Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

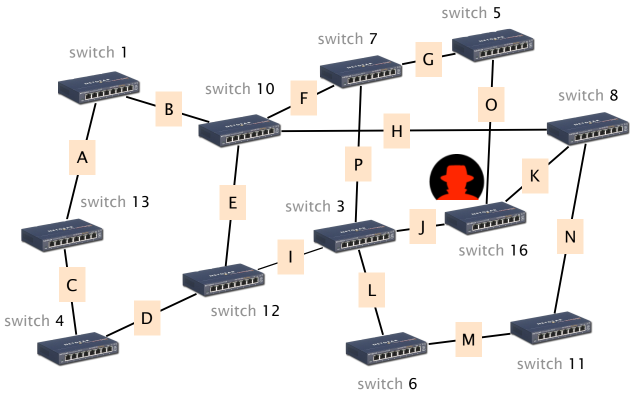
Prof. Laurent Vanbever
Networked Systems Group

Communication Networks

Solution: Exercises week 5 & 6 – Ethernet, Switching, Internet Protocol & Forwarding

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.

IPv4 vs. IPv6

a) In the lecture you heard about IPv4 and IPv6. Why was IPv6 introduced? What is the main difference?

Solution: The main motivation for IPv6 is the IPv4 address exhaustion. Even though Network Address Translation (NAT) could temporarily solve the problem, there are no longer enough IPv4 addresses / subnets for all the devices connected to the Internet. The main difference is the higher number of bits for each IP address (128 instead of 32). Furthermore, IPv6 also handles e.g. fragmentation or header options in a different way.

b) How many IPv4 and IPv6 addresses exist? Is it possible to use all the addresses for hosts in the Internet?

Solution: IPv4: $2^{32} \approx 4.3 * 10^9$

IPv6: $2^{128} \approx 3.4 * 10^{38}$

No, it is not possible to use all the addresses. Some address spaces are reserved e.g. for private addresses. Other addresses are used to identify the network/router or as broadcast addresses.

c) Assuming there are 7.5 billion people in the world, how many IPv4/IPv6 addresses are theoretically available per person?

Solution: IPv4: $2^{32}/(7.5 * 10^9) \approx 0.57$

IPv6: $2^{128}/(7.5 * 10^9) \approx 4.5 * 10^{28}$

d) Even though IPv6 has been standardized more than 10 years ago, it still has very limited coverage. What are the reasons why the deployment of IPv6 is so slow?

Solution: Every network device, which has to interact with the network layer, needs to be able to understand the new IPv6 addresses and the corresponding header. It is therefore not possible to switch from IPv4 to IPv6 on one specific day. Upgrading the hardware is costly and especially for end-users there is no real motivation. At the moment, everything seems to work well with IPv4 addresses.

IPv4 Calculations

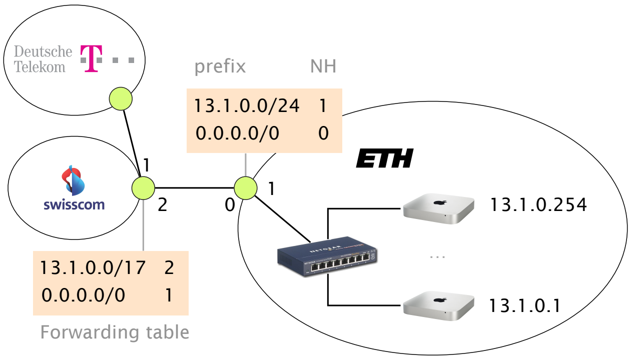
Each row in the following table describes an IP network. Fill in the missing values.

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

The Art of Defaulting Properly (Exam Style Question)

Consider this simple network configuration between ETH and Swisscom. Assume that ETH owns a large IP prefix 13.1.0.0/17, but only uses 13.1.0.0/24 to address its internal hosts. For simplicity, we assume that ETH and Swisscom operators configure their forwarding table statically and rely on the use of a default route (0.0.0.0/0).



prefix	NH
13.1.0.0/24	1
0.0.0.0/0	0

13.1.0.0/17	2
0.0.0.0/0	1

Where are my IP packets going?

a) How many IP addressable addresses does ETH “own” in total?

Solution: $2^{(32-17)} - 2$

b) Give the first and last IP address that ETH can use for addressing a host.

Solution: 13.1.0.1 and 13.1.127.254

c) Suppose Swisscom receives a packet for 13.1.0.66 from Deutsche Telekom. What is the path taken by this IP packet?

Solution: Swisscom/1 → Swisscom/2 → ETH/0 → ETH/1

d) Suppose Swisscom receives a packet for 13.1.66.1 from Deutsche Telekom. What is the path taken by this IP packet?

Solution: Swisscom/1 → Swisscom/2 → ETH/0 → Swisscom/2 → ETH/0 → ...

e) What eventually happens to the packet for 13.1.66.1? As an attacker observing this, could you use this observation to congest the ETH-Swisscom link more easily? Explain why (or why not).

Solution: It will eventually gets dropped as the TTL reaches 0. Permanent forwarding loops can be used to perform a Denial of Service (DoS) attack with few resources. Here an attacker can simply start sending fake traffic to 13.1.66.1 which will start “pilling up” on the Swisscom ↔ ETH link. The actual damages will depend on: *i)* the rate at which the attacker can send; *ii)* the TTL of the packets; as well as *iii)* the actual capacity of the link. Observe that the induced congestion negatively impact *all* traffic, including traffic destined to 13.1.0.0/24.