Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Networked Systems
ETH Zürich — seit 2015

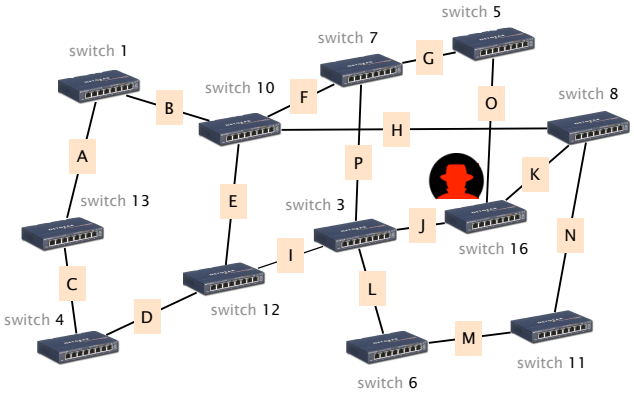
Communication Networks

Prof. Laurent Vanbever

Solution: Exercise week 5 – Ethernet & Switching

Spanning-Tree (Exam Style Question)

Consider this network composed of 12 Layer 2 (Ethernet) switches.



Compute a valid spanning tree, with and without hacker

a) Use the Spanning-Tree Protocol (STP) described in the lecture to compute a spanning tree. The numbers next to each switch indicate the switches identifier (switch 1 has ID "1"). Each link is labeled with a letter. Indicate the set of links (the letters, in alphabetical order) that are not part of the STP after the protocol has converged.

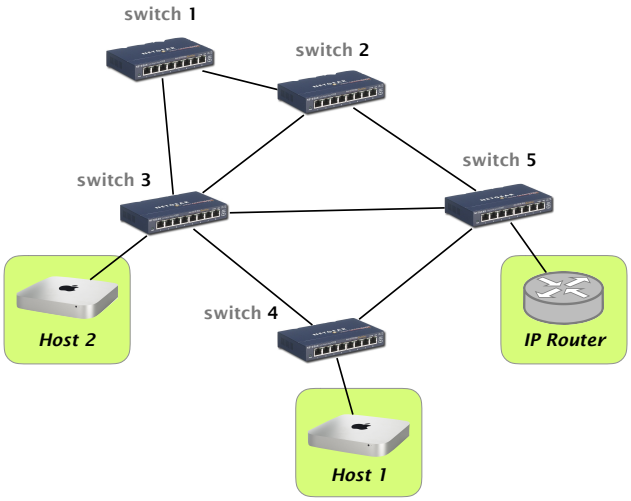
Solution: [D,I,J,M,O] since tie-breaking is done based on the switch ID.

b) As described in the course, STP is not the most secure protocol. Assume now that a hacker managed to take over switch 16 and starts pretending that the switch ID is "1". Concretely, there are now two switches with ID "1" in the network. Indicate the set of links that the attacker will manage to attract traffic from, once the protocol has converged. Is the network still connected?

Solution: [I,J,K,L,N,O,P]. And, *no*, the network is not connected anymore.

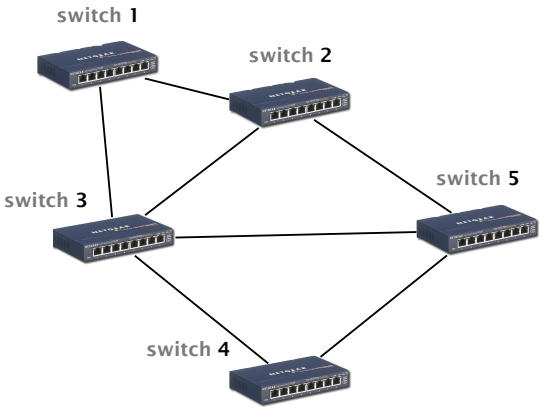
Moving Target (Exam Style Question)

Consider the switched network depicted in the figure below. It is composed of 5 Ethernet switches, two hosts (connected to switch 3 and 4, respectively) and one IP router acting as default gateway for the hosts. For redundancy reasons, the network exhibits cycles and each switch therefore runs the Spanning Tree Protocol (STP). All links have a unary cost. When equal-cost paths to the root are encountered, switches break the tie based on the sender ID (lower is better).



An Ethernet network running the spanning tree protocol.

a) In the figure below, cross all the links that end up **deactivated** in the final state, once all the switches have converged on the final spanning tree.



Solution: Links $(4,5)$, $(3,5)$ and $(2,3)$ end up disabled.

b) Perhaps unsurprisingly, a *lot* of traffic is exchanged between Host 1 (resp. Host 2) and Internet destinations. Briefly explain **two distinct reasons** why this configuration is not optimal in terms of network utilization/throughput.

Solution: Any communication between Host 1 (resp. Host 2) and IP router goes over 4 (resp. 3) links. Plus, these links are shared meaning Host 1 and Host 2 will be competing for throughput.

c) Realizing that there is a problem with their configuration, the network operators ask you (a fresh network engineer!) to help them improve their network performance. Briefly explain how you would adapt the configuration of the spanning tree protocol (i.e., the switches identifier and/or the link costs) so as to maximize the throughput between Host 1 (resp. Host 2) and Internet destinations.

Solution: Flipping the switch IDs so that the now-switch 5 becomes the root (e.g. making it switch 1 and the now-switch 1, switch 5).

