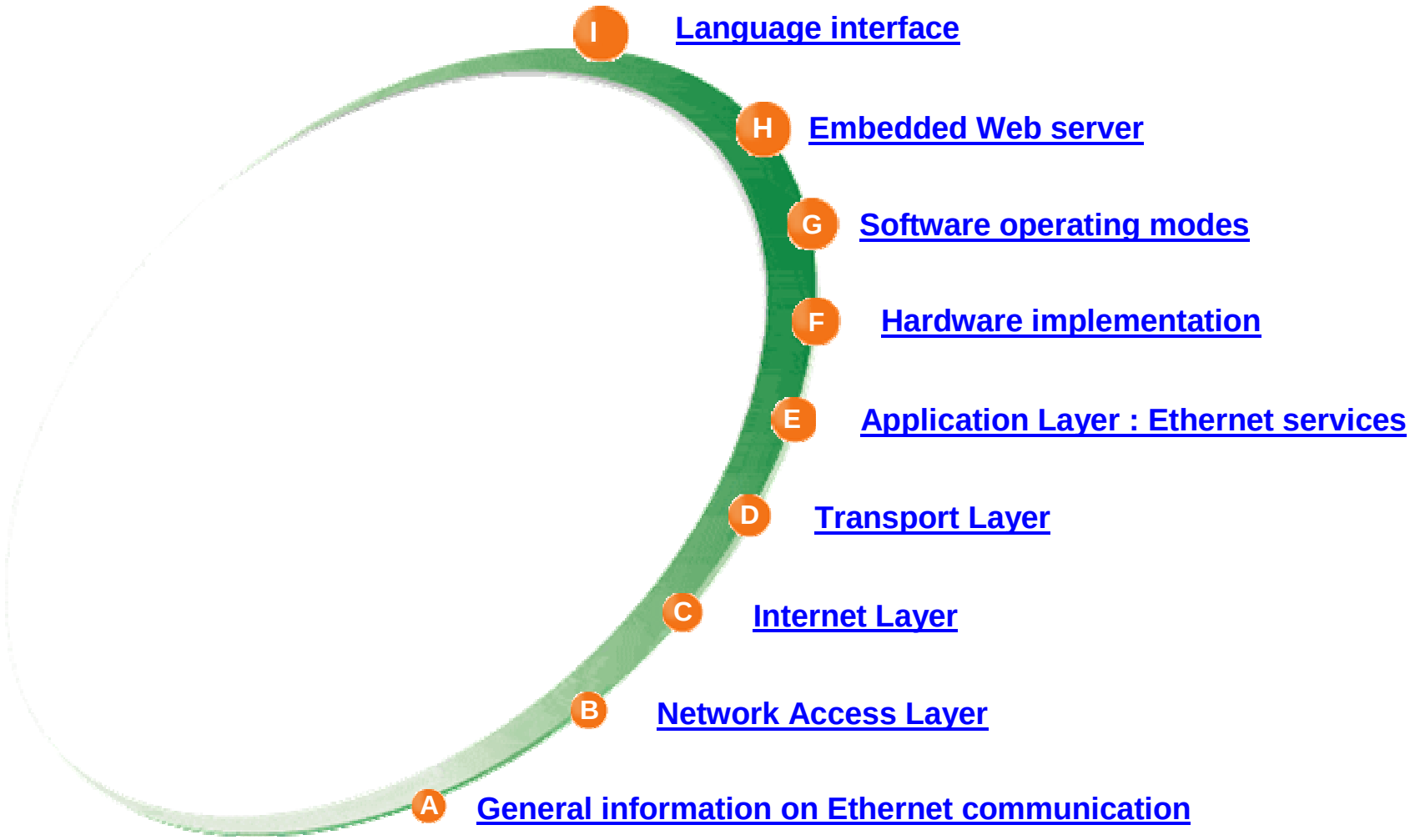
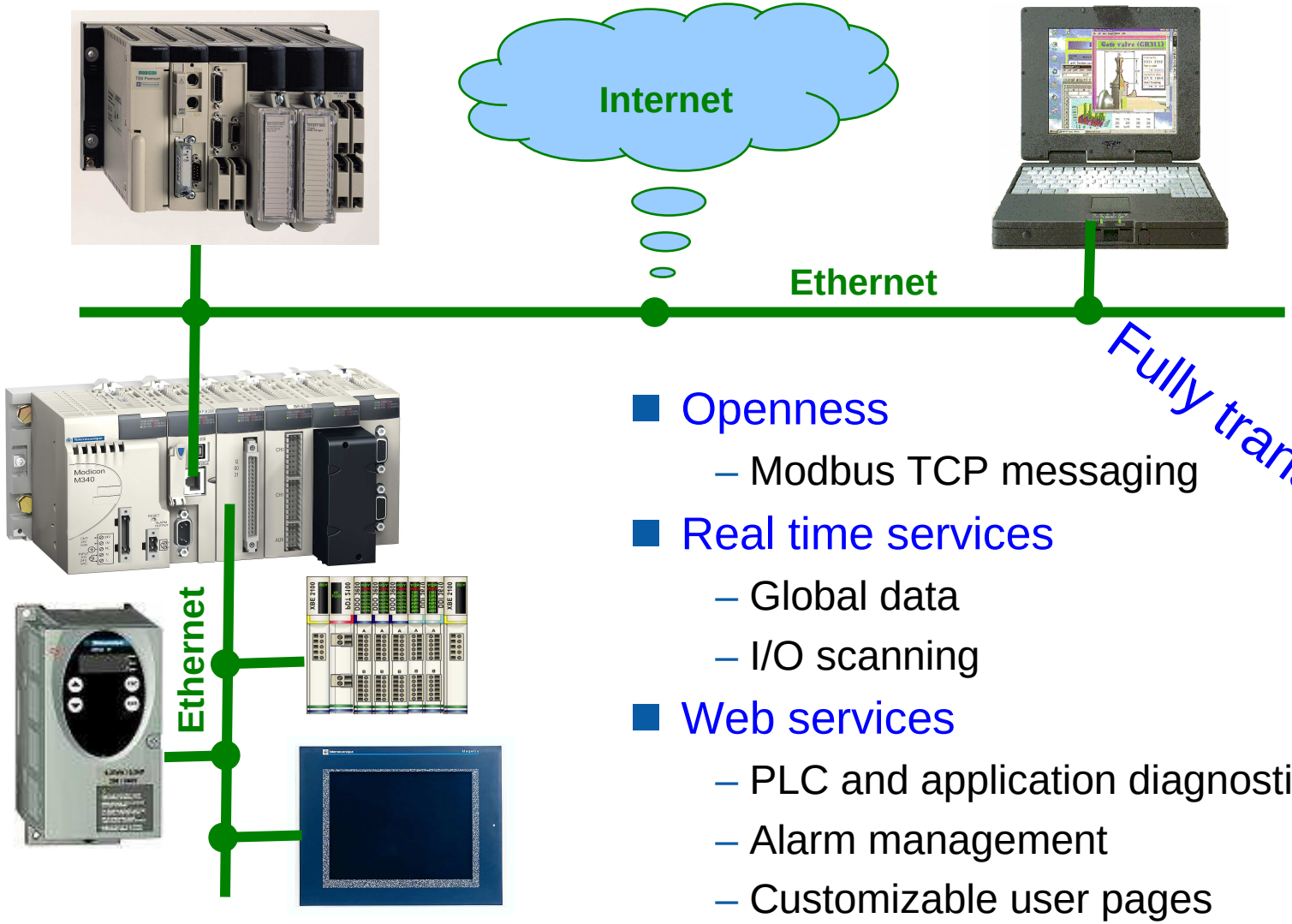
Modicon M340 : Ethernet communication



General information on Ethernet communication

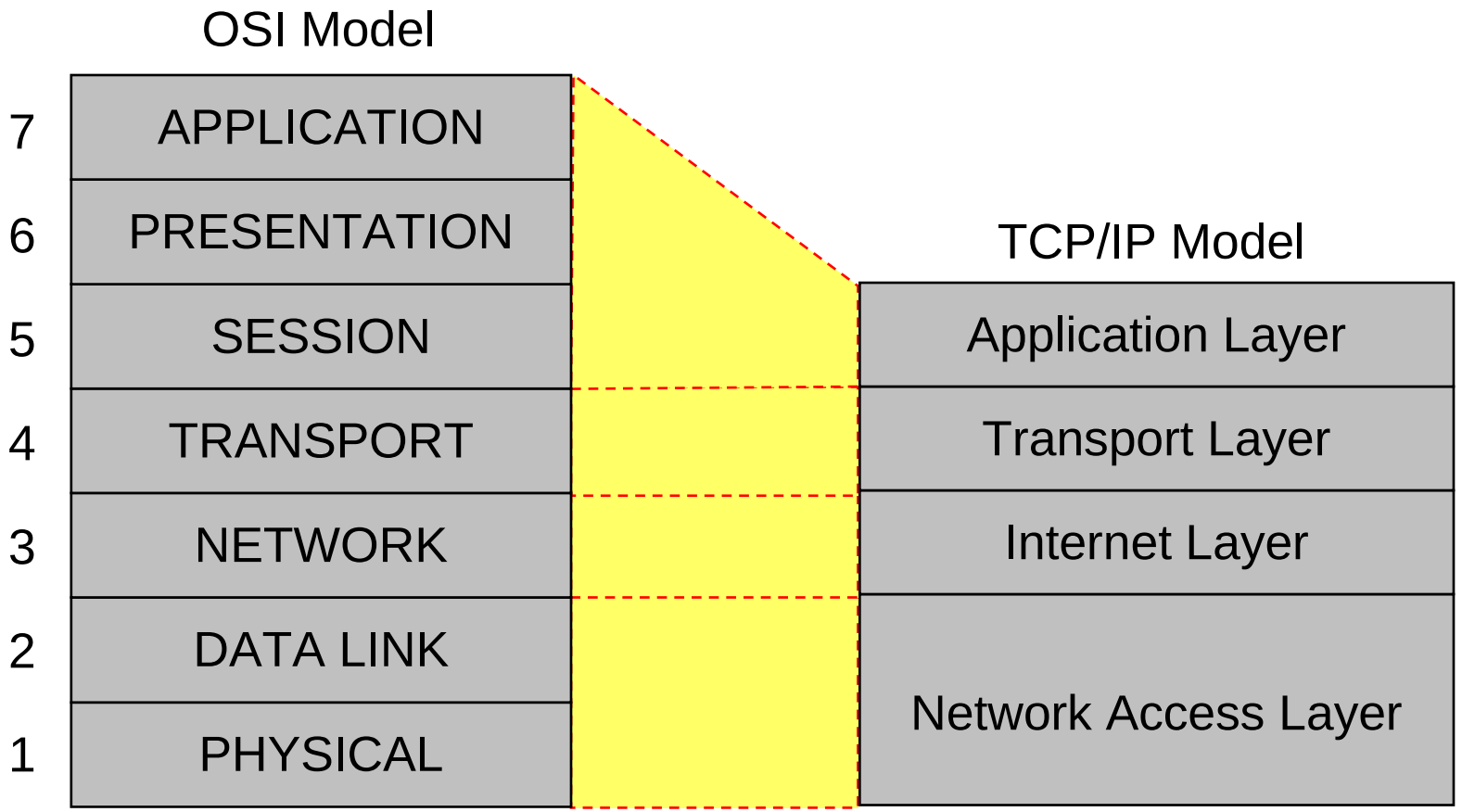
Ethernet communication overview



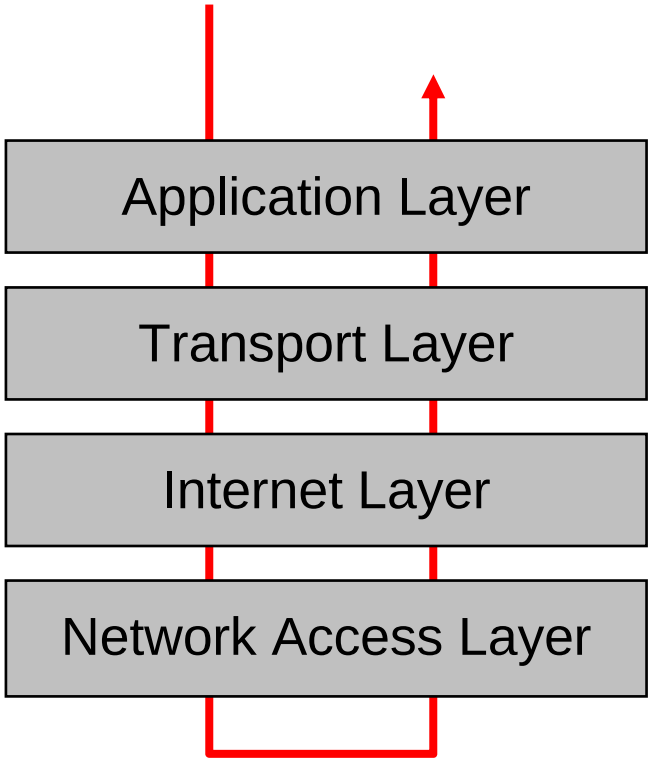
- Openness
  - Modbus TCP messaging
- Real time services
  - Global data
  - I/O scanning
- Web services
  - PLC and application diagnostic
  - Alarm management
  - Customizable user pages

Fully transparent ready

Correspondance between OSI Model and TCP/IP Layer Model

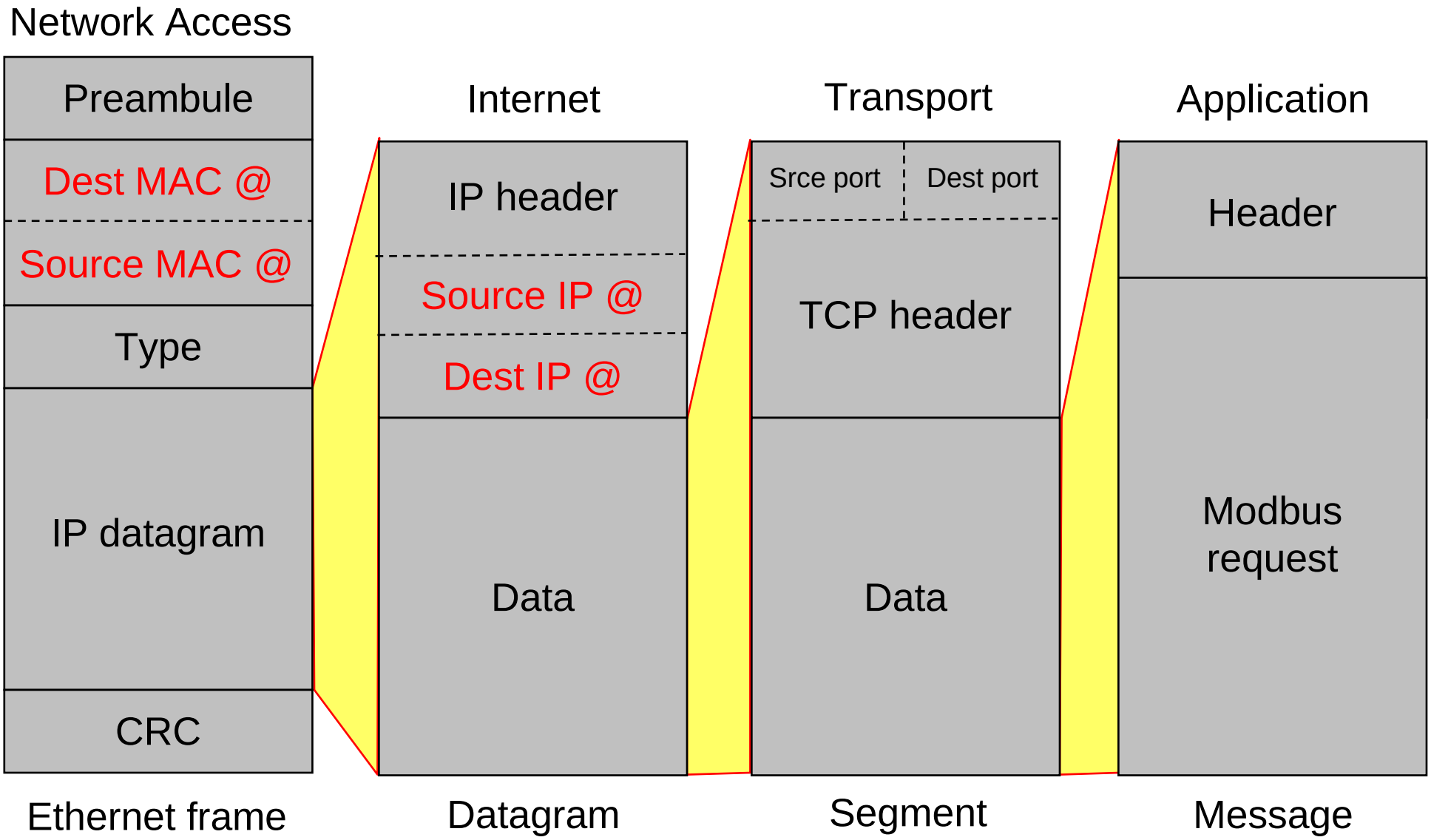


TCP / IP Layer



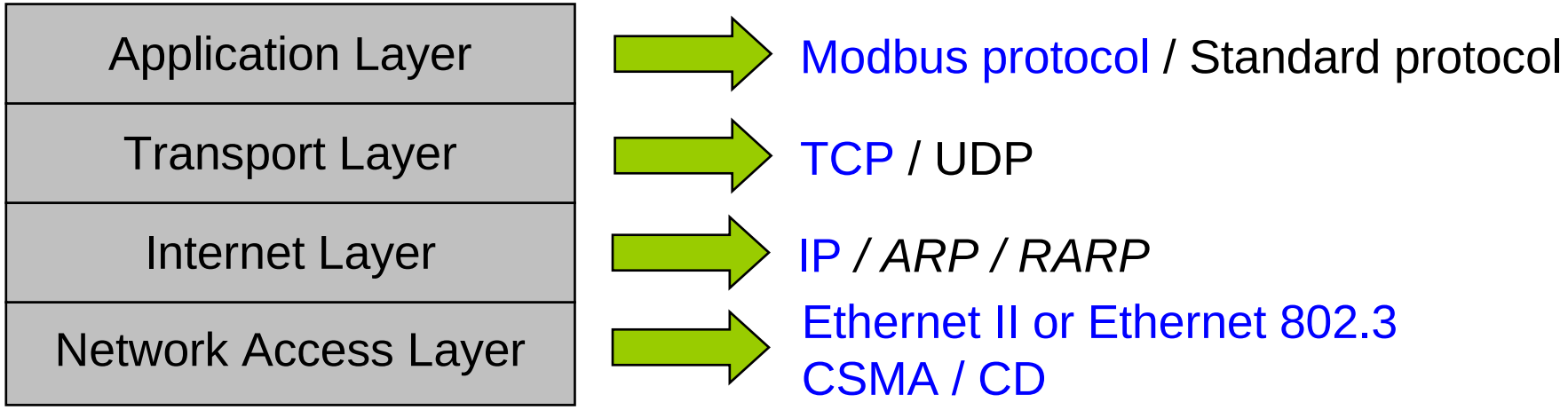
- Ethernet data is modified when crossing the different layers (adding a header)
- Network Access Layer defines the form to transmit the data whatever the type of physical link (Ethernet frame)
- Internet Layer defines the packet of data (datagram)
- Transport Layer manages data routing and data integrity
- Application Layer manages Modbus protocol and all standard applications (SMTP, FTP, …)

Encapsulated data



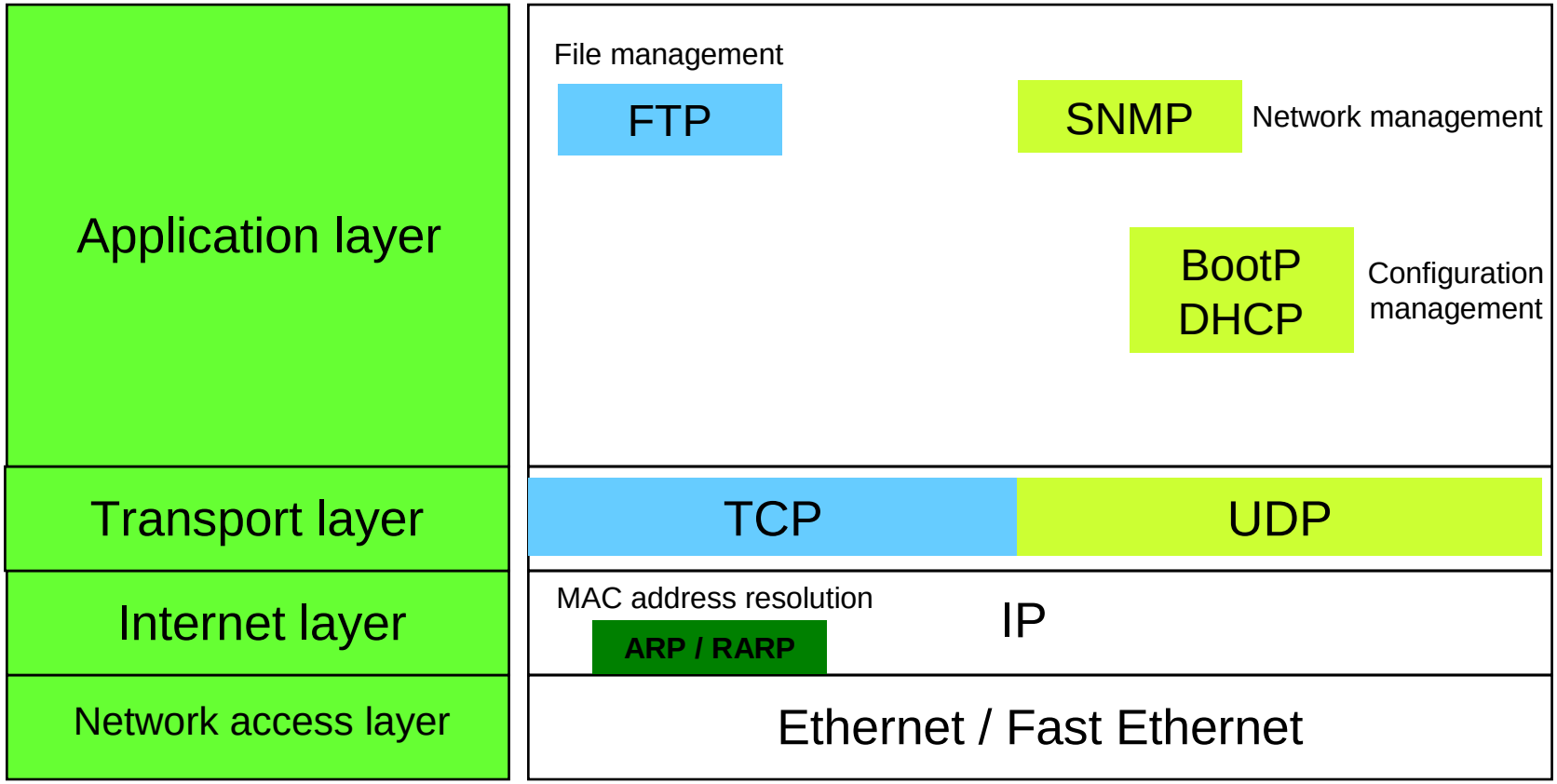
Ethernet protocols

TCP/IP Model



TCP : Transmission Control Protocol
IP : Internet Protocol
UDP : User Datagram protocol
CSMA / CD : Carrier Sense Multiple Access / Collision Domain
ARP : Address Resolution Protocol
RARP : Reverse Address Resolution¨Protocol

