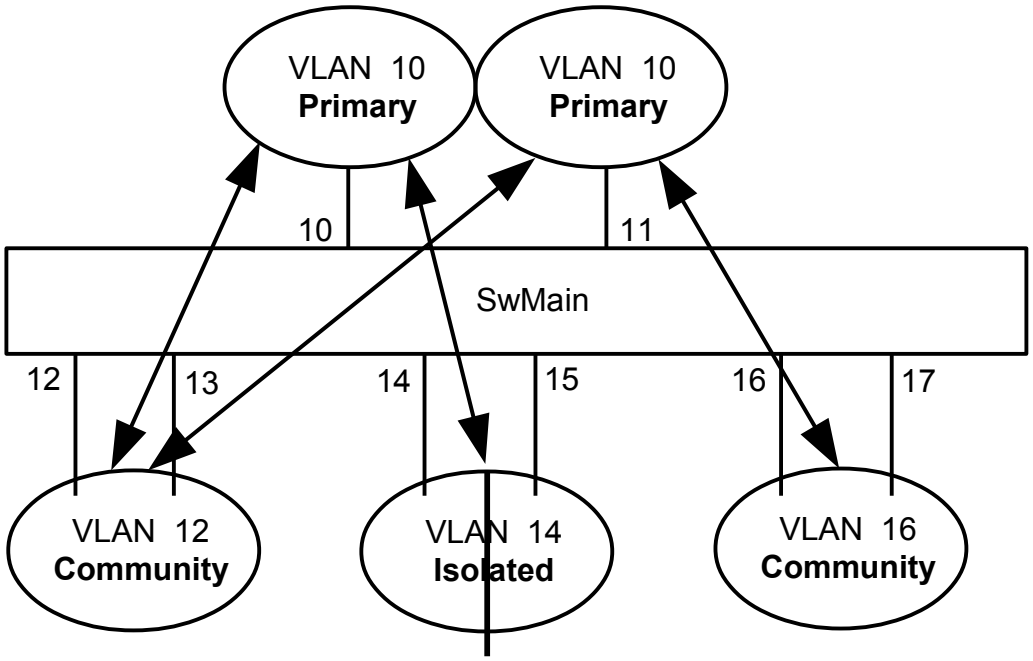
5. [2 marks] A L2 network incorporates many "best practices": it has the 5 different types of VLANs, splits user traffic into 4 different VLANs, and has redundancy because each switch has 2-3 trunk links. What is the optimal number of MST instances for this network? **Justify** your answer (… or else you get 0 marks).

   Generally, there isn't much point running more MST instances than actual links! Having more MST instances than links just means that two (or more) choices will be duplicates. The only adjustment to this rule is that MST instance **0** always exists, so the most accurate answer is: max # of instances = # of links + 1

6. Consider the following configuration commands:

```
SwMain(config)# vlan 12
SwMain(config-vlan)# private-vlan community
SwMain(config-vlan)# vlan 14
SwMain(config-vlan)# private-vlan isolated
SwMain(config-vlan)# vlan 16
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 0/12 - 13
SwMain(config-if)# switchport mode private-vlan host
SwMain(config-if)# switchport private-vlan host-association 10 12

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

a. [3 marks] Draw a **clear** diagram showing the logical organization created by the configuration above.



b. [5 marks] Assume: devices **A**, **B**, ... **F** are connected to ports fa0/**12**, fa0/**13**, ... fa0/**17**, consecutively; devices **X** & **Y** are connected to fa0/**10** & fa0/**11**, all of which are "up/up".
Important: marks will be deducted for incorrect answers so **NO** guessing!

b.1. A ping originating from host X (fa0/10) could successfully reach which host(s)?
A, B, C, D, Y

b.2. A ping originating from host Y (fa0/11) could successfully reach which host(s)?
A, B, E, F, X

b.3. A ping originating from host A (fa0/12) could successfully reach which host(s)?
X, Y, B

b.4. A ping originating from host C (fa0/14) could successfully reach which host(s)?
X

b.5. A ping originating from host E (fa0/16) could successfully reach which host(s)?
Y, F

c. [3 marks] Give real-world examples for each category of *device* in the above scenario.

