TCP/IP élements

Denis Lubineau

Outline

TCP/IP stack Tutorial

IP addressing

Routing

- **LAB-0.1 : Test routing with NOC**

- **LAB-0.2: Test routing with Stormshield Firewall**

- **Exercises : Different network structures**

Outline

- Internet protocol
  - Introduction
  - Addressing mechanisms
  - IP routing
  - IP packets format

- ICMP

- TCP et UDP

- Routing

- Applications and exercises

FACTORI 4.0
Erasmus +

1969: ARPANET

- Experimental implementation of a packet switching network.
  Goal : reliable data transmission able to resist to nuclear attacks

1975: Implementation

- ARPANET reaches the operational stage.
  Management delegated to the "Defence Agency Communication
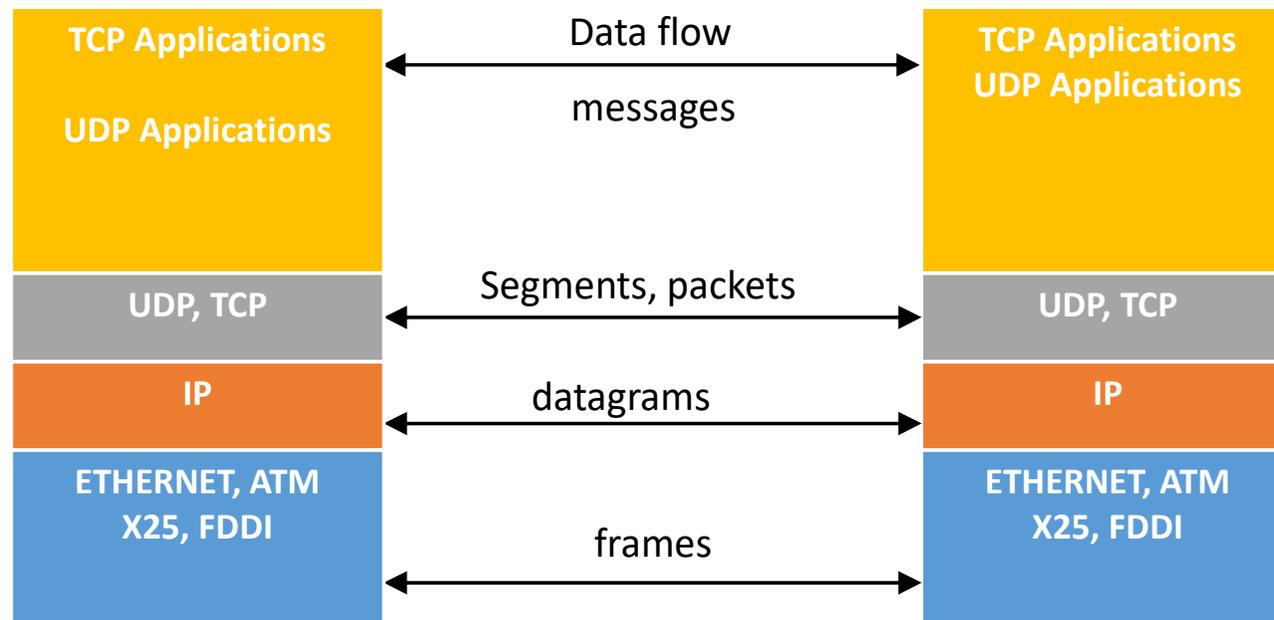
1983: TCP/IP MILLET Std

- TCP/IP Protocols are adopted like military standards, like Berkeley UNIX(Unix BSD).The Internet terminology (MILNET + ARPANET) appears.

UNIX and TCP/IP

- A new stack is developed to deal with the large deployment of Internet

2000-2010: IPv6 family

TCP/IP terminology

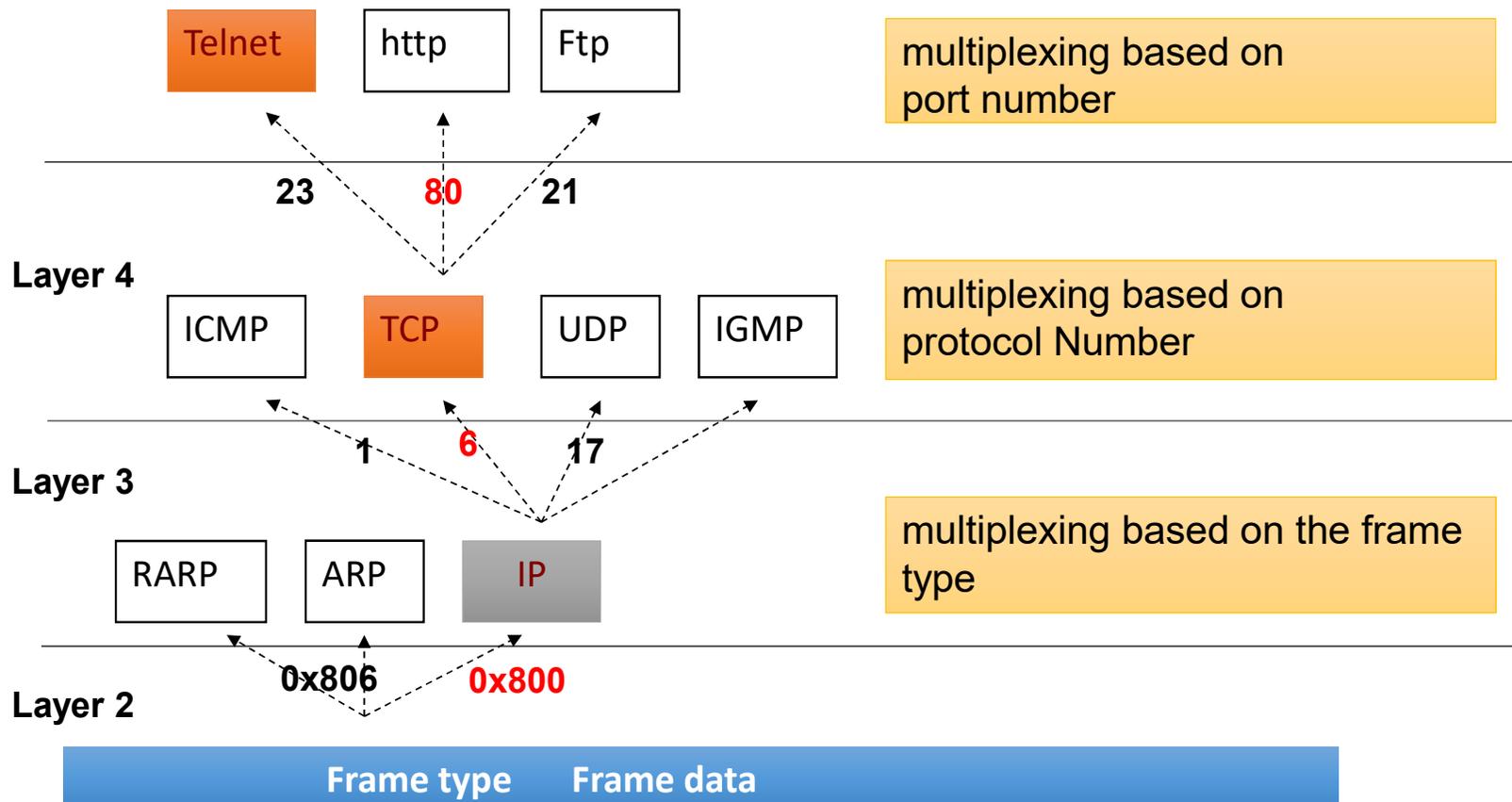| TCP Applications UDP Applications	Data flow messages	TCP Applications UDP Applications
UDP, TCP	Segments, packets	UDP, TCP
IP	datagrams	IP
ETHERNET, ATM X25, FDDI	frames	ETHERNET, ATM X25, FDDI