Typical TCP / IP stack



Communication protocols : ARP (*Address Resolution Protocol*) / RARP (*Reverse Address Resolution Protocol*)
Configuration protocols : BootP (*Bootstrap Protocol*) / DHCP (*Dynamic Host Configuration Protocol*)
Application protocols : FTP (*File Transfer Protocol*) / SNMP (*Simple Network Management Protocol*)

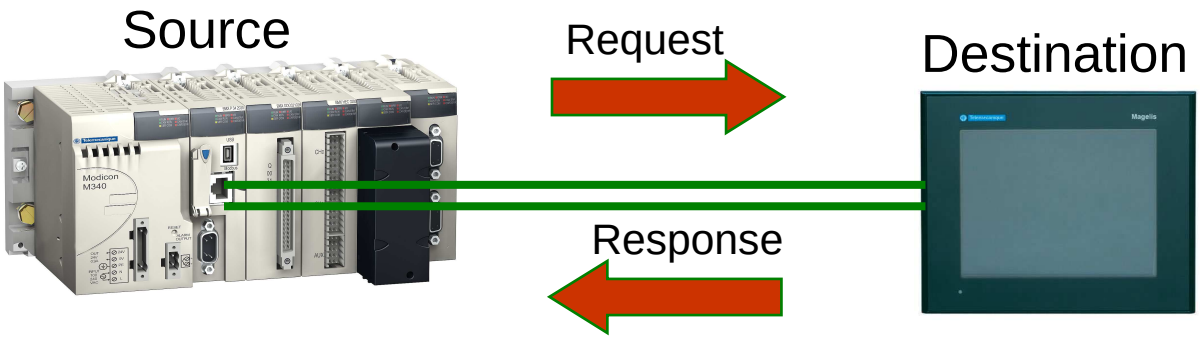
Network Access Layer

Physical Interface

- Ethernet
  - Twisted pair / fiber optic / wireless link / coax
  - 3 types of geometric arrangement for nodes and links (topology) : bus, star and ring
  - RJ45 10/100 BASE-T connector

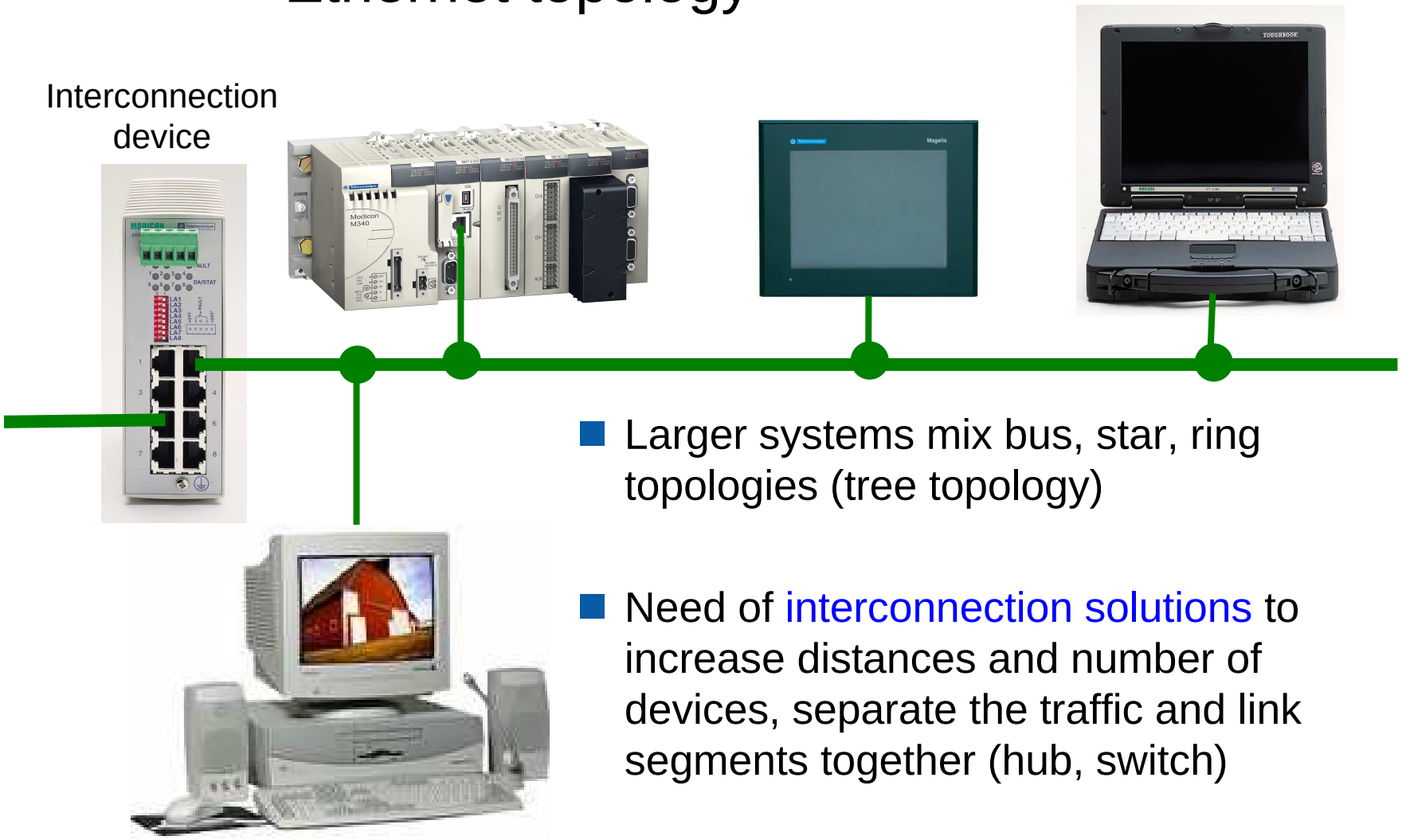
- Modicon M340 modules
  - Line speed is self adapted : 10 or 100 Mbits/s
  - Half or Full duplex
  - Automatic management of straight and cross-over cables

Half / Full duplex principle



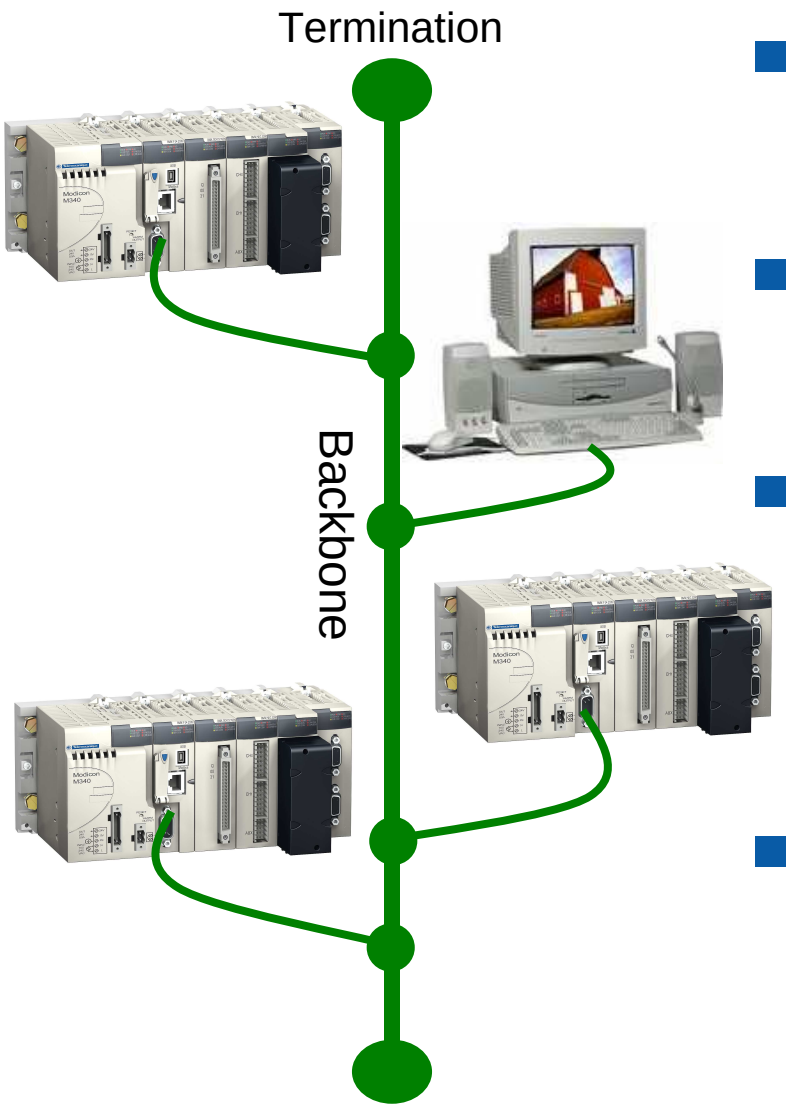
- Half duplex
  - Same medium for communication
  - Signals pass in both directions but not simultaneously
- Full duplex
  - Lines for transmission and reception are separated
  - Signals pass in both direction simultaneously
  - Response time is better than half duplex

Ethernet topology



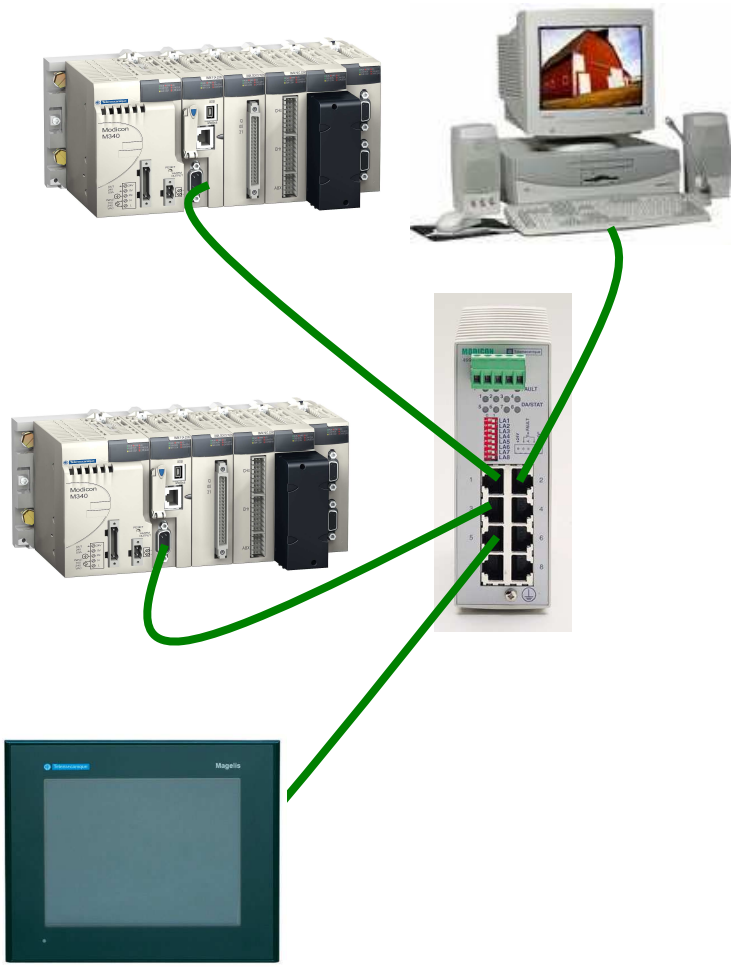
- Larger systems mix bus, star, ring topologies (tree topology)
- Need of interconnection solutions to increase distances and number of devices, separate the traffic and link segments together (hub, switch)

Bus topology (remind)



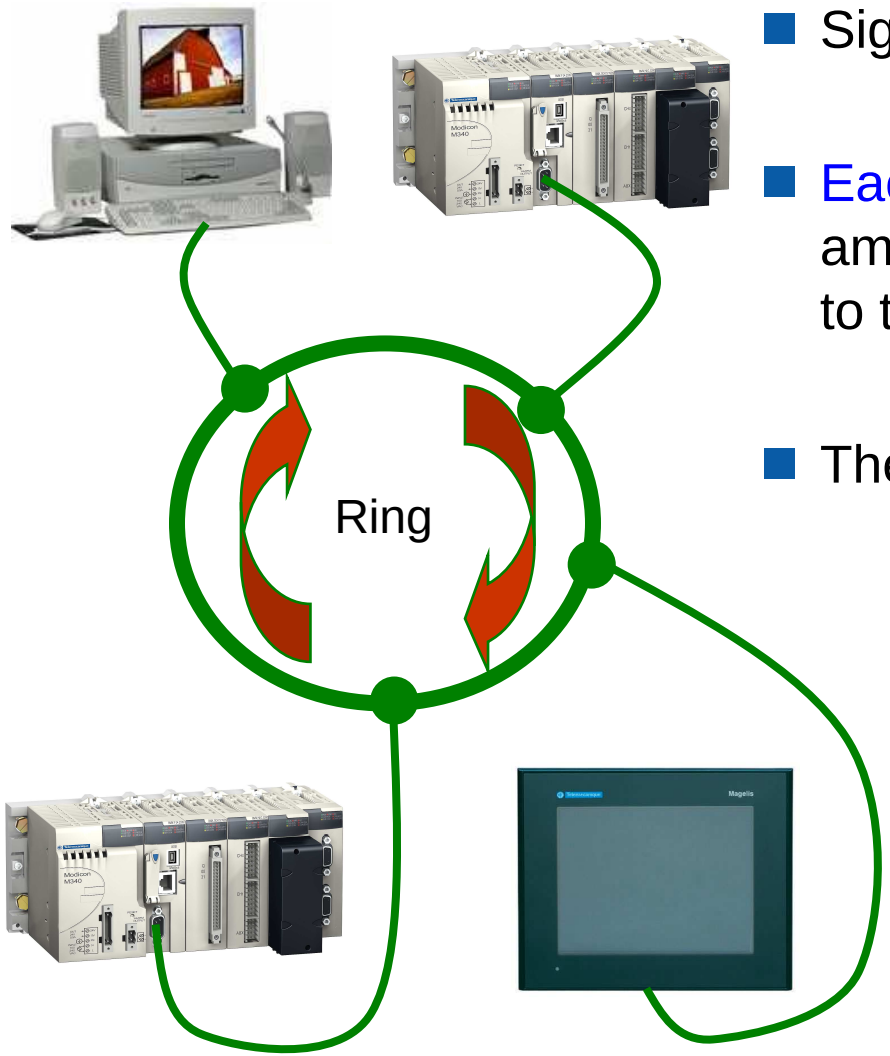
- All devices (nodes) are connected on a single cable (backbone)
- Signals travel in both directions from the source node
- If the path is broken at any point the system fails
  - Lack of termination causes excessive noise on the network and nodes are unable to determine if the network is available
- Use a backbone to interconnect other LAN sections

Star topology (remind)



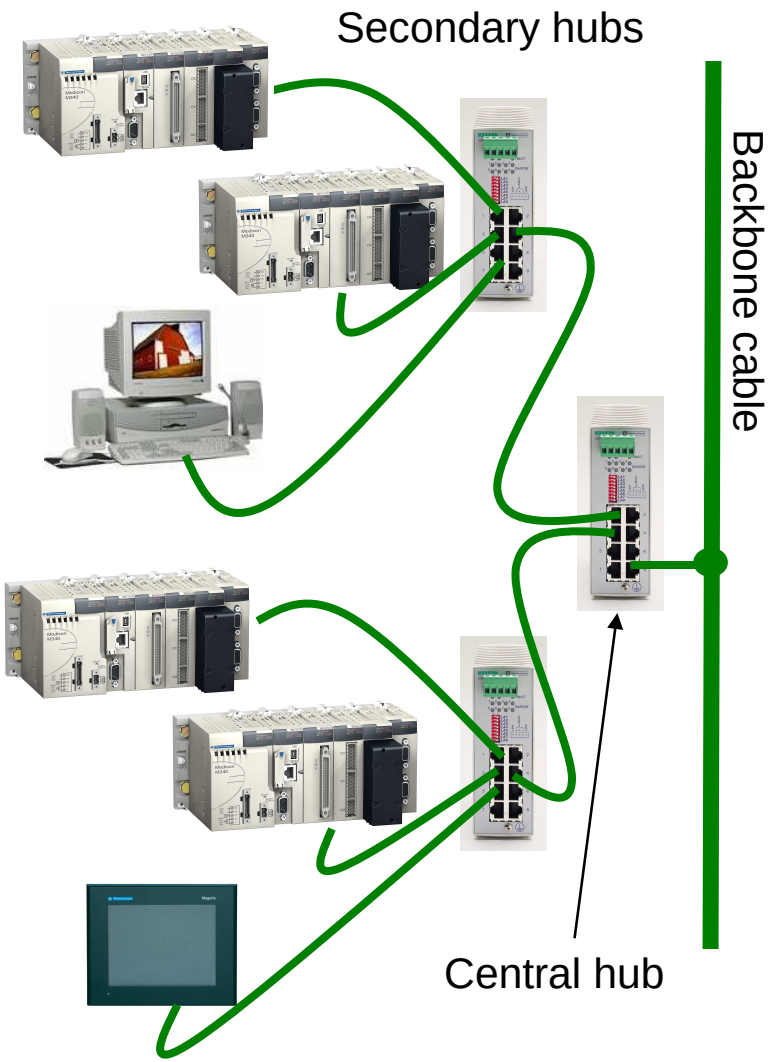
- Devices are connected through a hub or a switch
- Message enters the hub and is broadcast to all other nodes
- A failed node do not affect the other nodes
- Hubs can be daisy chained together to form larger networks
- Fast and easy to install and expand
- 100 m maximum between node and hub

Ring topology (remind)



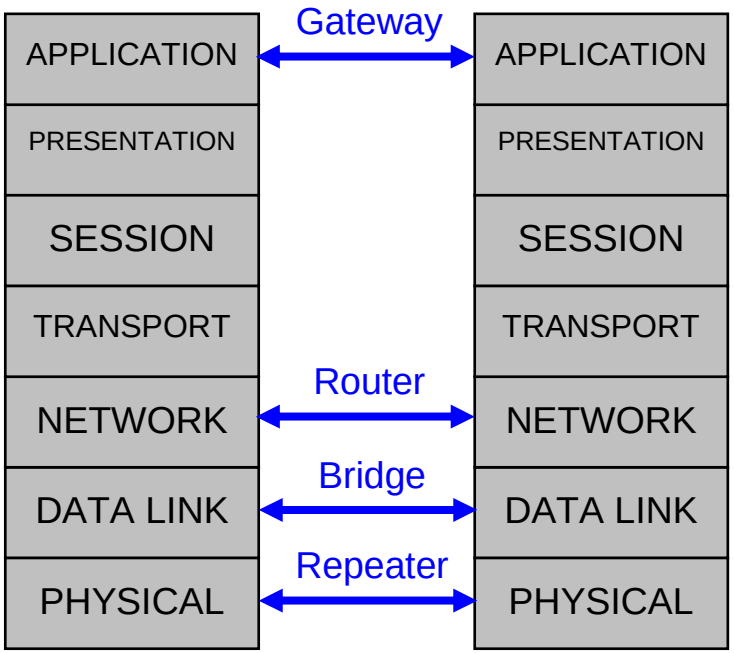
- Signals pass in one direction only
- Each device acts as a repeater which amplifies the signal before transmitting it to the next device of the ring
- The ring is broken if one device fails

Tree topology (remind)



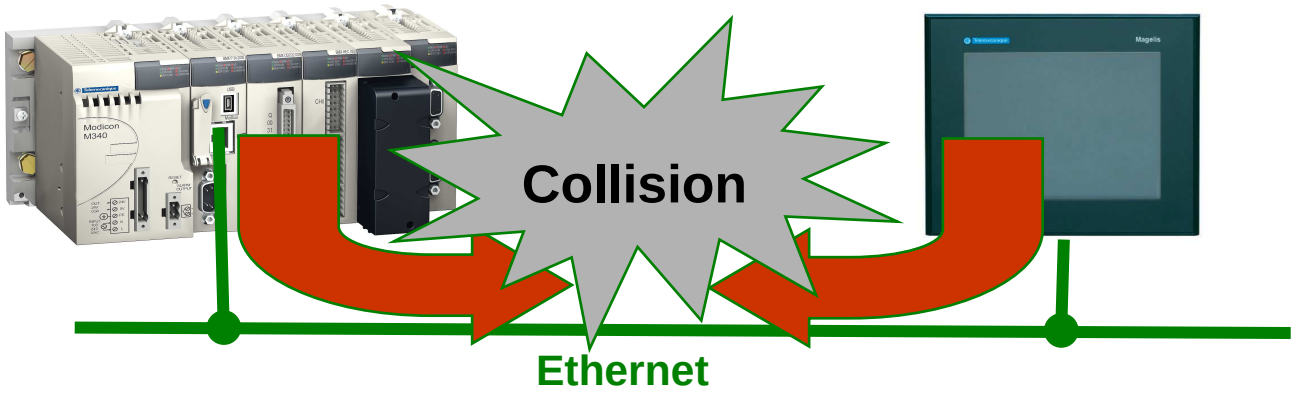
- Combines characteristics of linear bus and star topologies
- Groups of star-configured devices are connected to a linear backbone cable
- Tree topology is appropriate to expand an existing network
- Allows more devices to be attached to a single central hub
- Network isolates and prioritizes communication from different devices

