Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Networked Systems
ETH Zürich — seit 2015

Communication Networks

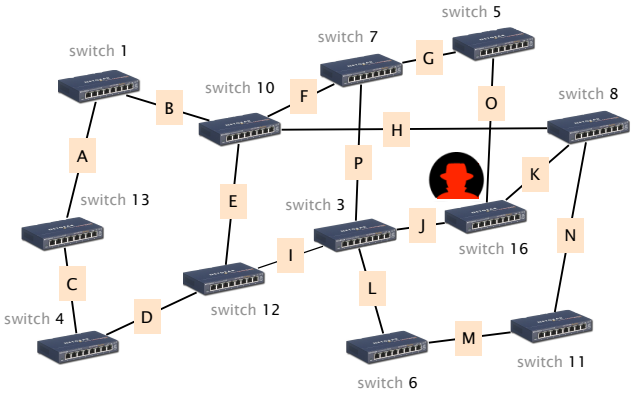
Prof. Laurent Vanbever

Solution: Exercise 4 – Ethernet & Switching and Internet Protocol (IP)

Ethernet & Switching (Part 2)

4.1 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.

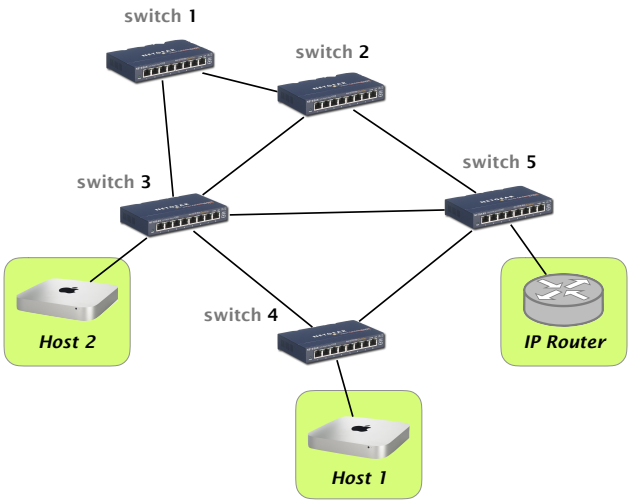
Solution: [D,I,J,M,O] since tie-breaking is done based on the switch ID.

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 will now be part of the attacker's spanning tree, 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.

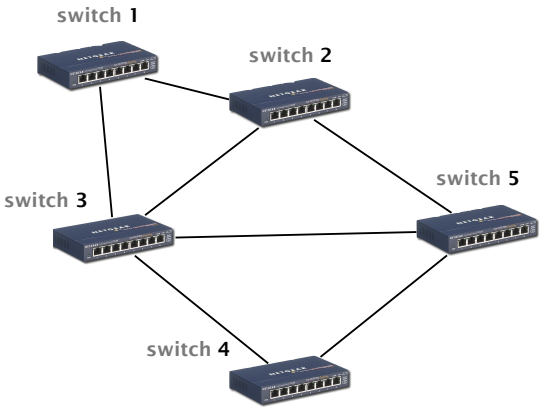
4.2 Moving Target (Exam Style Question)

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.

Internet Protocol (IP)

4.3 IP Calculations

Each row in the following table describes an IP network. Fill in the missing values.

Solution:

Slash–notation	Netmask–notation	First usable address	Last usable address	Broadcast address
10.0.0.0/24	10.0.0.0/255.255.255.0	10.0.0.1	10.0.0.254	10.0.0.255
126.127.128.0/17	126.127.128.0/255.255.128.0	126.127.128.1	126.127.255.254	126.127.255.255
12.34.32.0/19	12.34.32.0/255.255.224.0	12.34.32.1	12.34.63.254	12.34.63.255
222.208.0.0/12	222.208.0.0/255.240.0.0	222.208.0.1	222.223.255.254	222.223.255.255
123.45.67.224/27	123.45.67.224/255.255.255.224	123.45.67.225	123.45.67.254	123.45.67.255

IPv6 addresses have a slightly different notation. Because the addresses are 128 bit long, we switch from a decimal notation to a hexadecimal one. In general, IPv6 addresses are represented by eight colon-separated blocks of up to four hexadecimal digits each. In a block, leading zeros can be omitted. Furthermore, we can use the "::" symbol to compress one or more consecutive zero blocks. However, the "::" symbol can only be used once in a single IPv6 address. As an example, the IPv6 address: 2001:0db8:0000:0000:0000:ff00:0042:8329 can be simplified to 2001:db8::ff00:42:8329.

a) You are the operator of an enterprise network. Your ISP is giving you a /96 subnet 2001::/96. How many addresses do you have available? Is that a reasonable subnet size compared with the currently available IPv4 addresses?

