PROFINET Diagnostics Software and Tools

Dr. Xiu Ji

Manchester Metropolitan University

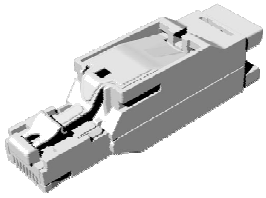
Content

www.mmu.ac.uk/profibus

- Static wiring test, diagnostics
- Live system diagnostics
- Basics of PROFINET

What is PROFINET?

- PROFINET is Standard Ethernet (IEEE 802.3).
- PROFINET is based on the “Fast Ethernet” or 100 BASE TX/FX.
- PROFINET is an Industrialised Ethernet, optimised for speed, determinism and durability.



Important IEEE 802.3 specs

Spec number	Speed	Standard description
IEEE 802.3 (a,b,i,j)	10 Mbps	**10 Base Ethernet** (there are different numbers associated with copper, fiber, coax and variants)
IEEE 802.3u	100 Mbps	**100 Base TX / FX** Fast Ethernet for copper (TX) and fiber (FX)
IEEE 802.3z IEEE 802.3ab	1000 Mbps	**1000 Base X** - Gigabit Ethernet over fiber (z) and copper (ab)
IEEE 802.3ae	10000 Mbps	**10BaseLR (etc..)** Ten Gigabit Ethernet over Fiber
IEEE 802.3x		Flow Control / Full Duplex

PROFINET is based on 100BASE-TX/FX, i.e. Fast Ethernet

Fibre optic medium

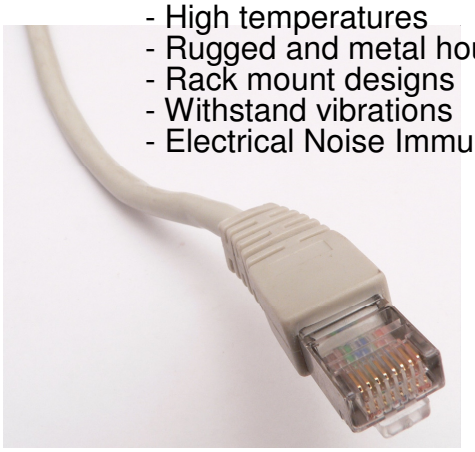
Twisted **2-pair** copper Cat 5 cable
Max. cable length of **100m** between devices

100 mbps

X: means any medium, copper or fibre, but redundant with 'T' or 'F'.
100BASE can also use un-twisted enhanced Cat 5 cable, i.e. Cat 5e.
STP: Shielded Twisted Pair, e.g. 100BASE-TX, STP. PROFINET only uses STP cables.
UTP: Unshielded Twisted Pair, e.g. 100BASE-TX, UTP.

What is Industrial Ethernet?

- Is this fit ?
  - High temperatures
  - Rugged and metal housing
  - Rack mount designs
  - Withstand vibrations
  - Electrical Noise Immunity

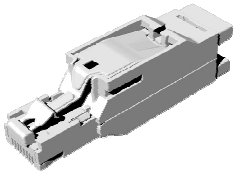


www.mmu.ac.uk/profibus

Connectors

Manchester Metropolitan University

IP20 RJ45



IP65 RJ45

IP65 M12

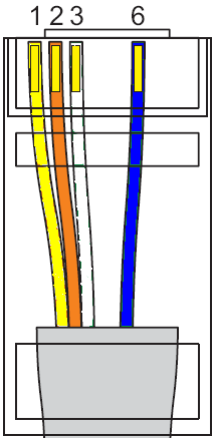
Customised heavy-duty

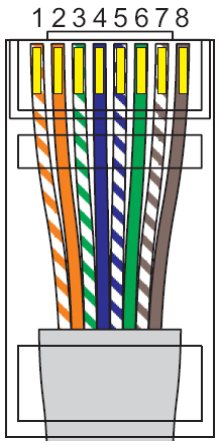
www.mmu.ac.uk/profibus

4 wires or 8 wires?

Manchester Metropolitan University

Pin	Functionality
1	Data (TX +)
2	Data (TX -)
3	Data (RX +)
4	e.g. Ground (-)
5	e.g. Ground (-)
6	Data (RX -)
7	e.g. Power (+)
8	e.g. Power (+)

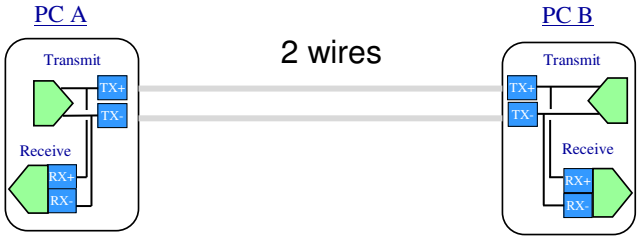




Half Duplex

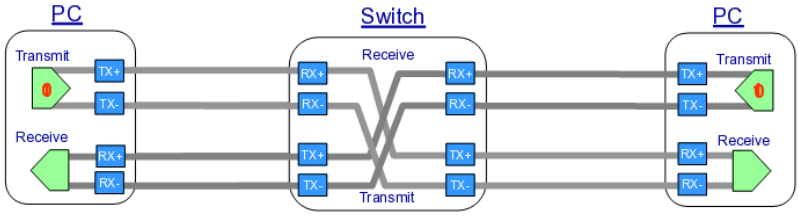
Half duplex Mode

- Data transmission can take place only in one direction at the same time
- uses two wires, twisted



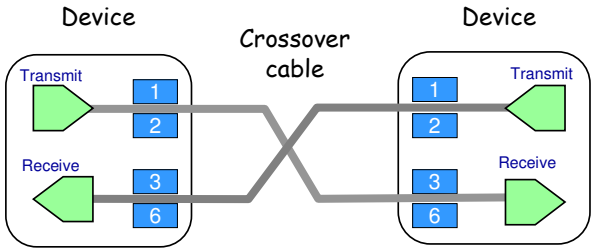
Full Duplex

- Full duplex mode, 4 wires
  - √ Transmission of data in two directions simultaneously
  - √ Use of 4 wires and switching technology
  - √ i.e. telephone



