

Digital communication: internet

J.-M Friedt

FEMTO-ST/time & frequency

`jmfriedt@femto-st.fr`

slides at `jmfriedt.free.fr`

March 14, 2021

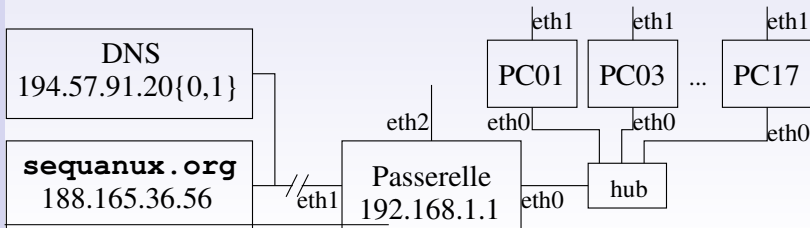
Objective of this presentation

- Understand some of the protocols used on the Internet ¹
- Principle of packet routing and network configuration
- Introduction to some of the most useful protocols
- Associated tools to trigger transactions and fetch answers
- Use for scripting transaction requests and traffic analysis, analyze security issues

¹K. Hafner & M. Lyon, *Where Wizards Stay Up Late*, Simon & Schuster (1998)

Internet compatible digital communication

- IP (*Internet Protocol*): decentralized packet routing²
- interfaces define how packets are transmitted to the next communication link
- routing rules define the destination of each data packet
- a maximum time of live of each packet limits the number of routing steps
- MAC address: physical address of each interface, unique
- IP address: virtual adresse associated with a geographic location
- MAC-IP relation: ARP
- IP-domain name relation: DNS (/etc/resolv.conf)



²W.R. Stevens, *TCP/IP Illustrated Vol. 1*, Addison & Wesley (1994)

OSI layers

- physical layer: Ethernet, 802.11 Wi-Fi (collision handling, data packets)
- presentation layer: IP
- session layer: ICMP, UDP, TCP, ARP
- notions de client-serveur et sockets \Rightarrow fork()

OSI model of network hierarchical layers ³

	Layer/function	example
7	Application	(DNS, FTP, NTP ...)
6	Data representation	(ASCII, EBDIC, ...)
5	Session	(socket)
4	Transport	(TCP, UDP)
3	Network Packets	(IP)
2	Medium Access Control	(AppleTalk, 802.3 "ethernet")
1	Physical	(RS232, Ethernet 10BaseT, 802.11 "Wi-Fi")

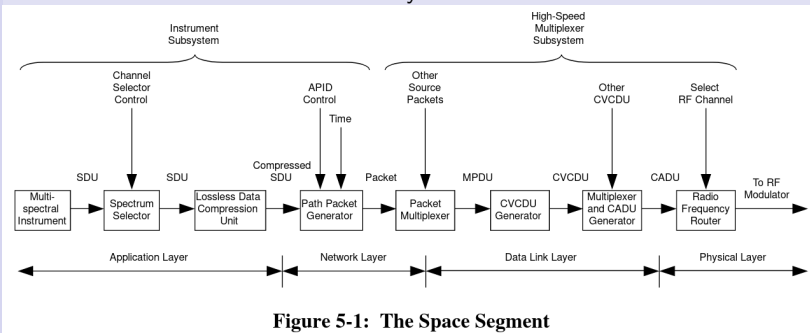
Any computer supporting IP defines local address: 127.0.0.1 (localhost)

³J.-M Friedt, *Decoding Meteor M2: QPSK, Viterbi, Reed Solomon and JPEG*
FOSDEM 2019, video at
https://archive.fosdem.org/2019/schedule/event/sdr_meteorm2n/ and
http://jmfriedt.free.fr/glmf_meteor_eng.pdf

OSI layers

- physical layer: Ethernet, 802.11 Wi-Fi (collision handling, data packets)
- presentation layer: IP
- session layer: ICMP, UDP, TCP, ARP
- notions de client-serveur et sockets \Rightarrow fork()

OSI model of network hierarchical layers ³



<https://public.ccsds.org/Pubs/120x0g2s.pdf>, p.26

Any computer supporting IP defines local address: 127.0.0.1 (localhost)

Network configuration on GNU/Linux

1 *interfaces: ifconfig eth0 192.168.1.1*

```
jmfriedt@dhcp-221:~/ $ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:48:54:55:09:6D
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::248:54ff:fe55:96d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1203876  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1616275  errors:0  dropped:0  overruns:1  carrier:0
          collisions:397422  txqueuelen:1000
          RX bytes:666243681 (635.3 MiB)  TX bytes:1888543246 (1.7 GiB)
          Interrupt:10  Base address:0xe800

eth1      Link encap:Ethernet  HWaddr 00:48:54:39:44:7A
          inet addr:172.16.120.21  Bcast:172.16.120.255  Mask:255.255.255.0
          inet6 addr: fe80::248:54ff:fe39:447a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5818227  errors:0  dropped:0  overruns:0  frame:0
          TX packets:3024232  errors:0  dropped:0  overruns:1  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:3049792520 (2.8 GiB)  TX bytes:1779165735 (1.6 GiB)
          Interrupt:11  Base address:0xec00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host

...
```

2 *routing table, automaticall filled for each sub-domain + gateway (default gateway),*

```
jmfriedt@dhcp-221:~/eagle$ /sbin/route
Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	eth0
172.16.120.0	*	255.255.255.0	U	0	0	0	eth1
default	172.16.120.254	0.0.0.0	UG	0	0	0	eth1

Network configuration on GNU/Linux

The “old way”: ifconfig

- `ifconfig -a`: all interfaces
- `ifconfig eth0 IP`: configure interface eth0
- `ifconfig eth0 up`: activate interface eth0
- `ifconfig eth0 down`: deactivate interface eth0
- `route add default gw IP2`: default routing gateway
- `route -n`: dump routing table
- `ifconfig eth0`: display statistics

The “new way”: ip

- `ip a`
- `ip a add IP dev eth0`
- `ip link set dev eth0 up`
- `ip link set dev eth0 down`
- `ip route add default via IP2`
- `ip r`
- `ip -s -h -a link`

Debian GNU/Linux: `net-tools` package to restore ifconfig

WiFi configuration on GNU/Linux