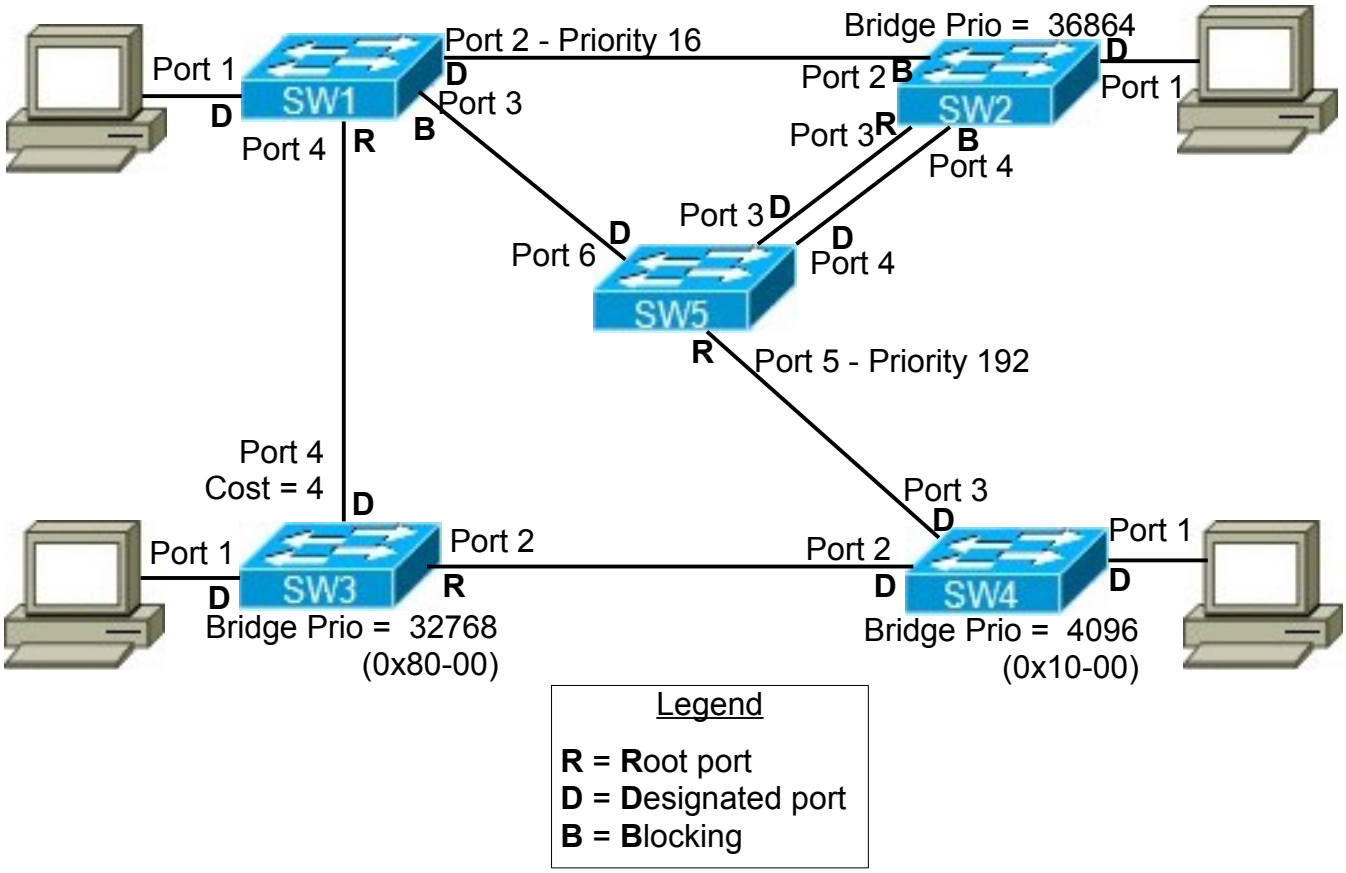
– X, Y (primary) may be servers or default gateways; accessible to **many** clients.
– C, D (isolated) may be printers, or clients for an ISP which shouldn't connect/interfere
– A, B and E, F are groups belonging to two different "companies" or entities and might be servers or hosts which need to interconnect

7. [3 marks] **Clearly** explain the **difference(s)** and **similarity(ies)** between Etherchannel and Flexlink connections. Under what circumstances (at what moments) would the two be acting "identically"?

[2 marks] Give at least **two** of the following answers:
Both provide L2 redundancy.
Flexlink is strictly limited to operating in link pairs; Etherchannel operates as 2-16 links.
Flexlink has at most **one** link operational; Etherchannel has up to 8 simultaneous links
Flexlink may *eliminate* need for STP; Etherchannel might still require STP
Flexlink pairs may terminate at *different* endpoints; Etherchannel has *identical* endpoints at both ends of the link.
Also accepted: Etherchannel has a load-balancing parameter, Flexlink does not.

[1 mark] The two would only be operating identically if Etherchannel only had exactly *one* remaining link functioning and Flexlink has at least one link functioning.