Interconnection devices



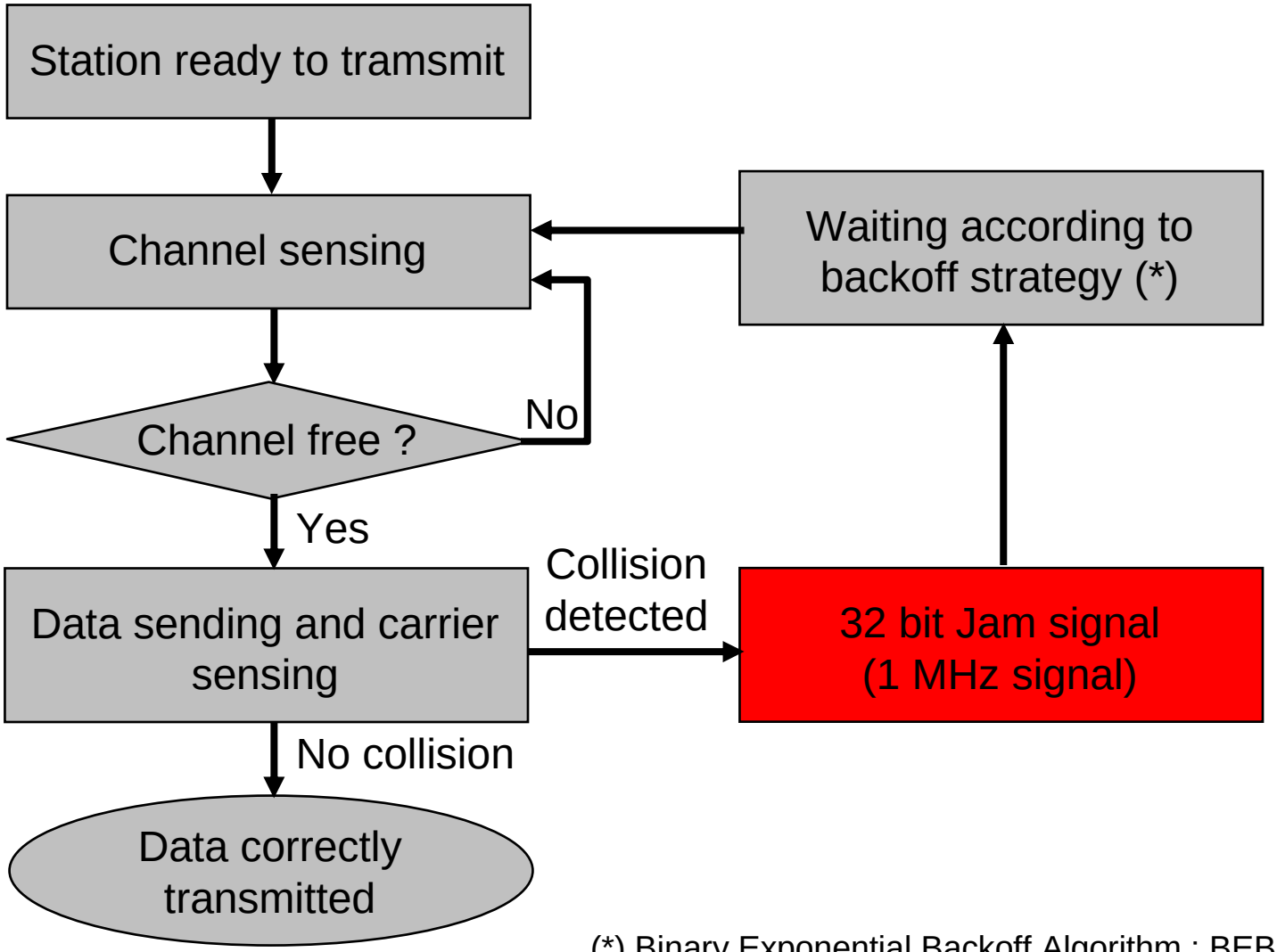
- Gateway to provide interconnection between 2 different networks (ie Modbus and Ethernet)
- Router to filter out network traffic
  - IP router divides a network into various subnetworks
  - **Firewall** is a router device with network security that can be configured to stop protocols, users, or type of data
- Bridge or Switch to create a physical segmentation
  - Provides routing of information between several physical segments
- Repeater or Hub to overcome signal attenuation and increase segment length (amplify and reshape the signal)

CSMA / CD access method



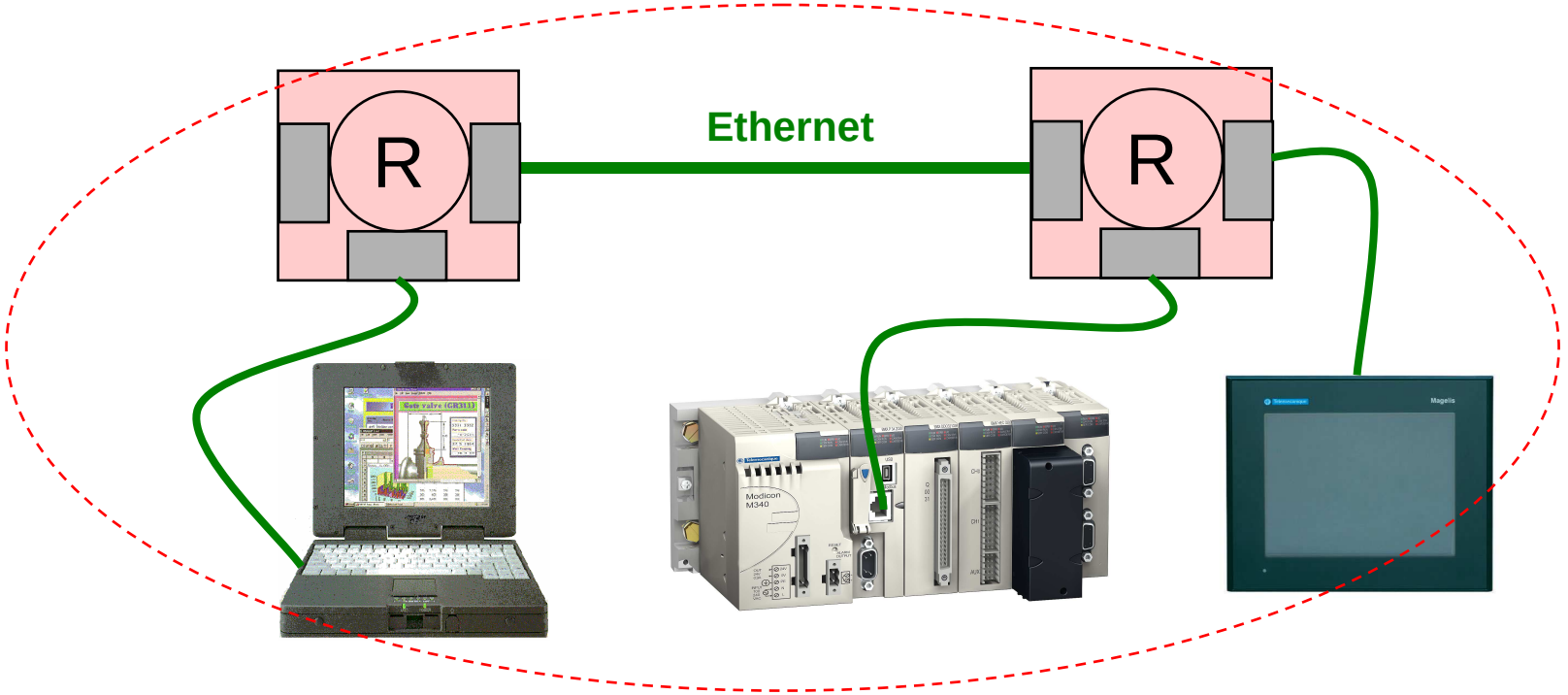
- Network access method : CSMA / CD (*Carrier Sense Multiple Access with Collision Detection*)
  - Before transmitting a message the device “listens” to the network
  - If the network is free the device starts to transmit then “listens” to its own message to verify that there is no collision (2 devices transmit at the same time)
  - In case of collision a jam signal is sent, the device waits for a random time then transmits again the message
- Collision signal is available in the same collision domain

CSMA / CD collision detection



(*) Binary Exponential Backoff Algorithm : BEB

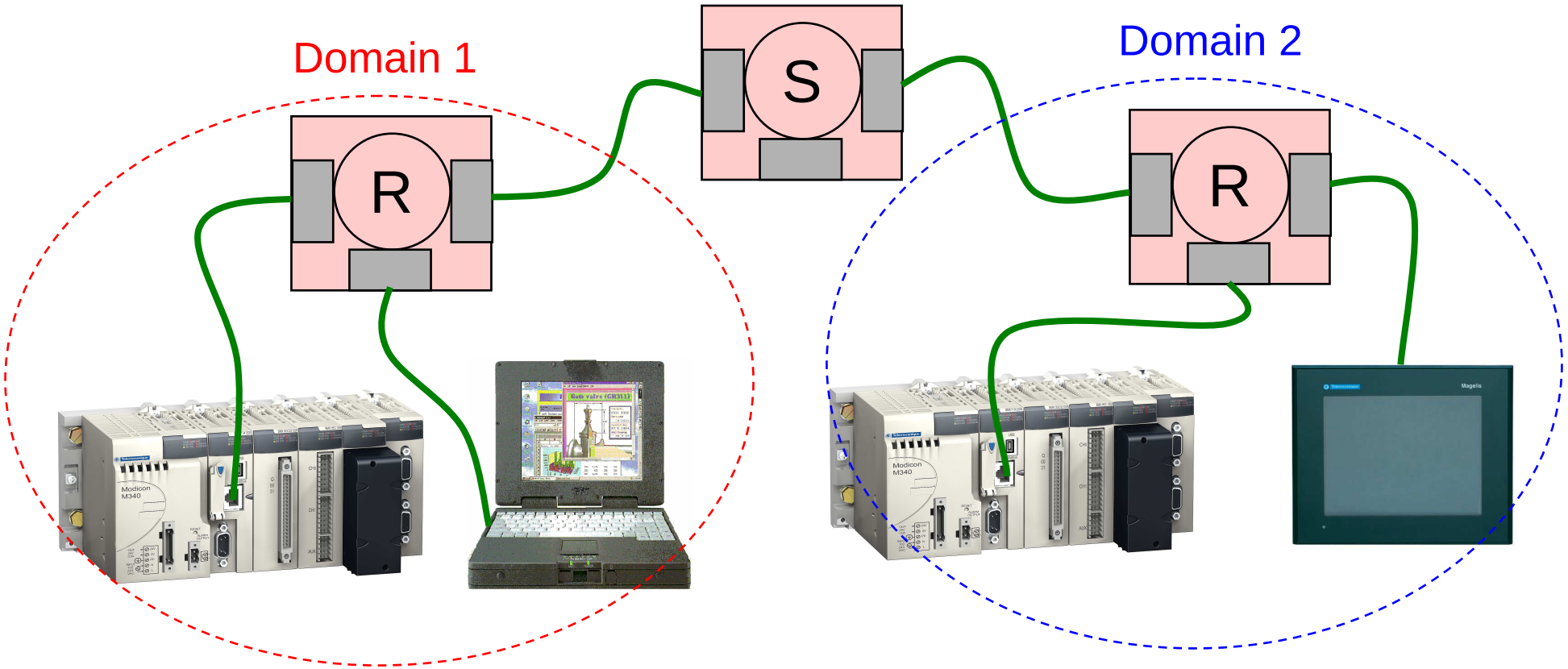
Same collision domain



Single collision domain

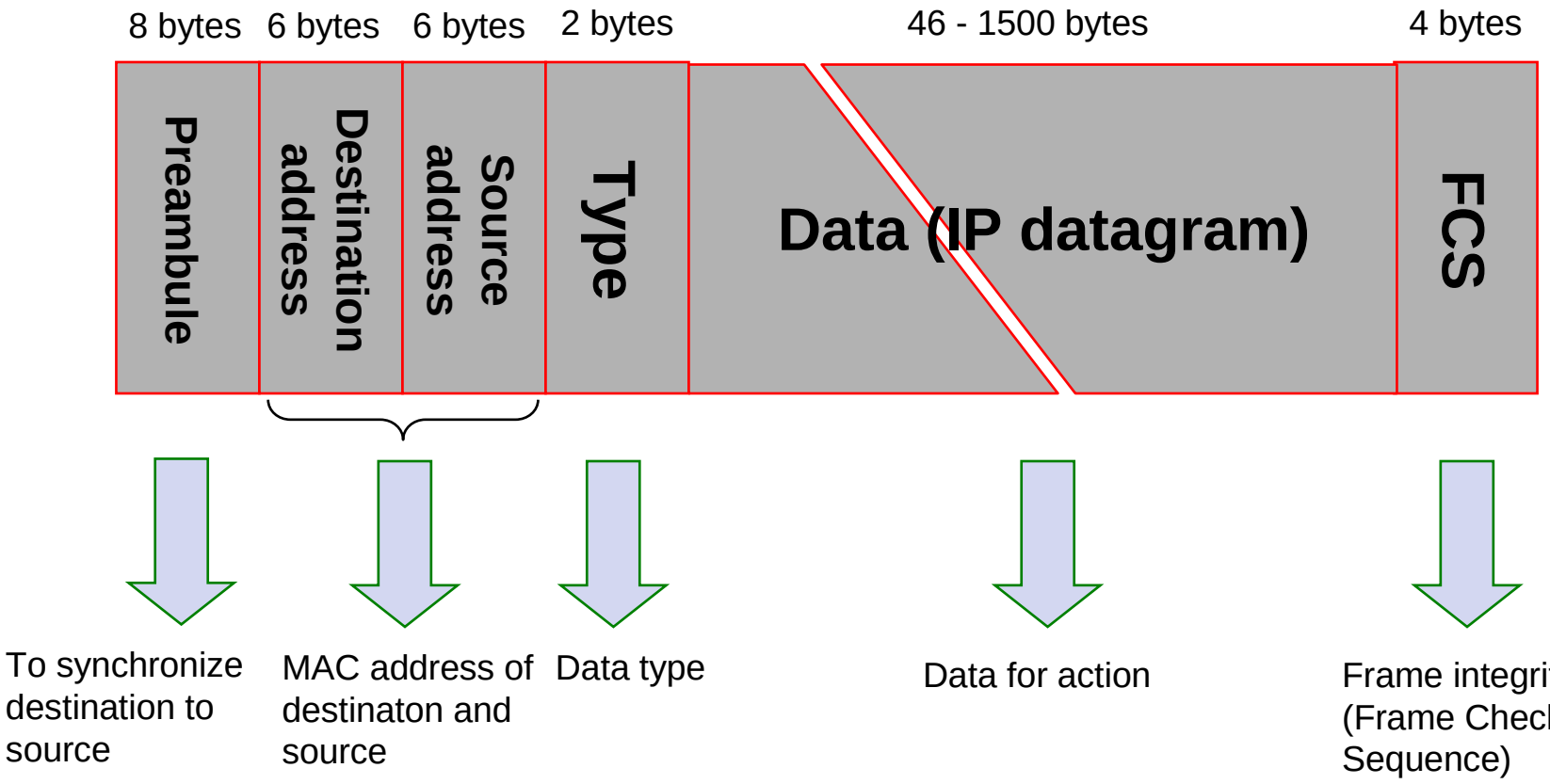
- Since repeaters (or hub) forward all the packets
- All devices are in the same collision domain

Separate collision domains

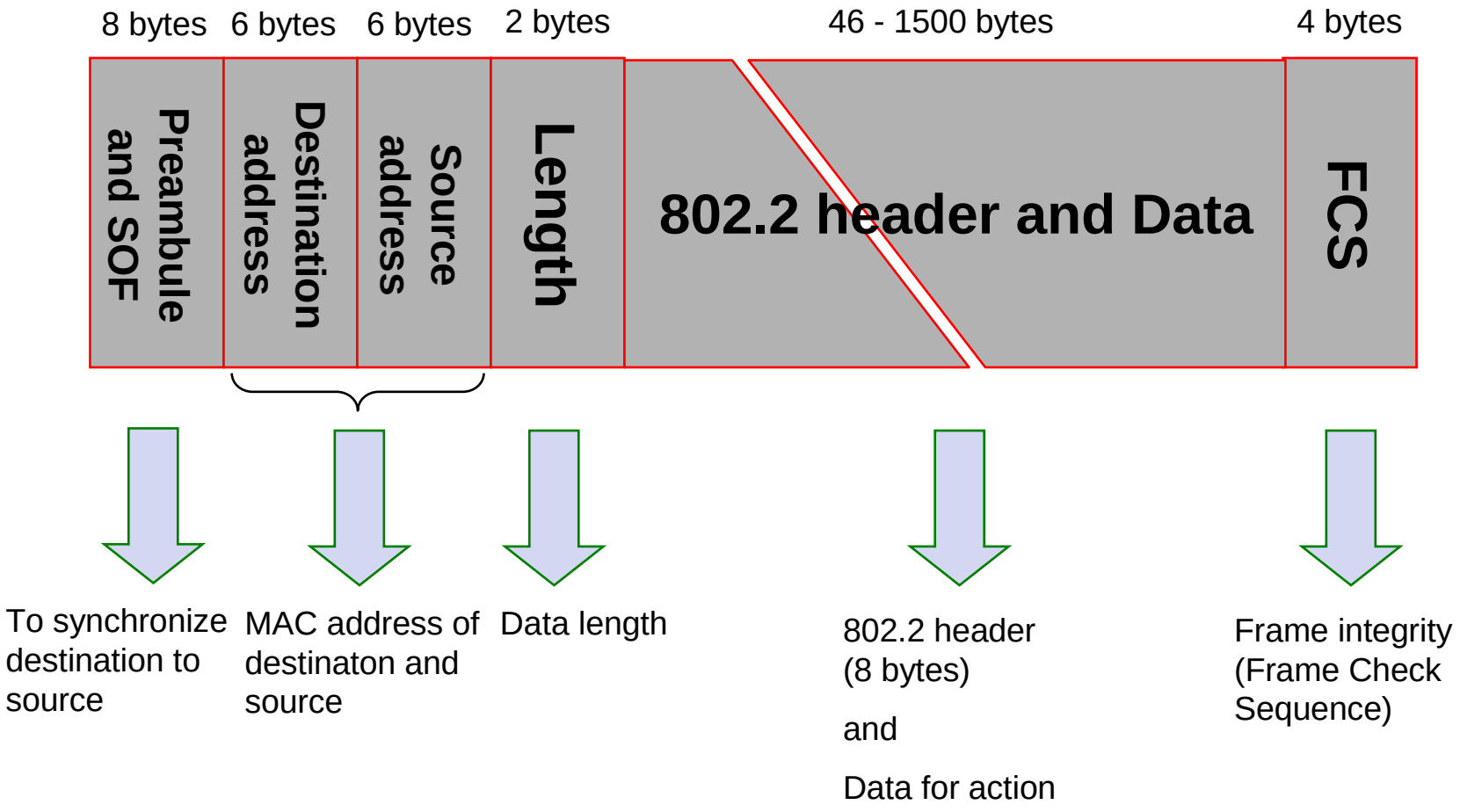


- Collision domain 1 and 2 are separated by a switch (or bridge or router)
- Switch receives and transmits information on separate ports
- Collision signals are not forward

Ethernet II frame



Ethernet IEEE 802.3 frame



MAC addresses

Manufacturer Device number

Manufacturer Group address

- Ethernet frame includes 2 MAC addresses
  - Destination address
  - Source address
- MAC address is unique
- MAC address has 6 bytes (unicast)
  - 3 first bytes are assigned to the manufacturer by IEEE (coherence and uniqueness)
    - Ie : 00.80.F4 for Telemecanique and 00.00.54 for Modicon
  - 3 next bytes indicate the device number
- Multicasting address
  - First bit of 3 last bytes = 1
  - Rest of bits = group address
- Broadcasting address : FF.FF.FF.FF.FF.FF

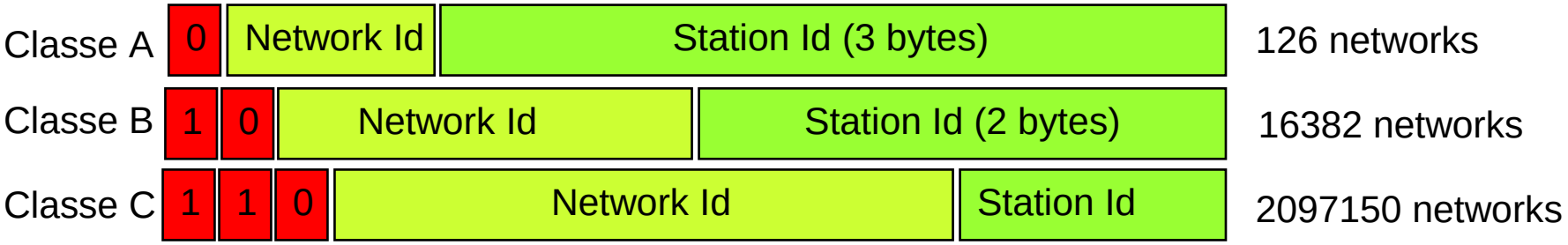
Internet Layer

IP protocol

- Manages the packets routing
  - Determine the next transit node depending on destination IP address
    - Direct routing if destination is on the same network
    - Indirect routing is on a different network (via a router)
- Choice of next node is depending
  - On the transmission delay
  - Flow rate
  - Security of transmission required
- Manages the formatting of frames (datagram)
  - Fragmentation / de-fragmentation of messages