```
root@satellite:/home/jmfriedt# iwlist scan | grep -B5 FreeW
Cell 07 - Address: EE:40:00:73:33:02
Channel:11
Frequency:2.462 GHz (Channel 11)    --
Quality=55/70  Signal level=-55 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 08 - Address: 2A:C1:B0:8A:83:C1
Channel:4
Frequency:2.427 GHz (Channel 4)    --
Quality=26/70  Signal level=-84 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
Cell 11 - Address: EE:40:00:73:33:03
Channel:11
Frequency:2.462 GHz (Channel 11)    --
Quality=55/70  Signal level=-55 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
Cell 22 - Address: 22:2A:C4:65:D5:D2
Channel:11
Frequency:2.462 GHz (Channel 11)    --
Quality=17/70  Signal level=-93 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 25 - Address: 92:84:62:B4:1C:56
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=16/70  Signal level=-94 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 28 - Address: 68:A3:78:00:F5:C5
Channel:4
Frequency:2.427 GHz (Channel 4)
Quality=19/70  Signal level=-91 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 29 - Address: 68:A3:78:00:F5:C6
Channel:4
Frequency:2.427 GHz (Channel 4)
Quality=16/70  Signal level=-94 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
Cell 33 - Address: 14:0C:76:B4:06:99
Channel:7
Frequency:2.442 GHz (Channel 7)
Quality=25/70  Signal level=-85 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
Cell 35 - Address: 14:0C:76:B4:06:98
Channel:7
Frequency:2.442 GHz (Channel 7)
Quality=25/70  Signal level=-85 dBm
Encryption key:off
ESSID:"FreeWifi"
```


WiFi configuration on GNU/Linux

```
root@satellite:/home/jmfriedt# iwlist scan | grep -B5 FreeW--
Cell 07 - Address: EE:40:00:73:33:02
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=55/70 Signal level=-55 dBm
Encryption key:off
ESSID:"FreeWifi"
--
Cell 08 - Address: 2A:C1:B0:8A:83:C1
Channel:4
Frequency:2.427 GHz (Channel 4)
Quality=26/70 Signal level=-84 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
--
Cell 11 - Address: EE:40:00:73:33:03
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=55/70 Signal level=-55 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
--
Cell 22 - Address: 22:2A:C4:65:D5:D2
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=17/70 Signal level=-93 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 25 - Address: 92:84:62:B4:1C:56
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=16/70 Signal level=-94 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 28 - Address: 68:A3:78:00:F5:C5
Channel:4
Frequency:2.427 GHz (Channel 4)
Quality=19/70 Signal level=-91 dBm
Encryption key:off
ESSID:"FreeWifi"
Cell 29 - Address: 68:A3:78:00:F5:C6
Channel:4
Frequency:2.427 GHz (Channel 4)
Quality=16/70 Signal level=-94 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
--
Cell 33 - Address: 14:0C:76:B4:06:99
Channel:7
Frequency:2.442 GHz (Channel 7)
Quality=25/70 Signal level=-85 dBm
Encryption key:on
ESSID:"FreeWifi_secure"
```

```
ifdown wlan0          # OR ifconfig wlan0 down
iwconfig wlan0 essid "FreeWifi" ap EE:40:00:73:33:02
ifup wlan0           # OR dhclient wlan0
```

Debian GNU/Linux: ifup and ifdown provided by ifupdown and configured in /etc/network/interfaces (man interfaces)

Using telnet to reach high level protocols – SMTP

SMTP: port 25
(cf /etc/services)

```
$ telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 rugged ESMTP Exim 4.84
HELO moi.ici
250 rugged Hello moi.ici [::1]
MAIL FROM: moi@ici.maison
250 OK
RCPT TO: jmfriedt@localhost
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
simple email
.
250 OK id=1YfXdU-0004C1-PT
QUIT
221 rugged closing connection
Connection closed by foreign host.
```

```
You have mail in /var/mail/jmfriedt
jmfriedt@rugged:~$ mail
Mail version 8.1.2 01/15/2001.  Type ? for
"/var/mail/jmfriedt": 1 message 1 new
>N 1 moi@ici.maison      Fri May 08 08:59
Message 1:
From moi@ici.maison Fri May 08 08:59:12 2015
Envelope-to: jmfriedt@localhost
Delivery-date: Fri, 08 May 2015 08:59:12 +0200
From: moi@ici.maison
Date: Fri, 08 May 2015 08:59:12 +0200

simple email
```

Using telnet to reach high level protocols – HTTP

- Requesting a web page through telnet – HTML web page structure
- HTTP ⁴ ⁵: port 80 (Apache web server) ⁶

```
jmfriedt@rugged:~$ telnet localhost 80
```

```
Trying ::1...
```

```
Connected to localhost.
```

```
Escape character is '^]'.  
GET http://localhost/
```

```
Hello World
```

```
This is a test.
```

```
Connection closed by foreign host.
```

or accessing through a proxy

```
telnet proxy-www.univ-fcomte.fr 3128
```

```
GET http://jmfriedt.free.fr/ HTTP/1.1
```

- Most useful protocols: **read RFC** at www.ietf.org/rfc
HTTP = RFC 2068 (Jan. 1997) and 2616 (Jun. 1999), SMTP = RFC 772 ⁷ (Sep. 1980) and 821 (Aug. 1982)

⁴J. Gillies & R. Cailliau, *How the Web Was Born: The Story of the World Wide Web*, Oxford Univ. Press (2000)

⁵T. Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*, HarperBusiness (2000)

⁶W.R. Stevens, *TCP/IP Illustrated Vol. 3*, Addison & Wesley (1996), chapitre 13 “HTTP: Hypertext Transfer Protocol”.

⁷tools.ietf.org/html/rfc772

Using telnet to reach high level protocols – FTP

- Requesting a file through telnet – FTP transactions
- FTP ⁸ (two connection – commands on port 21 and file transfer)