The Network layer (Internet)

- IP Protocol : connectionless protocol.
  - Datagram definition
  - Addressing scheme
  - data flow, segmentation,

- ICMP Protocol : control.
  - flow management, node presence, saturation, etc…

- Protocols ARP and RARP
  - Mapping between network and physical addresses on Ethernet networks

- Serial line Protocols: PPP and alternatives
  - telephone line protocols.
  - PPP, PPPoE, PPPoA: IP encapsulation on serial lines.
  - PPTP: VPN Tunnels

TCP/IP stack

FACTORI 4.0
Erasmus +

Telnet	http	Ftp

multiplexing based on port number

23   **80**   **21**

Layer 4

ICMP	TCP	UDP	IGMP

multiplexing based on protocol Number

1   **6**   **17**

Layer 3

multiplexing based on the frame type

RARP	ARP	IP

0x806   **0x800**

Layer 2

Frame type	Frame data

Unix: /etc/protocols; /etc/services

IP addresses

- Address : 32 bits sequence
- identifies a single host on the network

- 32 bits: 1 0 0 0 0 1 1 0   0 0 0 1 1 0 0 0   0 0 0 0 1 0 0 0   0 1 0 0 0 0 1 0

- Hex: 86   18   08   4
- Decimal Coding: 134.24.8.66
- An address:

@ network	@host

Size depends on the network class

IP addresses: classes

class A

| 0 | @ hosts |

128 networks, 16 million machines

class B

| 10 | @ network | @ hosts |

class C

| 110 | @ network | @ hosts |

class D

| 1110 | @ multicast |
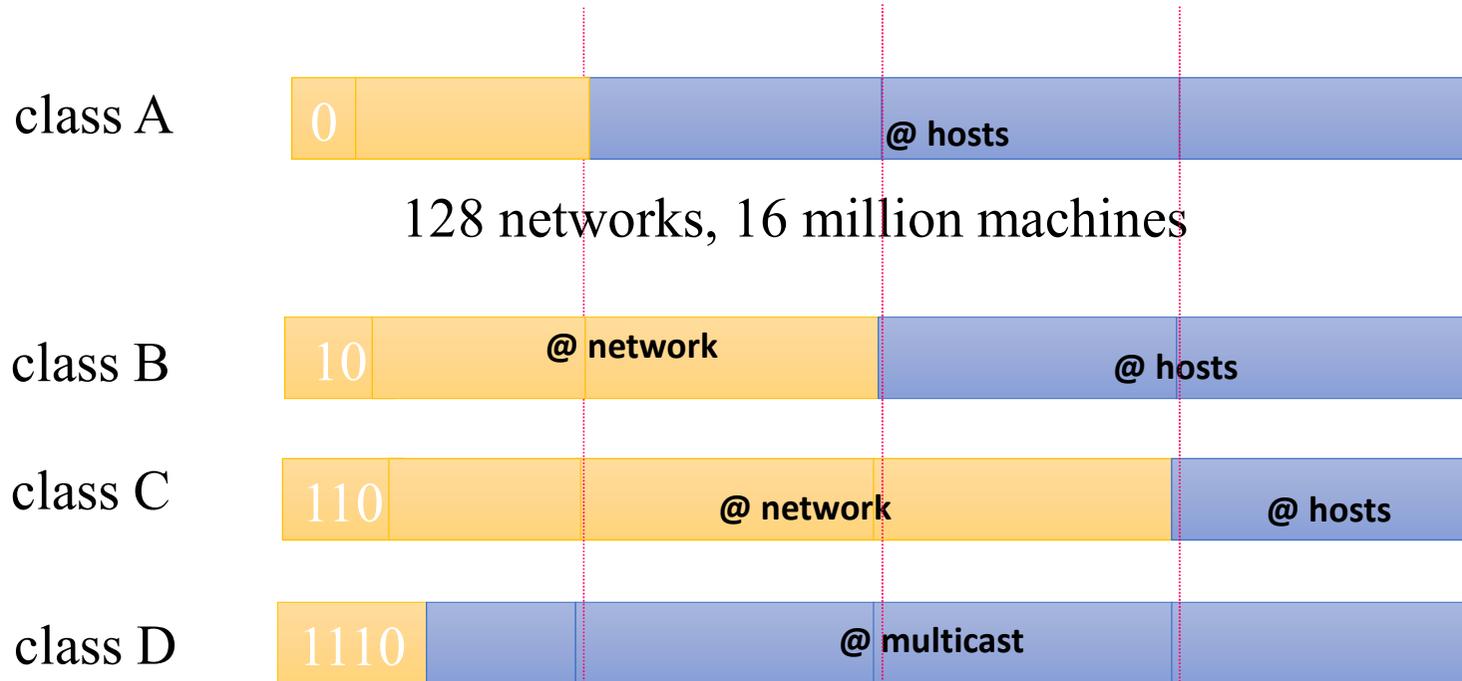
Specific addresses: class A : 0.0.0.0
                       class A : 127.0.0.0

@ network	@ hosts		
n	x=32 - n		

10	0	0	0
0000 1010	0000 0000	0000 0000	0000 0000
	Bloc size = 2^x addresses	USABLE = 2^x-2 addresses	First address = Network Address
			Last address = Broadcast Address
	1111 1111	1111 1111	1111 1111
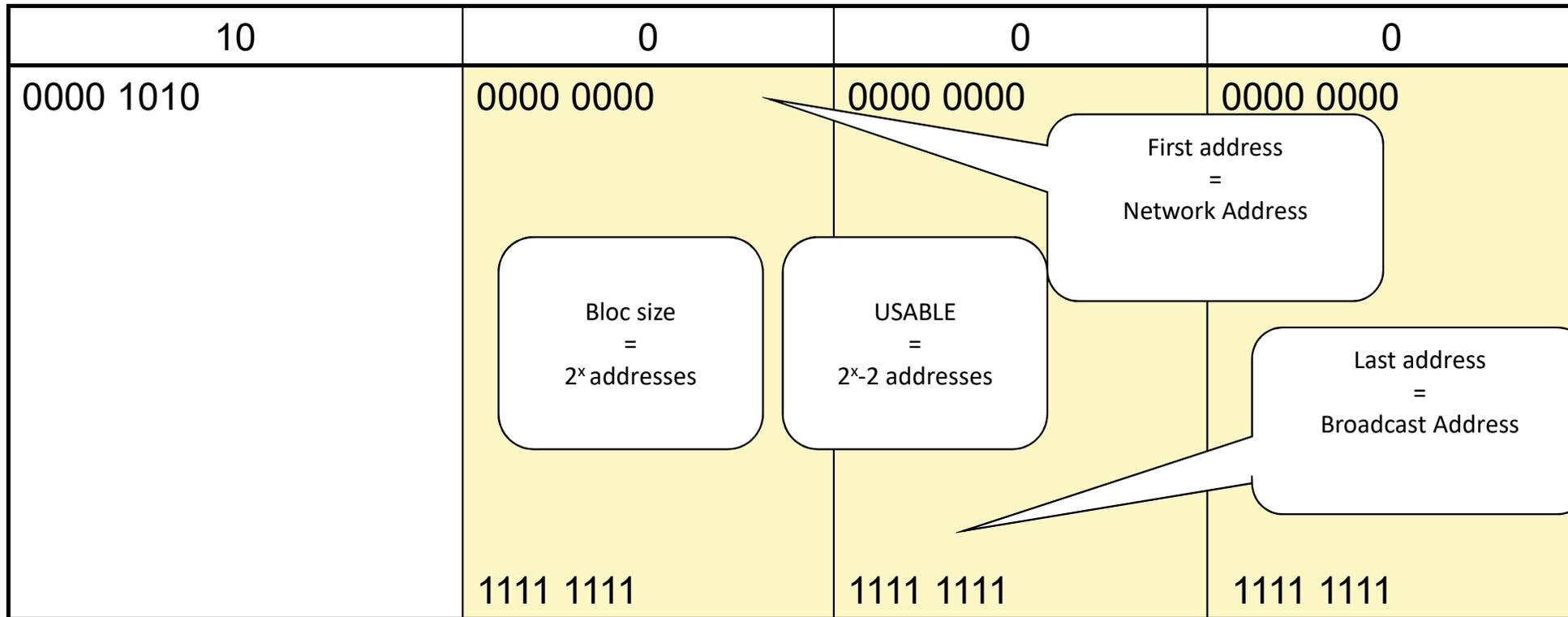
IP addresses: Subnetting