IP address

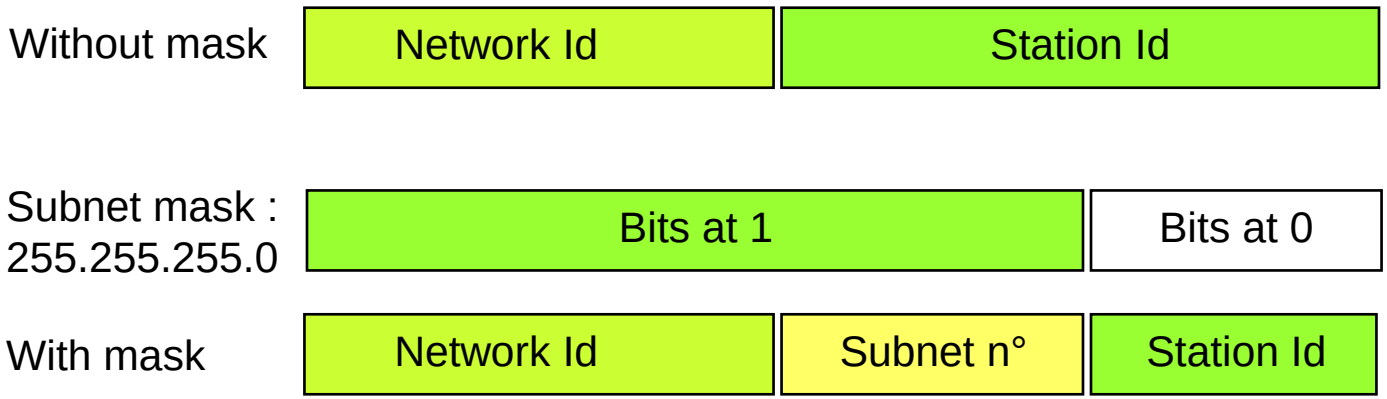
- Each device on Internet or Intranet has a unique IP address coded on 4 bytes, which identify the network and station adresses
- IP addresses are organized in 4 classes : A, B, C and D
  - Classes A – C : used for normal links
  - Class D : use for multicast addresses



Class	Range	Min Submask
A	0.0.0.0 to 127.255.255.255	**255**.128.0.0
B	128.0.0.0 to 191.255.255.255	**255.255**.128.0
C	192.0.0.0 to 223.255.255.255	**255.255.255**.128
D	224.0.0.0 to 239.255.255.255	/

Subnetwork masking

- Allows to break down the station Id into
  Subnetwork number and Station Id
- 1 IP network address for several logical sub networks



Example with subnetwork mask

- AND operation between Destination address and Subnetwork mask
- Result is compared with Source address
  - Equal : the destination is local (on the same network)
  - Different : the destination is for an other network. The messages are routed to the Default gateway address
- Example with mask 255.255.240.0

Network address	139.158.000.000	
Subnetwork number	000.000.048.000	
Station number	000.000.000.010	
IP address	139.158.48.10	10001011.10011110.0011 0000.00001010
Subnetwork mask	255.255.240.0	11111111.11111111.1111 0000.00000000
Result		**10001011.10011110.0011**0000.00000000

Transport Layer

TCP protocol

- Manages opening and closing of TCP connection
  - Client / server TCP connection via a TCP port
  - TCP / IP socket feature
- Manages data (packets) segmentation
  - TCP segment
- Manages flow control
  - Packet sending
  - Acknowledgement
- Guarantee data integrity
  - Segment checksum calculation

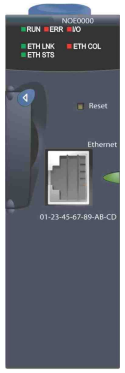
Ports and sockets

- TCP multiplexes multiple connections to a single host using sockets and ports (ie at same time you can open several browers and download a FTP file)
- A port number is coded on 16 bits so a computer interface can use 65536 ports
  - Incoming packets know the IP address and the port they are destined for (destination port is a part of the TCP protocol field)
- Some famous ports
  - FTP uses port 21 (for control) and 20 (for data)
  - SMTP (Simple Mail Transfer Protocol) uses port 25
  - BootP server uses port 67
  - HTTP uses port 80
  - SNMP uses 161
  - Modbus TCP messaging uses port 502
- The combination of an IP address and a port number is a unique address named socket

Application Layer : Ethernet services

Ethernet services according to modules

BMX P34 2020 / 2030



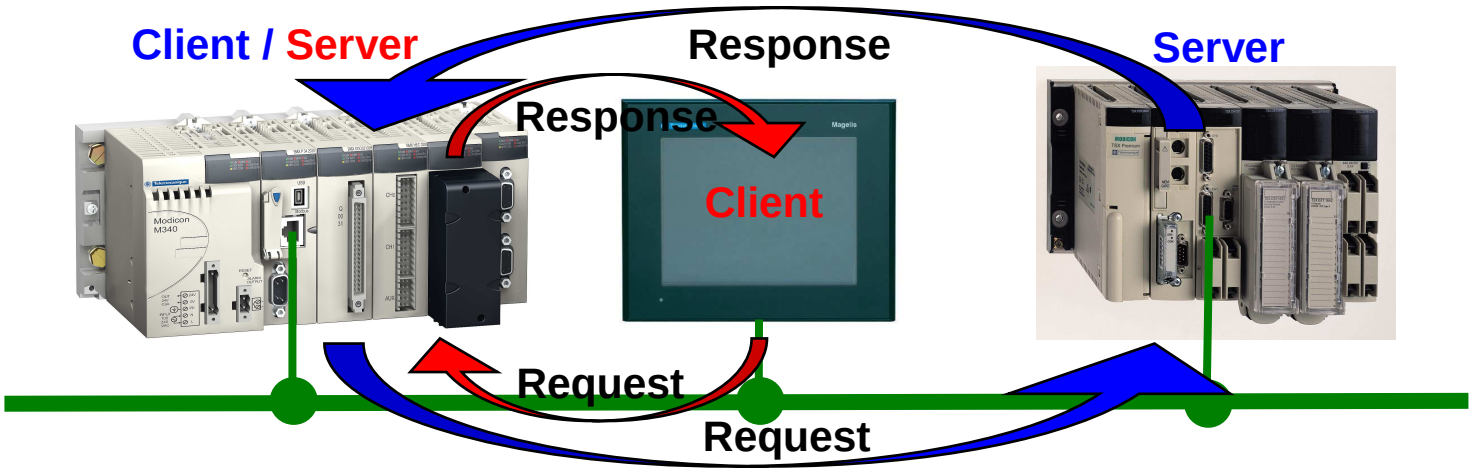
BMX NOE 0100

Service	NOE module	Processors
Modbus TCP messaging	Yes	Yes
BootP / DHCP client	Yes	Yes
DHCP server	Yes	Yes
FDR server	Yes	No
SNMP	Yes	Yes
Global data	Yes	No
I/O scanning	Yes	No
Software loading via FTP (firmware)	Yes	Yes
Embedded http server	Yes	Yes
Diagnostic from Web pages	Yes	Yes
User-customizable Web pages	Yes (*)	No

(*) with memory card installed (Class C server)

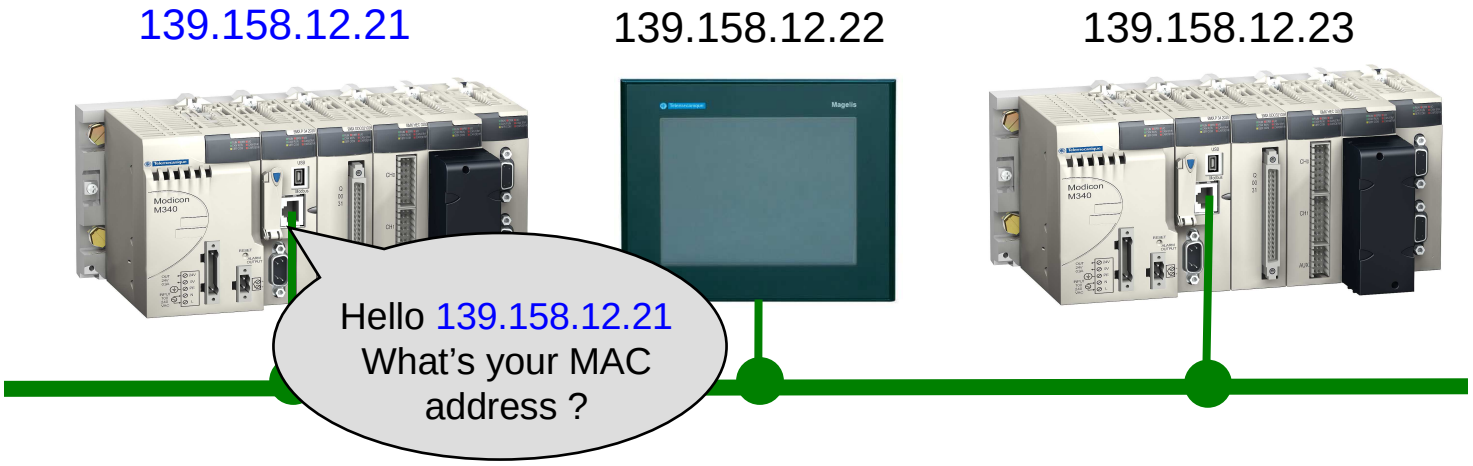
Modbus TCP messaging

- Port 502 is reserved for Modbus TCP messaging
- Modbus messaging can be used to exchange automation data on both Ethernet TCP/IP and Internet as well as other application data (file, web pages, e-mail, …)
- Port 502 can communicate in client mode or server mode
  - In server mode port 502 messaging can process up to 8 requests and responses (Read bits, Write words, …) / PLC cycle
  - In client mode port 502 messaging can process up to 16 requests and responses / PLC cycle



ARP and RARP

- ARP protocol is used to make correspondance between the IP addresses an the associated physical addresses (MAC address)
- The correspondance table is saved on cache memory
- When a Ethernet module is power on it broadcasts it's IP address to verify that any other module responds (the IP address is unique)



ARP : Address Resolution Protocol / RARP : Reverse Address Resolution Protocol

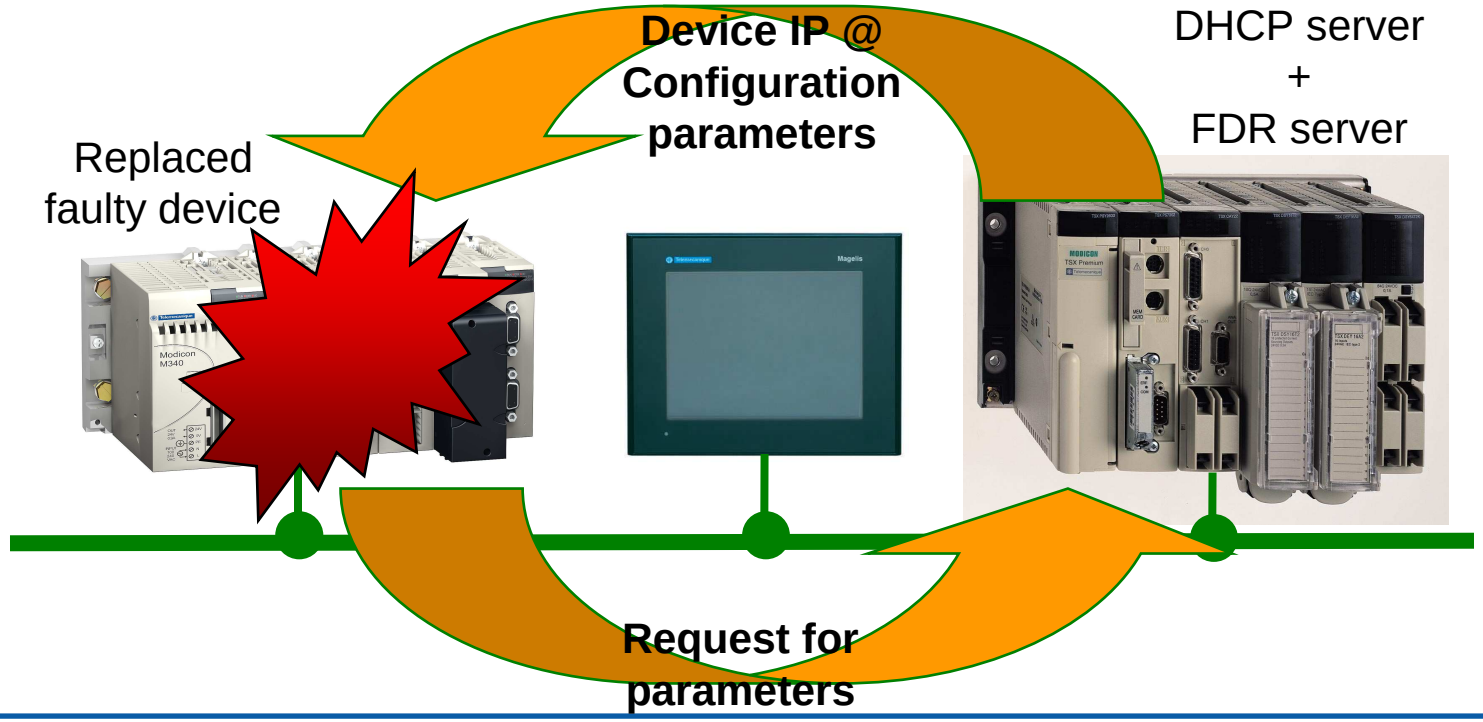
BootP / DHCP service

- BootP or DHCP service allows a device to get its IP address from an address server
- NOE module or Ethernet processors can be configured as a BootP client or a DHCP server.
- DHCP server also responds to a BootP request

BootP : Bootstrap Protocol / DHCP : Dynamic Host Configuration Protocol

Faulty Device Replacement service

- FDR service gives IP address and configuration parameters to a remote device
- DHCP server gives IP address from the name given to the station (Device name). FTP/TFTP server saves then recovers configuration parameters to the station
- NOE module is a FDR server

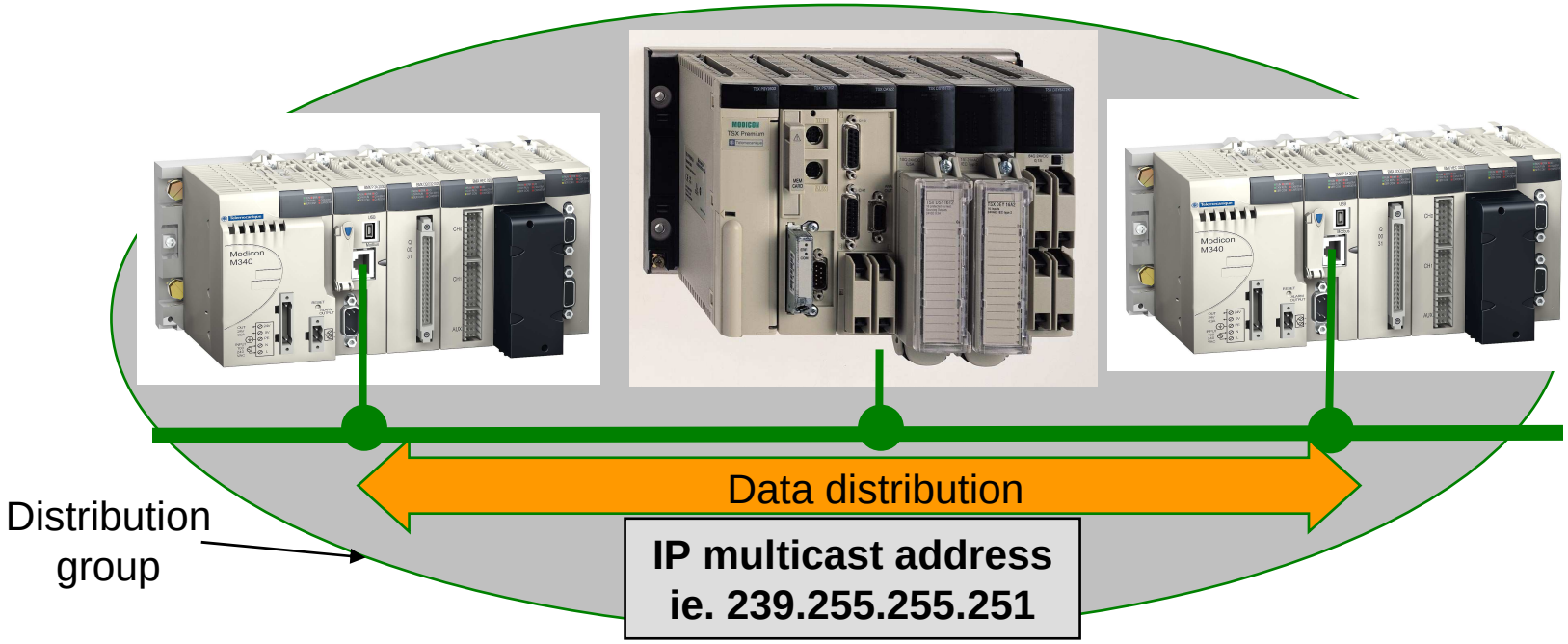


Simple Network Management Protocol

- SNMP protocol allows network administrators to monitor and control all Ethernet architecture components, ensuring rapid diagnostic if a problem occurs
  - Servers, workstations, routers, switches, …
- Management system comprise managers and agents
  - Manager send requests to agents to supervise a part or the entire network (*Get_Request, Get_Next_Request, Set_Request*)
  - Agents : each supervised device has one or more software modules named agent that transmit to the manager information on the device (hardware information, configuration parameters, statistics, …)
- Network management protocol uses UDP transport layer
- Each agent contains a MIB database (Management Information Base) which collect all objects exchanged
  - Network manager can read or write information on the MIB
  - 2 levels of MIB : standard MIB II or Schneider private MIB

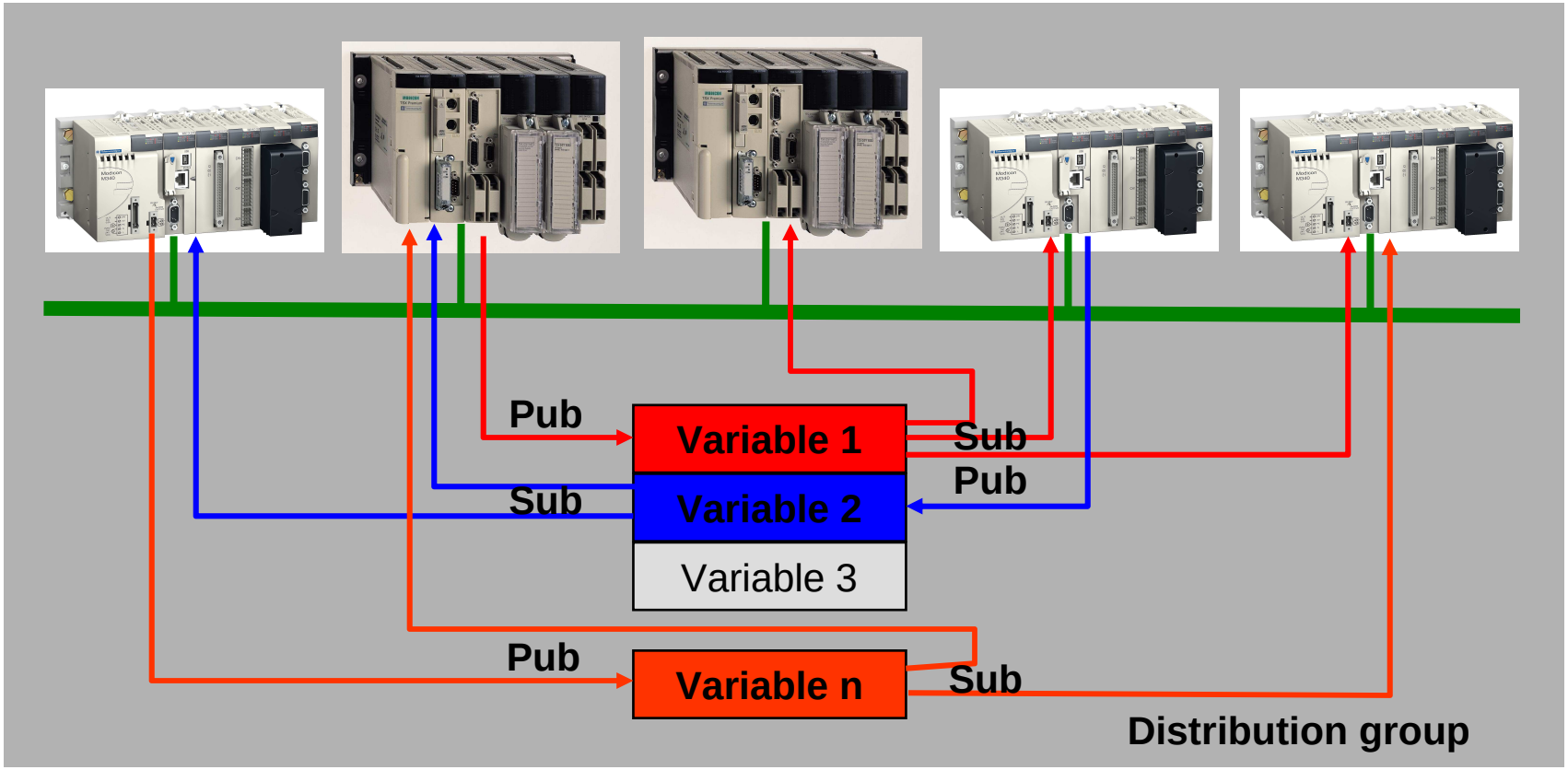
Global data service

- Automatic and real time exchanges between stations
  - Data are exchange in a same distribution group
  - To synchronize remote applications or share variables
- 64 stations can exchange data inside a group
  - Using standard producer / consumer mechanisms to optimize performance and maintain a minimum network load