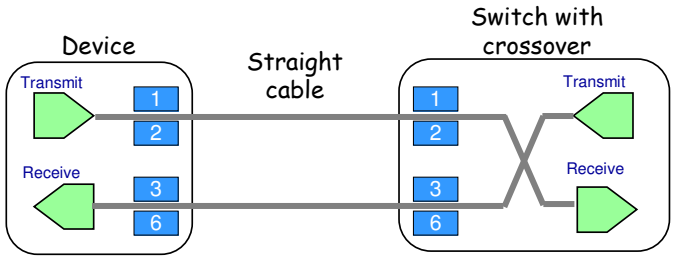
Straight and Crossover Cables

- Ethernet devices must be connected so that the transmitter in one device is connected to the receiver in another.
- When connecting one device directly to another (e.g. a PC to a field device), a “cross-over” cable is required:



Straight and Crossover Cables

- When using a switch or hub to connect devices, the switch normally provides the crossover for us.
- Therefore, when using switches, “straight” cables are used to connect the device to the switch:

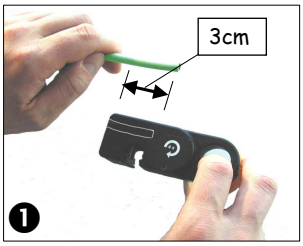


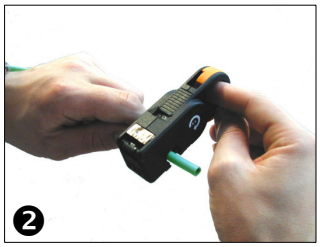
Modern switches provide “auto-crossover”, where they are able to automatically provide crossover as required.

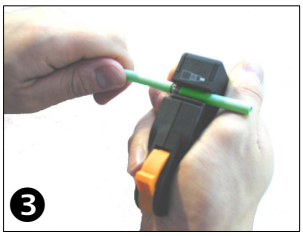
Cable Test Tools

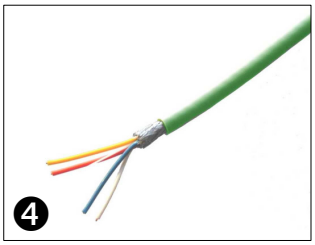
- There are many different cable test tools available for checking Ethernet cables.
- These range in price from less than £100 pounds to over £3000.

Stripping Tools

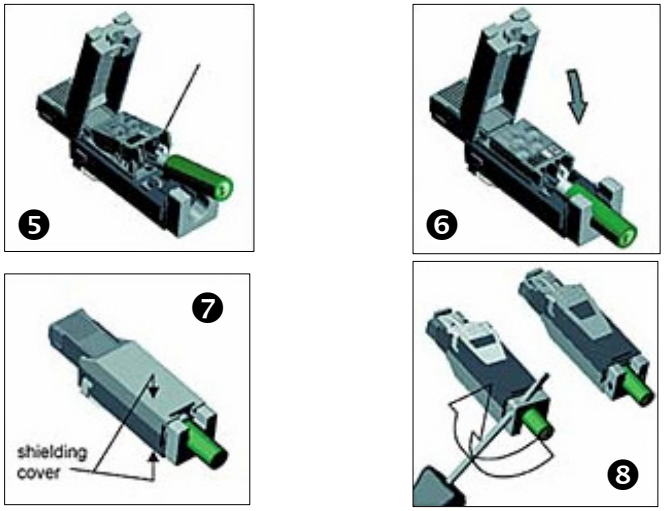






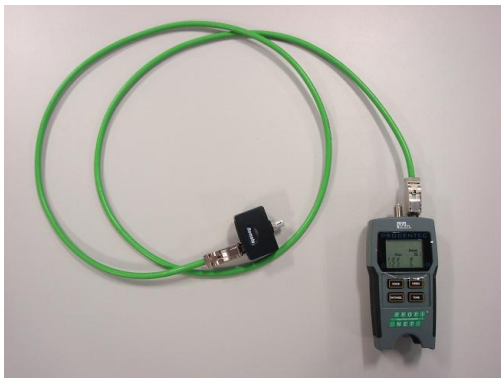


Insulation Displacement Connectors



Cable Tester

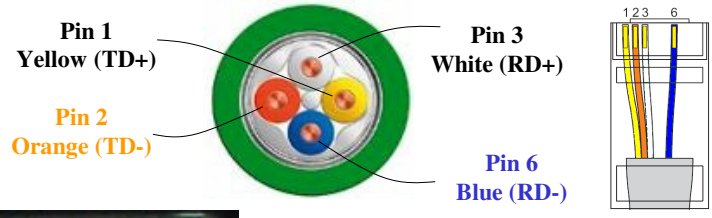
- Connect the test plug at one end and the tester at the other end.
- Detect many wiring faults:
  - √ Wire break
  - √ Short circuit
  - √ Swapped wires

