Test 2: NET3011 – Advanced Switching

Winter 2012

Time: 60 minutes; Test scored out of: 46 Total Marks available: 50
(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. Be sure to **mark your name (both written and bubbled)** on the scantron answer sheet.

3. All multiple choice answers should be circled on this test paper **and** then marked on the scantron answer sheet.

4. All multiple choice questions are worth 1 mark, unless otherwise noted.

5. For multiple choice questions, if you do not find an answer which is clearly the correct choice, choose the *best* answer.

6. 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. Which statement is true about the local SPAN configuration on switch SW1?

```
SW1(config)# interface Fa3/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# end

SW1(config)# interface Fa3/21
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access VLAN 10
SW1(config-if)# end

SW1(config)# monitor session 1 source interface Fa3/1
SW1(config)# monitor session 1 destination interface Fa3/21
SW1(config)# end
```

(a) The SPAN session transmits to a device on port Fa3/21 a copy of all traffic that is monitored on port Fa3/1. **correct**

(b) The SPAN session transmits to a device on port Fa3/21 a copy of all traffic that is monitored on port Fa3/1, but only if port Fa3/1 is configured in VLAN 10.

(c) The SPAN session transmits to a device on port Fa3/21 a copy of all traffic that is monitored on port Fa3/1, but only if port Fa3/1 is configured as trunk.

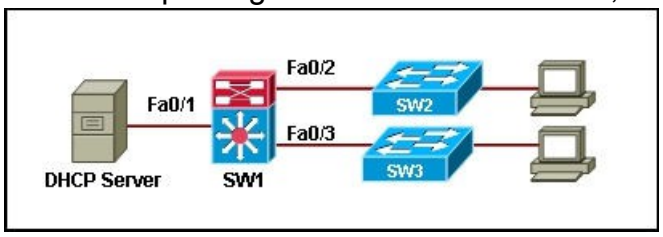
(d) The SPAN session transmits to a device on port Fa3/21 only a copy of unicast traffic that is monitored on port Fa3/1. All multicast and BPDU frames will be excluded from the monitoring process.

(e) None of the above.

2. All access ports on a switch are configured with the administrative mode of dynamic auto. An attacker, connected to one of the ports, sends a malicious DTP frame. What is the intent of the attacker?

(a) VLAN hopping **correct**
(b) DHCP spoofing attack
(c) MAC flooding attack
(d) ARP poisoning attack
(e) DAI attack

3. A network engineer is securing a network against DHCP spoofing attacks. On all switches, the engineer applied the **ip dhcp snooping** command and enabled DHCP snooping on all VLANs with the **ip dhcp snooping vlan** command. What additional step should be taken to configure the security required on the network?



(a) Issue **ip dhcp snooping trust** command on all uplink interfaces on SW1, SW2 & SW3 **Y**
(b) Issue the **ip dhcp snooping trust** command on all interfaces on SW2 and SW3
(c) Issue the **ip dhcp snooping trust** command on all interfaces on SW1, SW2, and SW3
(d) Issue the **ip dhcp snooping trust** command on all interfaces on SW1, SW2, and SW3 except interface Fa0/1 on SW1.

4. Which countermeasure can be implemented to determine the validity of an ARP packet, based on the valid MAC-address-to-IP address bindings stored in a DHCP snooping database?
   (a) DHCP spoofing
   (b) dynamic ARP inspection **correct**
   (c) CAM table inspection
   (d) MAC snooping

5. How should unused ports on a switch be configured in order to prevent VLAN hopping attacks?
   (a) Configure them with the UDLD feature.
   (b) Configure them with the PAgP protocol.
   (c) Configure them as trunk ports for the native VLAN 1.
   (d) Configure them as access ports and associate them with an unused VLAN. **correct**

6. Given the configuration shown for ALSwitch, what is the end result?

```
ALSwitch# configure terminal
ALSwitch(config)# aaa new-model
ALSwitch(config)# aaa authentication dot1x default group radius
ALSwitch(config)# dot1x system-auth-control
ALSwitch(config)# interface fastethernet 0/1
ALSwitch(config-if)# dot1x port-control force-authorized
ALSwitch(config-if)# end
```

   (a) forces all hosts that are attached to a port to authenticate before being allowed access to the network
   (b) disables 802.1x port-based authentication and causes the port to allow normal traffic without authenticating the client **correct**
   (c) enables 802.1x authentication on the port
   (d) globally disables 802.1x authentication

7. What is one way to mitigate spanning-tree compromises?
   (a) Statically configure the primary and backup root bridge. **correct**
   (b) Implement private VLANs.
   (c) Place all unused ports into a common VLAN (not VLAN 1).
   (d) Configure MAC address VLAN access maps.