1 network: Network address /n

n bits

sub-division of a network
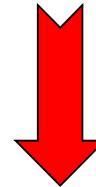
2 networks: Network address /n+1

n bits

(n+1) bits

IP: Header definition

8 bits	8 bits	8 bits	8 bits
Ver.	IHL	TOS	Total length
Identification		Flags	Fragment offset
TTL		Protocol	Header Checksum
Source address			
Destination address			
options			Pad.

20 bytes

32 bits
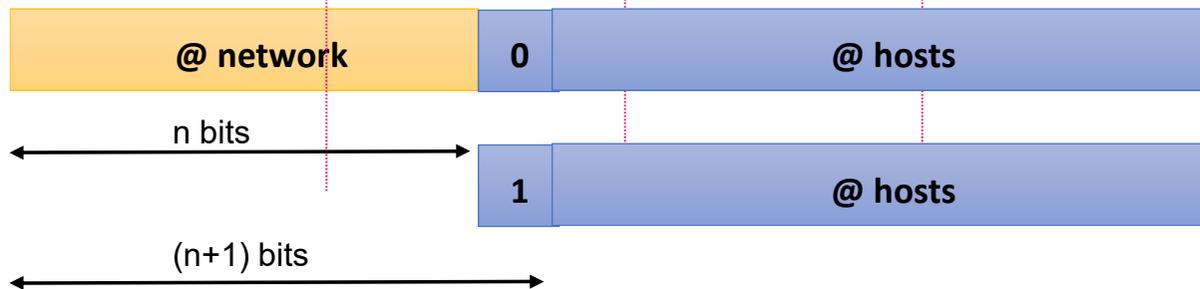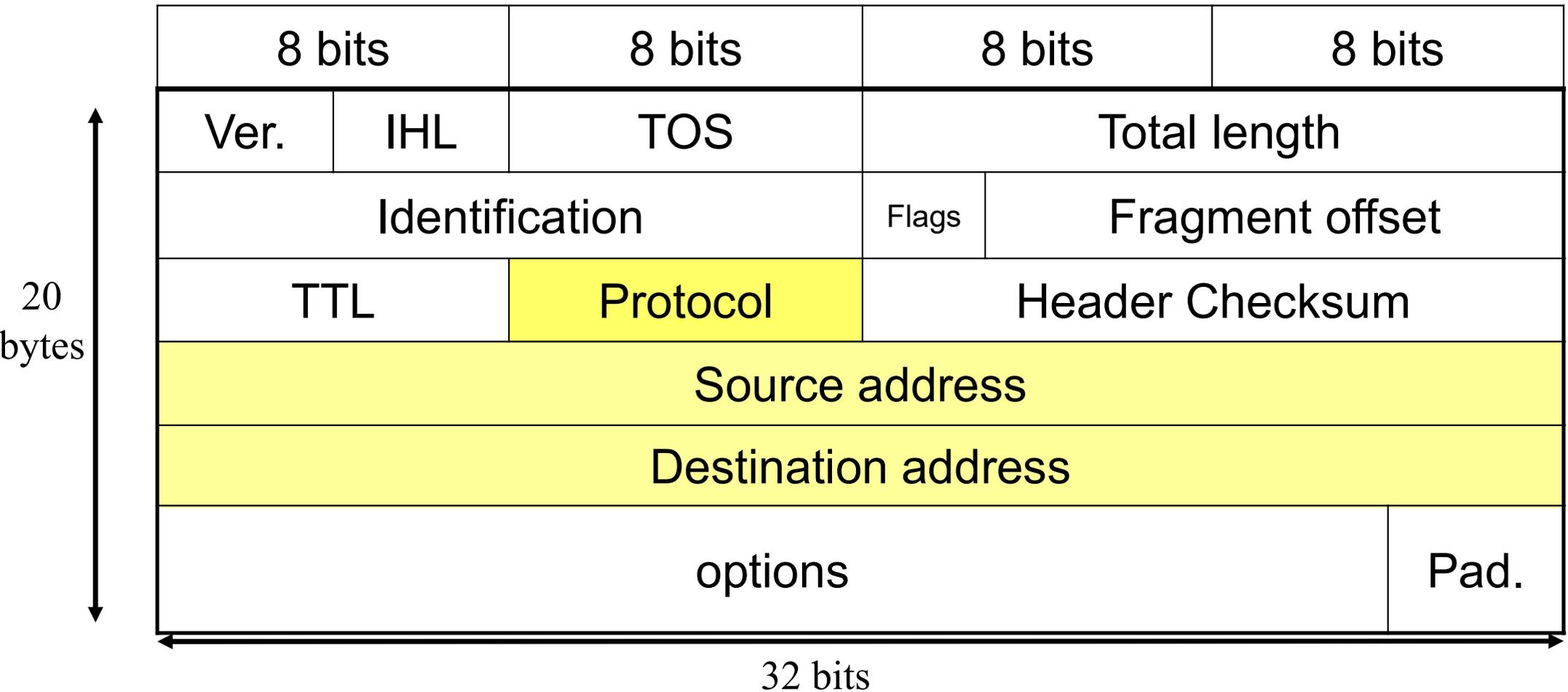
ICMP (RFC 792)

- IP Protocol Nb=1

Generic format

Type	Code	Checksum
identifier		Seq. Number
Optional data		

ICMP types : Summary

- 0   Echo reply
- 3   Destination unreachable
- 4   Source quench
- 5   Redirect
- 8   Echo
- 11   Time exceeded
- 12   Parameter problem
- 13   Timestamp
- 14   Timestamp reply
- 15   Information reply

Transport protocol : UDP

Unreliable (connectionless)
Used by DNS, RPC (thus NFS), SNMP...

