Filtering Database and Backward Learning Algorithm

Notes:

Although the lab devices used in the exercises are commercially called routers, they integrate a four port switch and operate according to the transparent bridging standards. Lab exercises will focus on such functionality.

This lab exercise can be carried out only in Torino NetLab

1. Preliminary Configuration

   A. WARNING!! Note that R7 has already been configured.

   B. Reset the configuration of R1,R2,R3 (Workplace1) or R4,R5,R6 (Workplace2). After reload

      i. Shutdown all unplugged interfaces (see figure above). Note that each device has four switched interfaces Fe0, Fe1, Fe2, Fe3.

      ii. Disable the spanning tree protocol by entering the following command in the configuration Terminal

      \[
      \text{NO SPANNING-TREE VLAN 1}
      \]

      iii. Set the aging time of the filtering database on R1,R2,R3 (Workplace1) or
R4,R5,R6 (Workplace2). To do this, enter the following command in the configuration Terminal.

**MAC-ADDRESS-TABLE AGING-TIME 30**

C. Reset the configuration of R8 (Workplace1) or R9 (Workplace2). After reload
   i. Shutdown all unplugged interfaces (see figure above). Note that each device has four switched interfaces Fe0, Fe1, Fe2, Fe3.
   ii. Disable the spanning tree protocol by entering the following command in the configuration Terminal.

   **NO SPANNING-TREE VLAN 1**

   iii. Configure the IP address of the L3 virtual interface associated to the default VLAN 1. To do this, enter the following commands in the configuration Terminal.

   **INTERFACE VLAN 1**
   **IP ADDRESS [ IP address][ Netmask]**
   **EXIT**

   iv. Setup the ARP entry related to the MAC address of Fe1: 0017.0ece.13ea (Workplace1) or Fe2: 0017.0ece.13ea (Workplace2) on R7. The two interfaces have the same MAC addresses because by default the Cisco IOS assigns the same address to all the L3 virtual interfaces.

   **ARP [R7 IP address] 0017.0ECE.13EA ARPA**

2. **Filtering Database Analysis**

   A. Obtain the MAC address of all the active interfaces and report a list of interfaces and corresponding MAC addresses for R1,R2,R3 (Workplace1) or R4,R5,R6 (Workplace 2).

   B. Read the filtering database on either R1,R2,R3 (Workplace1) or R4,R5,R6 (Workplace2). Type the following command in privileged EXEC mode.

   **SHOW MAC-ADDRESS-TABLE.**

C. Are the MAC addresses listed at point A present in the filtering databases obtained at point B? Why?

D. PING R7 either from R8 (Workplace1) or from R9 (Workplace2) and capture all packets exchanged between the devices using Analyzer. Please note that R7, R8 and R9 have already been configured in such a way that MAC addresses of their counterparts are already in their ARP cache (i.e., no ARP packet will be generated as a consequence of the PING command). Type the following command in privileged EXEC mode.

   **PING [ R7 ip address ]**
E. Save and provide the capture file

F. Read the filtering database either on R1,R2,R3 (Workplace1) or on R4,R5,R6 (Workplace2). Type the following command in privileged EXEC mode

```
SHOW MAC-ADDRESS-TABLE.
```

G. Are the MAC addresses listed at point A present in the filtering databases obtained at point F? Why? **Warning:** please go back to point C and check your answer!

H. So why is the result obtained at point F different from what obtained at point B? List the entries that have appeared in the filtering databases obtained at point F thanks to the PING just performed. Which devices are they related to?

I. Why R2,R3 (Workplace1) or R5,R6 (Workplace2) do not learn the MAC address of Fe1 (Workplace1) and Fe2 (Workplace2) on R7?

3. **L2 LOOP Detection**

   A. Activate Fe2 on R2 and R1 (Workplace1) or Fe1 on R6 and R4 (Workplace2); the new topology is depicted in the following diagram:

```
Workplace 1

Workplace 2

```

```
**WARNING:** The command you are going to enter may generate a broadcast storm which could make the switches unavailable (i.e., you could be no longer able to interact with the switch!). This would force teachers to manually shutdown the switches, with consequent possible long periods of system unavailability...

Broadcast storm usually does not happen in this configuration (it could be interesting to try to understand why!) but, as said, it could in some cases. In order to minimize this possible issue, please follow these instructions:

1. Before continuing with point B of this part of the assignment, enter the configuration mode on R2 (Workplace1) or R6 (Workplace2) `[Router# configure terminal]`
2. Then enter the Fe2 (Workplace1) or Fe1 (Workplace2) configuration mode `[Router# interface FastEthernet 2]` and
3. Prepare the command to shutdown Fe2 (Workplace1) or Fe1 (Workplace2) `without launching it` `[Router# shutdown]`
4. Launch the capture and enter the PING command on R8 (Workplace1) or R9 (Workplace2), as described in the following point B
5. **VERY IMPORTANT:** Press **ENTER** on the R2 (Workplace1) or R6 (Workplace2) configuration terminal in order to launch the “shutdown” command after a few (no more than 2-3) seconds. This will open the loop, thus avoiding a “heavy” broadcast storm and allowing you not to lose the control of the switch.

   B. **PING** R7 either from R8 (Workplace1) or from R9 (Workplace2) and capture all packets exchanged between the devices with Analyzer. Please note that R7, R8 and R9 have already been configured in such a way that MAC addresses of their counterparts are already in their ARP cache (i.e., no ARP packet will be generated because of the PING command). Type the following command in **privileged EXEC mode**.

   ```
PING [ R7 ip address ]
```

   C. Save and provide the capture file

   D. Please explain the differences of this capture from the one obtained at point 2.F and motivate the reason of these differences.