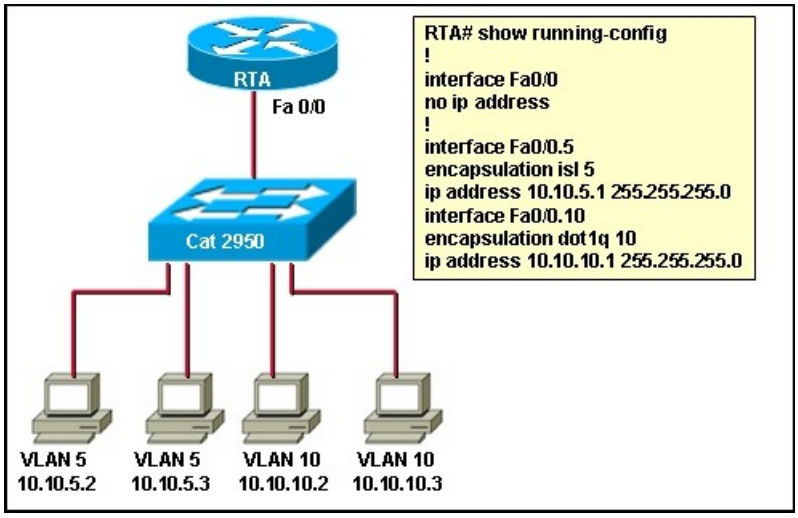
8. What is one way to mitigate ARP spoofing?
   (a) Enable dynamic ARP inspection. **correct**
   (b) Configure MAC address VLAN access maps.
   (c) Enable root guard.
   (d) Implement private VLANs.

9. What are two purposes for an attacker launching a MAC table flood? (Choose **best** two.)
   (a) to initiate a man-in-the-middle attack
   (b) to initiate a denial of service (DoS) attack **correct**
   (c) to capture data from the network **correct**
   (d) to gather network topology information
   (e) to exhaust the address space available to the DHCP

10. A client sends a request for an IP address to a DHCP server. Which DHCP message to the client will provide the configuration parameters that include an IP address, a domain name, and a lease for the IP address?
    (a) DHCPDISCOVER
    (b) DHCPOFFER **correct**
    (c) DHCPREQUEST
    (d) DHCPACK
    (e) DHCPNACK

11. A DHCPREQUEST message has been sent from the client to the DHCP server. What information is included in the message?
    (a) initial message to locate a DHCP server
    (b) formal request for the offered IP address **correct**
    (c) confirmation that the IP address has been allocated to the client
    (d) denial message to reject the first offer from the DHCP server
    (e) 65536

12. Refer to the exhibit and the partial configuration taken on router RTA. Users on VLAN 5 cannot communicate with the users on VLAN 10. What should be done to fix the problem?



    (a) A dynamic routing protocol should be configured on the router

    (b) Two static routes should be configured on the router, each pointing to each subnet

    (c) The Fa0/0 interface should be configured with a primary IP address of 10.10.5.1/24 and a secondary IP address of 10.10.10.1/24
    (d) The subinterfaces of the router should be configured with 802.1Q encapsulation **correct**

13. [2 marks] Give the names of the three types of STP, including their IEEE designation, in order of their speed **and** efficiency (poorest first, best last).

    1 mark for names: Common STP; IEEE 802.1D (one instance or with Cisco, 1 per VLAN)
    Rapid STP; IEEE 802.1w (rapid, but still one instance per VLAN)
    Multiple STP; IEEE 802.1s (typically one instance per link)

14. [1 mark (Bonus?)] Did you pay enough attention during lab? Below is a snippet of output from the command "show spanning-tree" from Dec 2011. Which version of STP is running?