8 bits	8 bits	8 bits	8 bits
Source PORT		**Destination PORT**	
LENTH		**CHEKSUM**	

8 bytes

32 bits
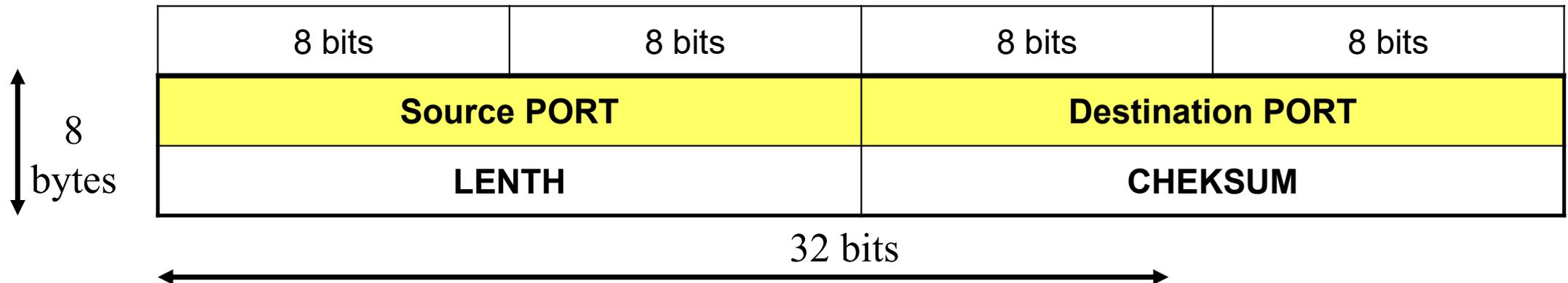
Transport protocol : TCP

connection-oriented Protocol, more complex than UDP

  acknowledgement delivery (ACK) and emission/reception counter

Flow management

  sliding windows / buffers

8 bits	8 bits	8 bits	8 bits
Source PORT		Destination PORT	
Sequence Number			
Acknowledgement Number			
Off	Reserved	Flags	Window
Checksum		Urgent pointer	
Options			Padding

20 bytes

32 bits
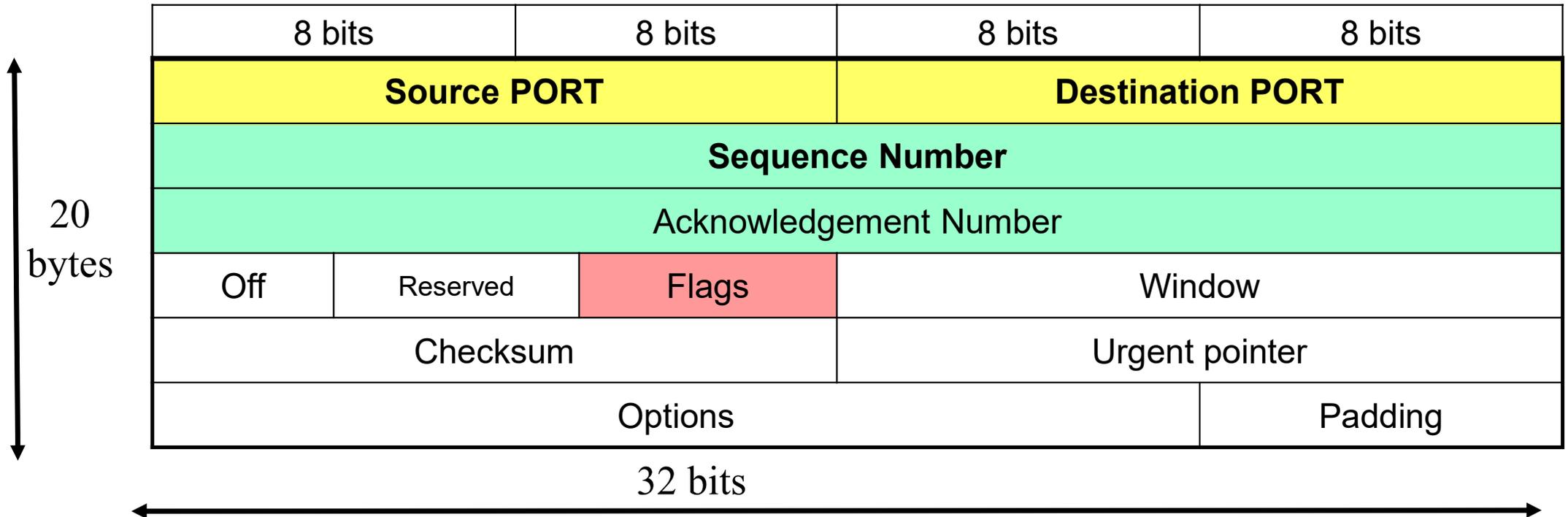
TCP: flags

- URG   :   Urgent Pointer field significant

- ACK : Acknowledgment field significant

- PSH : Push Function

- RST : Reset the connection

- SYN : Synchronize sequence numbers

- FIN : No more data from sender

Outline

- Internet protocol
  - Introduction
  - Addressing mechanisms
  - IP routing
  - IP packets format
- ICMP
- TCP et UDP
- Routing