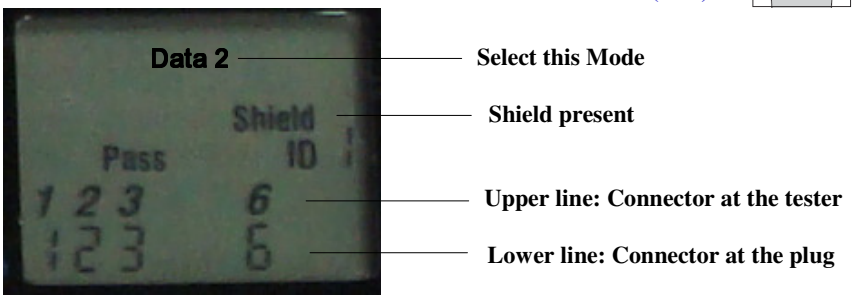


Good wiring

www.mmu.ac.uk/profibus

Manchester Metropolitan University

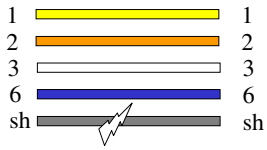




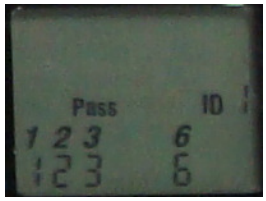
Wiring faults

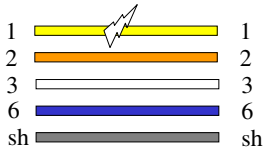
www.mmu.ac.uk/profibus

Manchester Metropolitan University

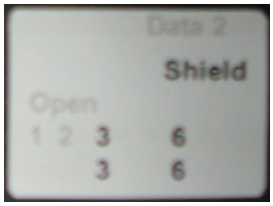


No shield or Shield broken

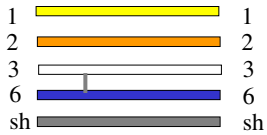




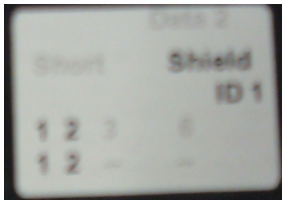
Wire break and Effected pins

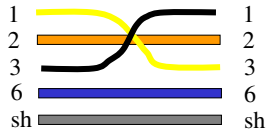


Wiring faults

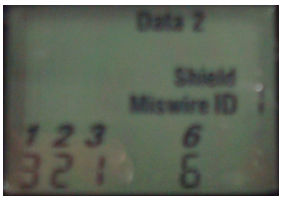


Short circuit, Second line indicated as --



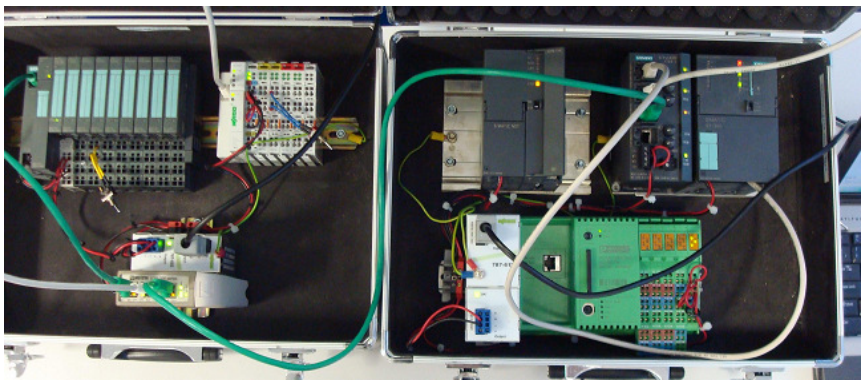


Yellow and White swapped



Practical Exercise

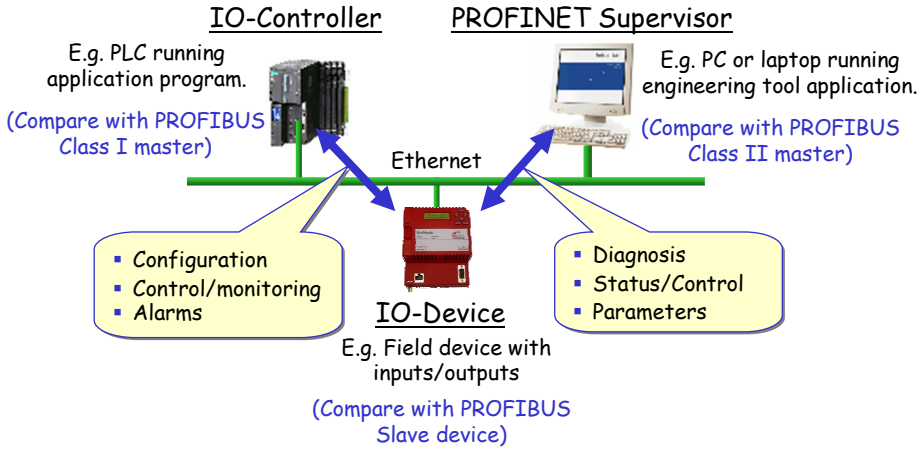
- Make up a cable and test on a live system.
- Watch for the connectivity indicators on the switch.



www.mmu.ac.uk/profibus

Configuration: PROFINET IO Systems

Manchester Metropolitan University

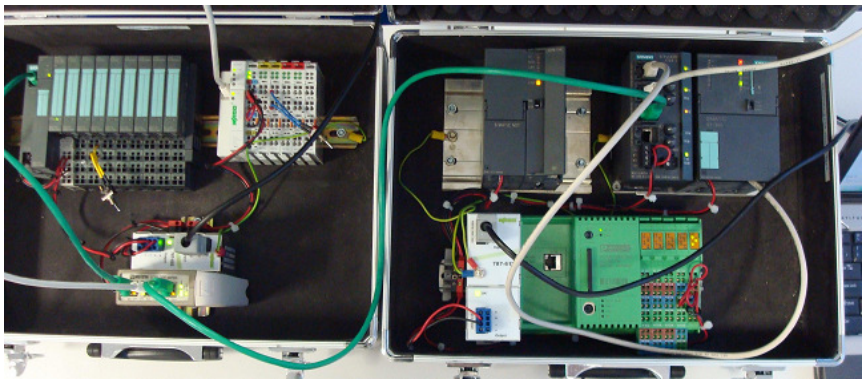


www.mmu.ac.uk/profibus

A PROFINET IO System

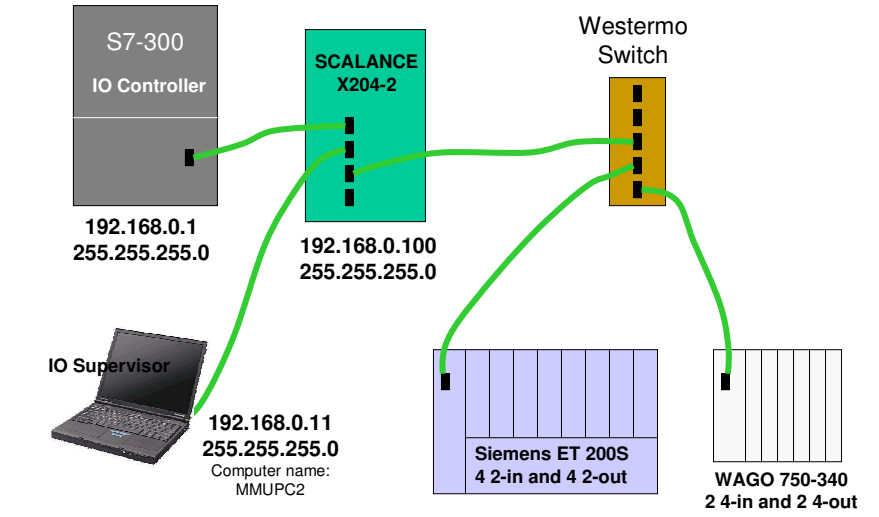
Manchester Metropolitan University

- Siemens S7-300 CPU 315-2 PN/DP Controller
- Siemens managed switch, SCALANCE X204-2
- Westermo 5-port unmanaged switch, SDW-500



