POLITECNICO DI TORINO

PROGETTO DI RETI LOCALI

Lab 1: Filtering database

Fulvio Risso

March 24, 2017

License

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

You are free:

- **to Share**: to copy, distribute and transmit the work

- **to Remix**: to adapt the work

Under the following conditions:

- **Attribution**: you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

- **Noncommercial**: you may not use this work for commercial purposes.

- **Share Alike**: if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

More information on the Creative Commons website (`http://creativecommons.org`).

Acknowledgments

The author would like to thank all the persons that contributed to those exercises. Particularly, special thanks go to Guido Marchetto.

1 Introduction

In this lab assignment we are going to simulate a configuration with two routers and three switches in order to analyze the behavior of the *Backward learning algorithm* and check the changes in the *Filtering database* of the switches.

2 Topology

The topology for this assignment is represented in the following picture:
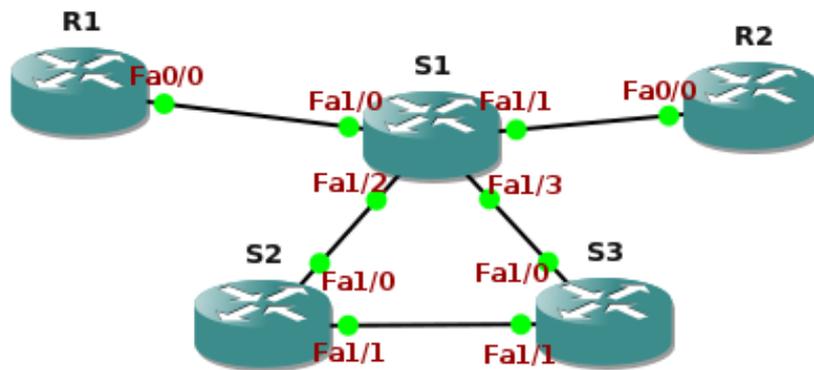
R1 and R2 are *Cisco 2691* routers that behave as hosts, acting as the source and the destination of a `ping`. Instead, S1, S2 and S3 are *Cisco 2691* devices acting as switches. In fact, they are equipped with the optional *NM-16ESW Etherswitch module* that provides switched interfaces, transforming a router into a switch (on those interfaces, while the native interfaces of the router are still *routed* interfaces).

3 Preparing the lab configuration

Log-in in the network emulation system, create the network topology as depicted in the figure above and start the devices. Finally, open all the configuration consoles of the network devices involved in the lab and be ready to interact with them.

3.1 Configuration tip

It is worthy noticing that *routed* interfaces (i.e., the ones you configure on the R1 and R2 devices) are *disabled* by default. Hence you have to turn them on by typing `no shutdown` from the interface configuration menu. Vice versa, *switched* interfaces (i.e., the ones you configure

on S1, S2 S3) are *enabled* by default. Hence you do not have to turn them on; obviously you have to type `shutdown` from the interface configuration menu if you want to turn them off.

Finally, please remember that *routed* and *switched* interfaces do not depend on the device they are attached to (e.g., *router* or *switch*), but refer to the physical hardware of the interface that determines their configuration. For instance, *routed* interfaces must be configured at L3, i.e. they accept network-layer commands (e.g., IP addresses); *switched* interfaces, instead, must be configured at L2 and accept only data-link layer commands (e.g. VLANs).

3.2 Routers (R1 and R2)

In this step you are going to set up the `FastEthernet0/0` interfaces in the routers, which will provide the source and the destination addresses for the `ping` transaction required in this lab assignment. For instance, you will not use the `R1` and `R2` as routers; they will act as simple hosts instead.

The following instructions apply to both `R1` and `R2`.

- Enter the interface configuration mode for `FastEthernet0/0`:

  ```
  enable
  configure terminal
  interface FastEthernet0/0
  ```

- Due to a bug in the simulator, the speed on a link between a routed and a switched interface is not negotiated automatically. Hence, you have to set it up manually here:

  ```
  speed 100
  duplex full
  ```

- It is important to disable the *keepalive* functionality of the interface, since it will interfere with the filtering database (when the keepalive functionality is enabled, the router periodically transmits LOOP packets which will be recorded by nearby switches, filling their filtering database. In a normal condition this would be good, but not in this lab assignment).

  ```
  no keepalive
  ```

- For the same reason you should disable the Cisco Discovery Protocol (*CDP*) that is sometimes active on the device:

  ```
  no cdp run
  ```

- Now you are going to setup the IP addresses for the interfaces:

  ```
  ip address 192.168.0.1 255.255.255.0 (on R1)
  ip address 192.168.0.2 255.255.255.0 (on R2)
  ```

- Turn the interface up by typing:

  ```
  no shutdown
  ```

Additionally, we suggest to set a static entry in the ARP cache of the routers to let they know each other interfaces' physical address, hence avoiding a broadcast packet (the *ARP Request*) before the `ping` transaction. First you need to determine the MAC address of the two `FastEthernet0/0` interfaces.