```
commande ...                               ... et data
$ telnet localhost 21                       $ telnet localhost 36982
USER anonymous                               -rw-r--r-- 0    May 8 09:50 fichier
EPSV                                         -rw-r--r-- 1002 May 8 09:47 fichier_de_tes
229 Extended Passive mode                  Connection closed by foreign host.
      OK (|||36982|)                        $ telnet localhost 36982
LIST                                        ceci est un fichier de test
RETR fichier                               Connection closed by foreign host.
```

- Most useful protocols: **read RFC** at www.ietf.org/rfc
FTP = RFC114 and followups, RFC542 (Aug. 1973), RFC959 (Oct. 1985)

⁸W.R. Stevens, *TCP/IP Illustrated Vol. 1*, Addison & Wesley (1994), chapitre 27
“FTP: File Transfer Protocol”.

Routing protocols

- IP: computer identification. Coupled with ARP, each name+domain is associated with a unique address.
- ICMP (ping), network management.
- UDP: datagram (non-connected) mode. Packets are broadcast on the network with no constraint on latency or being received.
- TCP: connected mode. Packets are received and their order is controlled. Resource intensive (TCP/IP **stack**)⁹
- services, protocol used and port to which the served is connected is standardized: `/etc/services`
- too little computational power makes an embedded system **vulnerable to DoS attacks.**

⁹E. Gergori, *Small Footprint ColdFire TCP/IP Stack*, Freescale AN5307 : 15 kB RAM et 35 kB flash

Client/server TCP/IP

```
#include <sys/socket.h>
#include <resolv.h>
#include <strings.h>
#include <arpa/inet.h>

#define MY_PORT      9999
#define MAXBUF      1024

int main()
{int sockfd;
 struct sockaddr_in self;
 char buffer[MAXBUF];

 sockfd = socket(AF_INET, SOCK_STREAM, 0); // ICI LE TYPE DE SOCKET
 bzero(&self, sizeof(self));
 self.sin_family = AF_INET;
 self.sin_port = htons(MY_PORT);
 self.sin_addr.s_addr = INADDR_ANY;

 bind(sockfd, (struct sockaddr*)&self, sizeof(self));
 listen(sockfd, 20);

 while (1)
 {struct sockaddr_in client_addr;
  int clientfd,addrlen=sizeof(client_addr);

  clientfd = accept(sockfd, (struct sockaddr*)&client_addr, &addrlen);
  printf("%s:%d connected\n", inet_ntoa(client_addr.sin_addr), ntohs(client_addr.sin_port));
  send(clientfd, buffer, recv(clientfd, buffer, MAXBUF, 0), 0);

  close(clientfd);
 }
 close(sockfd);return(0); // Clean up (should never get here)
}
```

- 1 socket (protocol)
- 2 bind (port)
- 3 listen (blocking wait)
- 4 accept
- 5 send/recv
- 6 close

Beware of *endianness*:
Internet, Java: big-endian
x86, ARM are little-endian

Easiest way of testing a TCP server: telnet IP port

UDP communication ¹⁰ :
A server is waiting for connections

```
#include <sys/socket.h>
#include <resolv.h>
#include <arpa/inet.h>

#define BUFSIZE      1024

void alltoupper(char* s)
{while ( *s != 0 ) *s++ = toupper(*s);}

int main()
{ char buffer[BUFSIZE];
  struct sockaddr_in addr;
  int sd, addr_size, bytes_read;

  sd = socket(PF_INET, SOCK_DGRAM, 0);
  addr.sin_family = AF_INET;
  addr.sin_port = htons(9999);
  addr.sin_addr.s_addr = INADDR_ANY;
  bind(sd, (struct sockaddr*)&addr, sizeof(addr));
  do {bzero(buffer, BUFSIZE);addr_size = BUFSIZE;
    bytes_read=recvfrom(sd,buffer,BUFSIZE,0, \
      (struct sockaddr*)&addr,&addr_size);
    printf("Connect: %s:%d %s\n",inet_ntoa(addr.sin_addr), \
      ntohs(addr.sin_port), buffer);
    alltoupper(buffer);
    sendto(sd,buffer,bytes_read,0,(struct sockaddr*)&addr, \
      addr_size);
  } while ( bytes_read > 0 );
  close(sd);return 0;
}
```

Client/serveur UDP/IP

A client connects to a server to trigger transactions

```
#include <sys/socket.h>
#include <resolv.h>
#include <arpa/inet.h>

#define BUFSIZE      1024

int main(int argc, char **argv)
{   char buffer[BUFSIZE];
    struct sockaddr_in addr;
    int sd, addr_size;

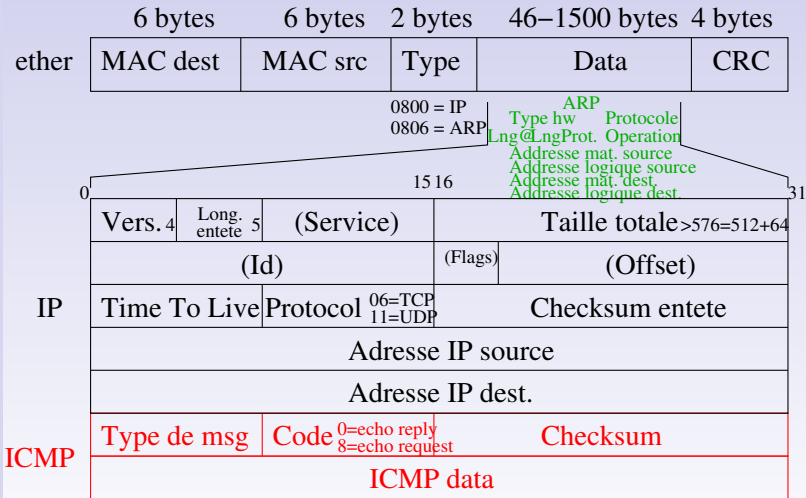
    if ( argc != 2 )
        {printf("usage: %s <msg>\n", argv[0]);exit(0);}
    sd = socket(PF_INET, SOCK_DGRAM, 0);
    addr.sin_family = AF_INET;
    addr.sin_port = htons(9999);
    inet_aton("127.0.0.1", &addr.sin_addr);
    sendto(sd, argv[1], strlen(argv[1])+1, 0, \
      (struct sockaddr*)&addr, sizeof(addr));
    bzero(buffer, BUFSIZE);
    addr_size = sizeof(addr);
    recvfrom(sd,buffer,BUFSIZE,0,(struct sockaddr*)&addr, \
      &addr_size);
    printf("Reply: %s:%d %s\n",inet_ntoa(addr.sin_addr), \
      ntohs(addr.sin_port), buffer);
    close(sd);
    return 0;
}
```

or echo "toto" | nc -u IP 9999

Cross-compilation to embedded targets – use of embedded OS

¹⁰<http://www.cs.utah.edu/~swalton/listings/sockets/programs/>

Raw IP et ICMP



Question: what is the protocol identified of ICMP in the IP header?

Raw IP & ICMP

