# Network Security Lab 2

Thijs ter Horst (4156749)
Simone van Veen (4605993)
Jarno Moree (4387333)
Nourdin Ait el Mehdi (4276825)

March 1, 2017

**Question 1** *As a starting point for your lab work, complete the figure with the MAC addresses of the four PCs.*

| Host | MAC address | IP address |
|---|---|---|
| H1 | `14:58:D0:15:60:C2` | `192.168.178.11` |
| H2 | `8E:89:A5:0D:7B:B8` | `192.168.178.12` |
| H3 | `6C:71:D9:56:EB:ED` | `192.168.178.13` |
| H4 | `00:22:19:10:87:71` (eth1) | `192.168.178.14` |

**Question 2** *With all three switches connected in a ring, the spanning tree protocol will determine which links are part of the spanning tree. Can you infer this from the link status lights on the switch ports? Explain why or why not. You can base the answer on your observation at which layer STP and the link light works and what information is available to each of them.*

The LEDs blink a certain color depending on the state of the port (amber: blocked by stp, green: data flowing etc, see page 2-13 of the switch manual).

**Question 3** *Generate some traffic (a ping is enough) and interpret what you see. Which of the links are active and how does the traffic flow? Draw the active topology of the network.*

No direct link exists between S2 and S1. Checked using Wireshark, ping H1 $\rightarrow$ H2 and we connected the port mirror on S2 0/1, where we measured no data. Also from H2-H1 there was no data over S2 0/1.

**Question 4** *Mark in the figure the switch acting as the tree's root in your diagram.*

Because there is no direct link between S2 and S1, STP wants to minimize the cost over all connectections and the cost over each link is equal, S3 has to be the root.

**Question 5** *What can an administrator do to change the root of the topology?*

The administrator can change the root by changing the priority of the switches. The lower priority value, the higher the actual priority. When all priorities are equal, changing the MAC address would also work. STP gives the device with the lowest MAC address value the highest actual priority.

**Question 6** *How is the spanning tree reestablished? How long does it take for STP to converge?*

At t=90 the network noticed that the link between S2 and S3 was broken. Then at t=118, the spanning tree re-established. Thus, it took 28 seconds for the network to re-establish The new tree still has S3 as root (its priority did not change), and there is a link between S3 and S1, and a link between S1 and S2.

**Question 7** *Using the trace you have collected, analyze which STP messages are flowing through the links at which time.*

When breaking an existing link, two messages with a topology change notification are sent through the network. The same two messages are sent when the network has been re-established.

**Question 8** *How does the tool modify the setup? Monitor the behavior of the tool, how and how often does it send such spoofed messages?*

We put H4 is S1 0/9, put H1 at S1 0/15 to make it listen to S1 0/1.
The tool does not modify the setup (yet), because the link it connected to is turned off by the switch (amber LED) because it recognizes an attack.

**Question 9** *Continue until you see the attack being successful. What might determine whether the attack is successful?*

We tried a lot of ports on S1, eventually also port 0/6: this becomes green instead of amber (like most other). An attack can only be successful when a port is configured as a trunk port (it accepts STP messages) instead of an access port (which does not accept STP messages but only normal traffic).

**Question 10** *Do you see the traffic flows between H1, H2, H3 appearing on H4? Which flows do you see, which don't you see?*

Even though H4 is root, H4 does not see any of the traffic between H1, H2 and H3. All traffic goes through S1, but that does not mean that H4 has access to the data.
Old topology: $S3 \rightarrow S1,\ S3 \rightarrow S2$.
New topology: $H4 \rightarrow S1,\ S1 \rightarrow S2,\ S1 \rightarrow S3$.

**Question 11** *Which additional information do the switches use for packet forwarding, and how does this information relate to STP? What would be necessary to intercept the traffic of all hosts in the simple network at H4? Describe the next step, but do not implement the attack.*

Switches use ARP to forward incoming packets to the correct outgoing link. STP determines which links are actives, and ARP messages follow these links.

Using ARP spoofing, H4 can receive messages that are destined to H1, H2 or H3.

**Question 12** *How would you estimate its performance against a modern desktop or laptop CPU?*

The CPU of the Catalyst 3500 is the PowerPC 403, which runs at 20-80MHz. Obviously, this is pretty slow.

**Question 13** *Explain what happens inside the switch during the attack. What is therefore the consequence to the traffic?*

The CPU has to process information in all BPDUs. Unfortunately, the CPU will be far too slow to handle a large amount of BPDUs sent by the DOS attacker. It will not have enough time to connect the correct ports, so data will be lost.

**Question 14** *How does the amount of injected control messages influence the CPU load?*

Obviously, when more packets are being sent, the CPU load increases. The increase seems to be linear with the number of control messages.

**Question 15** *As the rate of packets increases, the CPU is loaded with processing the spoofed requests. How many control messages per second are necessary before the switch does not properly function anymore?*

-

**Question 16** *Could an administrator configure a network in such a way that claiming a root role through forged BPDUs would be impossible? Is this a practical countermeasure?*

Yes, that would be possible, by only configuring the ports to which a switch is connected as trunk ports, and all other ports should be access ports. Also, unauthorized access to the switches should be prevented. This is a practical counter measure, because switches are not being replaced every day anyway, so it is not that impractical when the switch setup is not flexible.

**Question 17** *Discuss the parameters these commands have, and evaluate which configurations are most suitable for your setup*

Enabling storm control allows the switch to limit the number of broadcast packets it forwards. This will also limit BPDU messages from a single source.

**Question 18** *Explain conceptually how your chosen protection scheme works and what happens now during an attack?*

Similar data from a single source is limited, and therefore it does not have to be processed. This should limit the CPU load immensely.