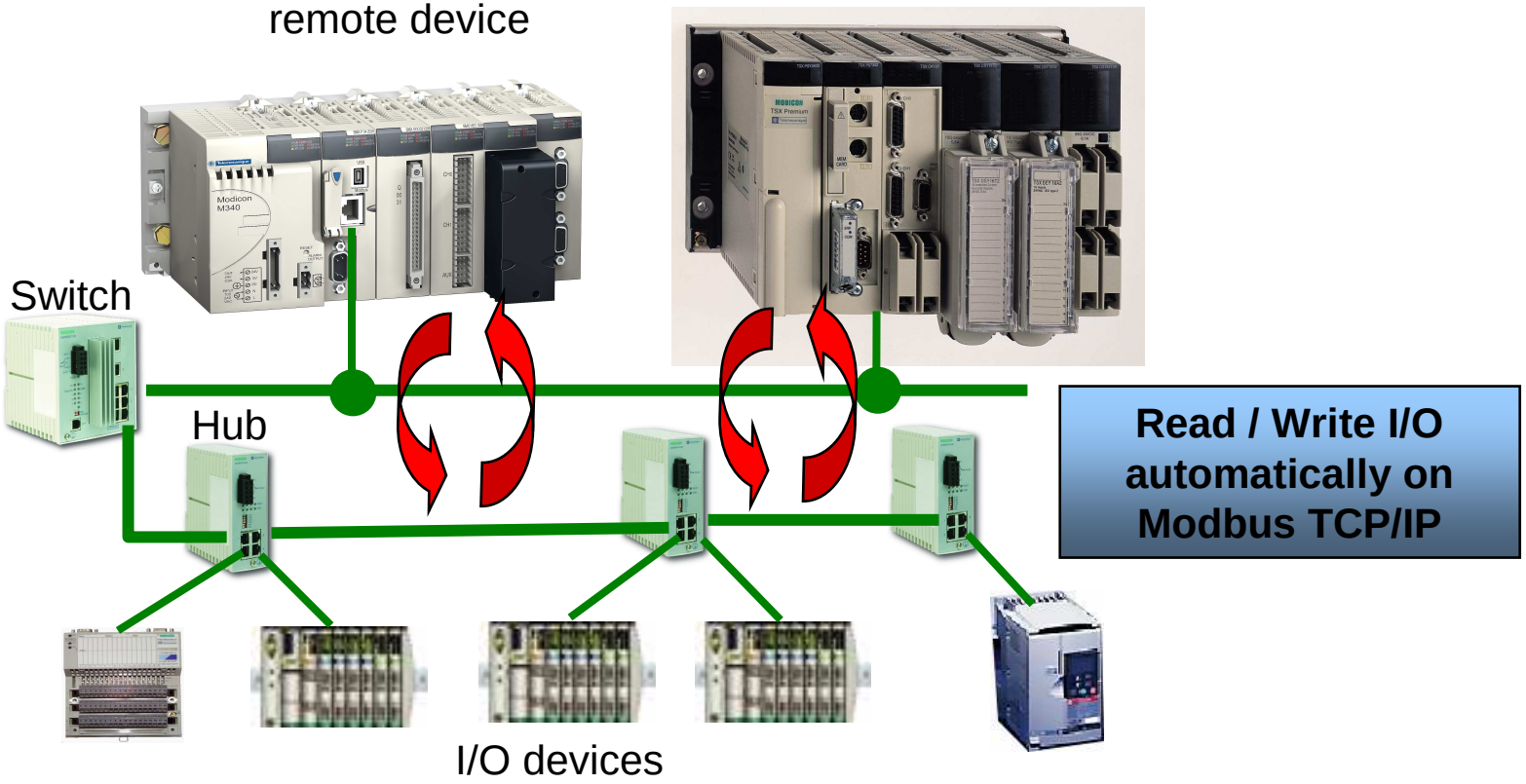
Global data characteristics

- Each station can publish 1 variable (up to 1024 bytes) and subscribe from 1 to 64 variables. A Health bit (status bit) indicates the validity of each subscription
- Publish / subscribe protocol on UDP/IP is used for data distribution



I/O scanning service

- Automatic and periodic read/write of remote Inputs/Outputs without programming
  - Read zone groups the values of remote inputs
  - Write zone groups the values of remote outputs
  - Scanning period is independant of PLC cycle and specific to each remote device

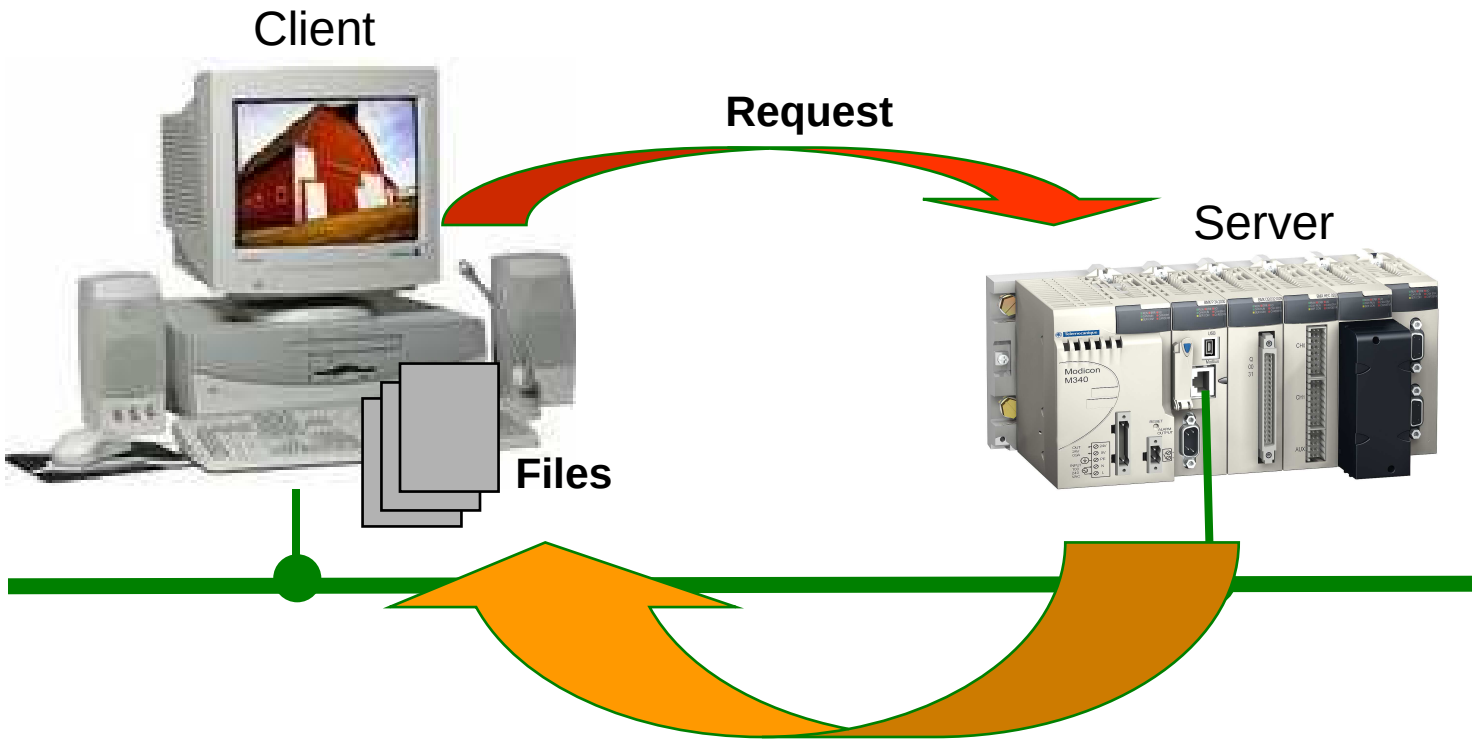


I/O scanning characteristics

- Scanning is performed only when PLC is in Run mode
- Manages TCP/IP connections with each remote device (one connection per scanned device)
- Scans inputs/outputs of the device using Modbus read/write requests on the TCP/IP profile
- Update the read and write zone in the application memory
- Refreshes the status bits for each remote device
- Applies preconfigured fallback values on a communication default

File loading via FTP protocol

- Protocol that enables exchange of files between 2 devices
- FTP works on a client / server principle

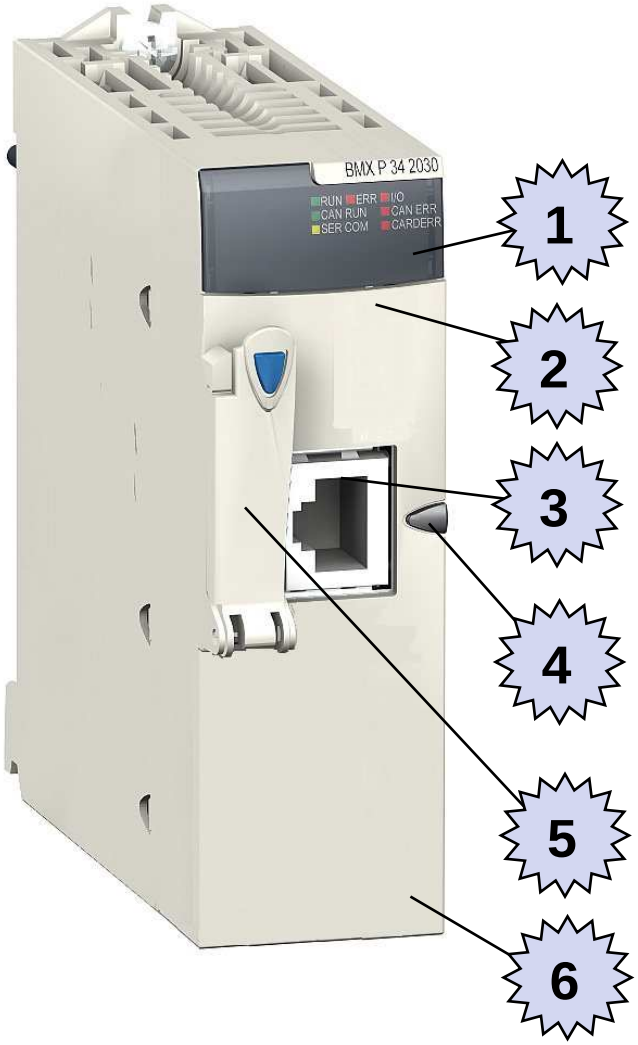


Hardware implementation

Processors with an integrated Ethernet port

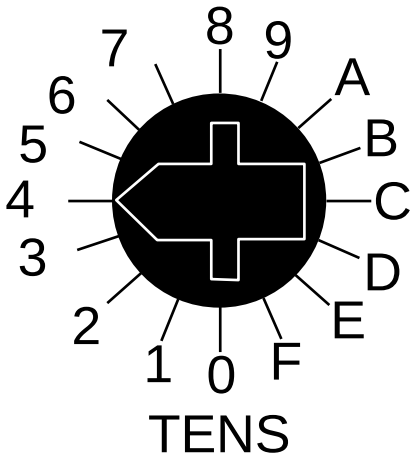
- Modules BMX P34 2020 / 2030
- Display panel (1)
- MAC address (2)
- Ethernet port (3)
- Green color location ring (4)
- SD memory card slot (5)
  - Store Schneider Web pages (Class B server)
- Rotary switches (on the back of the module)

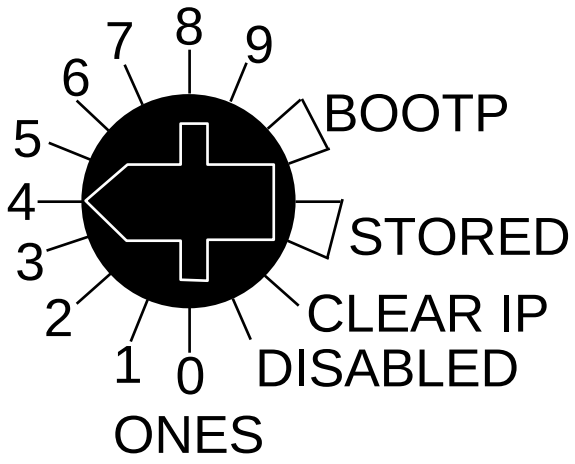
Module NOE



- Modules BMX NOE 0100
- Display panel (1)
- MAC address (2)
- Ethernet port (3)
- Green color location ring (4)
- SD memory card slot (5)
  - Store Web pages (Schneider and user) and log files (FDR server)
  - Class B server by default (*BMX RWS B008M*)
  - Class C server with *BMX RWS C016M* memory card
- Reset button (6)
- Rotary switches (on the back of the module)

Rotary switches





- 2 rotary switches used to set IP address of device
- CLEAR IP
  - Device uses default IP address based on MAC address (4 last bytes in hexadecimal values are converted in decimal)
  - Example : MAC address 00.00.54.10.2D.12 gives the derived IP address 84.16.45.18
- BOOTP
  - Device gets an IP address from a BootP server
- STORED
  - Device uses application's configured IP address
  - If IP address not configured module use default IP address
- Device name
  - **TENS** (xx = 0 to 15) and **ONES** (y = 0 to 9) digits
  - Uses to define the default device name of the module to obtain IP address from a **DHCP server**
  - BMX_2020_xxy / BMX_2030_xxy / BMX_0100_xxy
- DISABLED
  - Port will not respond to communication

Visual diagnostic of communication line

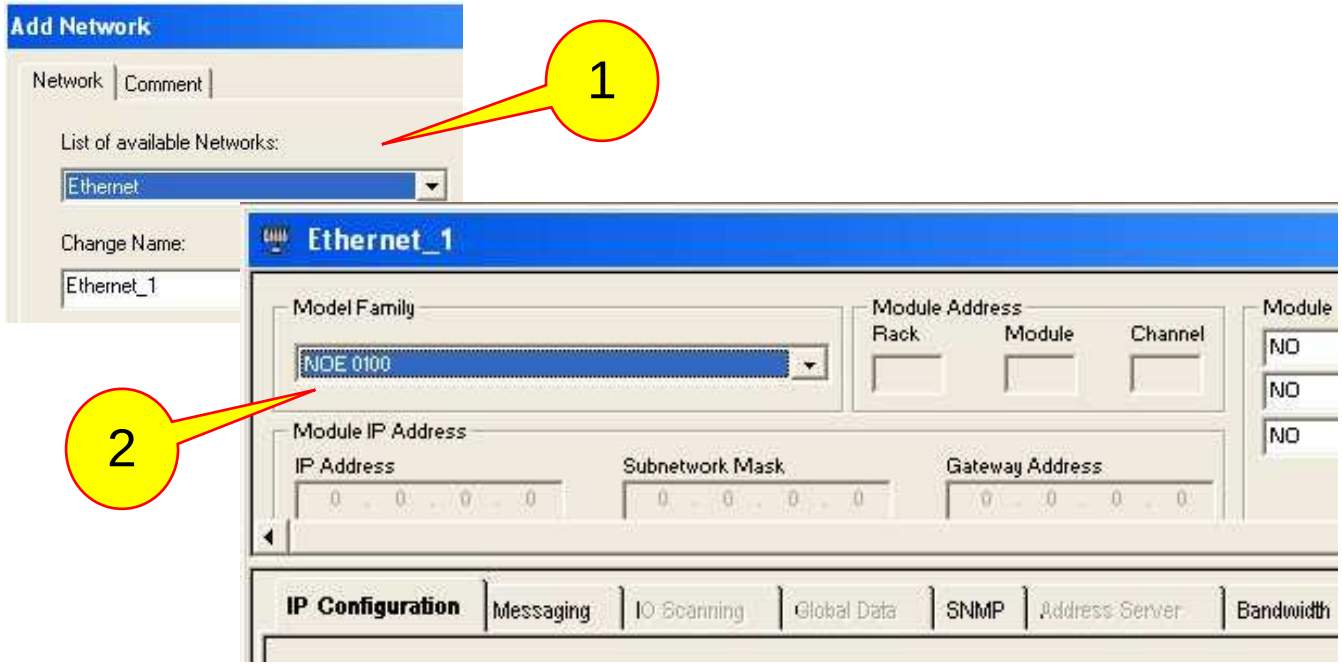
- Colors and flashing patterns of the LEDs indicate the status and operating condition of the communication line

Label	Color	Pattern	Meaning
ETH LNK	Green	ON	Link detected
	Flashing	Flashing	Communication activity
ETH COL	Red	ON	Collision detected
ETH STS	Green	ON	Communication OK
		2 flashes	Invalid MAC address
		3 flashes	Link not connected
		4 flashes	Duplicate IP address
		5 flashes	Waiting for a served IP address
		6 flashes	Safe mode – default IP
		7 flashes	Configuration conflict

Software operating modes

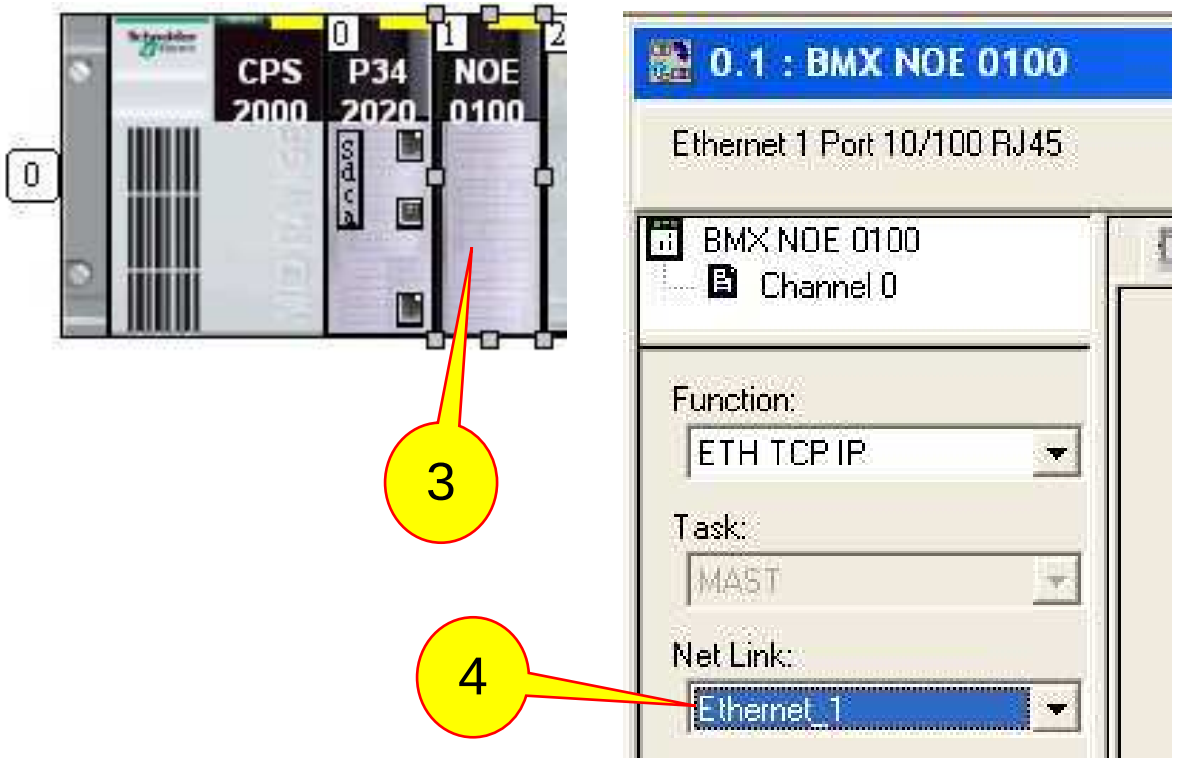
Principle to configure an Ethernet network

- Create the logical network (1)
  - Add a new network
  - Choose Ethernet and define the name of the logical network
- Configure the logical network (2)
  - From the application browser open logical network (ie Ethernet_1)
  - Configure the network : messaging, global data, …(see following slides)

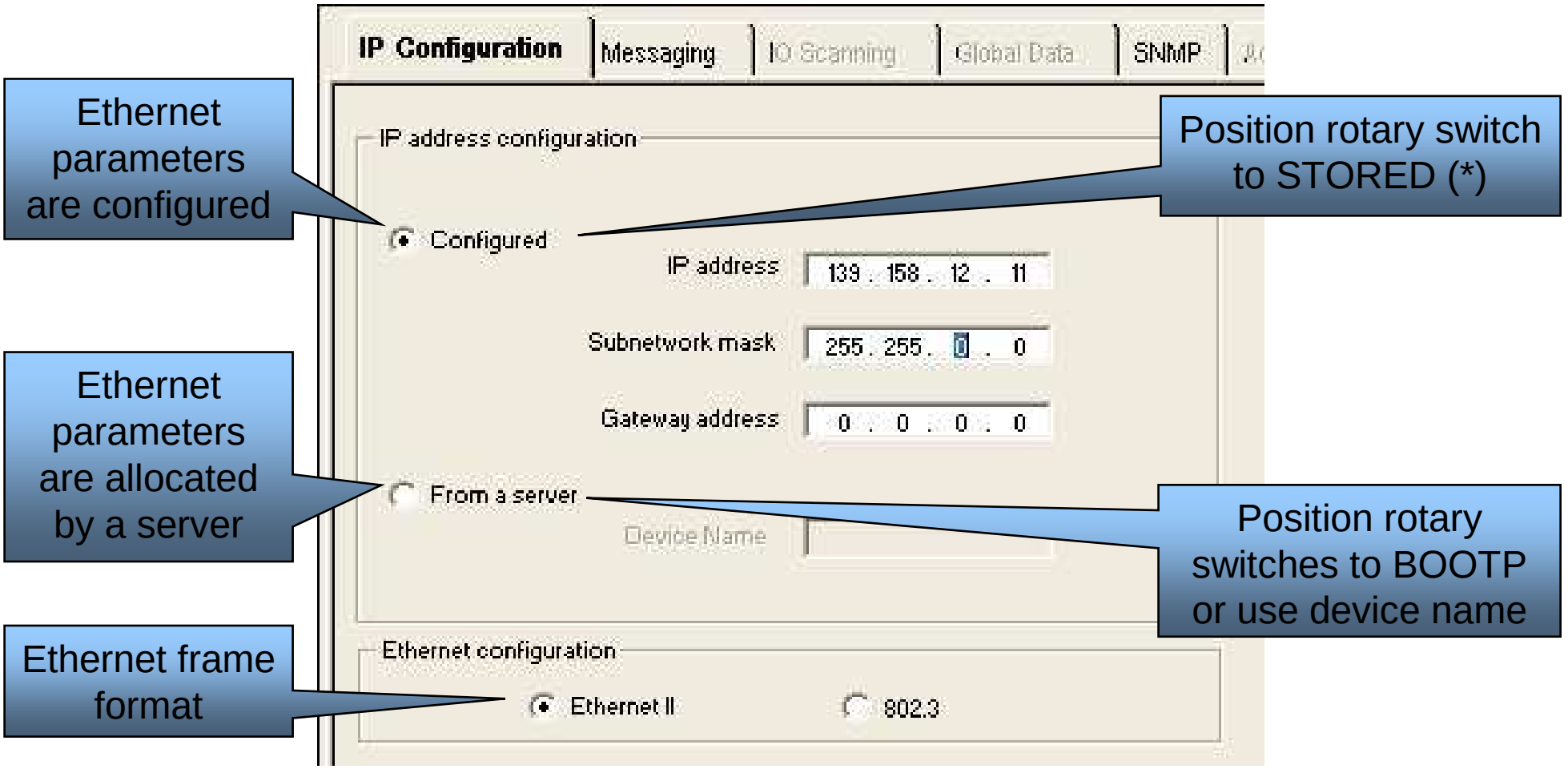


Principle to configure an Ethernet network (cont)