```
J.-M Friedt $ arp -a
? (192.168.0.1) at 00:13:d3:8d:d3:97 [ether] on eth0
$ arp -d 192.168.0.1
$ ping 192.168.0.1

# tcpdump -i eth0 -XX # XX = show ethernet header
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:06:33.462038 ARP, Request who-has 192.168.0.1 tell 192.168.0.11, length 28
    0x0000:  ffff ffff ffff cc7e e75f cf6e 0806 0001  .....~_.n....
    0x0010:  0800 0604 0001 cc7e e75f cf6e c0a8 000b  .....~_.n....
    0x0020:  0000 0000 0000 c0a8 0001  .....
16:06:33.462590 ARP, Reply 192.168.0.1 is-at 00:13:d3:8d:d3:97 (oui Unknown)
    0x0000:  cc7e e75f cf6e 0013 d38d d397 0806 0001  .~_.n.....
    0x0010:  0800 0604 0002 0013 d38d d397 c0a8 0001  .....
    0x0020:  cc7e e75f cf6e c0a8 000b 0000 0000 0000  .~_.n.....
    0x0030:  0000 0000 0000 0000 0000 0000  .....
16:06:33.462607 IP 192.168.0.11 > 192.168.1.1: ICMP echo request, id 1906, length 60
    0x0000:  0013 d38d d397 cc7e e75f cf6e 0800 4500  .....~_.n..E.
    0x0010:  0054 1191 4000 4001 a6bb c0a8 000b c0a8  .T..@.@.....
    0x0020:  0101 0800 ff64 0772 0001 e9c2 4c55 c90c  ....d.r....LU..
    0x0030:  0700 0809 0a0b 0c0d 0e0f 1011 1213 1415  .....
    0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  .....!"#$.
    0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
    0x0060:  3637 67
```

Raw IP & ICMP

Good understanding of network protocols useful for applications related to

- security: firewall or dedicated router. Packet filtering (`iptables`) with short packet management latency
- remote instrument control. Even without considering data security, prevent DoS attacks.
- handling all layers is often not needed on embedded systems: understanding the whole communication hierarchy allows for selecting only the useful parts (e.g raw-IP).

In previous examples, `socket` argument defined the transport protocol (`SOCK_DGRAM` (UDP), `SOCK_STREAM` (TCP)).

`SOCK_RAW` \Rightarrow 20 byte header with source and destination IP @, followed by payload to be communicated (routed)

```
45 00 00 34 19 a9 00 00 3c ff 66 20 7f 00 00 01    <- source = 127.0.0.1
7f 00 00 01 30 30 30 30 30 30 30 30 30 30 30 30    <- dest = 127.0.0.1
```

MAC spoofing

- most modern interfaces (Ethernet, WiFi) configure the hardware MAC address by software

```
# /sbin/ifconfig eth0
```

```
eth0: flags=4096<BROADCAST,MULTICAST> mtu 1500
```

```
inet 192.168.1.55 netmask 255.255.255.0 broadcast 192.168.1.255
```

```
ether cc:7e:e7:5f:cf:6e txqueuelen 1000 (Ethernet)
```

```
[...]
```

```
# /sbin/ifconfig eth0 hw ether c4:d9:87:12:ea:3c
```

```
# /sbin/ifconfig eth0
```

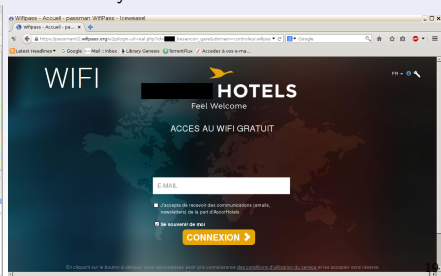
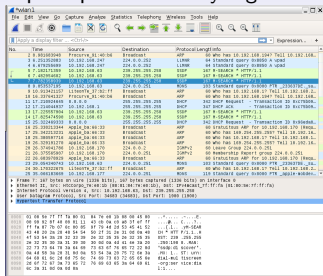
```
eth0: flags=4096<BROADCAST,MULTICAST> mtu 1500
```

```
inet 192.168.1.55 netmask 255.255.255.0 broadcast 192.168.1.255
```

```
ether c4:d9:87:12:ea:3c txqueuelen 1000 (Ethernet)
```

```
[...]
```

- captive portals identify registered customers by their MAC address ...



MAC spoofing

- most modern interfaces (Ethernet, WiFi) configure the hardware MAC address by software

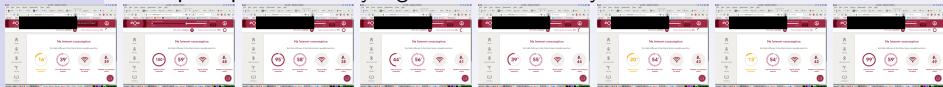
```
# /sbin/ifconfig eth0
eth0: flags=4098<BROADCAST,MULTICAST> mtu 1500
      inet 192.168.1.55 netmask 255.255.255.0 broadcast 192.168.1.255
      ether cc:7e:e7:5f:cf:6e txqueuelen 1000 (Ethernet)
```

[...]