Packet Processing in a router

FACTORI 4.0 Erasmus +

192.168.1.0 /24	*	IF1
172.16.1.0 /24	*	IF2
182.168.1.0 /24	*	IF3
12.168.1.0 /24	*	IF4

Postprocessing

IP_src | IP_dst

Preprocessing

IP_src | IP_dst

IP_src | IP_dst

ROUTING

IP_src | IP_dst

P_src | IP_dst

Frame building

Frame extraction

IP_src | IP_dst

P_src | IP_dst

Input Interface

If1

If2   *If3*   *If4*

IP_src | IP_dst

IP_src | IP_dst
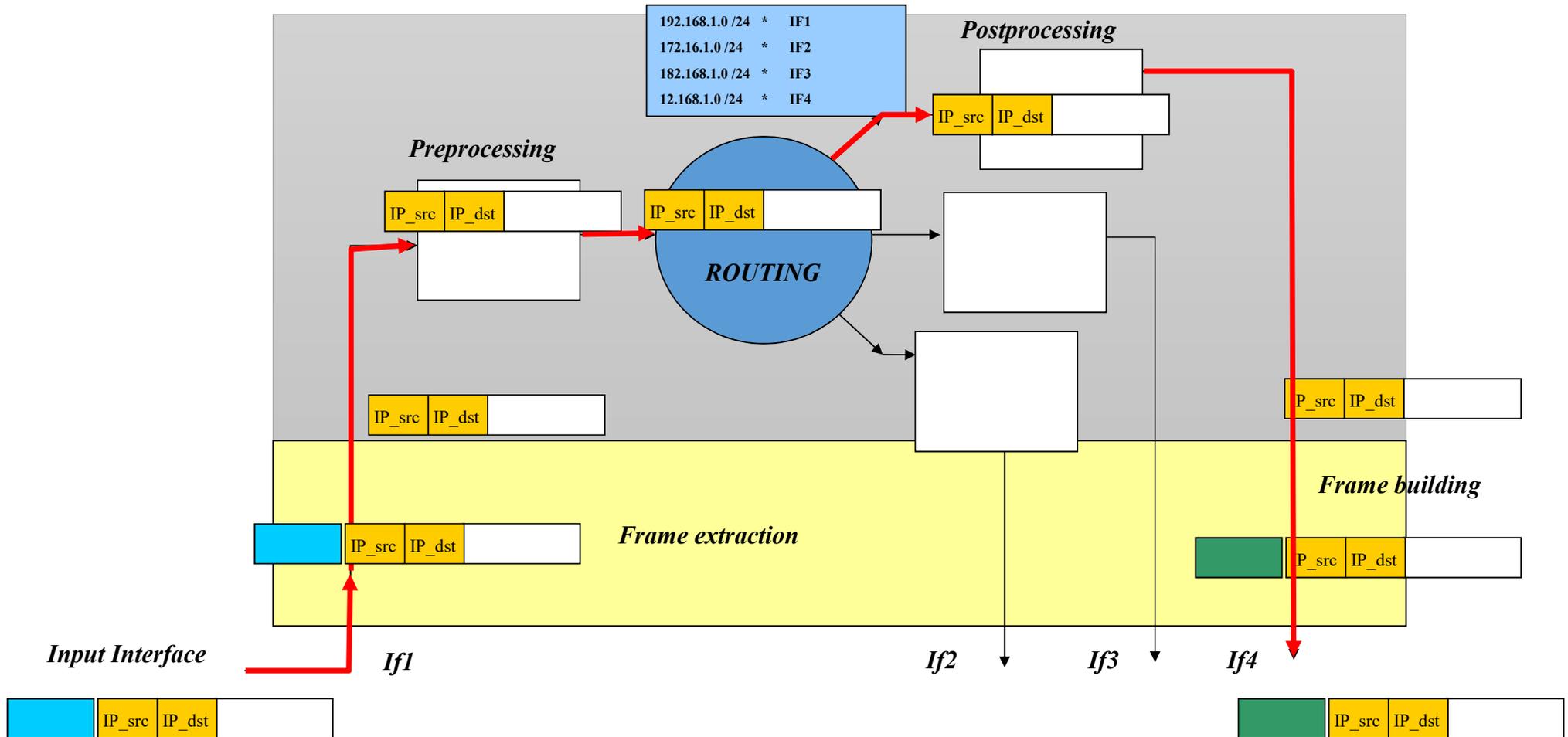
IP routing

- 1°)   Choosing an output interface : Routing and routing table

  - The routing table contains the needed information to choose a route

  - Each layer 3 machine contains a routing table (hosts, routers…)

- 2°)   The packet should be encapsulated in a frame
  - How to build a frame ?
    - The Ethernet example

Example

Packet Routing

Selection		OUTPUT	
Network	Mask	Gateway	Interface
4.0.0.0	/8	*	eth0
5.0.0.0	/8	*	eth1
2.0.0.0	/8	5.0.0.1	eth1
3.0.0.0	/8	5.0.0.2	eth1
0.0.0.0	/0	5.0.0.3	eth1

4.0.0.2

4.0.0.2

4.0.0.2

4.0.0.2

4.0.0.2

IP_src | IP_dst
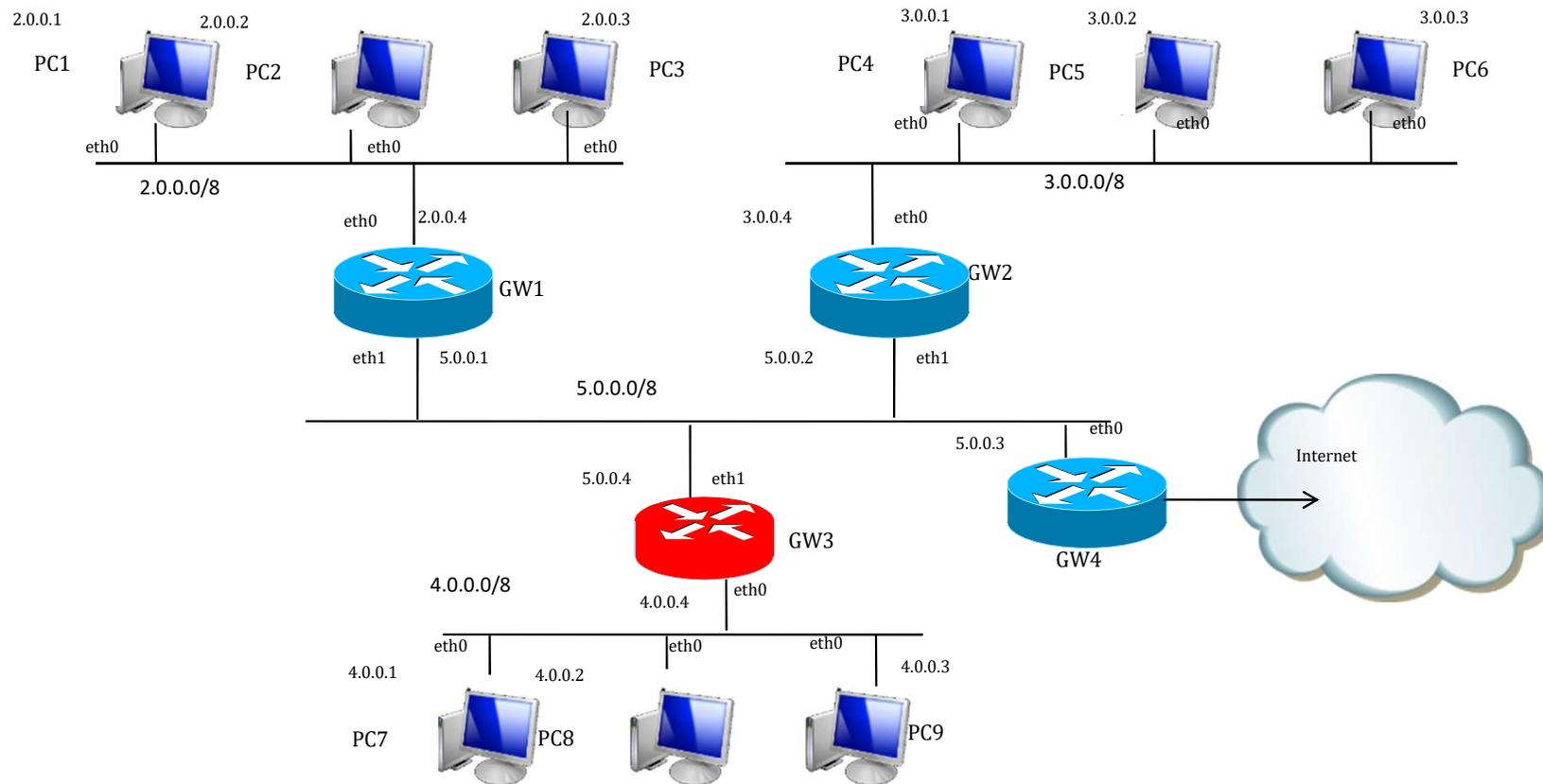
What is routing

Select the best route according to the destination address : DA

The routing table contains 4 essential parameters : NW MASK GW IF

1. Choose a route (a line in the table)

   For each line
   ⇨ If (Dst.A AND MASK) = Network   then this Route is OK

   If several routes , longest prefix match is applied

2. Build the frame and send it trough the specified output
   if GW = *, the destination network is directly connected
   if GW = A.B.C.D, a fram containing the packet is sent to next Gateway

Exercise : route selection accoring to LPM

▪ Table de routage

Réseau	Masque	Passerelle	sortie
152.77.65.192	/27	*	if1
152.77.65.0	/26	152.77.65.193	if1
152.77.65.0	/25	152.77.65.194	if1
152.77.65.128	/26	152.77.65.195	if1
0.0.0.0	/0	152.77.63.254	if0

▪ Quelle décision prise si

DST_A= 152.77.65.4   ?

DST_A= 152.77.65.65   ?

DST_A= 152.77.65.130   ?

DST_A= 152.77.65.193   ?

DST_A=152.77.65.227   ?

