Homework 4: Spanning Tree
Contents

I. Intro 4
  1. Legend 5
  2. Methodology 6

II. Exercises 7
  3. Spanning tree 8
    3.1. Exercise n. 1 8
    3.2. Exercise n. 2 9
    3.3. Exercise n. 3 10
    3.4. Exercise n. 4 11
    3.5. Exercise n. 5 12
    3.6. Exercise n. 6 13
    3.7. Exercise n. 7 14
  4. Rapid Spanning Tree 15
    4.1. Exercise n. 8 15
    4.2. Exercise n. 9 16
    4.3. Exercise n. 10 17
    4.4. Exercise n. 11 18
    4.5. Exercise n. 12 19
    4.6. Exercise n. 13 20
    4.7. Exercise n. 14 21
  5. Multiple Spanning Tree 22
    5.1. Exercise n. 15 22
  6. Traffic Analysis 23
    6.1. Exercise n. 16 23
III. Solutions

7. Spanning tree
   7.1. Solution for exercise n. 1 ........................................... 25

8. Rapid Spanning Tree
   8.1. Solution for exercise n. 8 ........................................... 27
   8.2. Solution for exercise n. 14 ......................................... 28

9. Multiple Spanning Tree
   9.1. Solution for exercise n. 15 .......................................... 29

10. Traffic Analysis
    10.1. Solution for exercise n. 16 ....................................... 31
Part I.

Intro
1. Legend

Spanning Tree Port Roles

- **O** — Root port
- **•** — Designated port
- **#** — Blocked port

Rapid Spanning Tree Port Roles

- **O** — Root port
- **•** — Designated port
- **••** — Edge port
- **•••** — Alternate port
- **••••** — Backup port
- **\slash** — Disabled port
2. Methodology

The outcome of the *Spanning Tree* can be easily obtained through the following steps:

1. Determine the *Root Bridge* (i.e. the bridge that has the best Bridge ID).

2. Determine the spanning tree across the entire network, selecting the *best paths* in the network toward each bridge.

3. For each bridge, select the *Root Port*:
   - In case the bridge has only one path toward the root bridge, that port will be the *Root Port*.
   - In case the bridge has multiple equivalent paths toward the root bridge, use the selection criteria in order to determine which is the best root port.

4. For each LAN, select the *Designated Port* (among the ports that are not root).

5. Put the remaining ports in *Blocking State*.

The outcome of the *RSTP* is definitely similar to the STP one, the difference being the criteria used to select the role of the ports that are blocked in STP (and that become either *Backup* or *Alternate*), and to the ports that are not connected to any bridge (that become *Edge* ports).

In fact, the main difference between RSTP and STP is in the intermediate algorithm (which is faster in RSTP), but the final outcome is basically the same. Therefore, as far as the exercise focus on the final outcome of the protocol and not in the intermediate steps for reaching that objective, the final outcome does not change (except for Backup, Alternate and Edge ports).
Part II.

Exercises
3. Spanning tree

3.1. Exercise n. 1

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.2. Exercise n. 2

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.3. Exercise n. 3

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.4. Exercise n. 4

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.5. Exercise n. 5

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.6. Exercise n. 6

Referring to the network topology depicted below, determine the final outcome of the Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
3.7. Exercise n. 7

Given the network topology in the figure below, configure the proper parameters in the switches so that switches on the left side of the building will send frames to the left switch in the basement, while switches on the right side of the building will send frames to the right switch in the basement. No VLANs are configured in the network.
4. Rapid Spanning Tree

4.1. Exercise n. 8

Due to a configuration error, both sides of a cable are connected to the same switch, as shown in the figure below. Explain what happens and motivate the answer. Consider both the STP and the RSTP protocols.
4.2. Exercise n. 9

Referring to the network topology depicted below, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
4.3. Exercise n. 10

Referring to the network topology depicted below, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
4.4. Exercise n. 11

Referring to the network topology depicted below, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
4.5. Exercise n. 12

Referring to the network topology depicted below, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
4.6. Exercise n. 13

Referring to the network topology depicted below, which resembles to a network of a two-floors building, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
4.7. Exercise n. 14

Referring to the network topology depicted below, determine the final outcome of the Rapid Spanning Tree Protocol, assuming that:

- the MAC address of the switch SW-x is 00:00:00:AA:AA:0x;
- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each “single” link and equal to 5 on each aggregated link;
- the Link Aggregation function is used to interconnect one switch to another when multiple links are available.
5. Multiple Spanning Tree