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------
Fa0/1            Desg FWD 19        128.1    P2p
```

COST = LOW; must be 802.1D!!

15. [1 mark] One type of STP introduces extra port roles of "Alternate" and "Backup". **Clearly** define each of these two roles (eg. with reference to the device that has these port roles).

Alternate: a blocking port (non-designated, non-root) on a non-designated switch
Backup: a blocking port (non-designated, non-root) on the designated switch

16. A. [1 mark] With STP, there are three types of "elections" to decide the role of each switch and each port. **Clearly** identify the three elections.

First: elect root bridge; Second: elect root port (ie. designated switch)
Third: elect designated port (for each segment)

B. [3 marks] Specify **exactly** what criteria are used for **each election** and what constitutes the "best" value in deciding a winner in **each election**. Each answer should start:
"To elect the _____, the following criteria are used in order: ..."

Direct question from Wk5Day2 lecture summary notes.
For **all elections**, the "best" value is **always the lowest** value.
To elect the **root bridge**, the following criteria are used in order:
- Bridge ID (= switch priority [1st]+ MAC address [2nd , tie breaker])

To elect the **root port**, the following criteria are used in order:
- Accumulated Cost to Root bridge (= received + cost of last link); lowest is best
- Bridge ID (of sender; = switch priority [1st]+ MAC address [2nd])
- Port ID (of sender; = port priority [1st] + port number [2nd])
- Port ID (of local switch; = port priority + port number [tie breaker])

To elect the **designated port** on a segment, the following criteria are used in order:
- Accumulated cost to Root bridge; lowest is best
- Bridge ID (of sender; = priority [1st]+ MAC address [2nd])
- Port ID (of all segment; = port priority + port number [tie breaker])

17. [3 marks] STP has three types of messages relating to "Topology". Give the name of each message, explain its usage **clearly** (eg. When? Why? Where?), and identify which version of STP uses that message.

Ref: Wk06Day1 lecture summary notes

Topology Change Notification (TCN) BPDU: sent upstream by a bridge to signal a topology change (until acknowledged by **TCA).** Used only in 802.1D STP.

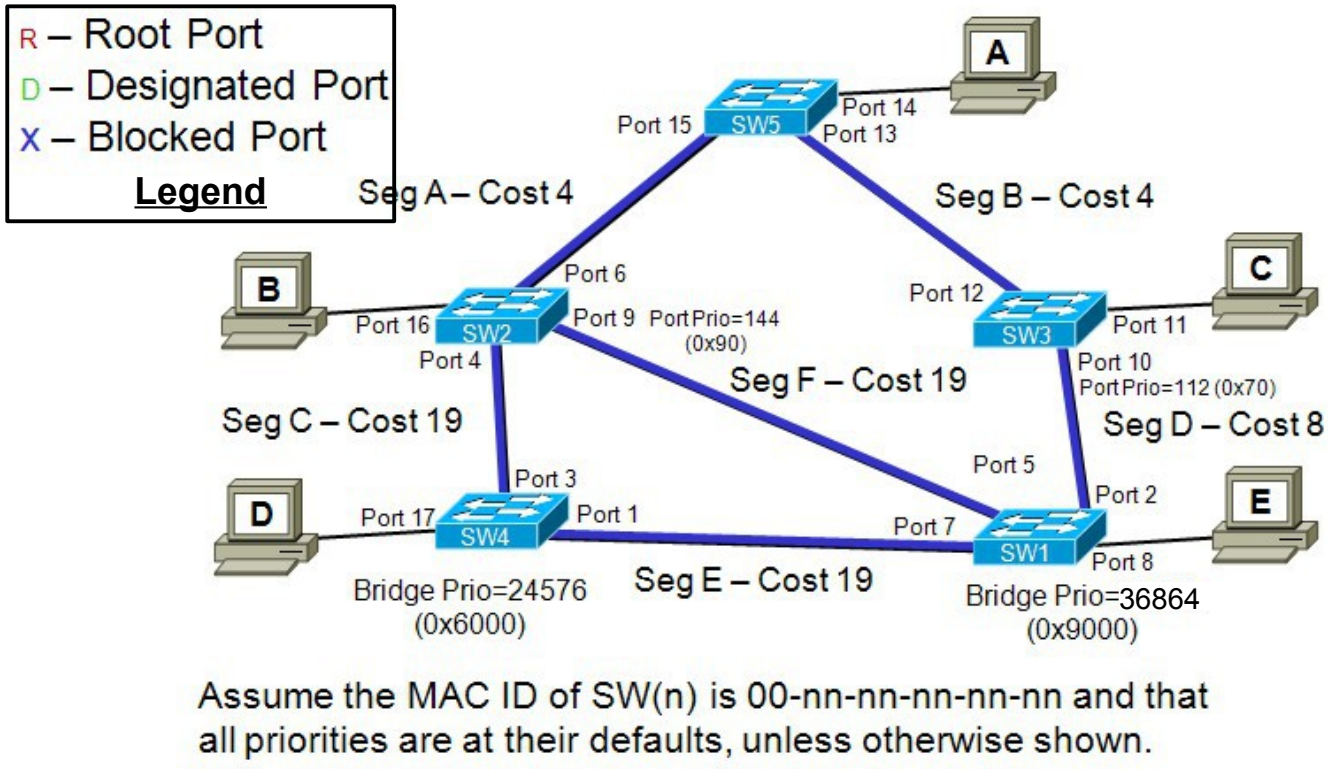
Topology Change ACK (TCA) flag: sent downstream to acknowledge (and terminate) TCN BPDUs. Used only in 802.1D STP.

Topology Change (TC) flag:

In 802.1D STP: only sent by root bridge downstream, to signal cache flushing

In 802.1w & 802.1s: sent by any/all bridges to signal TC; results in cache flushing

18. Study the diagram below carefully. Assume all values are **default** unless otherwise noted.



Assume the MAC ID of SW(n) is 00-nn-nn-nn-nn-nn and that all priorities are at their defaults, unless otherwise shown.

A. [1 mark] **Circle** the root bridge. **Switch 4 is the root bridge**

B. [5 marks] Label the diagram with the state of **all ports** after the network has converged.