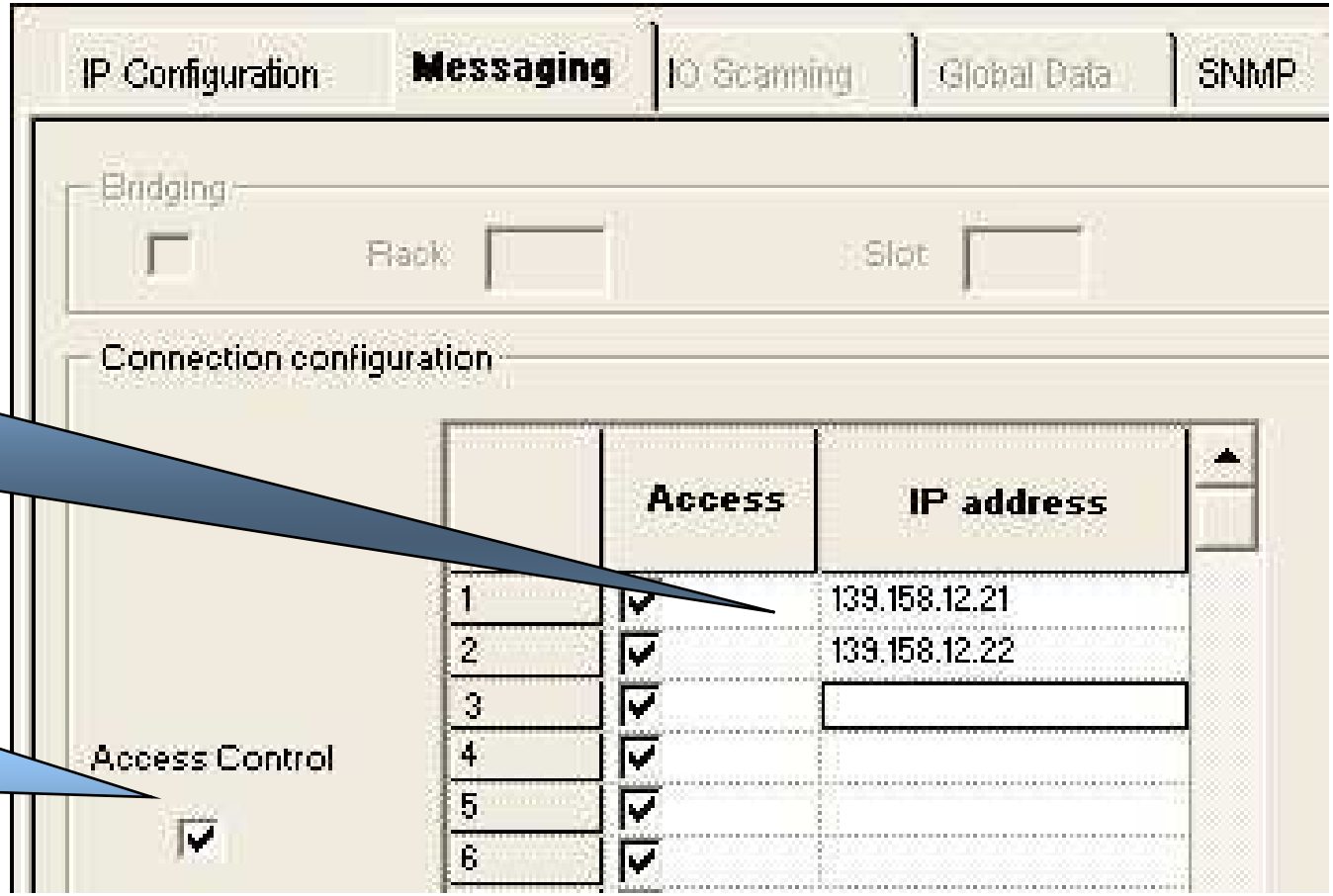
- Define the communication module (3)
  - Processor or NOE module
- Associate the logical network to the communication module (4)



Configuration of IP parameters



Configuration of TCP/IP messaging



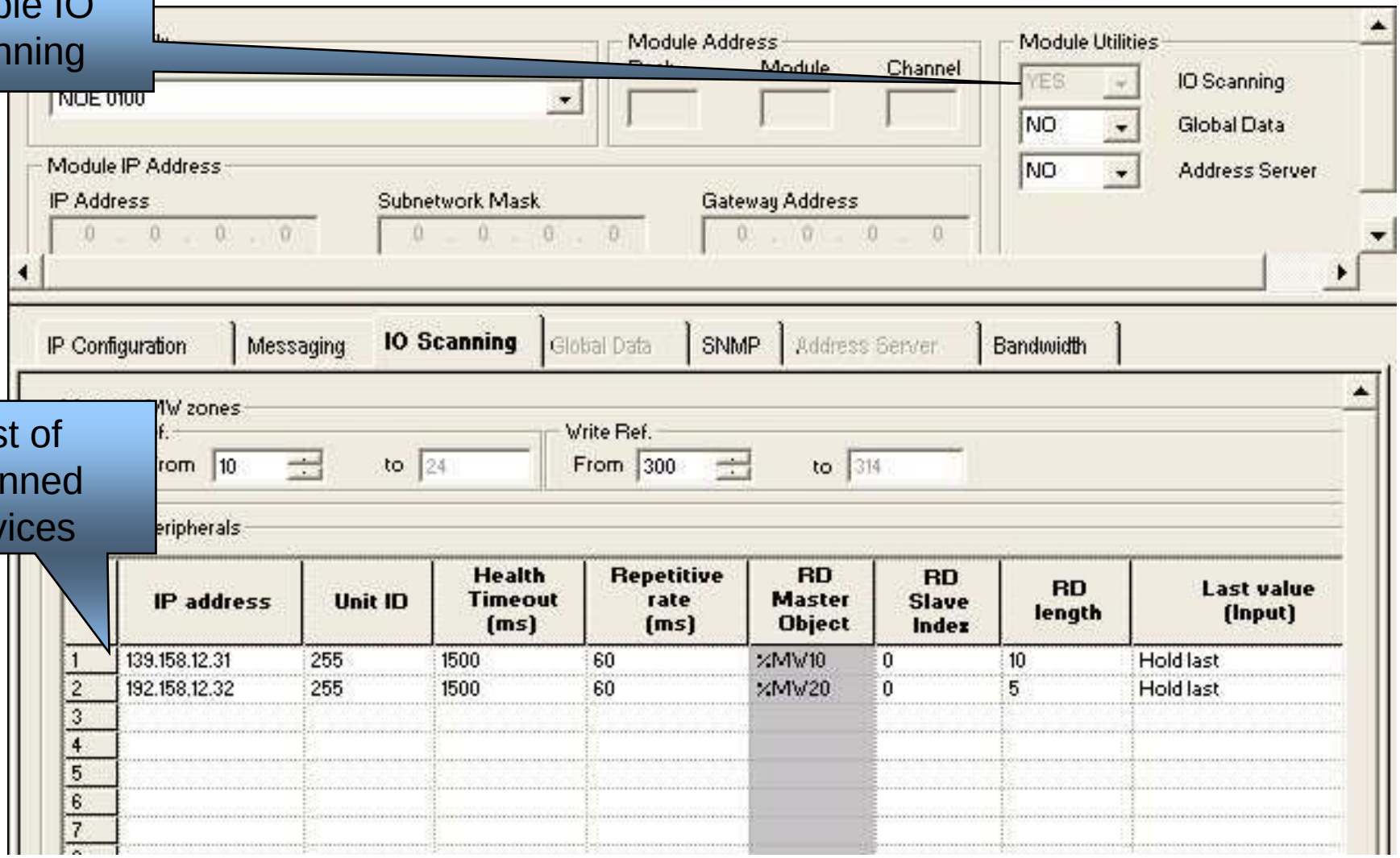
Remote devices which can access to port 502 of the module

Enable access control to the module

Configuration of I/O scanning

Enable IO scanning

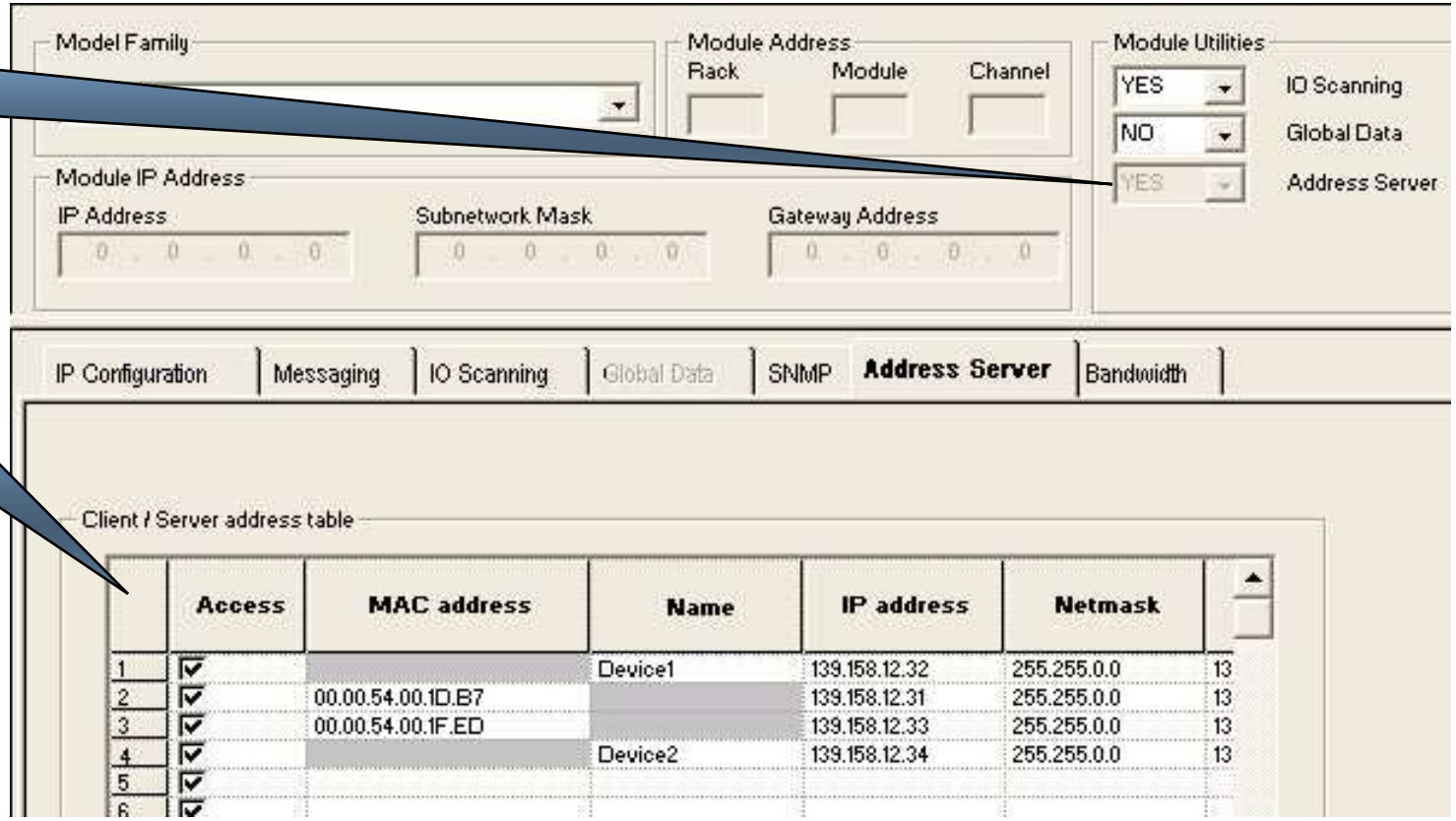
List of scanned devices



Configuration of address server

Enable address server BooP / DHCP

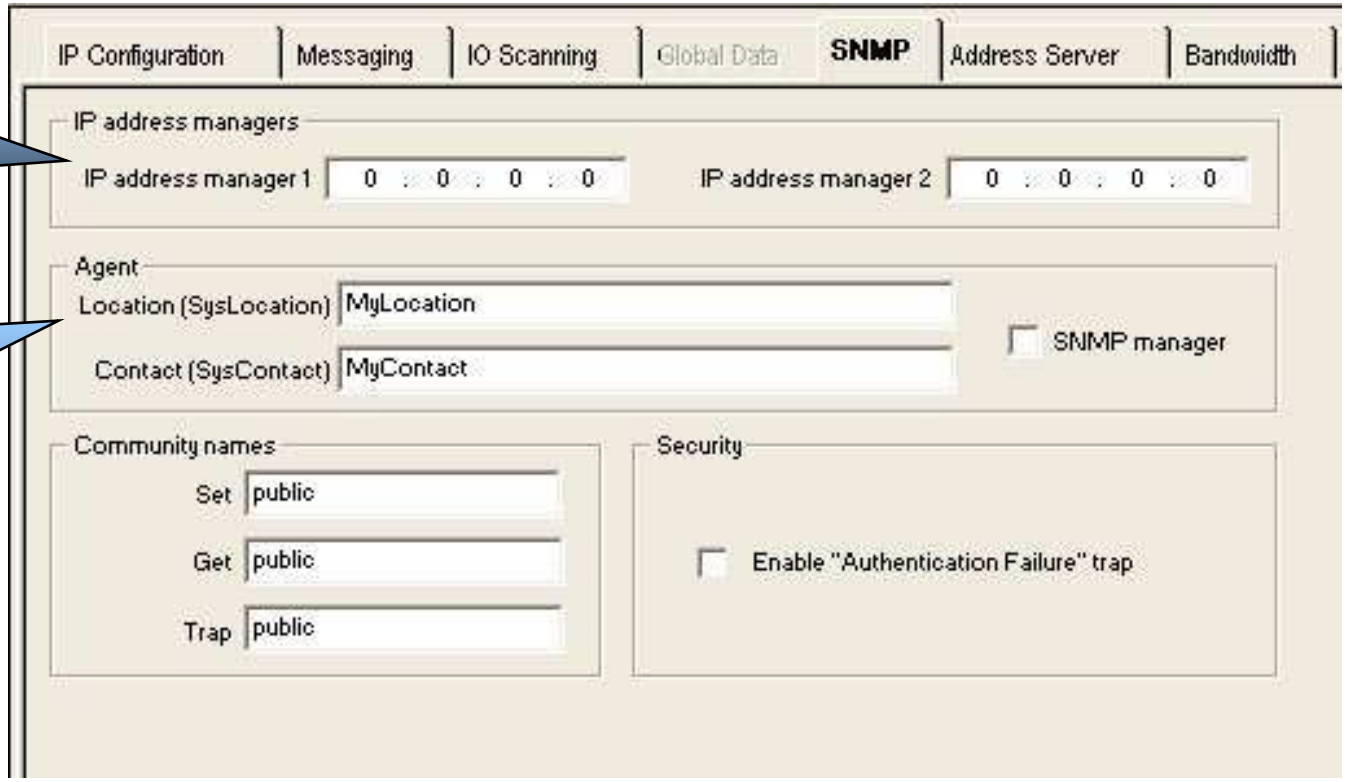
IP parameters of served devices



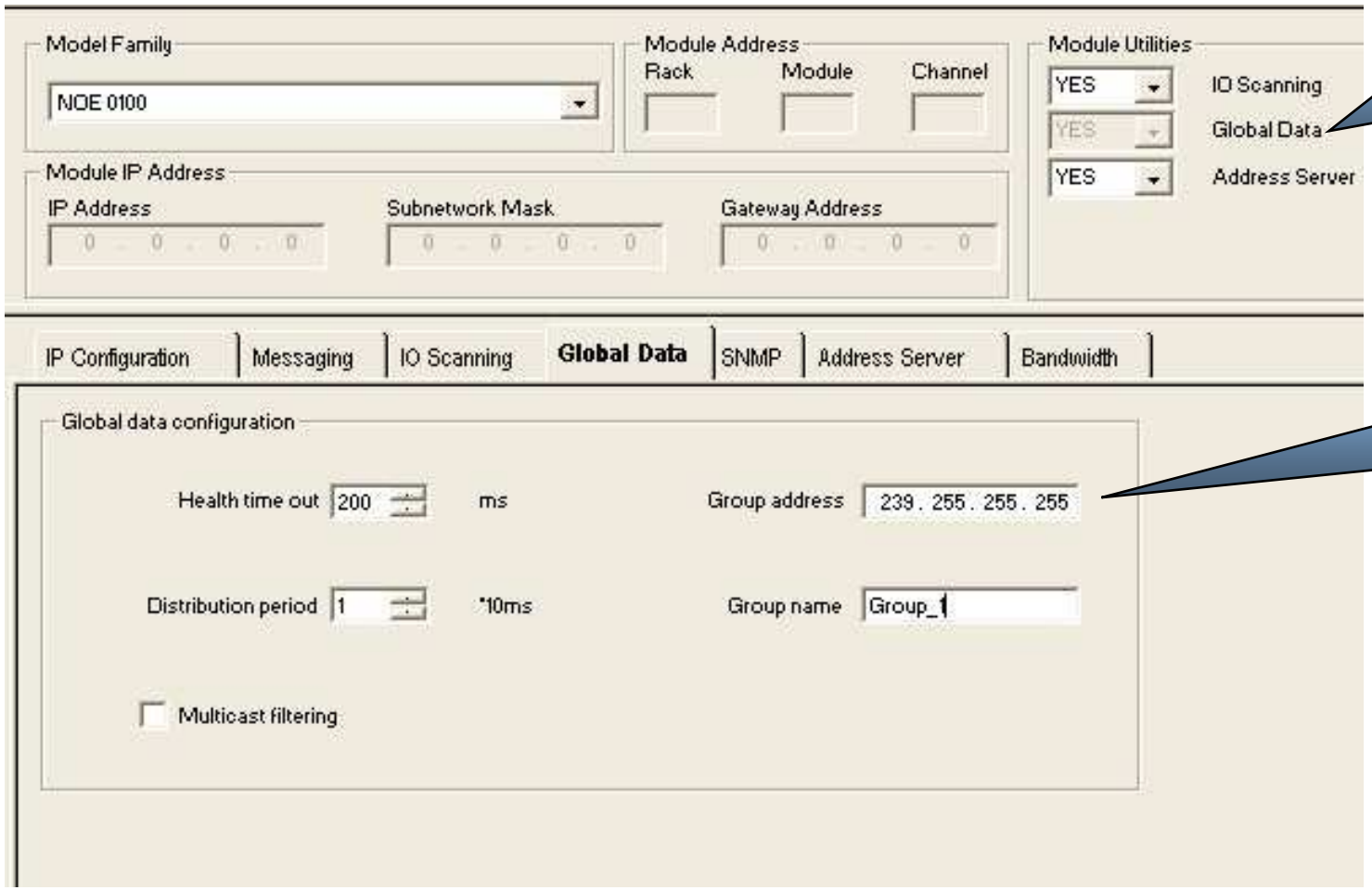
Configuration of SNMP agent

IP address of managers

Agent information



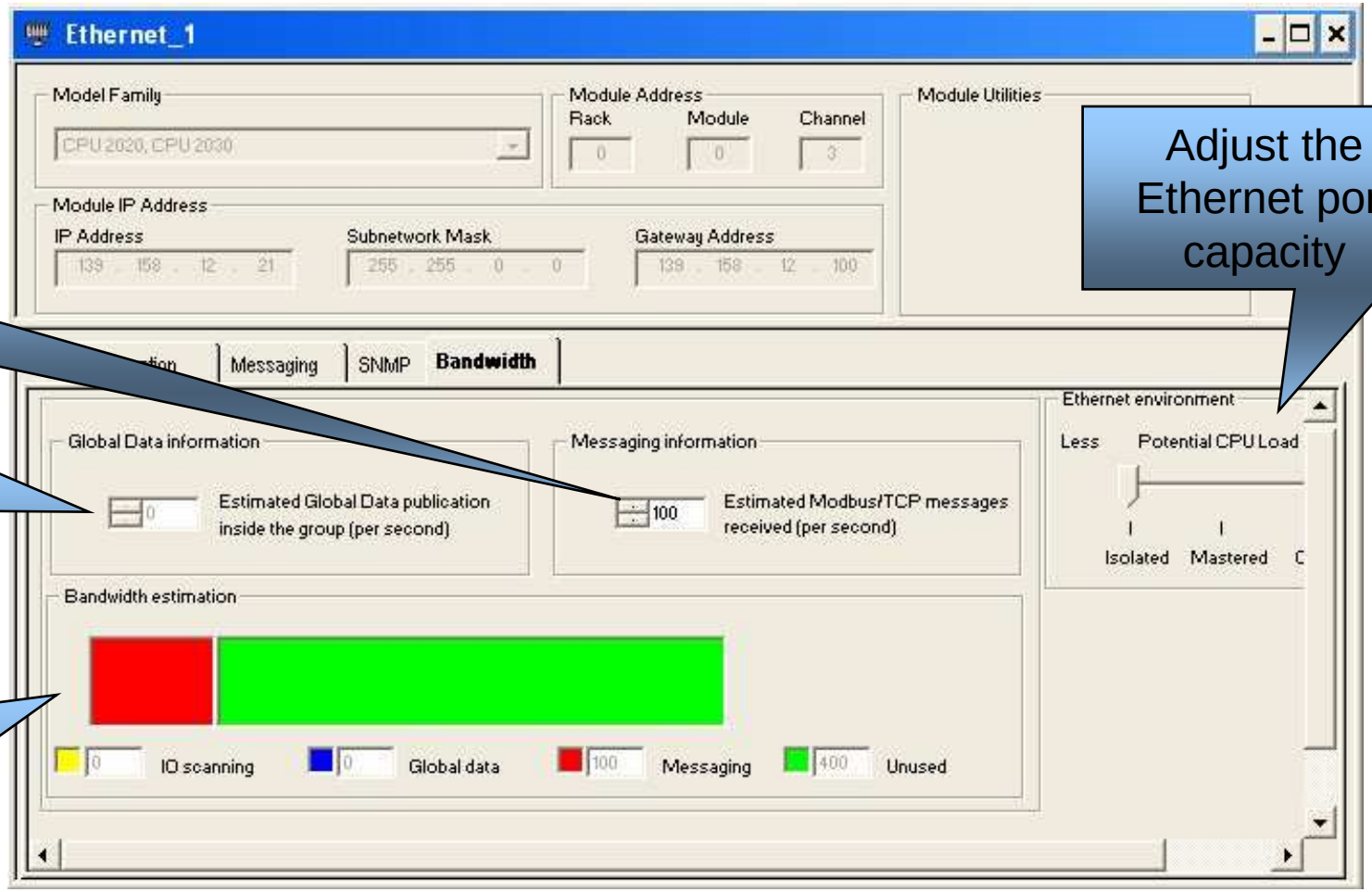
Configuration of Global data



Enable Global data

IP address of distribution group

Bandwith checking



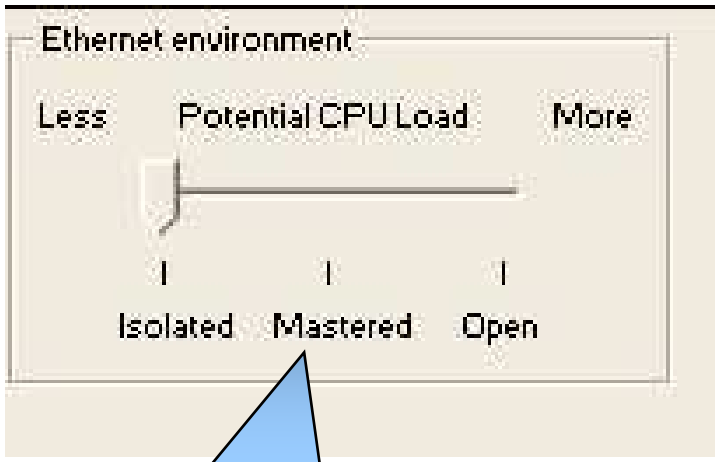
Define number of transactions per second