Routing table in a host

Network	Mask	Gateway	Interface
4.0.0.0	255.255.255.0	*	IF1
0.0.0.0	0.0.0.0	4.0.0.4	IF1
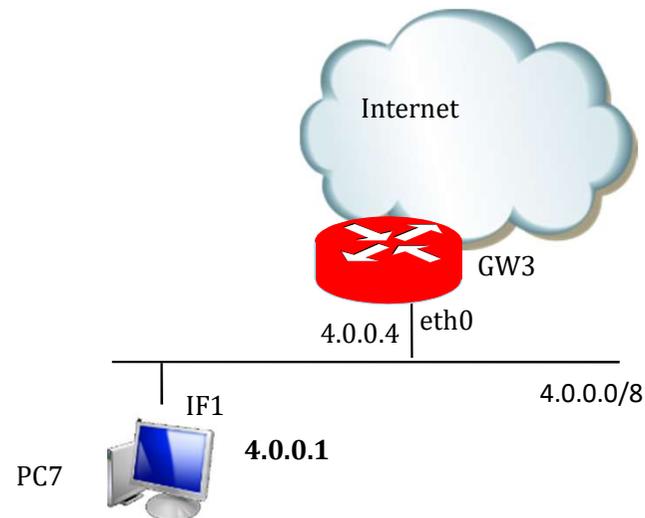
Internet

GW3

4.0.0.4 eth0

IF1

4.0.0.0/8

PC7 4.0.0.1

Device configuration

The first 2 parameters are useful to know the local IP address and the local network

The last one is only useful to join the router. (Used in ARP requests)

Windows routing table

```
C:\>route print

===========================================================================

IPv4 routing table

===========================================================================

Active routes

Network Destination        Netmask          Gateway        Interface  Metric
      0.0.0.0              0.0.0.0        192.168.0.254    192.168.0.200     55
   192.168.0.0         255.255.255.0       On-link        192.168.0.200    311

===========================================================================

Persistent Routes:
   None
```

Outline

- Internet protocol
  - Introduction
  - Addressing mechanisms
  - IP routing
  - IP packets format
- ICMP
- TCP et UDP
- Routing
- Applications and exercises

Outline

TCP/IP stack Tutorial

    IP addressing

    Routing

- **LAB-0.1 : Test routing with NOC**

- **LAB-0.2: Test routing with Stormshield Firewall**

- **Exercises : Different network structures**

Lab 0.1 : test routing with NOC

MIRROR (copy of all frames)

PLC SIMULATOR
192.168.0.1

InetAutomate
192.168.0.0/24

ControlExpert
172.16.12.200

192.168.0.128

172.16.12.254

172.16.0.0/24

······· Ethernet/IP BackPlane

MIRROR (copy of all frames)

NOC

PLC SIMULATOR
192.168.0.1

InetAutomate
192.168.0.0/24

192.168.0.128

172.16.12.254

ControlExpert
172.16.12.200

172.16.0.0/24

NOC configuration

- Next gateway possible to
Another newtwork
192.168.0.100

192.168.0.128

172.16.12.254

172.16.0.100
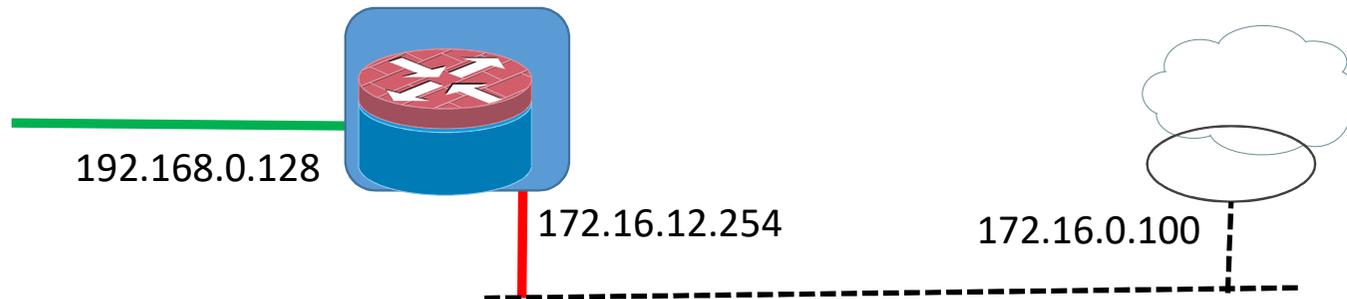
Cf. Book p.

▪ PLC Configuration

▪ ControlExpert Machine configuration

Outline

TCP/IP stack Tutorial

IP addressing

Routing

▪ LAB-0.1 : Test routing with NOC

▪ **LAB-0.2: Test routing with Stormshield Firewall**

▪ **Exercises : Different network structures**

Lab 0.2 : test routing with FW

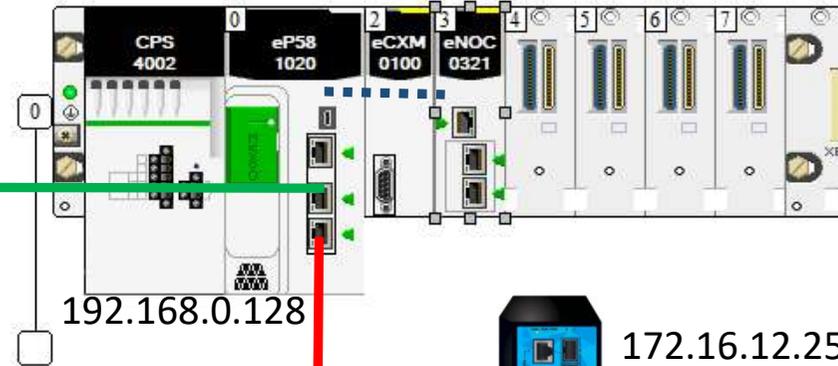**PLC SIMULATOR**
192.168.0.1

InetAutomate

192.168.0.0/24

······· *Ethernet/IP BackPlane*

192.168.0.128

ControlExpert
172.16.12.200

172.16.12.254

172.16.0.0/24

FW

FW

PLC SIMULATOR
192.168.0.1

InetAutomate

192.168.0.0/24

192.168.0.254

3

172.16.12.254

2

ControlExpert
172.16.12.200

172.16.0.0/24

Connectivity tests

■ From ControlExpert

```
C:\Users\user>tracert 192.168.0.1

Tracing route to PLC [192.168.0.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  172.16.12.254
  2     2 ms     1 ms     2 ms  PLC [192.168.0.1]
```

■ From PLC

```
C:\Users\user>tracert 172.16.12.200

Tracing route to DESKTOP-IJPPEJD [172.16.12.200]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  192.168.0.254
  2     3 ms     1 ms     2 ms  DESKTOP-IJPPEJD [172.16.12.200]
```