www.mmu.ac.uk/profibus

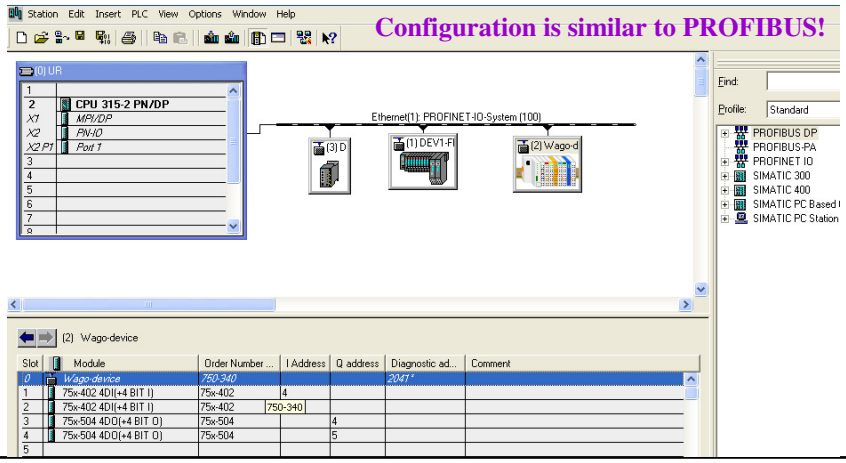
Step 1



www.mmu.ac.uk/profibus

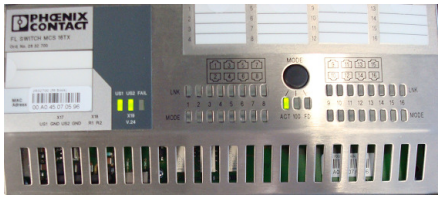
"Drag & Drop" and Assign Device Name

- IO Controller automatically assign IP addresses based on its domain addresses.



Addressing

- Device addresses are NOT set by DIP switch. Instead, “Device Name” concept is used.
- IO devices much have a device name.
- Every device has a unique MAC address. (Media Access Control)
- MAC Address must be printed on every IO device.
- MAC Address is used for real-time communication.
- IP Address is used only for non-real-time data exchange, e.g. configuration and parameterisation.
- IP addresses are allocated by IO Controller every time during start-up or restart.

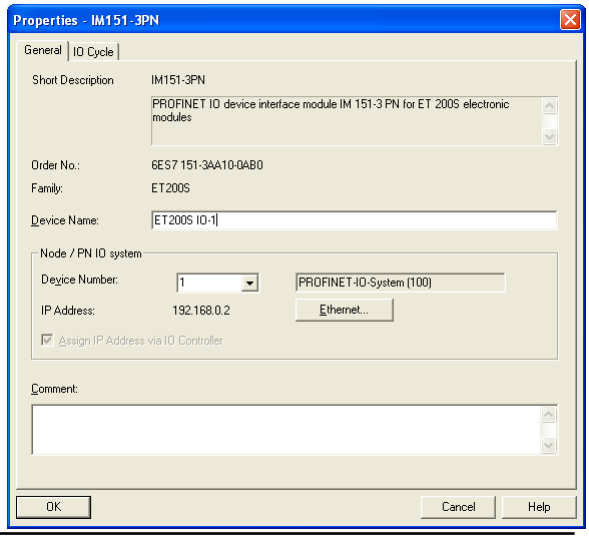


Addressing

- Start-up always takes place over the non-real-time TCP/UDP/IP channel.
- MAC addresses and device names (at default or if assigned) are revealed at this stage.
- IP addresses are then allocated based on their MAC addresses.
- The device name is vital in setting up IP addresses.
- Device name must be set correctly.
- Once the device name and IP address are correct the IO controller can initiate communication with the device.

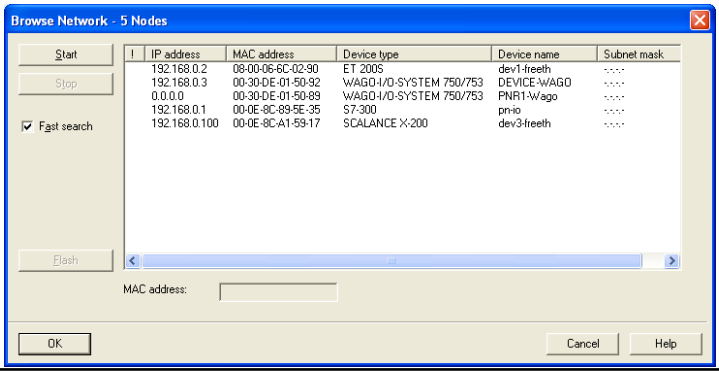
Download or change device name

- There are tools available for changing device names.
- Changing device names within a configuration tool stores the names within the project.



Initial Communication

- Communication between Controller and Supervisor
  - √ via LAN
  - √ Supervisor: Laptop with Siemens S7 HW-Config application
  - √ Controller: Siemens S7-300 CPU with RJ45 interface
  - √ **Scan or Browse Network**: MAC address and device name are revealed.