```
# /sbin/ifconfig eth0 hw ether c4:d9:87:12:ea:3c
# /sbin/ifconfig eth0
eth0: flags=4098<BROADCAST,MULTICAST> mtu 1500
      inet 192.168.1.55 netmask 255.255.255.0 broadcast 192.168.1.255
      ether c4:d9:87:12:ea:3c txqueuelen 1000 (Ethernet)
```

[...]

- captive portals identify registered customers by their MAC address ...

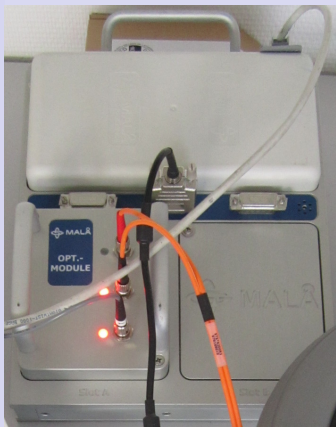


Resetting download quota on the SNCF WiFi connection

J.-M Friedt, *Modélisation et utilisation d'une parabole : application au wifi*,
Opensilicium 20 44–55 (Oct.-Dec. 2016)

Raw Ethernet

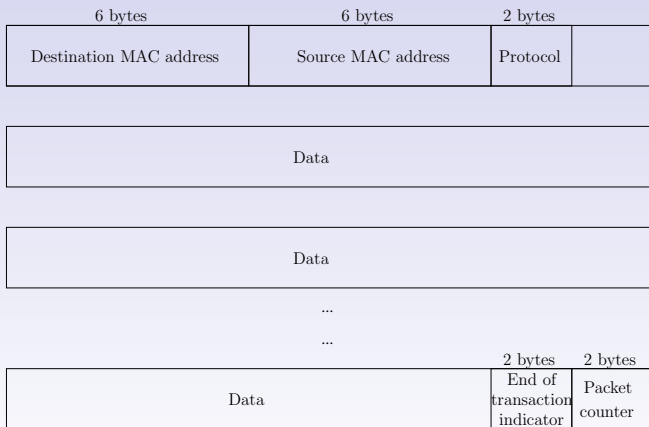
Embedded systems with little computational power: raw-Ethernet (Malå ProEx ¹¹), no routing (point to point communication PC-RADAR)



¹¹<http://sourceforge.net/projects/proexgprcontrol/>,
A. Hugeot, J.-M Friedt, *A low cost approach to acoustic filters acting as GPR cooperative targets for passive sensing*, IWAGPR 2015

Raw Ethernet

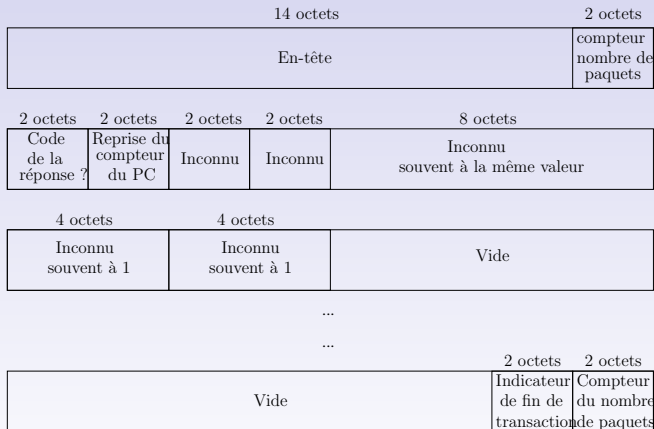
Embedded systems with little computational power: raw-Ethernet (Malå ProEx ¹¹), no routing (point to point communication PC-RADAR)



¹¹<http://sourceforge.net/projects/proexgprcontrol/>,
A. Hugeot, J.-M Friedt, *A low cost approach to acoustic filters acting as GPR cooperative targets for passive sensing*, IWAGPR 2015

Raw Ethernet

Embedded systems with little computational power: raw-Ethernet (Malå ProEx ¹¹), no routing (point to point communication PC-RADAR)



¹¹<http://sourceforge.net/projects/proexgprcontrol/>,
A. Hugeot, J.-M Friedt, *A low cost approach to acoustic filters acting as GPR cooperative targets for passive sensing*, IWAGPR 2015

Listening packets ... tcpdump

Example: tcpdump port 80 -i lo -X