Outline

TCP/IP stack Tutorial
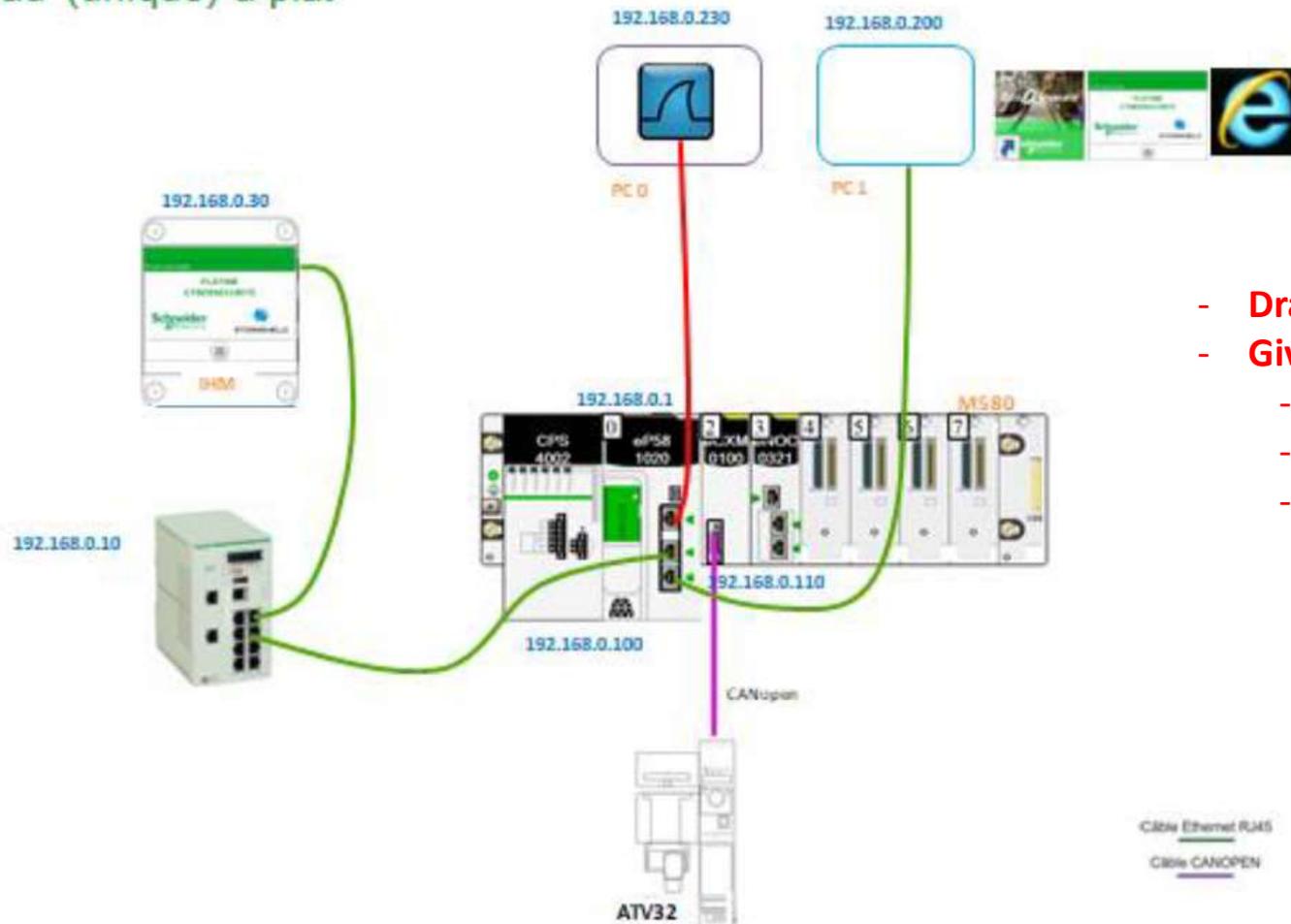
    IP addressing

    Routing

- **LAB-0.1 : Test routing with NOC**
- **LAB-0.2: Test routing with Stormshield Firewall**

- **Exercises : Different network structures**

Different structures

Système M580 – Phase 1 (IP 192.168.0.0)

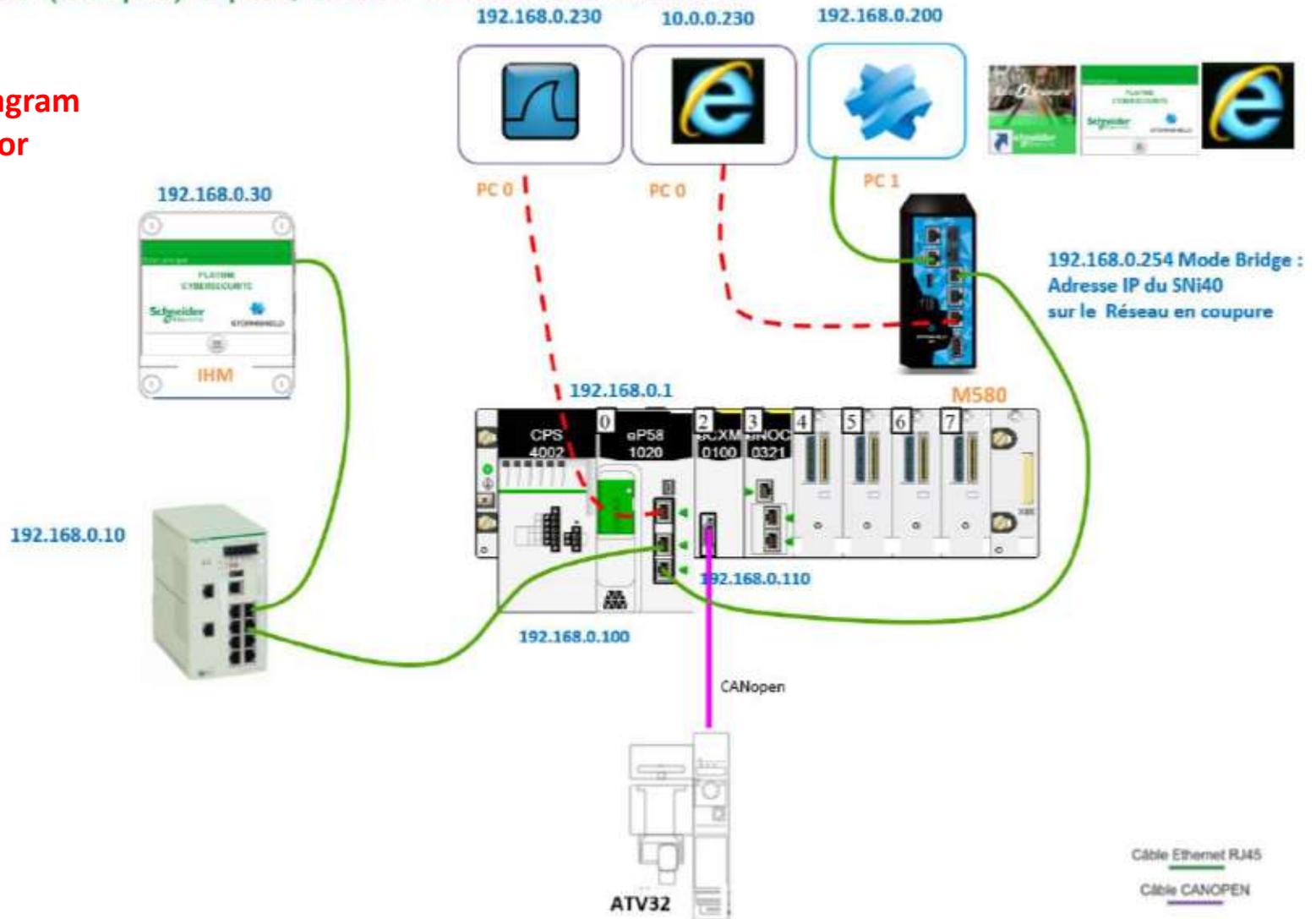Réseau (unique) à plat

- Draw the logical diagram
- Give routing table for
    - PC0
    - PLC
    - PC1

Système M580 – Phase 2 (IP 192.168.0.0)