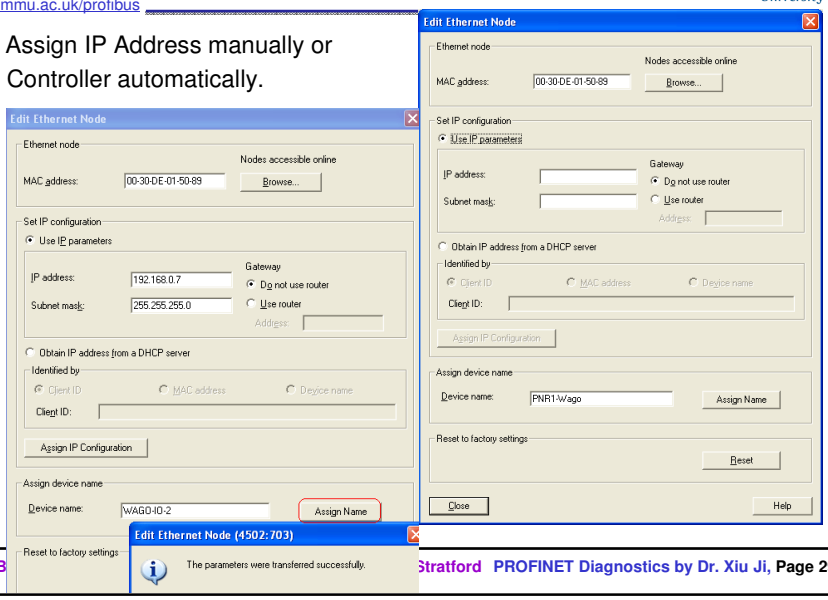


MAC address and device name

www.mmu.ac.uk/profibus

Manchester Metropolitan University

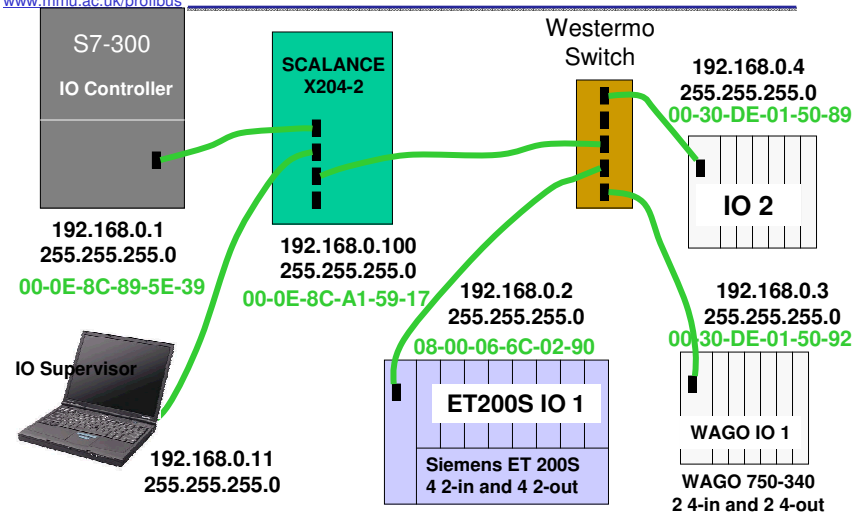
- Assign IP Address manually or via Controller automatically.



Step 2

www.mmu.ac.uk/profibus

Manchester Metropolitan University



Step 3a: Write a program

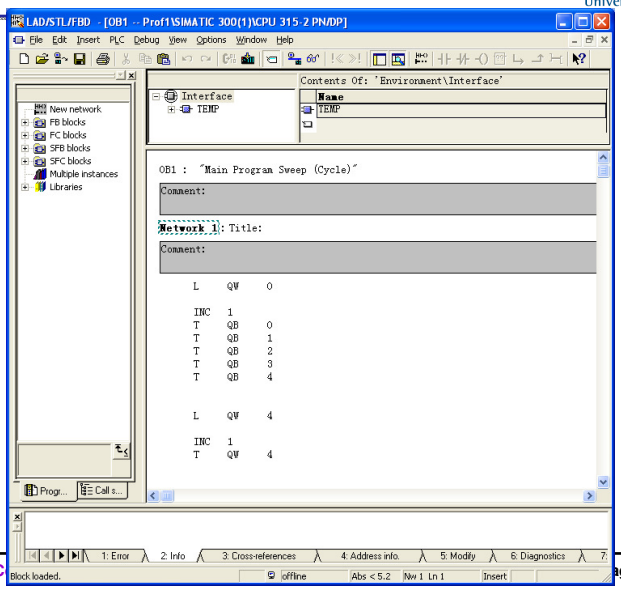
- Write a simple program in OB1 and download it to Controller.

```
L     QW0      //load Output Word 0
INC   1        //increment it with 1
T     QB0      //write it to Output Byte 0
T     QB1      //write it to Output Byte 1
T     QB2      //write it to Output Byte 2
T     QB6      //write it to Output Byte 3
T     QB7      //write it to Output Byte 4
T     QW8      //load Output Word 4

L     QW4      //load Output Word 4
INC   1        //increment it with 1
T     QW4      //write it to Output Word 4
```


Step 3b: Write a program

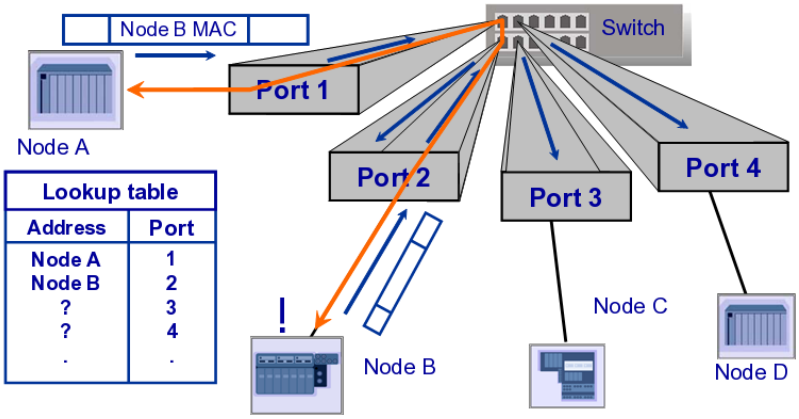
- Program:



Learning MAC Addresses

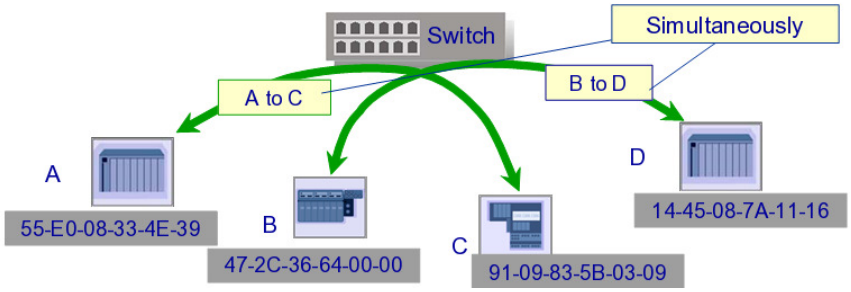
www.mmu.ac.uk/profibus

- Switch knows which device is on which port and hence directs traffic/data to where is intended to be rather than flooding the network.



Switching Technology

www.mmu.ac.uk/profibus



A switch remembers the ports:

- If swapping plugs, it takes time to re-figure out the ports
- Power off a device first, swap plugs if required, and then power on the device.