Define number of publications per second

Theoretical estimation of bandwith

Adjust the Ethernet port capacity

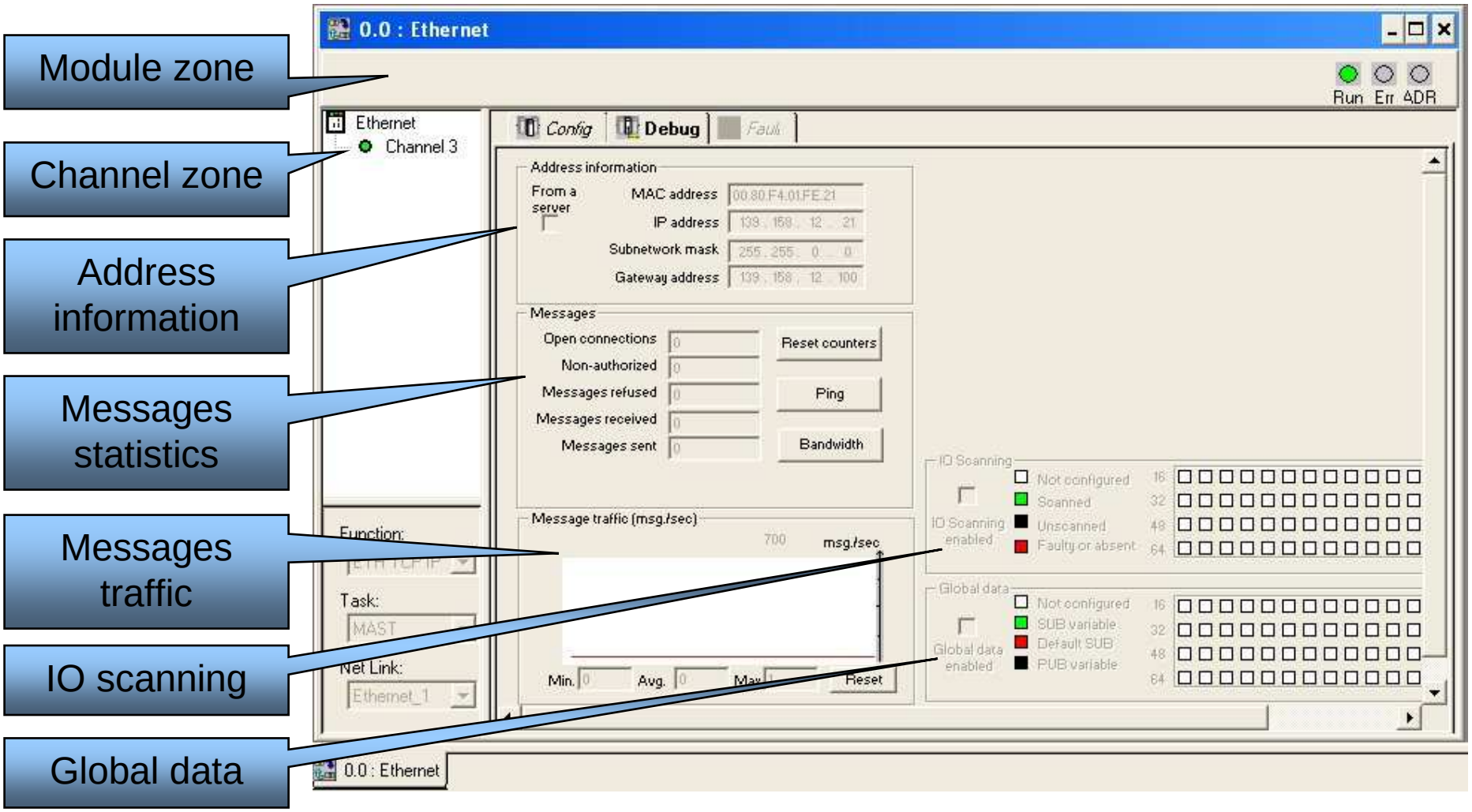
Ethernet port capacity



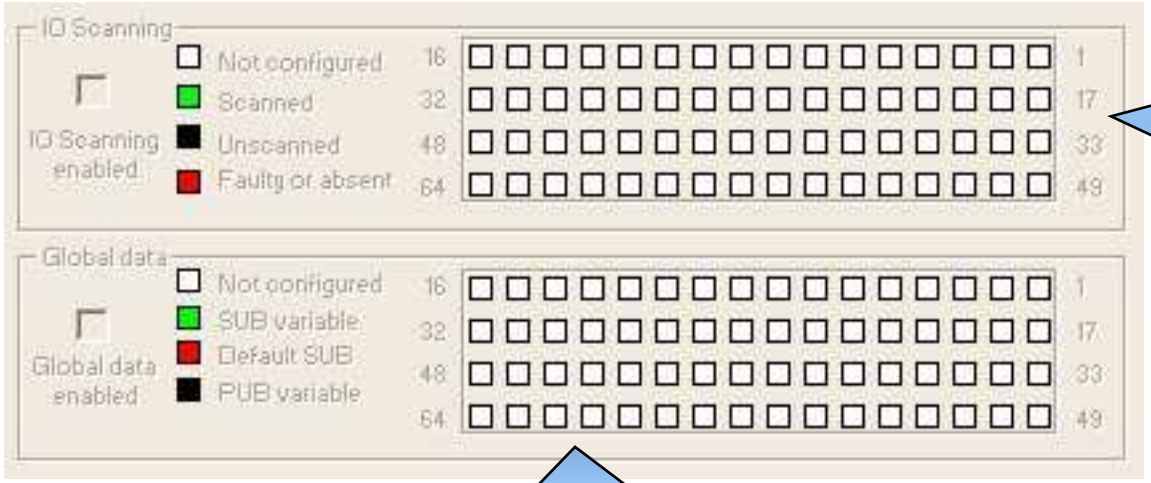
Adjust the Ethernet port capacity of the processor (Isolated by default)

- Performance of Ethernet communication is depending of the number of exchanges
  - Application (messaging Modbus TCP/IP, I/O scanning, Global data, HTTP or FTP requests)
  - Unexpected exchanges
- NOE module can manage 2000 messages/s (incoming + outgoing) but the embedded port of a processor can manage only 500 messages/s with a CPU load lower than 50%
- Depending of your Ethernet environment you can adjust the port capacity of the processor to exchange more than 500 messages/s
  - Isolated network : if the number of messages is lower than 700 per second the CPU load for Ethernet never exceed 50%
  - Mastered network : CPU can absorb 1400 messages per second, but Ethernet can use until 80% of CPU ressources
  - Open network : CPU can absorb 2100 messages per second, but Ethernet can use 95% of CPU ressources
- If the network is disturbed or the number of messages greater than 500 per second, it's recommended to use a BMX NOE module

Module debugging



Debugging IO scanning and global data



If IO scanning function is activated display the status of each configured device : scanned, faulty or absent (1)

If Global data function is activated display the status of the global data variables : SUB (2) or PUB

(1) No Modbus request is sent to the device when Not configured or Unscanned

(2) Default SUB when the subscribed variable is not received in the health timeout limit

Embedded Web server

Web services

- Standard Web services are available on Ethernet processors and NOE communication module
  - Rack display
  - Data editor
  - Ethernet diagnostic pages (Global data, messaging, …)
  - Statistic page

- User Web pages and user files are available on NOE module equipped with a *BMX RWS C016M* memory card (Class C server)

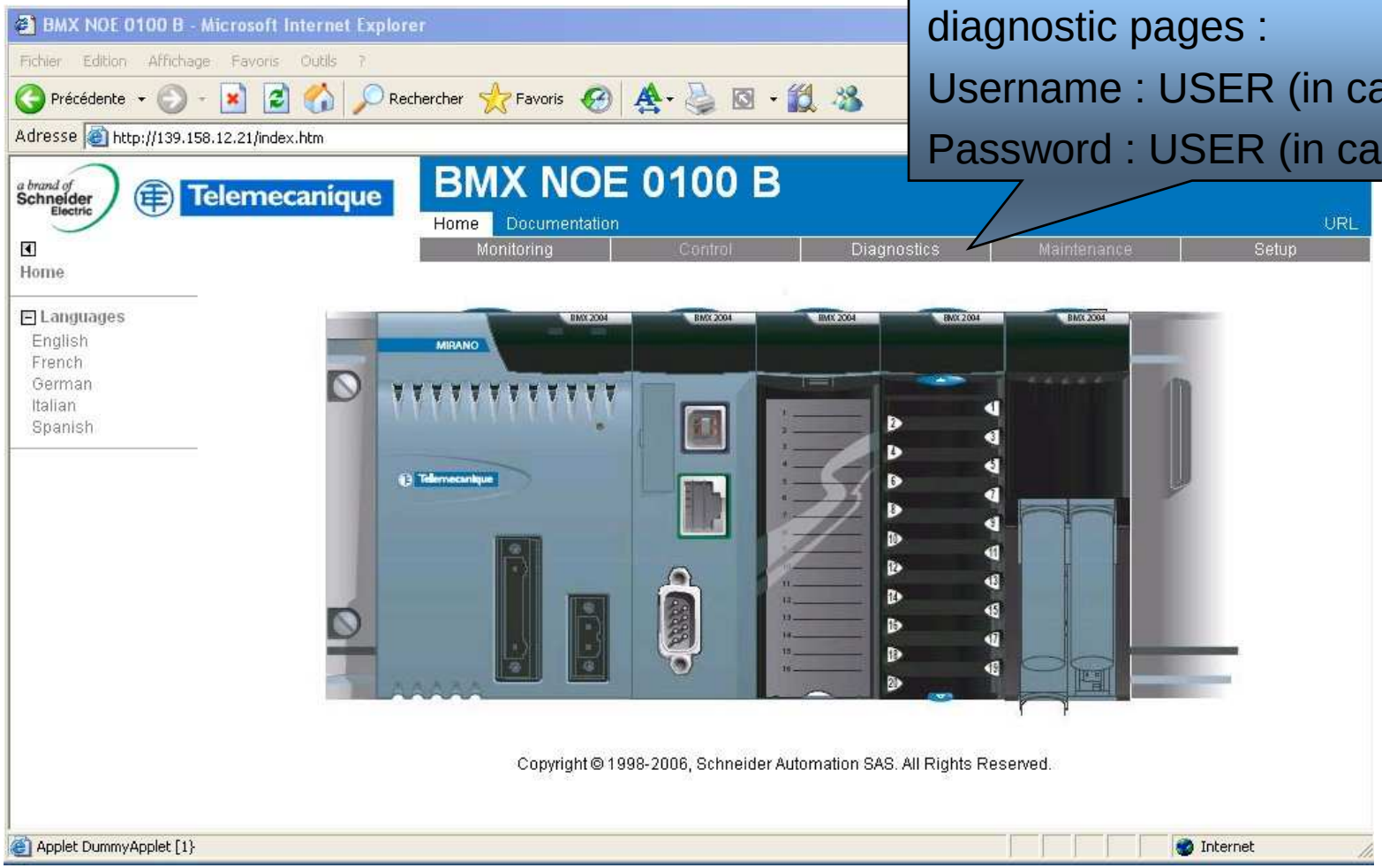
- By default communication NOE module is equipped with a *BMX RWS B008M* memory card that can save user files (Class B server for FDR service)

Web server : home page

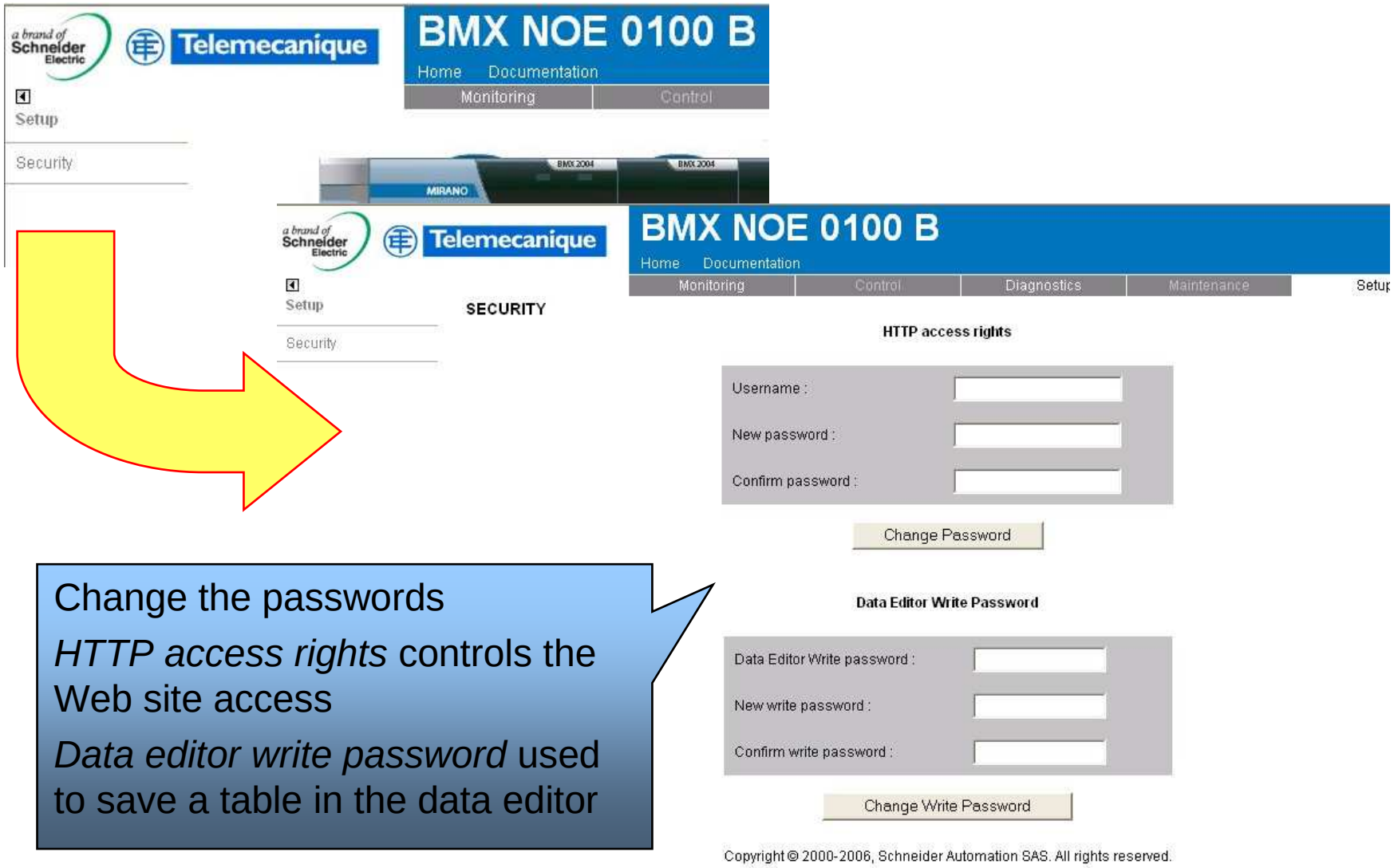
Access to Setup, monitoring or diagnostic pages :

Username : USER (in caps)

Password : USER (in caps)



