

Network training

Maël Auzias

Fall 2014

Contents

1	Introduction	2
1.1	Classification	2
1.2	Topologies	2
1.3	TCP connection	2
1.4	TCP or UDP?	2
1.4.1	Sensors	2
1.4.2	Website	2
1.5	FTP	2
1.5.1	Is FTP secure?	2
1.5.2	FTP and TCP	2
1.6	DNS	3
1.6.1	Some news	3
1.6.2	Which one?	3
1.7	Ping-pong	3
1.7.1	Are you there?	3
1.7.2	Who has this IP?	3
2	Physical layer	3
2.1	General	3
2.1.1	Aims	3
2.1.2	Name it	3
2.2	Encoding, encrypting, decoding	4
2.2.1	Encrypt?	4
2.2.2	Encode it	4
2.2.3	Decode it	4
2.3	For <i>Oh</i> For error	5
2.3.1	Calculate it	5
2.3.2	Validate it	5
2.3.3	Correct it	5

1 Introduction

1.1 Classification

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

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 are 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. Following questions are related to these 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 these images:

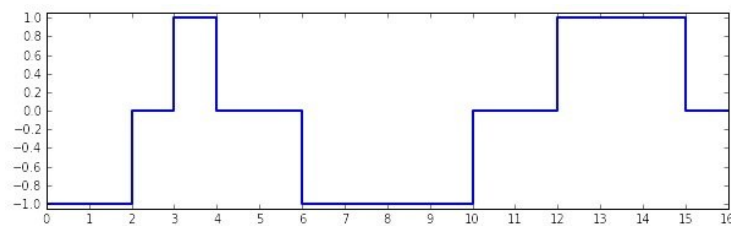


Figure 1: MLT3 encoded

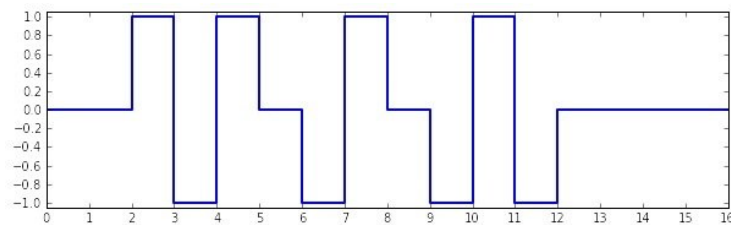


Figure 2: AMI encoded

2.3 For *Oh*For error

2.3.1 Calculate it

What would be the output of the binary: 0b0011 0000 1110 1001 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 these received data correct? NB: detection values are in square brackets.

1. Using repetition (2), was received: 0b0011 0011 0000 0000 1110 1001 1001 1001
2. Using parity (odd), was received: 0b1011[1] 1010[0] 1100[1] 0111[1]
3. Using parity (even), was received: 0b1011[1] 1010[0] 1100[1] 0111[1]
4. Using checksum (over 4 bit), was received: 0b0011 0111 0010 0010 1110 1001 1101 1001 [1011]
5. Using MD5, was received the string (without the quotes!): "that's way too long..."
the md5 sum: [3be37cad170213a8ad936c0640e3238b]

2.3.3 Correct it

to be done...