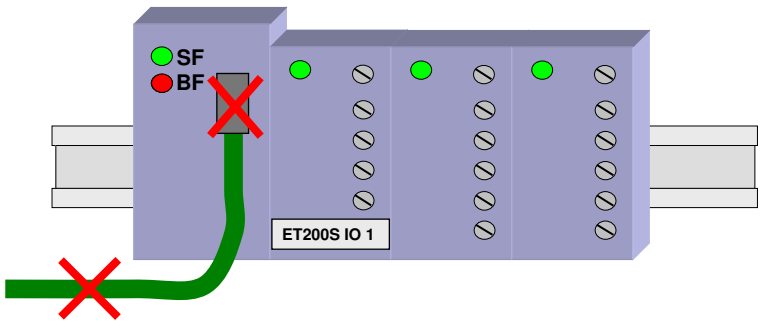
Diagnostics

- PROFINET provides fast and thorough diagnostics covering almost every component of a PROFINET network.
- Diagnostics are structured hierarchically, starting with the device information and moving down to the ladder to the module and channel diagnostics.
- Network and system status are also available.
- In case of a fault, the station name, module number, channel number, channel type, and information about the error itself are displayed and can be accessed.

Diagnostics are similar as in PROFIBUS!

Communication faults

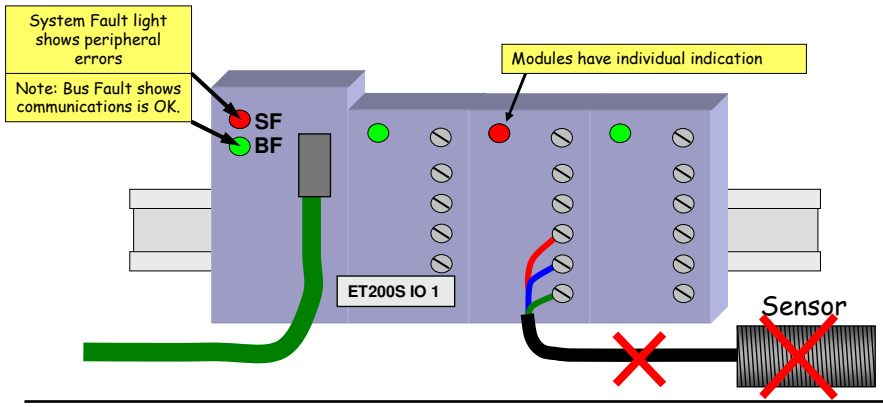
- Mainly caused by poor network wiring or layout or cable/connector deterioration.
- Can be permanent or intermittent.



Peripheral faults

www.mmu.ac.uk/profibus

- Caused by sensor/actuator failure or wiring faults.
- Again faults can be intermittent.

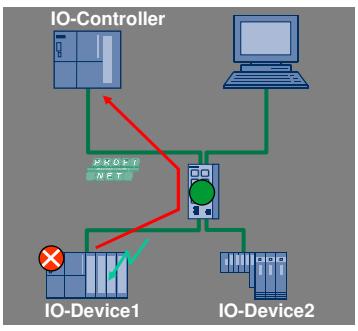


Diagnostics

www.mmu.ac.uk/profibus

√ The switch passes on the PROFINET diagnostics of an IO device to CPU.

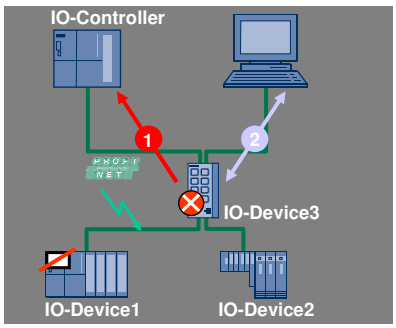
√ CPU evaluates and report the diagnostics

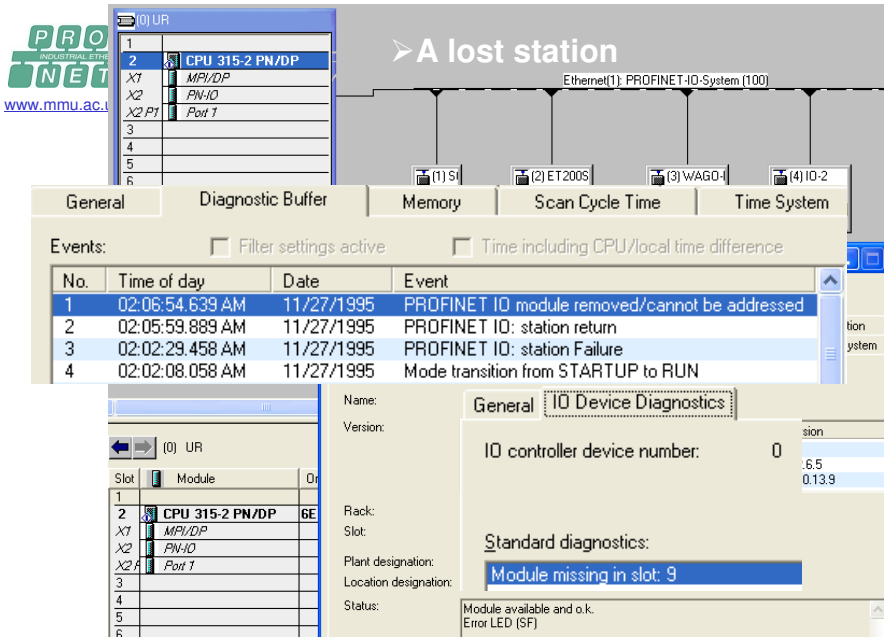


√ **The switch reports network disturbances as PROFINET-diagnostics to the IO-Controller (1)**

√ **Configuration of the Switch as IO-Device (GSDML)**

√ **Additional SNMP channel, e.g. for reporting on a Supervisor (2)**



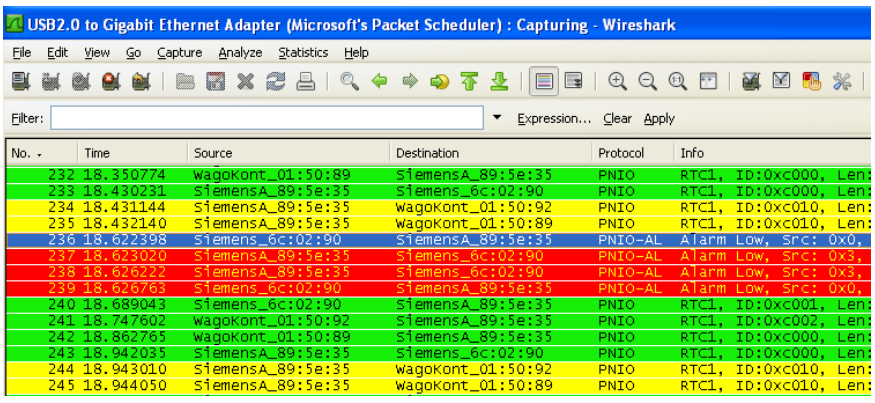


Diagnostics using analysers

www.mmu.ac.uk/profibus

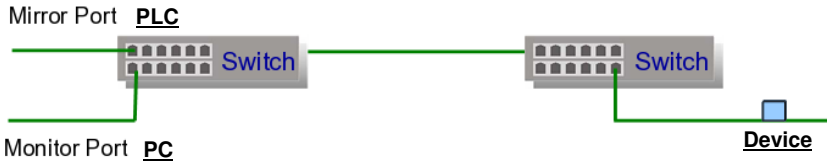
Manchester Metropolitan University

- Free tool, Wireshark.
- The alarms are captured.