SW1: R=7,D=2,8,X=5 SW2: R=4,D=6,9,16 SW3: R=12,D=11,X=10 SW4: D=all SW5: R=15, D=13,14

19. [1 mark] **Clearly** define / explain how the BID is created or determined for a switch.

BID (In order) = 4 bit priority value + 12 bit VLAN ID + 48 bit MAC address (= 8 bytes)

[1 mark] **Clearly** define /explain how the Port ID is created or determined.

Port ID (in order) = 8 bit port priority value + 8 bit port number (locally assigned)

20. [12 Marks] We studied 9 enhancements or options to STP (ref: Wk06Day1). Five (5) of them are purely for link & topology management ie. they aren't trying to improve security. Four (4) of them provide both protection against silly configuration mistakes **and** added security against hackers. Give **three** pieces of information **about each** of the four: (1) name it; (2) **clearly** define what it does or how it operates; (3) **clearly** describe the type of attack it would prevent. For item (2), be sure to note any differences between configuring it globally or on a specific interface.

4 STP security options: (A) Name; (B) how it works; (C) attack it prevents

The no-extra-security: portfast, uplink fast, backbone fast, loop guard, UDLD, flex links

Would you believe I miscounted? There's only 3 that provide any extra security. Sorry!

The names of the **3** others: BPDU guard, BPDU filtering, Root guard

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

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

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

Root guard: prevents any switch attached to the port from becoming the root bridge
- ports receiving superior BPDUs go **root-inconsistent** (a listening state)
- root guard can only be configured on individual interfaces (not globally)

All three prevent a rogue switch from becoming a root bridge; important because:
– a rogue root bridge pulls traffic away from intended links, possibly allowing eavesdropping, man-in-the-middle attacks, or DOS attacks (due to higher-speed links being disabled as a consequence of the new root bridge position; eg. pg 155)

BPDU filtering can prevent reconnaissance attacks: we want to prevent the attacker from learning other bridges MAC addresses (part of BID) and possibly IP addresses (via ARP) so that targets are **not** identified for other types of attacks.

BPDU guard and filtering can prevent DOS attacks whereby the attacker constantly causes the ~50 sec reconvergence time of 802.1D STP topology reconfiguration eg. "I'm the root bridge" and then 50 sec later, "I'm not the root bridge", repeatedly.

21. [7 Marks] We studied four (4) main categories of L2 security attacks and methods to protect against them. Give the following information about **at least three** of them: (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 item 2. **Note**: all items for this question must be **different** from the last question. *Quality counts!!*

3 L2 Attacks: (A) Name & description; (B) Prevention method

~2 marks per type of attack, up to a max of 7 marks. I'm looking for correct info to **give** marks rather than looking for reasons to deduct marks.