5.1. Exercise n. 15

Referring to the network topology depicted below, determine the final outcome of the Common and Internal Spanning Tree (CIST), assuming that:

- the Bridge Priority of each bridge is set to the default value, unless differently specified;
- the Port Path Cost is equal to 10 on each link, unless differently specified.
6. Traffic Analysis

6.1. Exercise n. 16

Given the network topology below, in which the Spanning Tree Protocol is not active, and assuming that:

- host H2 is generating a frame transporting and ICMP Echo Request packet (shown in the picture) toward H1
- host H1 has the MAC address of host H2 in its ARP cache
- the filtering database of the switches is empty

Detail a possible behavior of the network and determine if that frame (or the reply that comes from H2) can create a broadcast storm.
Part III.

Solutions
7. Spanning tree

7.1. Solution for exercise n. 1

Root Bridge Election
Considering that all the switches have the same Bridge Priority, SW-0 is elected as root because it has the lowest MAC address (00:00:00:AA:AA:00).

Root Ports Election
SW-1 and SW-2 will elect respectively Fe1 and Fe0 as root ports because they feature the lowest cost towards the root bridge (they are directly connected to the root bridge).

On switch SW-3, both ports Fe0 and Fe1 feature the same cost toward the root bridge. However, port Fe0 receives a BPDU with a better bridge identifier, and therefore is elected root port.

Designated Ports Election
Fe2 on SW-2 is elected as designated port for Ethernet C as it features the lowest cost towards the root bridge.

For Ethernet A, the designated port is Fe0 on SW-0 (it is the only port that connects that network to the rest of the net), while for the same reason the designated port on Ethernet B is the port Fe0 on switch SW-1.

Blocked Ports
All the remaining ports will be moved in blocking state. This applies to:

- Port Fe1 on switch SW-3;
- Port Fe2 on switch SW-3.
8. Rapid Spanning Tree

8.1. Solution for exercise n. 8

Spanning Tree Protocol
If the STP is enabled on the switch, each port receives the BPDU sent by the other port:

- **Fe1** receives a BPDU that has the same Root Path Cost contained in the transmitted BPDU, but with an higher Port Identifier. Therefore, the priority of the Configuration BPDU received is lower than that of the transmitted BPDU.

- **Fe2** receives a BPDU that has the same Root Path Cost contained in the transmitted BPDU, but with a smaller Port Identifier. Therefore, the priority of the Configuration BPDU received is higher than the one of the transmitted BPDU.

Since port Fe1 generates BPDUs with higher priority than port Fe2, the former port has higher priority. Therefore Fe1 is marked as *Designated*, while Fe2 is set in the *Blocking State*.

Rapid Spanning Tree Protocol
If the RSTP is enabled on the switch, the Designated port selection is exactly the same of STP and consequently port Fe2 will be blocked. Therefore, the Fe2 interface state is set to *Discarding*, while its role is set to *Back-up*, and not to *Alternate*, because the received Configuration BPDU has exactly the same Bridge Identifier of the one sent by Fe2.
8.2. Solution for exercise n. 14

- If Link Aggregation is enabled each pair of links interconnecting two switches is aggregated in one single logical link.

- Each switch has a virtual logical interface connected to each end-point of the logical aggregated pairs of links connected to the switch itself.

- The RSTP is applied on top of the logical network overlay obtained aggregating the pairs of links.

Therefore the outcome of the Rapid Spanning Tree Protocol for the previous network, using the Link Aggregation for interconnecting the switches, is the following:
9. Multiple Spanning Tree

9.1. Solution for exercise n. 15

In the network there are four MST Region and one SST Region.

- Inside each MST region the normal RSTP is applied to define the Internal Spanning Tree (IST).

- The Highest Priority Bridge is located in Region 1 (priority 4420): this is elected as the CIST Root Bridge.

- According to the IEEE 802.1s standard each MST region behaves like a single bridge in the CIST Topology: for each MST region a CIST Regional Root (the bridge of the region which is nearest to the CIST Root Bridge) is elected and the entire region behaves as a single bridge whose parameters are those of the CIST Regional Root Bridge.

  - Region 1, containing the CIST Root Bridge, behaves as a single bridge whose parameters are those of the CIST Root Bridge. In this case the CIST Root Bridge is also the Region 1 IST Root Bridge because it has the lowest BID of the region.