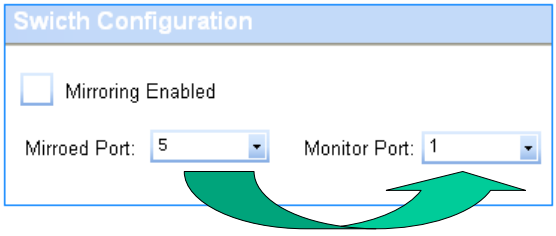


Port Mirroring

- **Port Mirroring** is used on a switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.
- Defining a mirror port duplicates all traffic on the mirror.
  - √ incoming and outgoing traffic
- Useful for monitoring the switch traffic on a certain port, the monitor port **for diagnostic reasons**.
  - √ e.g. with Ethereal / Wireshark analyser
- **Available in managed switches or as a dedicated device.**

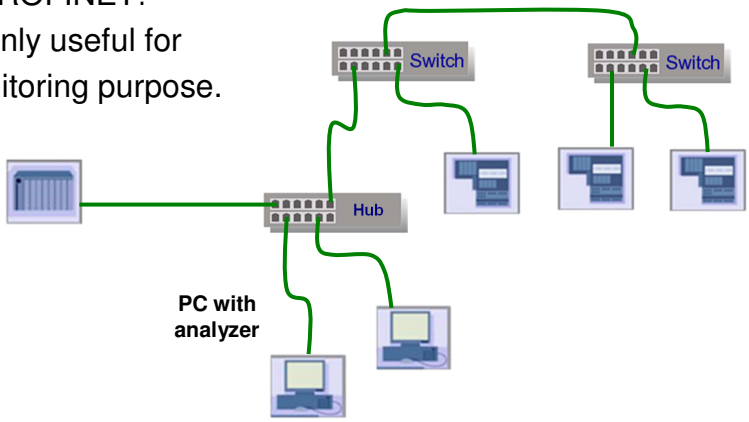


Setup Switch for Monitoring

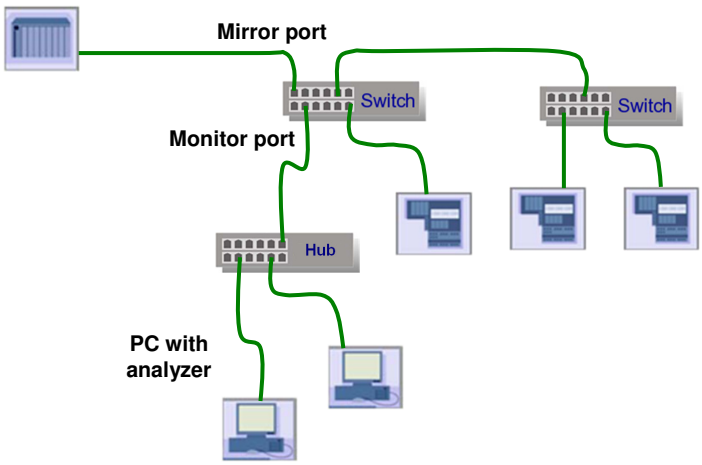


Monitoring

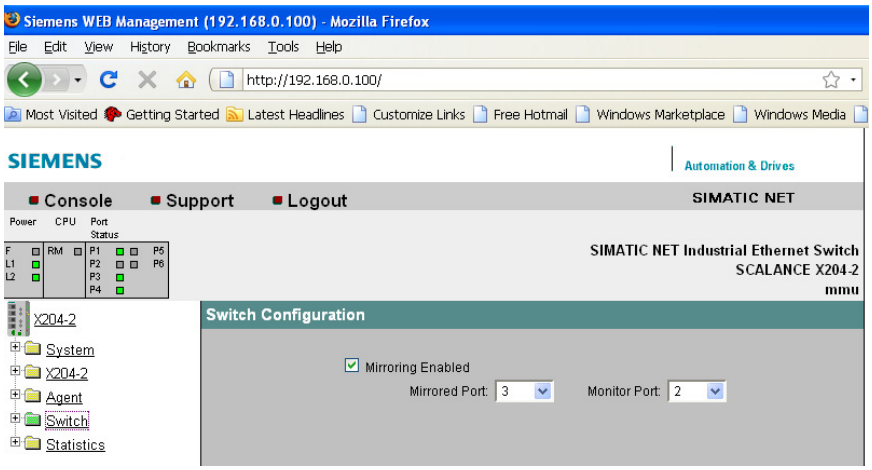
- Hubs should NOT be used In PROFINET!
- Only useful for monitoring purpose.



Monitoring

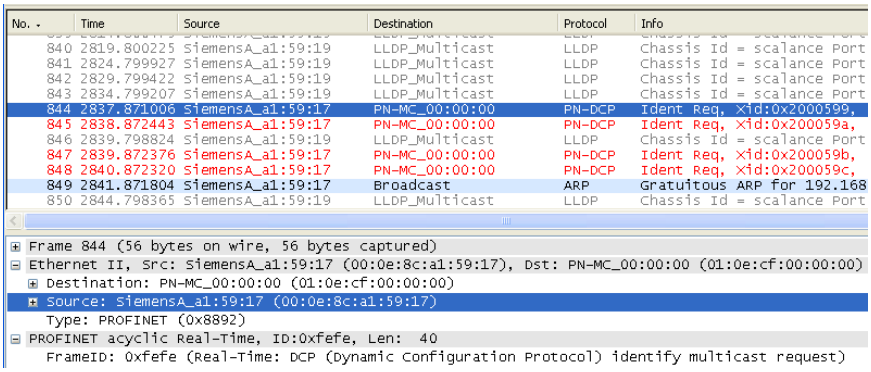


Mirror and monitor ports



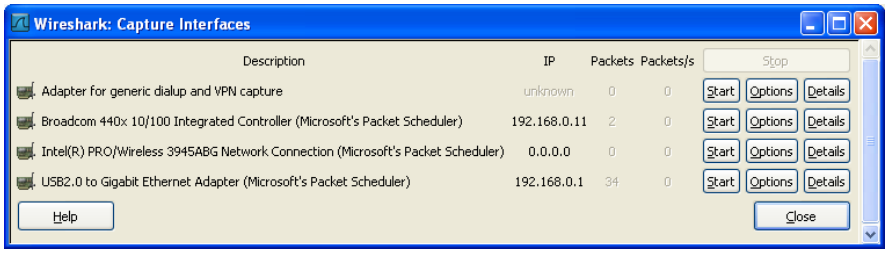
Non-monitoring Port

- On non-monitoring port of a switch, only multicast or broadcast messages are captured.



