Network training

Maël Auzias

Fall 2014

1 Introduction

1.1 Classification

Give a concrete example of each of the following kinds of networks (name some entities):

1. BAN,
2. PAN,
3. LAN,
4. WAN.

1.2 Topologies

Give a concrete example of each of the following network topologies:

1. Bus,
2. Star,
3. Fully connected.

1.3 TCP connection

According to TCP (RFC761 (January 1980)), what are the sequences used in order to establish a connection between two hosts?

1.4 TCP or UDP?

1.4.1 Sensors

You are creating a network application using sensors. The sensors can receive requests to change their settings (rate of measurement, range...) and they continuously send their measurements.

1. Should request packets (settings) be sent with UDP or TCP? Why?
2. Should measurement packets be sent with UDP or TCP? Why?

1.4.2 Website

Does HTTP (RFC2616 (June 1999)) rely on TCP or UDP? Why?

1.5 FTP

1.5.1 Is FTP secure?

According to the file ftp-connect.pcap is FTP secure? What could you do to use it more securely?

1.5.2 FTP and TCP

According to the file ftp-disconnect.pcap , does FTP respect the TCP protocol to close a connection?

1.6 DNS

1.6.1 Some news

According to the file nslookup.pcap what is:

1. the DNS server?
2. the domain name for which the IP address is needed?
3. the IP address of the domain if any?

n

1.6.2 Which one?

According to the file nslookup-whoseone.com.pcap what is:

1. the DNS server?
2. the domain name for which the IP address is needed?
3. the IP address of the domain if any?

1.7 Ping-pong

1.7.1 Are you there?

According to the file ping.pcap :

1. what is the node 127.0.0.1 doing?
2. Is the node 127.0.0.2 on the network?

1.7.2 Who has this IP?

According to the file arp.pcap and to ARP (RFC826 (November 1982)). What is the source trying to do? What is ARP used for? If ever a host does not respond to ping (i.e., for security reasons), how could you check if the host is up anyway ?

2 Physical layer

2.1 General

2.1.1 Aims

What are the layer-1 goals?

2.1.2 Name it

What is the common (*commercial*) name of:

1. IEEE 802.11
2. IEEE 802.15.1
3. IEEE 802.15.4

What is IEEE 802.15 related to? What does WPAN stand for?

2.2 Encoding, encrypting, decoding

It is important to know what are the differences between encoding and encryption. The following questions are related to theses subjects.

2.2.1 Encrypt?

What are the differences between encoding and encryption?
What are the two main kinds of encryption? Their advantages?
Name three well known cryptographic methods and three well known encoding methods.

2.2.2 Encode it

The string `"Zp"` (which does not mean anything but has a nice binary value) is, according to ASCII, `0x5a70`. Encode it using:

1. Multi-Level Transmit
2. Alternate Mark Inversion
3. Manchester (or differential Manchester)
4. Biphase Mark Code

2.2.3 Decode it

What are the ASCII characters of theses images:

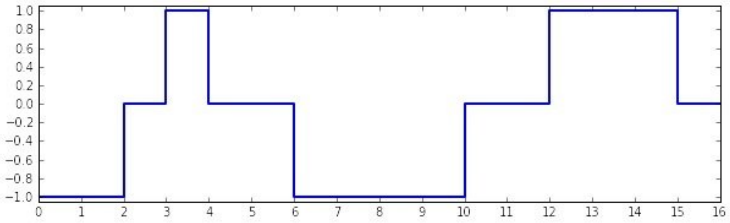

Figure 1: MLT3 encoded

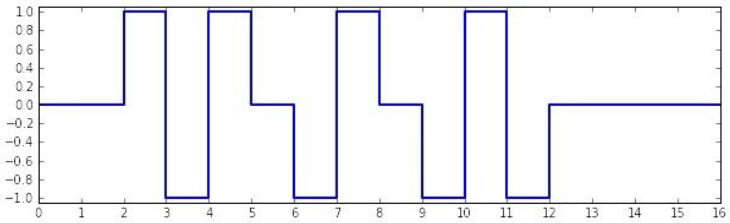

Figure 2: AMI encoded

2.3 For*Oh*For error

2.3.1 Calculate it

What would be the output of the binary: `0b0011 0000 0100 0001` using the error detection methods:

1. Repetition (2)
2. Parity (odd)

3. Parity (even)
4. Checksum (over 4 bit)
5. MD5 hash

2.3.2 Validate it

Are theses received data correct? NB: detection values are in square brackets.

1. Using repetition (2), was received: `0b0011 1110 1001 [0011 1110 1001]`
2. Using parity (odd), was received: `0b1011 1010 1100 0111 [1]`
3. Using parity (even), was received: `0b1011 1010 1100 0111 [1]`
4. Using checksum (over 4 bit), was received: `0b0011 0111 0010 0010 1110 1001 1101 1001 [1011]`
5. Using MD5, the string was received (without the quotes): `"that's way too long..."` the md5 sum: `[3be37cad170213a8ad936c0640e3238b]`

2.3.3 Correct it

By using MDPC (Multidimensional parity-check code) the data received are: `0x01 09 0e 06 03 09 0b 0c`. Are the data correct? What would be the correction?