- Exit from the configuration mode by typing

  `end`

  Then show the characteristics of the network interface by typing

  `show interface FastEthernet0/0`

  The second line should look similar to the following:

  ```
  Hardware is Gt96k FE, address is <address> (bia <address>)
  ```

- Copy the address you see. If you typed the `show interface` command in the R1 console, go to the R2 console and write[1]:

  ```
  configure terminal
  arp 192.168.0.1 <address> arpa
  ```

- Then use the `show interface` command in R2 and configure R1's ARP cache. Check if everything is right by exiting the configuration mode and typing `show arp` in the privileged mode. On R1 you should see something like this:

  ```
  Protocol  Address          Age (min)  Hardware Addr   Type    Interface
  Internet  192.168.0.1              -   c003.54a8.0000  ARPA    FastEthernet0/0
  Internet  192.168.0.2              -   c004.54a8.0000  ARPA
  ```

  Note: Since hardware addresses may change among different simulation runs, you may need to repeat this step if you save and later reload the configuration.

3.3 Switches (S1, S2 and S3)

Here you are going to manually "break the loop" among the switches and then disable the spanning-tree protocol, entering in a condition in which broadcast storms are not possible (since the physical topology does not have loops). From this point on, the instructions are going to be less "verbose" leaving you a little more to think about how to do things.

- On the S1 switch configure the `FastEthernet1/3` interface (it is on the link connecting S1 to S3). Shut it down to break the loop.

Perform the following operations on all the switches:

- Disable the spanning tree protocol:

  `no spanning-tree vlan 1`

- Make the entries in the filtering database expire quickly (30 seconds instead of 5 minutes):

  `mac-address-table aging-time 30`

---

[1]Obviously, the word `<address>` in the reported command must be replaced by the MAC address learned in the previous step.

This step is not strictly required, but it facilitates the lab since it allows the filtering databases of the switches to return in their initial conditions quickly, without having to wait for 5 minutes.

4 Analysis of the Filtering Database

The setup of the lab is now done. We can begin the real work of this assignment.

1. Obtain the hardware address of all the active interfaces and list the obtained interfaces and their corresponding addresses. Repeat this step for all switches (`S1`, `S2` and `S3`).

   Tip: A useful command is `show interface`.

2. Read the filtering database on S1, S2 and S3. Use the following command in the privileged mode:

   `show mac-address-table`

3. Are the MAC addresses listed at point (1) present in the filtering databases obtained at point (2)? Why?

   Note: please note that the switches will configure a static MAC address for internal purposes, associated to the VLAN 1 virtual interface (the address marked with type *self* when printing the filtering database). This address will be always present and it should not be considered in the current lab assignment. Its meaning will be more clear when VLANs and virtual VLAN interfaces will be presented.

4. Start the packet capture. Right-click on each of the links in the topology and choose *Start capture*. Note that a different wireshark window is now open for each link.

5. Ping `R2` from `R1`. Please note that you have already configured `R1` and `R2` in such a way that MAC addresses of one another are already in their ARP cache (i.e., no ARP packet will be generated as a consequence of the ping command).

   Tip: the `ping` command is available on Cisco routers when in privileged mode.

6. Stop the capture. Right-click on each of the links and choose *Stop capture*. You can see the packets captured on each link through wireshark.

7. Check again the filtering database on `S1`, `S2` and `S3`. Are the MAC addresses listed at point (1) present in the filtering databases obtained right now? Why? Are there any other MAC address present? Which interfaces do they refer to?

   Note: this operation has to be carried out before the expiration of the *aging time*, currently set to 30 seconds. In case you were unable to do so in time, please repeat the item (5).

8. Why `S2` and `S3` do not learn the MAC address of the `FastEthernet0/0` interface of `R2`?
   Tip: captured packets may help you to provide an answer.

9. Let's imagine to start a continuous PING between routers R1 and R2, and let's imagine to check the filtering databases of switches S1 and S2 after a while (e.g., 10 minutes). Will the filtering database of switch S1 contain an entry related to the R1's MAC address? And what about the switch S2? Why?

5 Loop detection

Warning! The commands you are going to enter will generate a broadcast storm which could make the switches unavailable (i.e., you could be no longer able to interact with the switch!). This may in turn break the hypervisor, needing a manual restart of the virtual machine. **So, please, pay attention on what you do!**

1. Re-enable the `FastEthernet1/3` interface on `S1` in order to re-activate a physical loop among the switches (command: `no shutdown`). Please note that you are now in a condition in which the broadcast storm is possible, since you have a physical loop among the switches and the spanning tree protocol is not active.

2. Stay in the interface configuration mode on `S1`'s console and type `shutdown` without pressing return, so that the command is ready to be entered. **Do not launch it now**, but prepare yourself to do so quickly, as soon as it will be needed.

3. **Read this step entirely before executing it.**
   - Start the packet capture on all the links in the topology.
   - Go to `R1`'s console. Ping `R2` from `R1`.
   - Go back immediately to the `S1`'s console and enter the `shutdown` command that you prepared before.
   - Stop the capture.

4. Download the capture file (it might be rather large).

5. Please *explain* and *motivate* the differences of this capture from the one obtained at point 4.6.