Recording

- Select a network interface to record telegrams/data exchange.



Normal Data

- Priority 6, relatively low.

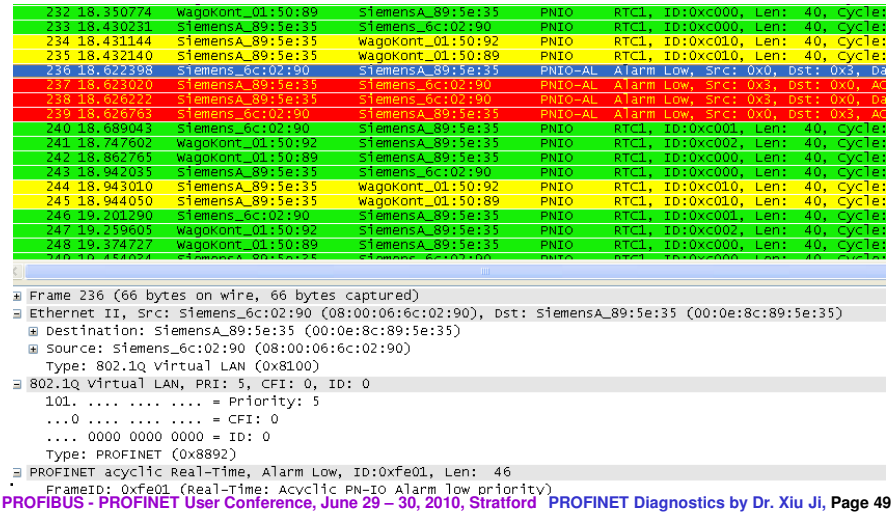
```
232 18.350774   WagoKont_01:50:89   SiemensA_89:5e:35   PNIO      RTC1, ID:0xc000, Len:  40, Cycle:
233 18.430231   SiemensA_89:5e:35   Siemens_6c:02:90    PNIO      RTC1, ID:0xc000, Len:  40, Cycle:
234 18.431144   SiemensA_89:5e:35   WagoKont_01:50:92   PNIO      RTC1, ID:0xc010, Len:  40, Cycle:
235 18.432140   SiemensA_89:5e:35   WagoKont_01:50:89   PNIO      RTC1, ID:0xc010, Len:  40, Cycle:
236 18.622398   Siemens_6c:02:90    SiemensA_89:5e:35   PNIO-AL   Alarm Low, Src: 0x0, Dst: 0x3, Da
237 18.623020   SiemensA_89:5e:35   Siemens_6c:02:90    PNIO-AL   Alarm Low, Src: 0x3, Dst: 0x0, Ac
238 18.626222   SiemensA_89:5e:35   Siemens_6c:02:90    PNIO-AL   Alarm Low, Src: 0x3, Dst: 0x0, Da
239 18.626763   Siemens_6c:02:90    SiemensA_89:5e:35   PNIO-AL   Alarm Low, Src: 0x0, Dst: 0x3, Ac
240 18.689043   Siemens_6c:02:90    SiemensA_89:5e:35   PNIO      RTC1, ID:0xc001, Len:  40, Cycle:
241 18.747602   WagoKont_01:50:92   SiemensA_89:5e:35   PNIO      RTC1, ID:0xc002, Len:  40, Cycle:
242 18.862765   WagoKont_01:50:89   SiemensA_89:5e:35   PNIO      RTC1, ID:0xc000, Len:  40, Cycle:
243 18.942035   SiemensA_89:5e:35   Siemens_6c:02:90    PNIO      RTC1, ID:0xc000, Len:  40, Cycle:
244 18.943010   SiemensA_89:5e:35   WagoKont_01:50:92   PNIO      RTC1, ID:0xc010, Len:  40, Cycle:
245 18.944050   SiemensA_89:5e:35   WagoKont_01:50:89   PNIO      RTC1, ID:0xc010, Len:  40, Cycle:
246 19.201290   Siemens_6c:02:90    SiemensA_89:5e:35   PNIO      RTC1, ID:0xc001, Len:  40, Cycle:
247 19.259605   WagoKont_01:50:92   SiemensA_89:5e:35   PNIO      RTC1, ID:0xc002, Len:  40, Cycle:
248 19.374727   WagoKont_01:50:89   SiemensA_89:5e:35   PNIO      RTC1, ID:0xc000, Len:  40, Cycle:
```

```
⊞ Frame 240 (64 bytes on wire, 64 bytes captured)
⊟ Ethernet II, Src: Siemens_6c:02:90 (08:00:06:6c:02:90), Dst: SiemensA_89:5e:35 (00:0e:8c:89:5e:35)
  ⊞ Destination: SiemensA_89:5e:35 (00:0e:8c:89:5e:35)
  ⊞ Source: Siemens_6c:02:90 (08:00:06:6c:02:90)
    Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN, PRI: 6, CFI: 0, ID: 0
    110. .... .... .... = Priority: 6
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0000 = ID: 0
    Type: PROFINET (0x8892)
⊟ PROFINET cyclic Real-Time, RTC1, ID:0xc001, Len:  40, Cycle:32800 (Valid,Primary,Problem,Run)
    FrameID: 0xc001 (0xC000-0xFAFF: Real-Time(class=1): Cyclic)
    CycleCounter: 32800
```

Alarms

www.mmu.ac.uk/profibus

- VLAN must be used. Alarms are Priority 5, higher than normal data.



Conclusion

www.mmu.ac.uk/profibus

- Static wiring test → handheld tools.
- Configuration errors → MAC addresses, device names and IP addresses.
- Live system diagnostics
  - √ Software supplied with IO Controller
  - √ Analysers, e.g. comprehensive and easy to use → Wireshark