8. Study the diagram below carefully. Assume 100 Mb links, all priorities and other values are at their **default**, and MAC ID of SW(n) is 00-nn-nn-nn-nn-nn-nn, unless otherwise shown.



A. [1 mark] Circle the root bridge. **Switch4 (lowest priority)**

B. [5 marks] Label the diagram with the state of all ports after the network has converged.
As shown above with symbols **R**, **D**, **B**

C. [2 marks] What is the **exact BID** for Switch 1? **Clearly** state any required assumptions.

BID = Priority + 12 bit ext + MAC = **80-00-01-00-11-11-11-11-11**, assuming VLAN = 1

D. [1 mark] After convergence, an administrator connects to SW5 and types:

```
Sw5(config)#  spanning-tree vlan 1 root primary
```

What is the new priority for Switch 5?

`root primary` sets priority 4096 lower than any existing priority, so will go to **0**
Will also accept **1** (ie. VLAN included in priority).

E. [1 mark] Later we decide that for Switch2, the **cost** associated with the link for port 4 should be 10. **Where** should that value be set?

Cost needs to be set locally, so on **Sw2** port 4

F. [1 mark] Later we decide that for Switch 2, the **port priority** used for STP calculations should be 112. **Where** should that value be set?

Port priority needs to be set "upstream", so **Sw5**, port 4

G. [1 mark] What is the **port priority** for port 6 on Switch 5?

Port 6 is at Default priority = 128

9. **A**. [2 marks] **Clearly** explain the attack that the command: **`switchport port-security`** is designed to protect against. (ie. What does the attacker *do*?)

   `port-security` protects against MAC table flooding where the attacker sends many, many frames (1000's) with spoofed source MAC addresses. This is done in an attempt to overflow the MAC address table of the victim switch. If successful, the switch ends up acting like a hub, flooding all traffic through all ports.

   B. [2 marks] There are two possible consequences of the above attack. **Clearly** explain both of them. (ie. What does the attacker get? What happens in the network?)

   1. Attacker (well, everyone actually) sees a copy of all traffic in a given VLAN, allowing for eavesdropping on critical info and potential theft of unencrypted passwords.

   2. DoS: since all traffic is being flooded to all ports in a given VLAN, there's the possibility of overwhelming or at least slowing down the whole L2 area for a given VLAN.

   C. [3 marks] There are three possible responses once **`switchport port-security`** has been activated. **Name** each of the responses and **clearly** explain what each does.

   Protect: simply drop frames with MAC source addresses that are not registered

   Restrict: drop frames with unregistered MAC addresses **and** send SNMP traps

   Shutdown: shutdown the port, putting it into the **`errdisable`** state

10. **A**. [1 marks] Some people describe VLAN hopping as a "one-way" or "unidirectional" attack. **Clearly** explain the reason for this description.

    VLAN hopping only allows traffic to flow *from* the attacker *to the target(s)*; the reverse flow doesn't happen, hence it is unidirectional.

    B. [1 mark] Give an example of another attack that can be used in conjunction with a VLAN hopping attack (ie. an attack that works even in "one-way" or "unidirectional" situations).

    MAC address (flooding) attacks to impair or DoS the network is one example of an attack that could work with VLAN hopping.

11. **A**. [3 marks] There are **three** Spanning Tree enhancements that provide both additional network *stability* ***and*** extra *security* against hackers. **Name** and **clearly** describe each of the three enhancements. **Clearly** differentiate any similar enhancements.

BPDU guard & BPDU filtering: need to differentiate these clearly eg. by their operation

BPDU filter: - local config: totally ignore (ie discard) all BPDUs (security feature)
- global config: lose portfast status if BPDU is received (no extra security)

BPDU guard: - receipt of BPDU causes a portfast port to go errdisable state
- there is no difference in behaviour whether locally or globally configured

Root guard: Prevents propagation of superior BPDUs from a port that is designated as *not* allowing for a root switch. The port is put into "root inconsistent" state. Root guard can only be configured on individual interfaces (not globally).

B. [1 mark] Which of the above enhancements work for **both** 802.1D and 802.1w ?

All three of them work for both CST or RST, although RST has functionality similar to globally-configured BPDU filter already built-in to Edge ports.
From Cisco "The configuration of the features such as PortFast, BPDUguard, BPDUfilter, root guard, and loopguard are applicable in rapid-PVST+ mode also. The usage of these features are the same as in PVST+ mode."
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807b0670.shtml

--- End ---

Additional work, notes, or rough work