0x01	0x09	0x0e
0x06	0x03	0x09
0x0b	0x0c	

Figure 3: Data received with MDPC

2.3.4 Half or full?

What is the difference between half and full duplex medium?

3 Data layer

3.1 General

3.1.1 Aims?

What are the main objectives of the data layer?

3.1.2 Composition

What are the sublayer of the data layer?

3.2 Ethernet packet decoding

According to the packet on the Figure 4, which machine tried to ping which machine? Give MAC and IP address of both machines.

3.3 Ping

For security reasons, the administrator of a machine disabled the ping response. How can you assure that this host is up or not (assuming no other security rules on the machine)?

0000	ff	ff	ff	ff	ff	ff	00	1b	11	09	aa	88	08	00	00	01
0010	08	00	06	04	00	01	00	1b	11	09	aa	88	c0	a8	ff	ff
0020	ff	ff	00	00	00	00	c0	a8	00	3c						

Figure 4: Layer 2 packet

3.4 CSMA/CA

What does this acronym stand for? What and how is it used for? Is there any differences for the CSMA/CA between half and full duplex medium?

4 Network layer

4.1 General

4.1.1 Aims?

1. What are the main objectives of the network layer?
2. What are the two main objectives of host addressing?
3. Does this layer use reliable communication? What is the difference between end-to-end packet transmission layer-2 and layer-3?
4. What is the routing used for? What is "load balancing"?

4.1.2 Adressing

1. How many bits does an IP address have?
2. What are the two parts of an IP address?
3. How many bits is each part? What does determine it?
4. How is a mask constituted?
5. How many addresses and nodes does theses mask allow: /31, /30, /24, /16, /8, /4?
6. What are the specifications of network and broadcast addresses?
7. What are the first and last **nodes** IP addresses of theses networks:
   - 192.168.2.0/24
   - 192.168.2.0/23
   - 172.13.0.0/16
   - 10.0.1.0/31
   - 10.0.2.0/30
8. Are theses IP addresses public or private?
   - 1.2.3.4
   - 192.168.2.35
   - 8.8.8.8
   - 208.67.222.222
   - 208.67.220.220

- 176.34.131.233
- 127.192.168.1
- 224.0.0.2
- 0.0.0.0

4.2 Designing

4.2.1 Subnetworks

Starting from the 192.168.0.0 IP address, calculate the subnet masks, subnetwork IP address, first node IP address, last node IP address and broadcast addresses for theses networks:

- 29 hosts,
- 60 hosts,
- 121 hosts.

All theses networks are on the same CIDR 192.168.0.0/24.

4.2.2 Inter-network

A inter-network is as follow:

- With two routers (A and B) within the subnetwork having 10.0.0.0 IP address.
- Router A has a subnetwork n1, with 40 hosts, having 192.168.3.64 IP address.
- Router A has a subnetwork n2, with 10 hosts, having 192.168.3.144 IP address.
- Router B has a subnetwork n3, with 1500 hosts, having 176.16.0.0 IP address.
- Router B has a subnetwork n4, with 30 hosts, having 176.31.25.224 IP address.

How many different subnetworks are in this network?
How many NIC (at least) do the routers A and B have?
Draw the schema of the network.
Design the network, using the best subnet mask for each subnet (subnet masks, subnetwork IP address, first node IP address, last node IP address, broadcast address).

4.3 CIDR

4.3.1 Subnetworks

The following networks are in a routing-table. Is it possible to combine routes? How? Which ones? What is

Destination	Gateway	Genmask	Iface
192.168.0.0	10.0.0.2	255.255.255.128	E0
130.1.2.0	10.0.0.6	255.255.0.0	E1
192.168.1.112	10.0.0.2	255.255.255.240	E0
192.168.3.0	10.0.0.2	255.255.248.0	E0
192.168.5.0	10.0.0.6	255.255.248.0	E1

Figure 5: Routing table example

the important information that is missing to route?

4.4 Routing

4.4.1 New route

A router just got an update with theses networks: 57.6.96.0/21, 57.6.104.0/21, 57.6.112.0/21, 57.6.120.0/21. If the routes uses the same NIC, can they be summarized?

4.4.2 New network

A router has a route for the range 29.18.0.0 to 29.18.128.255 into the route 29.18.0.0/17. A new 1024-addresses network, from 29.18.60.0 to 29.18.63.255, got advertised on a new interface of the router. Should the CIDR be spread out?

4.4.3 Next hop?

A router has the routing table: What will the router do with packets being destined to:

Address/mask	Next hop
135.46.56.0/22	Iface 0
135.46.60.0/22	Iface 1
192.53.40.0/23	Router 1
0.0.0.0	Router 2

Figure 6: Routing table

- 135.46.63.10
- 135.46.57.14
- 135.46.52.2
- 192.53.40.7
- 192.53.56.7

4.4.4 Two or one router?

Lot of firm use two routers in case of one crashes. Is the NAT-ing possible?

4.5 IPv6

If 1 million IPv6 addresses are allocated at each picosecond, how long does it take to allocate the last one (assume that there are no special IPv6)?

5 Transport layer

5.1 Is UDP useless?

As both are not reliable, why can't users send IP packet instead of UDP ?

5.2 UDP and TCP

Why don't they use PID instead of (random) port to access to a socket?