  - In Region 2, the BP 4860 Bridge is directly connected to Region 1, so it is elected as the CIST Regional Root. In this case the CIST Regional Root is also the Region 2 IST Root Bridge because it has the lowest BID of the region.

  - In Region 3 there is only one switch hence the CIST Regional Root Bridge and IST Root Bridge election is trivial. Assuming that all the links have equal costs, and remembering that each MST region behaves as a single bridge, the BPDUs received from Region 2 have a lower path cost towards the CIST Root Bridge hence the port connected to the Region 2 is elected as the Root Port.

  - Also in Region 4 there is only one switch and the CIST Regional Root Bridge and IST Root Bridge election is trivial. Having two ports connected to the Region 2, the received BPDUs have exactly the same BID, hence the Root Port election is based on the Port Identifier fields of the received BPDUs: because the port on the right of the BP 4960 switch receives BPDUs from the Fe1 port of the Region 2 CIST Regional Root Bridge, while the other receives BPDUs from its Fe2 port, the BP 4960 right port is elected as Root Port.
10. Traffic Analysis

10.1. Solution for exercise n. 16

Since the MAC(H1) is not in the filtering database of the switches, the frame is sent in flooding by all the switches and, having a circular path at the physical layer, the frame enters in a loop. Being flooded on all the interfaces of the switches, the frame will also reach host H1 that can reply to the ICMP Echo Request with an Echo Reply packet (in fact, MAC(H2) is known, as specified in the text exercise).

When the ICMP Echo Reply packet reaches interface Fe2, the switch SW-2 learns that address. Consequently, it associates the value of that MAC address (i.e., 00:00:00:11:11:11) to its interface Fe2. Therefore, all the frames directed to that MAC address are now forwarded to that interface and hence the loop created by the previous frame is broken. In other words, all the many copies of the ICMP Echo Request packet that were still circulating are taken out of the network and sent to host H1, which will then receives many copies of the same Echo Request.

However, the flooding problem appears again with the new packet, which is directed to station 00:00:00:22:22:22. In fact, we know that all the switches have the MAC address 00:00:00:22:22:22 in their filtering databases, but, due to the unpredictable behavior of the previous loop, we do not know which port is associated to that address. We know, however, that for every switch, the filtering database will associate the MAC address 00:00:00:22:22:22 to either ports Fe0 or Fe1, i.e. the ports that were part of the loop, since the previous frame (sent by 00:00:00:22:22:22) looped along this path.

Therefore, the final configuration of the filtering databases will be unpredictable, and each switch can have the MAC(H1) associated to either its port Fe0 or Fe1. Therefore, the filtering database will result in one among the 8 cases detailed in the following table, which describes also what will happen to the new frame sent by H1:

<table>
<thead>
<tr>
<th>SW-1</th>
<th>SW-2</th>
<th>SW-3</th>
<th>ICMP Reply (H1 → H2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fe0</td>
<td>Fe0</td>
<td>Fe0</td>
<td>Loop between SW-2 and SW-1</td>
</tr>
<tr>
<td>Fe0</td>
<td>Fe0</td>
<td>Fe1</td>
<td>Loop between SW-2 and SW-1</td>
</tr>
<tr>
<td>Fe0</td>
<td>Fe1</td>
<td>Fe0</td>
<td>Loop between SW-1 and SW-3</td>
</tr>
<tr>
<td>Fe0</td>
<td>Fe1</td>
<td>Fe1</td>
<td>Loop between SW-2, SW-1 and SW-3</td>
</tr>
<tr>
<td>Fe1</td>
<td>Fe0</td>
<td>Fe0</td>
<td>Loop between SW-2, SW-3 and SW-1</td>
</tr>
<tr>
<td>Fe1</td>
<td>Fe0</td>
<td>Fe1</td>
<td>Loop between SW-2 and SW-3</td>
</tr>
<tr>
<td>Fe1</td>
<td>Fe1</td>
<td>Fe0</td>
<td>Loop between SW-3 and SW-1</td>
</tr>
<tr>
<td>Fe1</td>
<td>Fe1</td>
<td>Fe1</td>
<td>Loop between SW-2 and SW-3</td>
</tr>
</tbody>
</table>
As it may be evident, in all the cases the ICMP Echo Reply packet will enter in a loop as well, although we do not now, a priori, which switches will be affected by the problem.

It is worthy noticing, however, that in any case the ICMP Echo Reply will never be delivered to H2 due to the data present in the filtering database, and therefore the ICMP Echo Request sent by H2 will always run into timeout.