Solution: You have $2^{128-96} - 1 = 4'294'967'295$ addresses available (no broadcast addresses in IPv6). This is as if you had all IPv4 addresses available exclusively for your enterprise network.

b) In your enterprise network, each host machine is identified by a unique ID starting from 1. Now that you have a lot of IPv6 addresses available, you decide to give each host a unique IP address. The host with ID 1 gets the first IPv6 address in your subnet (2001::1), the host with ID 2 the second IP address and so on. Complete the following table:

Solution:

IPv6 address	**host ID**
2001::5	5
2001::E	14
2001::3A5	933
2001::FFFF:FFFF	4 294 967 295
2001::3:0	196 608

4.4 Detective work

You just started your first job as a network operator of a small network. To get more familiar with the network, you look at a packet trace captured at a switch. The trace contains packets from multiple hosts and one router connected by a (layer 2) switch. The router acts as default gateway, providing access to the Internet and is assigned the first IP address in the subnet. Each row in the following table represents one packet observed at the switch.

SRC MAC Address	DST MAC Address	SRC IP Address	DST IP Address
6a:00:02:49:a1:a0	11:05:ab:59:bb:02	65.222.11.1	65.222.8.2
6a:00:02:49:a1:a0	da:15:00:00:01:11	65.222.11.1	65.222.16.1
da:15:00:00:01:11	11:05:ab:59:bb:02	129.132.103.40	65.222.8.2
11:05:ab:59:bb:02	40:34:00:7a:00:01	65.222.8.2	65.222.15.254
11:05:ab:59:bb:02	ac:00:0a:aa:10:05	65.222.8.2	65.222.9.99
ac:00:0a:aa:10:05	01:05:3c:34:00:02	65.222.9.99	65.222.13.255
6a:00:02:49:a1:a0	da:15:00:00:01:11	65.222.11.1	65.222.8.1

a) Can you identify all the hosts that are part of the local network?

Solution: The local hosts are all the sources and destinations that do not have to go through the default gateway (e.g., their MAC address is not replaced by the MAC address of the router):

- 65.222.11.1
- 65.222.8.2
- 65.222.9.99
- 65.222.15.254
- 65.222.13.255

b) Can you reconstruct the IP subnet used to address the hosts within that local network?

Solution: First, we should note, that the router MAC address is only used for IP sources or destinations outside the local subnet (router is used as gateway) or for packets from/towards the router. With this in mind, we can identify the lowest subnet address from the packets (65.222.11.1 -> 65.222.8.1) and (65.222.11.1 -> 65.222.8.2) as 65.222.8.1. Furthermore, we can infer that 65.222.15.254 still belongs to the local subnet (65.222.8.2 -> 65.222.15.254) but 65.222.16.1 is a destination outside of the network (65.222.11.1 -> 65.222.16.1). We can therefore identify the used subnet as 65.222.8.0/21.

4.5 Summer Pruning (Exam Question 2018)

Consider an IP router with a forwarding table composed of the 9 entries depicted on the left. Write down (on the right) an equivalent forwarding table by combining entries together into shorter ones such that the resulting table has the least number of entries. Your reduced forwarding table should be such that the forwarding decision made by the router for any IP packet is equivalent to the initial one.

Solution:

prefix	next-hop
82.130.32.0/20	1
82.130.64.0/20	1
82.130.80.0/20	2
82.130.96.0/20	1
82.130.112.0/21	1
82.130.120.0/21	1
82.130.122.0/24	1
82.130.123.0/24	1
82.130.124.0/24	2

prefix	next-hop
82.130.32.0/20	1
82.130.64.0/18	1
82.130.80.0/20	2
82.130.124.0/24	2

Answer to the same question as above considering the forwarding table below instead (left) in which an extra default route is defined.

Solution:

prefix	next-hop
0.0.0.0/0	1
82.130.32.0/20	1
82.130.64.0/20	1
82.130.80.0/20	2
82.130.96.0/20	1
82.130.112.0/21	1
82.130.120.0/21	1
82.130.122.0/24	1
82.130.123.0/24	1
82.130.124.0/24	2

prefix	next-hop
0.0.0.0/0	1
82.130.80.0/20	2
82.130.124.0/24	2