```

jmfriedt@rugged: ~
root@rugged:/home/jmfriedt# tcpdump -i lo -X
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
11:30:54.890446 IP6 localhost.38026 > localhost.httpe: Flags [S], seq 3573235918, win 43690, options [mss 65476,sackOK,TS val 1688894 ecr 0,nop,wscale 7], length 0
0x0000: 6000 0000 0028 0640 0000 0000 0000 0000  ....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000  .....
0x0020: 0000 0000 0000 0001 948a 0050 d4fb 40ce  .....P..@.
0x0030: 0000 0000 a002 aaaa 0030 0000 0204 ffc4  .....0.....
0x0040: 0402 080a 0019 c53e 0019 c53e 0103 0307  .....>.....
11:30:54.890470 IP6 localhost.httpe > localhost.38026: Flags [S], seq 1135632453, ack 3573235919, win 43690, options [mss 65476,sackOK,TS val 1688894 ecr 1688894,nop,wscale 7], length 0
0x0000: 6000 0000 0028 0640 0000 0000 0000 0000  ....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000  .....
0x0020: 0000 0000 0000 0001 0050 948a 4781 daa6  .....P..G...
0x0030: d4fb 40cf a012 aaaa 0030 0000 0204 ffc4  .....@.....
0x0040: 0402 080a 0019 c53e 0019 c53e 0103 0307  .....>.....
11:30:54.890494 IP6 localhost.38026 > localhost.httpe: Flags [S], seq 1, ack 1, win 342, options [nop,nop,TS val 1688894 ecr 1688894], length 0
0x0000: 6000 0000 0020 0640 0000 0000 0000 0000  ....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000  .....
0x0020: 0000 0000 0000 0001 948a 0050 d4fb 40cf  .....P..@.
0x0030: 4781 daa6 8010 0156 0028 0000 0101 080a  G.....V.(.....
0x0040: 0019 c53e 0019 c53e  .....>.....
11:30:54.890504 IP6 localhost.38026 > localhost.httpe: Flags [P,], seq 1:414, ack 1, win 342, options [nop,nop,TS val 1688899 ecr 1688894], length 413
0x0000: 6000 0000 01b4 0640 0000 0000 0000 0000  ....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000  .....
0x0020: 0000 0000 0000 0001 948a 0050 d4fb 40cf  .....P..@.
0x0030: 4781 daa6 8018 0156 01c5 0000 0101 080a  G.....V.....
0x0040: 0019 c543 0019 c53e 4746 5420 2f20 4854  ....C...GET./HT
0x0050: 5450 2f31 2e31 0d0a 48f7 7374 3a20 6c6f  IP/1.1.Host:lo
0x0060: 6381 015f 6773 740d 0e5f 2835 22d1 015f  calhost_user=ig
0x0070: 656e 743e 204d 677a 636c 6c61 2f35 2e30  ent:Mozilla/5.0
0x0080: 2028 8321 313e 204c 636e 7578 2069 3e38  (KHTML;Linux;168
0x0090: 3e3b 2072 7e3a 3331 2e30 2820 4765 636e  6;rv:31.0)Geck
0x00a0: 6f2f 3230 3130 3031 3031 2046 6872 6566  o/20100101.Firef
0x00b0: 6f78 2f33 312e 3020 4963 6577 6561 7365  ox/31.0;Linux;se
0x00c0: 6c2f 5331 2e35 2e33 0d0a 4163 6365 7074  /31.5.3;.Accept
0x00d0: 5a20 7465 3974 2e68 746e 6e2e 6370 706e  ;text/html,application/xhtml+xml
0x00e0: 6363 6174 636f 6e2f 7898 746d 6c2b 786d  ;application/xml
0x00f0: 6c2c 6170 706c 6363 6174 636f 6e2f 786d  ;img,S,*/*;q=0.
0x0100: 6c3b 713d 302e 39c2 2a2f 2a3e 713d 302e  8;.Accept-Langua
0x0110: 380d 0a41 6363 6570 742d 4e61 6e67 7561  get;en-US,en;q=0
0x0120: 6765 3a20 656e 2d65 532c 656e 3b71 3490  ;.Accept-Encod
0x0130: 2e35 0d0a 4163 6365 7074 2a46 6e63 6f64  ing;gzip,deflat
0x0140: 636e 6731 2067 7a68 702c 2064 6566 6e61  to;.INT;.1;.Conn
0x0150: 7465 0d0a 444e 543e 2031 0d0a 436f 6e6e

```


Listening packets ... tcpdump

Example: tcpdump port 80 -i lo -X

```

jmfriedt@rugged: ~
0x0120: 6765 5a20 686e 2d65 532c 686e 3b71 5d90 set-cookie=
0x0130: 2e35 0f4a 41b3 5365 7074 2d65 6e62 6f64 .; .accept-encod
0x0140: 686e 673a 2067 7a69 702c 2064 6566 6c61 ine; gzip, defla
0x0150: 7465 0d0a 444e 543a 2031 0d0a 436f 6e6e te; .INT; .,Conn
0x0160: 6563 7469 6f6e 3a20 6b65 6570 2d61 6c69 action; keep-ali
0x0170: 7665 0d0a 0d0a ve.....
11:29:13.002767 IP6 localhost.http > localhost.38024: Flags [.], ack 303, win 350, options [nop,nop,TS val 1663422 ecr 1663422], length 0
0x0000: 6000 0000 0020 0640 0000 0000 0000 0000 .....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000 .....
0x0020: 0000 0000 0000 0001 0050 9488 84ac 0c3d .....P.....=
0x0030: 4271 c33d 8010 015e 0028 0000 0101 080a Bq;.....B.....
0x0040: 0019 61be 0019 61be .....a.
11:29:13.003061 IP6 localhost.http > localhost.38024: Flags [P.], seq 1:315, ack 303, win 350, options [nop,nop,TS val 1663422 ecr 1663422], length 314
0x0000: 6000 0000 015a 0640 0000 0000 0000 0000 .....Z@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000 .....
0x0020: 0000 0000 0000 0001 0050 9488 84ac 0c3d .....P.....=
0x0030: 4271 c33d 8018 015e 0152 0000 0101 080a Bq;.....B.....
0x0040: 0019 61be 0019 61be 4854 5450 2f31 2e31 .....a..HTTP/1.1
0x0050: 2032 3030 204f 4b0d 0a44 6174 653a 2057 .200.OK.;.Date;W
0x0060: 6564 2c20 3036 204d 6179 2032 3031 3520 ed.;.06.May.2015.
0x0070: 3039 3a32 393a 3135 2047 4e54 0d0a 6365 09:29:13.GMT.;Se
0x0080: 7276 6572 3a20 4170 61b3 6065 2f32 2e34 rver; .Apache/2.4
0x0090: 2e31 2020 2044 6562 6369 6e29 0d0a 4e61 .0.(Debian);.Le
0x00a0: 7374 2d4d 6f64 6866 6865 643a 2067 6564 st-Mod/Friedt;Mod
0x00b0: 2c20 3036 204d 6179 2032 3031 3520 3039 .;06.May.2015.09
0x00c0: 3a32 303a 3534 2047 4e54 0d0a 4854 6167 :20:54.GMT.;ETag
0x00d0: 3a20 2231 662d 3531 3536 3634 6665 3131 .;"1f-616664f6e1
0x00e0: 6463 3322 0a0a 4163 6365 7074 2d62 616e dc3";.Accept-Ran
0x00f0: 6765 733a 2062 7974 6573 0d0a 436f 6e74 ges; bytes; .Cont
0x0100: 6567 7469 3a20 3331 0d0a ent-length; .L;
0x0110: 4b65 6570 2d41 6c69 7665 3a20 7469 6e65 Keep-Alive; time
0x0120: 6f75 743d 352c 206d 6178 3a31 3030 0d0a out=5.;.max=100.;
0x0130: 436f 6e6e 6563 7469 6f6e 3a20 4b65 6570 Connection;.Keep
0x0140: 2d41 6c69 7665 0d0a 436f 6e74 656e 742d -Alive.;.Content-
0x0150: 5479 7065 3a20 7465 7874 2f68 746d 6c0d Type;.text/html.
0x0160: 0a0d 0a08 656c 6e6f 2057 6f72 6e64 0a0a .;.Hello,World..
0x0170: 4365 6369 2065 7374 2075 6e20 7465 7374 Ceci.est.un.test
0x0180: 2e0a ..
11:29:13.003070 IP6 localhost.38024 > localhost.http: Flags [.], ack 315, win 350, options [nop,nop,TS val 1663422 ecr 1663422], length 0
0x0000: 6000 0000 0020 0640 0000 0000 0000 0000 .....@.....
0x0010: 0000 0000 0000 0001 0000 0000 0000 0000 .....
0x0020: 0000 0000 0000 0001 9488 0050 4271 c33d .....P[Bq;=
0x0030: 84ac 0d77 8010 015e 0028 0000 0101 080a .....U.....
0x0040: 0019 61be 0019 61be .....
11:29:17.908610 IP6 localhost.http > localhost.38024: Flags [F.], seq 315, ack 303, win 250, options
0x0000: 6000 0000 0020 0640 0000 0000 0000 0000 .....@.....

```