Setup : Security page

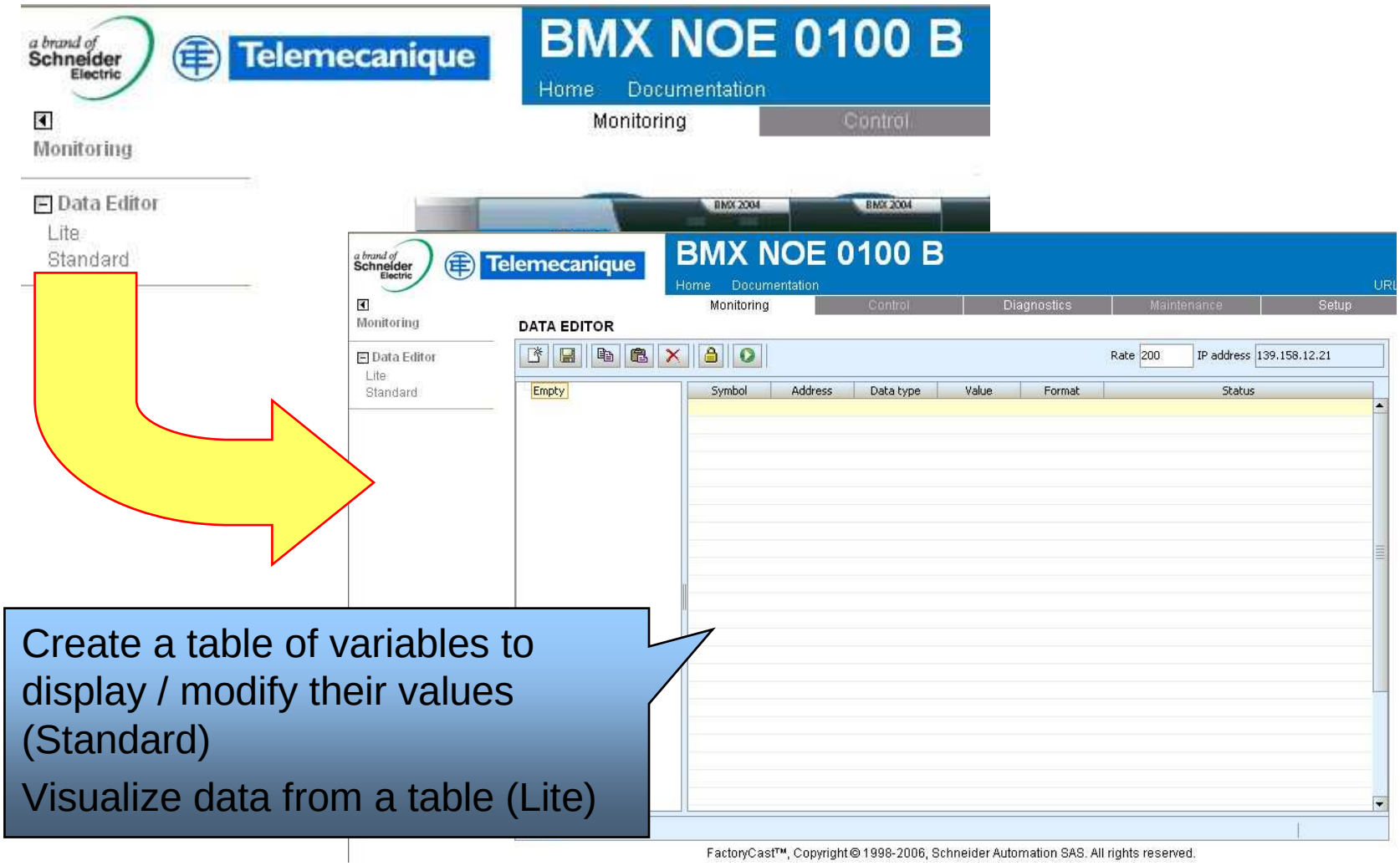


Change the passwords

HTTP access rights controls the Web site access

Data editor write password used to save a table in the data editor

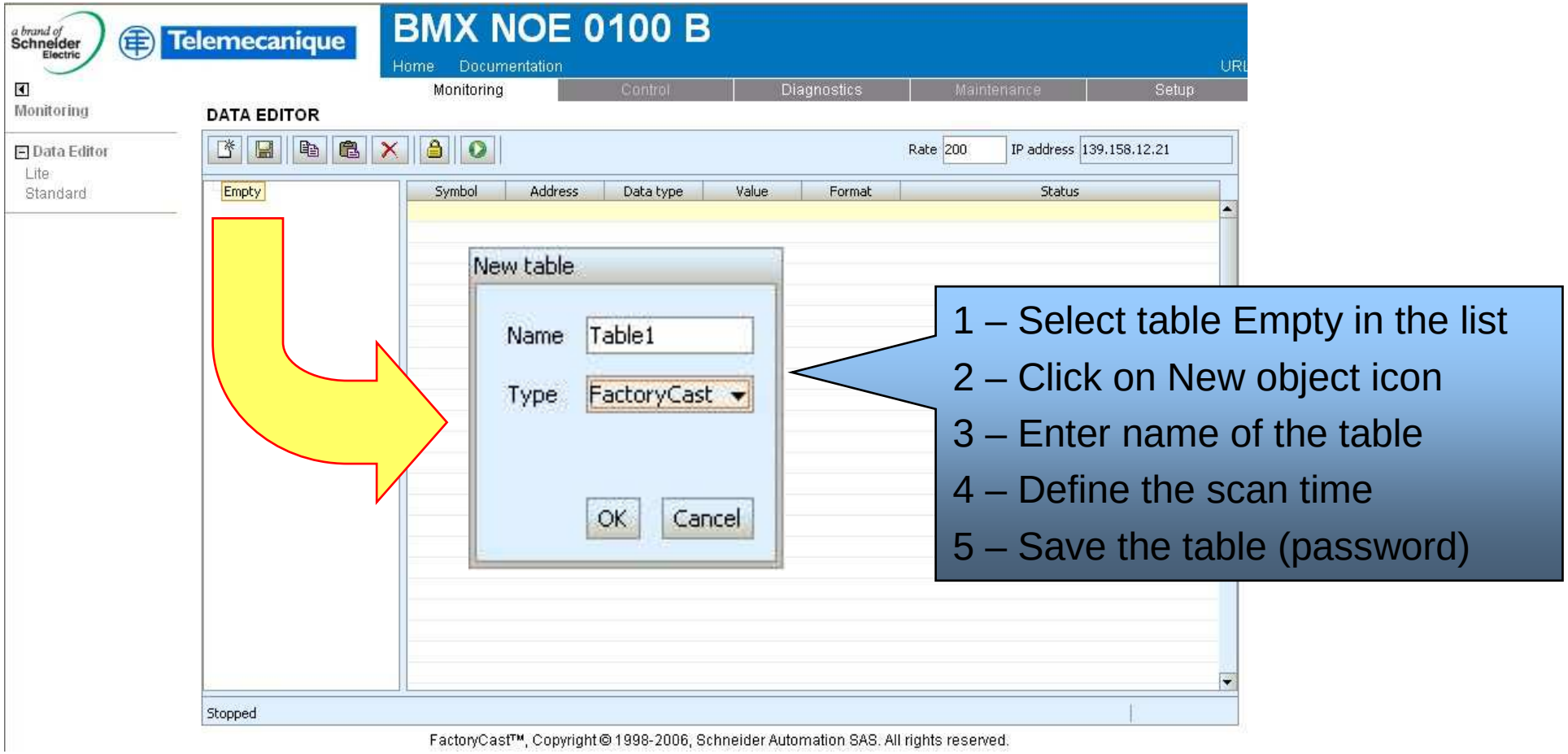
Monitoring : data editor pages



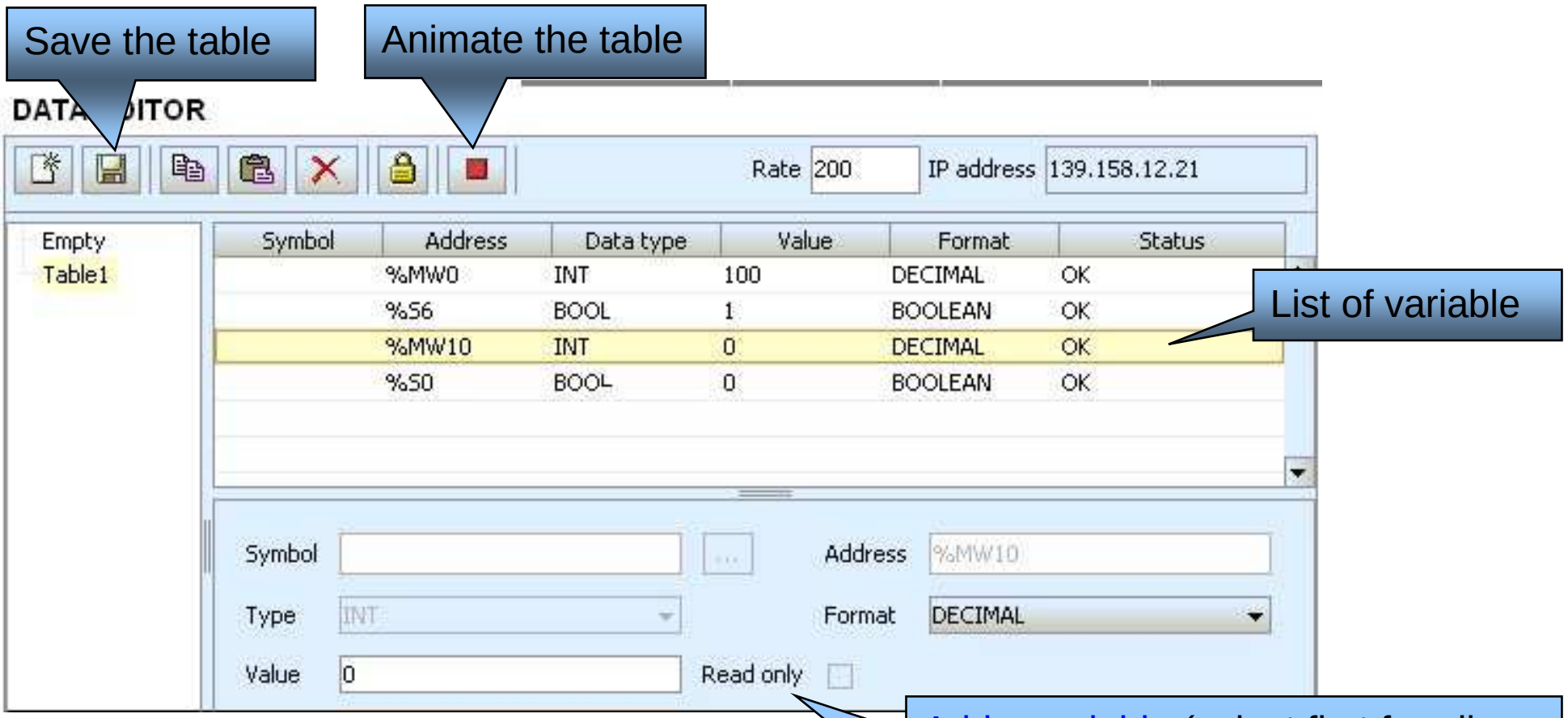
Create a table of variables to display / modify their values (Standard)

Visualize data from a table (Lite)

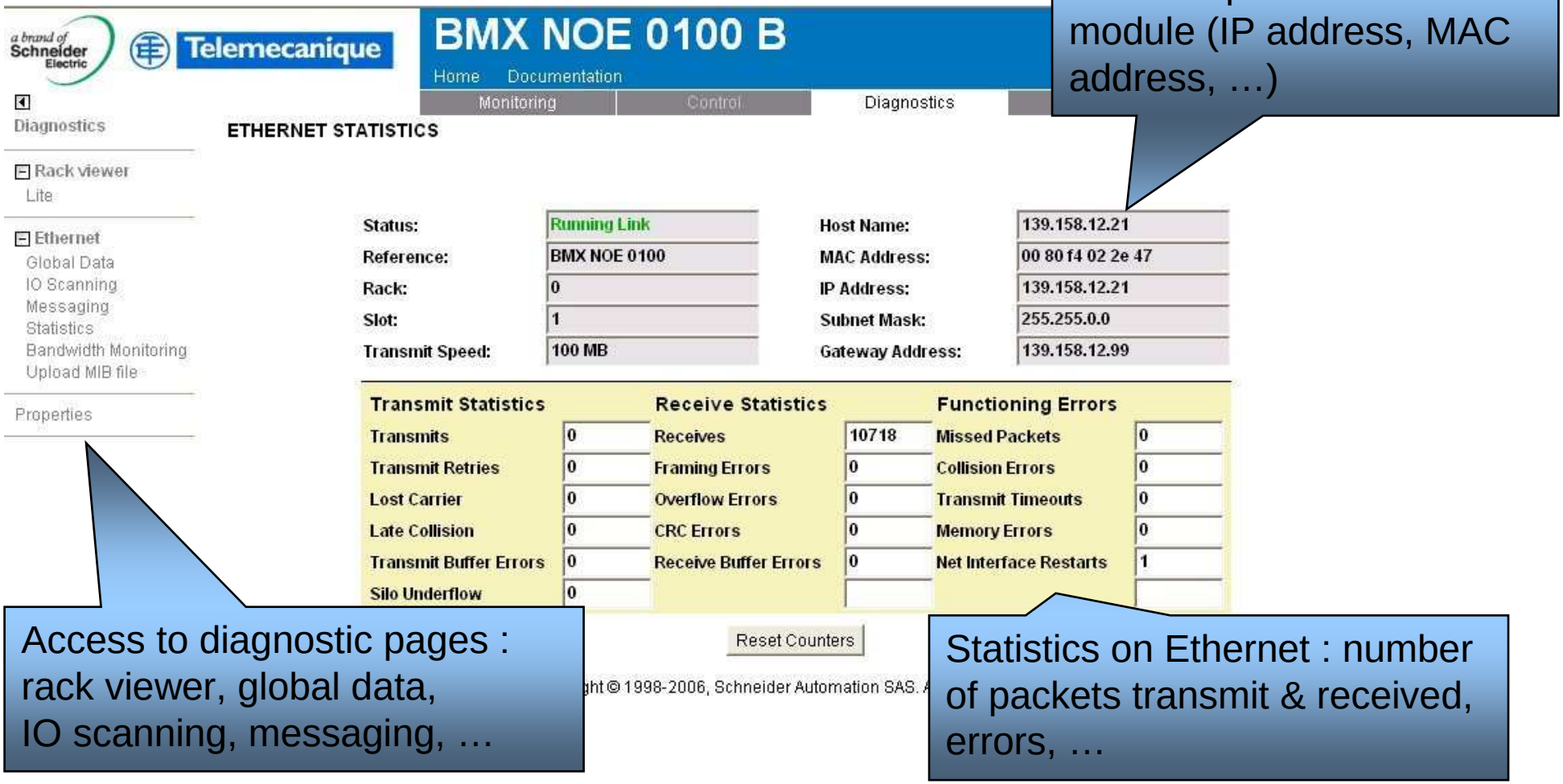
Data editor : create a table



Data editor : add variable / modify value



Diagnostic pages : statistics

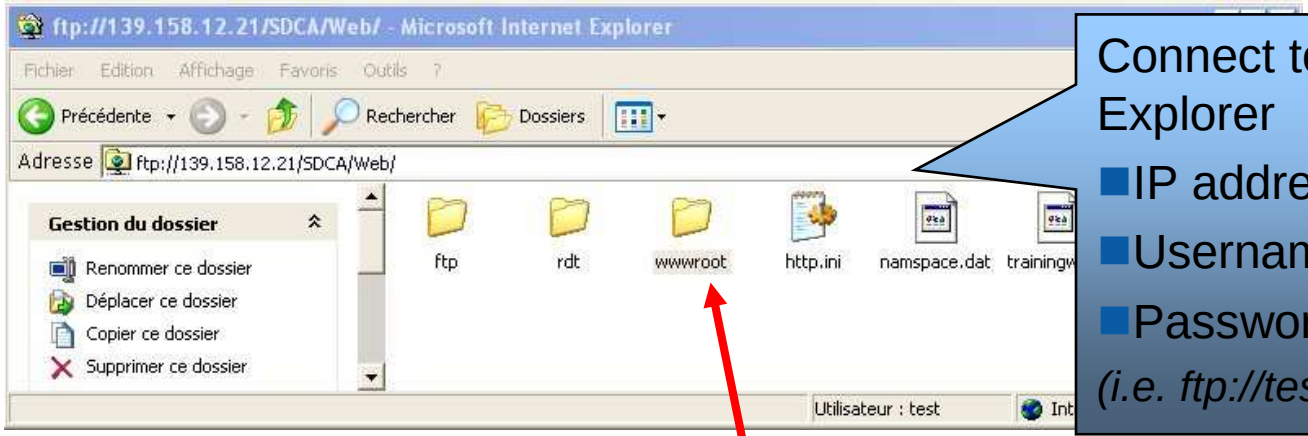


Ethernet parameters of the module (IP address, MAC address, …)

Access to diagnostic pages : rack viewer, global data, IO scanning, messaging, …

Statistics on Ethernet : number of packets transmit & received, errors, …

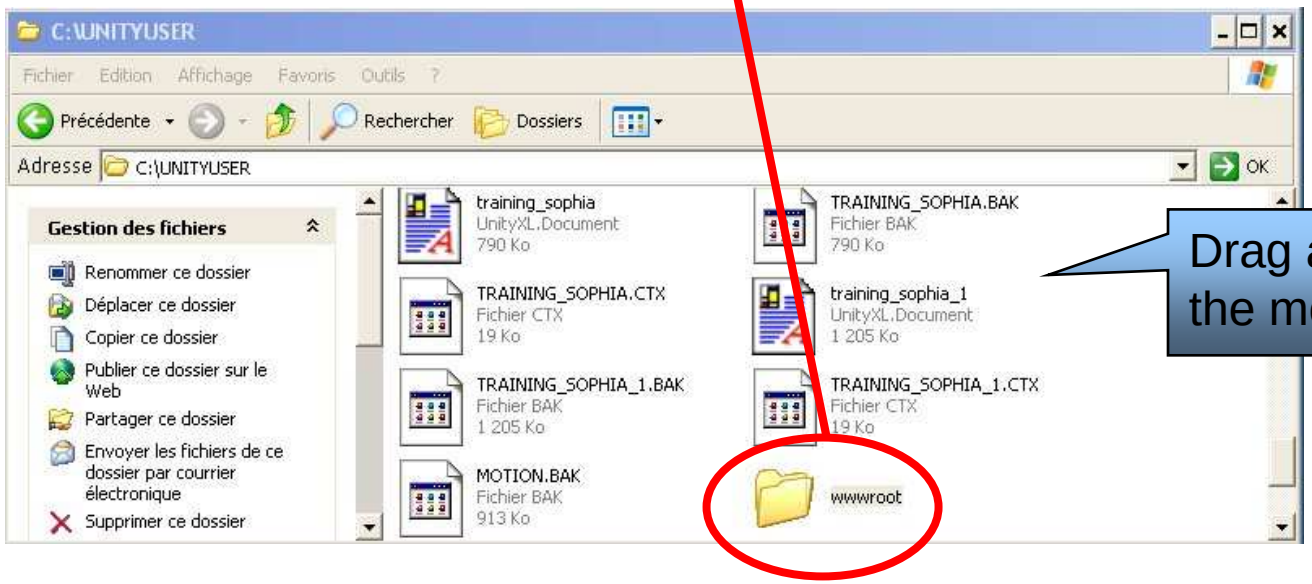
Transfer to the module (ftp server)



Connect to the module with Internet Explorer

- IP address in ftp
- Username : *test*
- Password : *testingpw*

(i.e. ftp://test:testingpw@139.158.12.21)



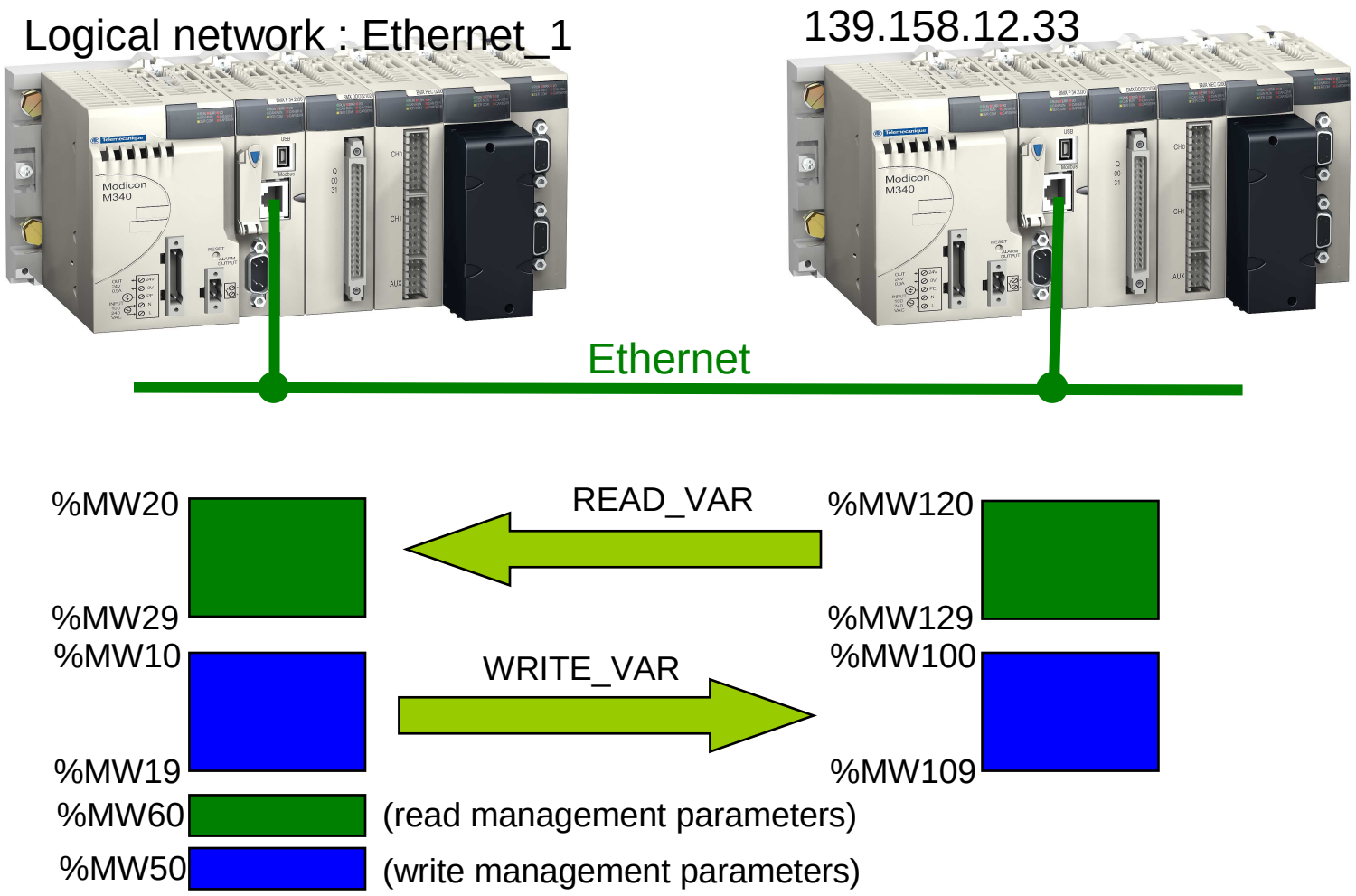
Drag and drop from your PC to the module

Language interface

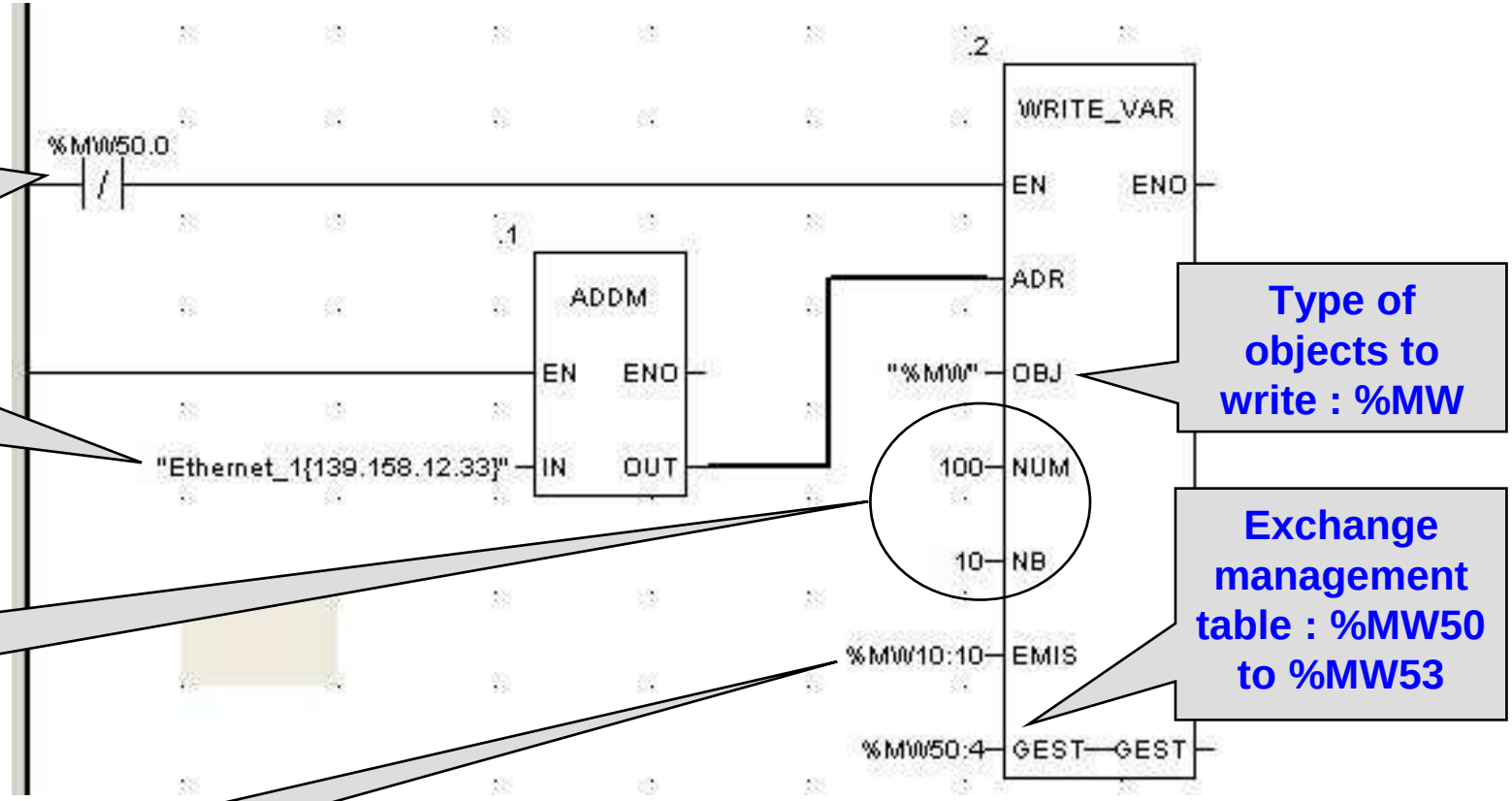
IODDT for Ethernet communication

- 2 IODDTs
  - T_COM_STS_GEN for all communication protocol
  - T_COM_ETH_BMX for Ethernet communication

Example of Read / Write data



Program to write data



Activity bit (bit 0) of management parameters

Ethernet address of remote equipement

Destination table %MW100 to %MW109

Table to write : %MW10 to %MW19

Type of objects to write : %MW

Exchange management table : %MW50 to %MW53