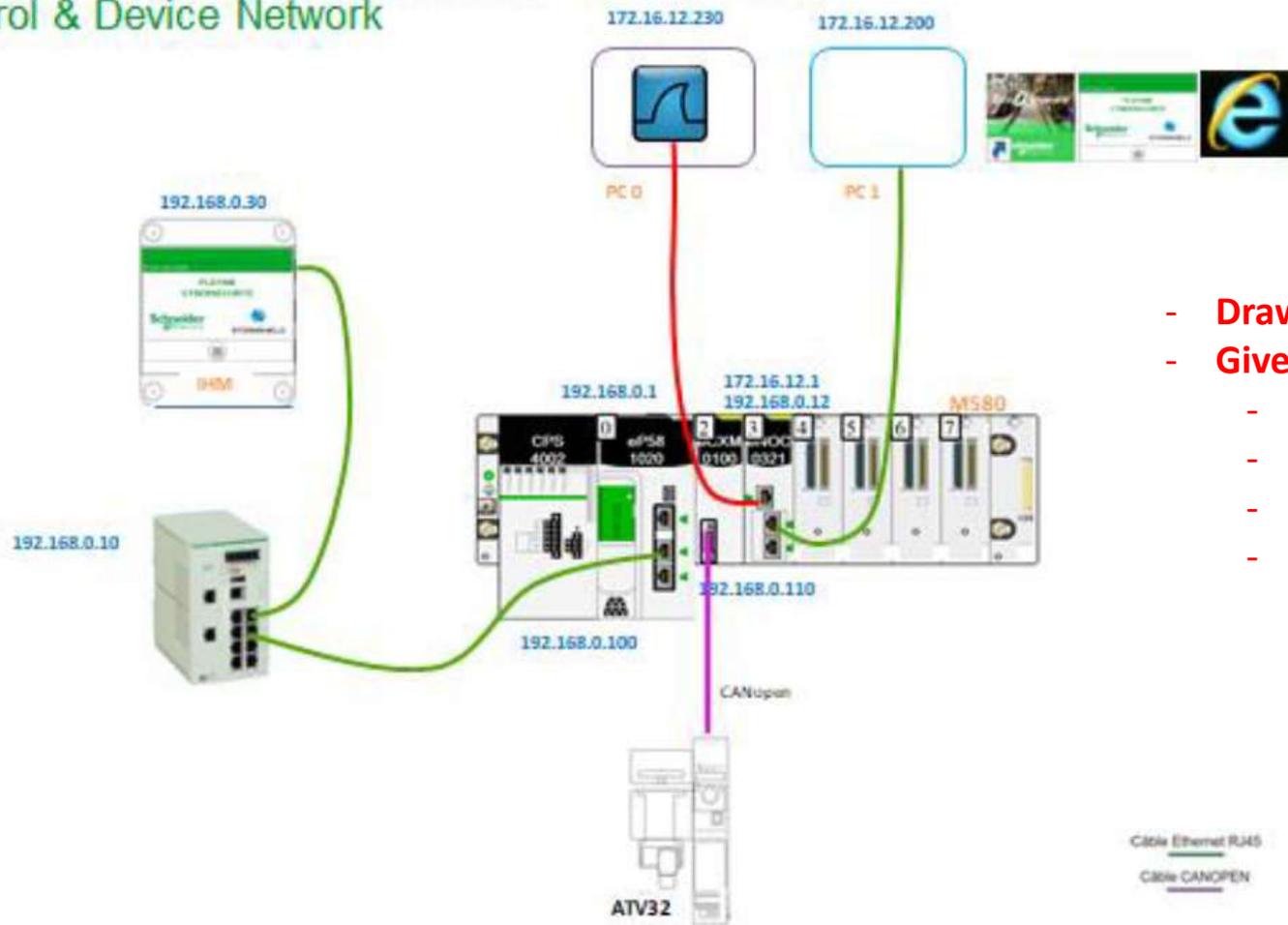## Réseau (unique) à plat, avec Firewall Stormshield

- Draw the logical diagram
- Give routing table for
  - PC0
  - PLC
  - PC1

192.168.0.230   10.0.0.230   192.168.0.200

PC 0   PC 0   PC 1

192.168.0.30

192.168.0.254 Mode Bridge :
Adresse IP du SNi40
sur le Réseau en coupure

IHM

192.168.0.1

CPS 4002   eP58 1020   BCXM 0100   eNOC 0321   M580
0   2   3   4   5   6   7

192.168.0.10

192.168.0.110

192.168.0.100

CANopen

ATV32

Câble Ethernet RJ45

Câble CANOPEN

Système M580 – Phase 3

Réseaux Séparés (IP 192.168.0.0 // 172.16.12.0)
Control & Device Network

- **Draw the logical diagram**
- **Give routing table for**
  - **PC0**
  - **PLC**
  - **PC1**
  - **NOC**

Système M580 – Phase 4

Réseaux Séparés & Firewall (IP 192.168.0.0 // 172.16.12.0)

- Draw the logical diagram
- Give routing table for
  - PC0
  - PLC
  - PC1
  - NOC
  - FW

- **Draw the logical diagram**
- **Give routing table for**
    - **PC0**
    - **PLC**
    - **PC1**
    - **NOC**
    - **FW**
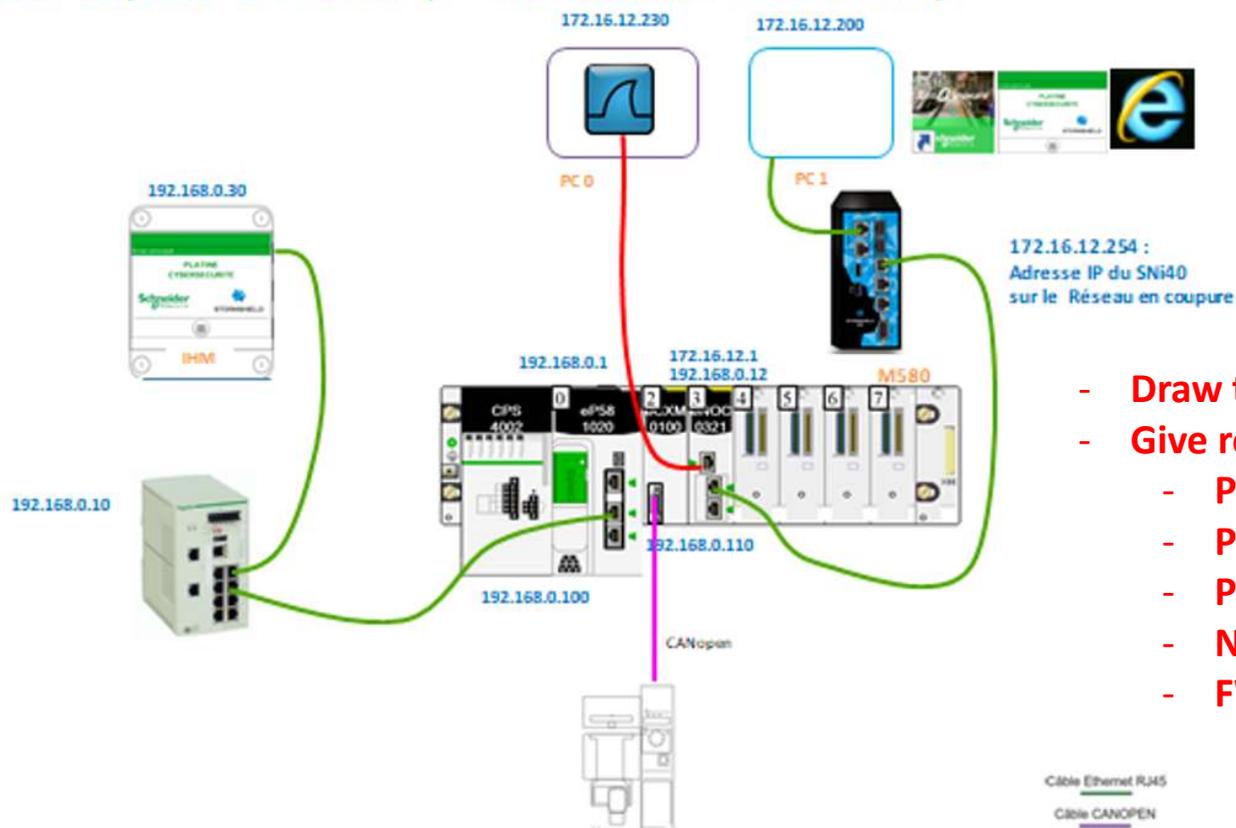
Système M580 – Phase 5

Réseaux Séparés & Firewall à Réseaux Séparés (IP 192.168.0.0 // 172.16.12.0 // 172.16.112.0)