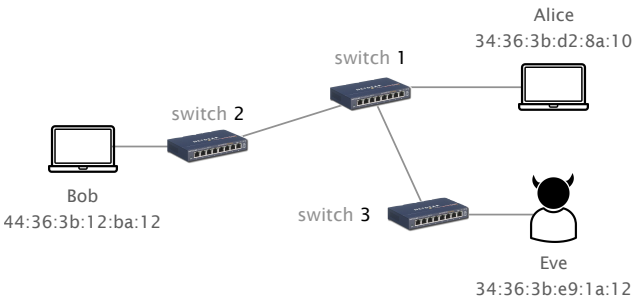
d) The network operators are happy with your changes. But they now realize that Host 1 and Host 2, in addition to exchanging a lot of Internet traffic, also exchange a lot of traffic between themselves. The network operators ask for your help again! They ask you to find a spanning tree configuration such that: *(i)* the number of hops between any of these three hosts (Host 1 and 2, and the router) is equivalent; and *(ii)* the number of hops is minimum.

Briefly explain how you would configure the spanning tree protocol to achieve these requirements, or why these requirements are impossible to achieve.

Solution: Requirements are impossible to get: Either the hosts are using their direct link with each other, or with the router. But they cannot all use the direct link between themselves as otherwise that would cause a loop which would be prevented by the spanning tree protocol anyway.

Duplicate MAC Address

Consider three hosts Alice, Bob, and Eve connected through the network below composed of 3 Layer 2 (Ethernet) switches.



In the beginning the tables of the learning switches are still empty. Bob starts sending Ethernet frames to Alice. Eve is curious and wants to know what Bob is sending to Alice.

a) What is the source and destination address in the Ethernet header for frames sent from Bob to Alice?

Solution: Source address: 44:36:3b:12:ba:12
Destination address: 34:36:3b:d2:8a:10

b) What do the switches do when they receive the frames?

Solution: Each switch adds a new entry to its table with the source MAC address and the incoming port. As the address of Alice is not yet in any of the switch tables, each switch floods the frame on all ports, but the port the packet came in on. This means the frame is sent to both Alice and Eve.

c) Due to the flooding, the frames are sent to both Alice and Eve. Does Eve actually receive the frames? (*hint:* promiscuous mode).

Solution: As long as Eve's Ethernet adapter is not set to promiscuous mode, the frame is not decapsulated and Eve will not receive it.

Alice starts acknowledging the received frames by sending frames to Bob.

d) Is Eve able to eavesdrop either on the frames being sent from Alice to Bob or on new frames sent from Bob to Alice? Explain.

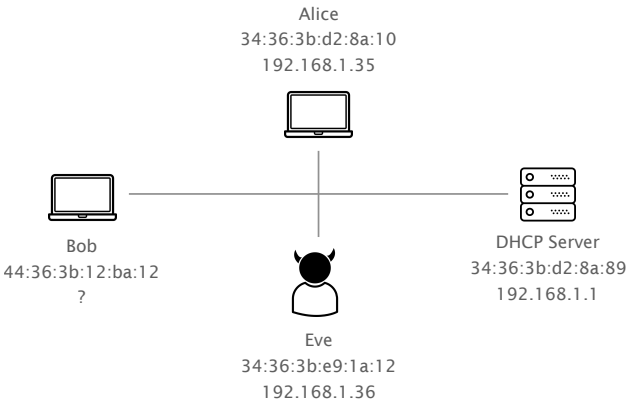
Solution: No. The frames from Alice to Bob will not be flooded as the switches already know the path. After the first frame from Alice reaches Bob, the switches have also learned over which ports Alice can be reached. Frames from Bob to Alice are therefore no longer flooded.

e) Can you think of a way for Eve to redirect the frames destined to Alice again to herself?

Solution: Eve can send an Ethernet frame destined to Bob with the source address set to the MAC address of Alice. The switches will update their tables and Eve will receive the frames for Alice as long as Alice does not send a packet.

Impostor

The three hosts Bob, Alice and Eve are all connected to the same network, which has a DHCP server.



Bob just connected to the network and wants to send important IP packets to Alice. Bob only knows the IP address of Alice (`192.168.1.35`) and his laptop is not yet configured with an IP address.

a) Explain all the steps that are necessary such that Bob's computer can finally send packets to Alice.

SRC MAC address	DST MAC address	Message type	Message content
44:36:3b:12:ba:12	ff:ff:ff:ff:ff:ff	DHCP discovery	I need an IP address
34:36:3b:d2:8a:89	44:36:3b:12:ba:12	DHCP offer	use 192.168.1.37
44:36:3b:12:ba:12	ff:ff:ff:ff:ff:ff	ARP request	Who has 192.168.1.35 Tell 192.168.1.37
34:36:3b:d2:8a:10	44:36:3b:12:ba:12	ARP reply	192.168.1.35 is at 34:36:3b:d2:8a:10

b) Eve is very interested to find out what Bob is sending to Alice. What could she do to intercept Bob's packets?

Solution: When Bob sends the ARP request to learn the MAC address of Alice, Eve also receives it as it is destined to the MAC broadcast address (`ff:ff:ff:ff:ff:ff`). If Eve can send a fake reply to Bob before Alice does so, she can make Bob believe that her MAC address is the one of Alice. This is called ARP spoofing.