```

jmfriedt@rugged: ~
jmfriedt@rugged:~$ cat /var/www/html/index.html
Ceci est un test.
jmfriedt@rugged:~$

```

BBC News - Home | Portail numérique FE... | Accédez à vos e-ma... | TorrentFlux

Hello World Ceci est un test.

debian | 1 | 2 | 3 | 4 | jmfriedt@rug... | Iceweasel | jmfriedt@rug... | jmfriedt@rug... | 11:30:07 AM

Listening packets ... wireshark

Ex-ethereal, wireshark provides a graphical user interface for analyzing packets

Wireshark 1.12.1 (Git Rev Unknown from unknown)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

Interface: Frequency: 1 monitor interfaces found

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	:::1	:::1	TCP	34	38022->80 [EST] Seq=0 Win=0 Len=0 MSS=6040 S...
2	0.000019000	:::1	:::1	TCP	94	80->38022 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 M...
3	0.000034000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=...
4	0.010705000	:::1	:::1	HTTP	388	GET / HTTP/1.1
5	0.010739000	:::1	:::1	TCP	86	80->38022 [ACK] Seq=1 Ack=303 Win=44800 Len=0 TSva...
6	0.011205000	:::1	:::1	HTTP	400	HTTP/1.1 200 OK (text/html)
7	0.011214000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=303 Ack=315 Win=44800 Len=0 TS...
8	1.083335000	:::1	:::1	HTTP	369	GET /favicon.ico HTTP/1.1
9	1.083533000	:::1	:::1	HTTP	586	HTTP/1.1 404 Not Found (text/html)
10	1.083545000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=586 Ack=815 Win=45952 Len=0 TS...
11	1.087472000	:::1	:::1	HTTP	399	GET /favicon.ico HTTP/1.1
12	1.087650000	:::1	:::1	HTTP	586	HTTP/1.1 404 Not Found (text/html)

0140 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection : Keep-A
0150 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 live..Content-Ty
0160 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 0d pe: text/html...
0170 0a 48 65 6c 6c 6f 20 57 6f 72 6c 64 0a 0a 43 65 .Hello World..Ce
0180 63 69 20 65 73 74 20 75 6e 20 74 65 73 74 2e 0a ci est u n test..

File: /tmp/wireshark pcapng_lo... Packets: 16 · Displayed: 16 (100.0%) · Dropped: 0 (0.0%) Profile: Default

http://localhost/ localhost

BBC News - Home Portail numérique FE... Accédez à vos e-ma... TorrentFlux

Hello World Ceci est un test.

```
jmfriedt@rugged: ~  
jmfriedt@rugged:~$ cat /var/www/html/index.html  
Hello World  
Ceci est un test.  
jmfriedt@rugged:~$
```

debian 1 2 3 4 jmfriedt... jmfriedt... *Loopba... Icevea... jmfriedt... jmfriedt... 11:25:20 AM

Listening packets ... wireshark

Ex-etherreal, wireshark provides a graphical user interface for analyzing packets

The screenshot shows the Wireshark 1.12.1 interface. The main pane displays a list of captured packets. The selected packet (No. 6) is an HTTP GET request. The packet details pane shows the structure of the request, including the Hypertext Transfer Protocol section. A terminal window in the foreground shows the user's shell prompt and a command to view the index.html file.

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000000	:::1	:::1	TCP	94	80->38022 [SYN] Seq=0 Win=43690 Len=0 MSS=65470 S...
2	0.000019000	:::1	:::1	TCP	94	80->38022 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 M...
3	0.000034000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=...
4	0.010705000	:::1	:::1	HTTP	388	GET / HTTP/1.1
5	0.010739000	:::1	:::1	TCP	86	80->38022 [ACK] Seq=1 Ack=303 Win=44800 Len=0 TSva...
6	0.011205000	:::1	:::1	HTTP	400	HTTP/1.1 200 OK (text/html)
7	0.011214000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=303 Ack=315 Win=44800 Len=0 TS...
8	1.083335000	:::1	:::1	HTTP	369	GET /favicon.ico HTTP/1.1
9	1.083533000	:::1	:::1	HTTP	586	HTTP/1.1 404 Not Found (text/html)
10	1.083545000	:::1	:::1	TCP	86	38022->80 [ACK] Seq=586 Ack=815 Win=45952 Len=0 TS...
11	1.087472000	:::1	:::1	HTTP	399	GET /favicon.ico HTTP/1.1

Frame 6: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on interface 0
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 6, Src: ::1 (:::1), Dst: ::1 (:::1)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 38022 (38022), Seq: 1, Ack: 303, Len: 314
Hypertext Transfer Protocol

```
0050 d1 c1 00 17 d1 c0 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2
0060 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK..D ate: Wed
0070 2c 20 30 30 36 20 4d 61 67 19 20 32 30 31 35 20 30 39 06 May 2015 09
0080 3a 32 32 3a 32 33 20 47 4d 54 0d 0a 53 65 72 76 0:22:23 GMT..Serv
0090 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 31 0er: Apache/2.4.1
00a0 80 20 28 44 65 62 69 61 6e 29 0d 0a 4c 61 73 74 0 (Debian)..Last
00b0 2d 4d 61 64 69 66 69 65 64 3a 20 57 65 64 2c 20 (Modifid: Wed,
00c0 30 36 20 4d 61 79 20 32 30 31 35 20 30 39 3a 32 06 May 2 015 09:2
00d0 30 3a 35 3a 20 47 4d 54 0d 0a 45 54 61 67 3a 20 0:54 GMT ..ETag:
00e0 22 31 66 2d 35 31 35 36 36 34 66 65 31 31 64 63 0if-5156 64f61ldc
00f0 33 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 3*..Acce pt-Range
0100 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 0s: bytes ..Conten
0110 74 2d 4c 65 6e 67 74 68 3a 20 33 31 0d 0a 4b 65 0t-Length : 31..Ke
0120 65 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 0ep-Alive : timeou
0130 34 2d 35 3a 20 47 4d 54 0d 0a 40 30 30 0d 0a 69 64 0f-5156 64f61ldc
```

Hypertext Transfer Protocol (htt... Packets: 16 - Displayed: 16 (100.0%) - Dropped

Terminal output:
jmfriedt@rugged: ~
jmfriedt@rugged:~\$ cat /var/www/html/index.html
Hello World!

TCP/IP tools

- traceroute

```
jmfriedt@vm1:~$ traceroute www.whitehouse.gov
traceroute to www.whitehouse.gov (23.214.186.191), 30 hops max, 60 byte packets
 1  10.10.0.254 (10.10.0.254)  0.377 ms  0.370 ms  0.362 ms
 2  vss-5b-6k.fr.eu (46.105.123.252)  0.954 ms  0.952 ms  0.947 ms
 3  rbx-g1-a9.fr.eu (178.33.100.29)  2.509 ms  2.509 ms  2.505 ms
 4  * * *
 5  ldn-5-6k.uk.eu (213.251.128.18)  48.180 ms  * *
 6  * * *
 7  ae10.mpr2.lhr2.uk.zip.zayo.com (64.125.31.194)  6.492 ms  8.722 ms  7.2
 8  ae5.mpr1.lhr15.uk.zip.zayo.com (64.125.21.10)  4.519 ms  4.515 ms  4.49
 9  94.31.61.250.IPYX-074083-001-ZY0.above.net (94.31.61.250)  4.504 ms  4.
10  a23-214-186-191.deploy.static.akamaitechnologies.com (23.214.186.191)  .
```

- nslookup

```
jmfriedt@rugged:~$ nslookup www.femto-st.fr
Server:          130.67.15.198
Address:         130.67.15.198#53
```

Non-authoritative answer:

```
Name:   www.femto-st.fr
Address: 195.83.19.10
```

HTTP tools

- Swiss army knife: nc (netcat)

```
echo -e "GET http://jmfriedt.free.fr HTTP/1.0\n\n" | nc jmfriedt.free.fr 80
```

- wget – GET method (answer: 0:47 1:57 2:25)

```
dest=Vesoul
```

```
wget -q -O- "http://reiseauskunft.bahn.de/bin/query.exe/fn?revia=yes&\nexistOptimizePrice=1&country=FRA&\ndbkanal_007=L01_S01_D001_KIN0001_qf-bahn_LZ003&\nignoreTypeCheck=yes&S=Besancon+Franche+Comte+TGV&REQ0JourneyStopsSOA=7&Z=${REQ0JourneyStopsZOA=7&trip-type=single&date=Me%2C+07.01.15&time=08%3A37&\ntimesel=depart&returnTimesel=depart&optimize=0&infant-number=0&tariffTravel\n\tariffTravellerReductionClass.1=0&tariffTravellerAge.1=&qf-trav-bday-1=&tar\n\tstart=1&qf.bahn.button.suchen=" | grep -A1 uratio | grep ^[0-9] | tr '\n' '
```

- curl – POST method

```
month=12
```

```
year=2014
```

```
curl -s --cookie-jar test --data \
```

```
"anzahlprofile=1&einheit=meter&vonkurz=LFPG&nachkurz=LYR+&landetime=&zwpunk\n\tadresse=&profil=profilangeben&day=15&month=$month&year=$annee&flightnumber=\n\tvon=PARIS%2C+FRANCE+++++++&uptime=00%3A30&obentime=04%3A00&flugho\n\tdowntime=00%3A30&nach=LONGYEARBYEN%2C+NORWAY+++++++&send=Send+request" \nhttp://www.helmholtz-muenchen.de/epcard/eng_flugoutput.php | grep Sv
```

Conclusion

Exercise: listen to the `lo` interface with `tcpdump` while running a ftp transaction. Can you see the login/password sent over the network?

Conclusion:

- Exploration of the various hierarchical layer of Internet network transactions (formally known as OSI layers)
- Description of high level protocols (SMTP, FTP, HTTP)
- Description of low level transactions (IP, TCP, UDP)
- Description of debugging tools (`tcpdump`, `wireshark`)

Perspectives:

- *data mining*¹² (automate collecting data over the Internet)¹³
- instrument control (embedded Linux)

¹²T. Segaran & J. Hammerbacher, *Beautiful Data – The Stories Behind Elegant Data Solutions*, O'Reilly Media (2009)

¹³J.-M Friedt, *Cartographier le bout du monde*, GNU/Linux Magazine France 185 (Sept. 2015)