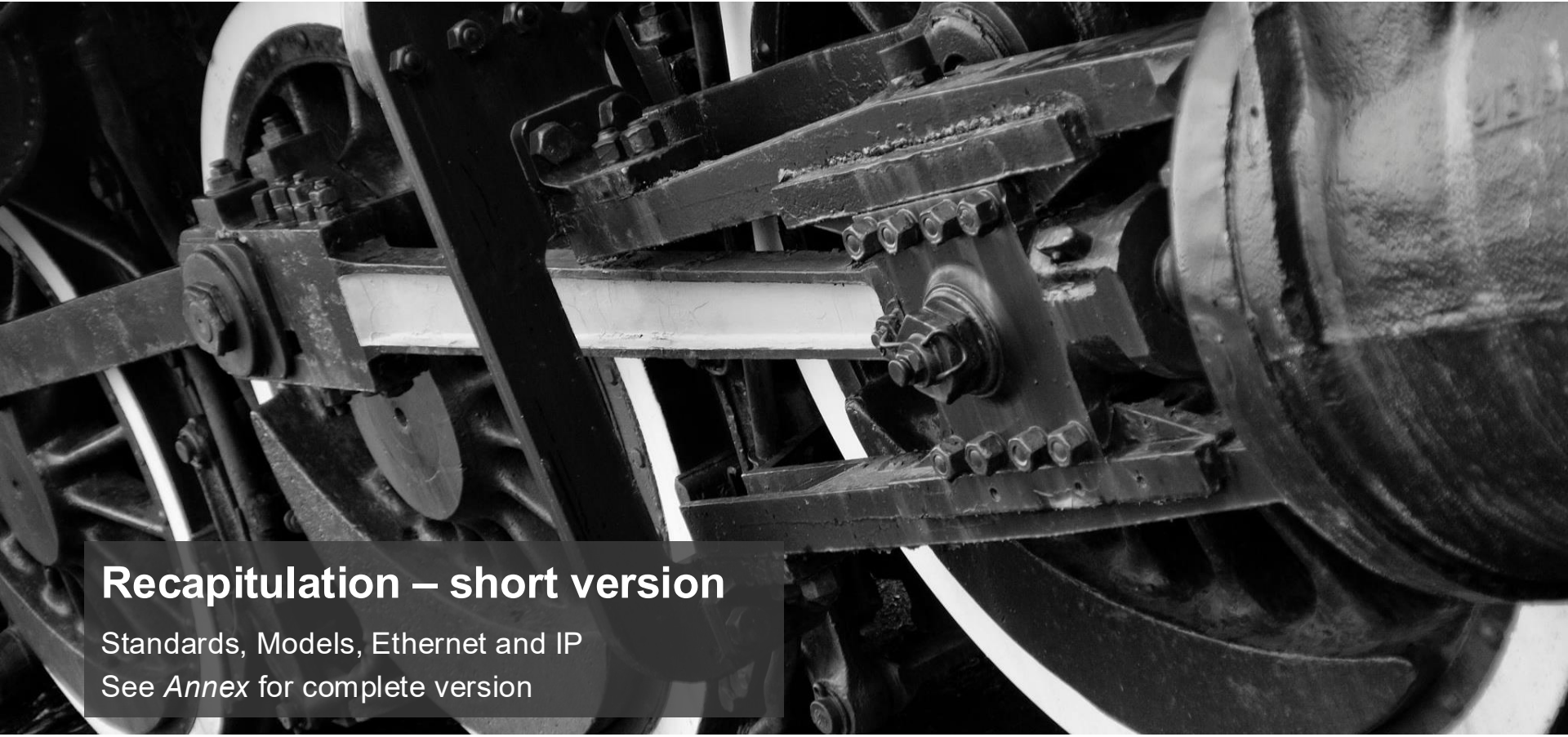
TSM_SecIndOpT

Communication technology relevant to OT environment (I) Version: 1.4

Luca Haab | 09.03.2026 | Cours MSE

swissuniversities



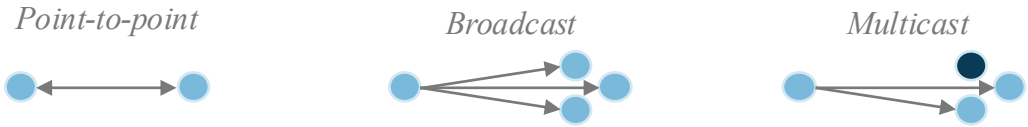
Recapitulation – short version

Standards, Models, Ethernet and IP

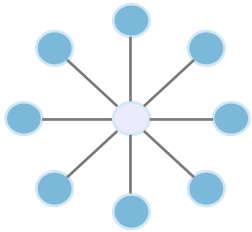
See *Annex* for complete version

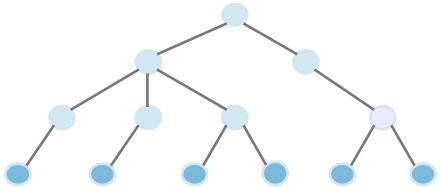
Topologies

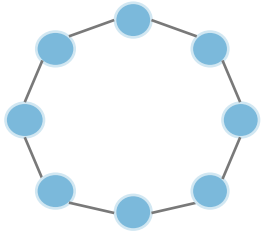
- Communication types

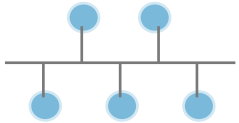


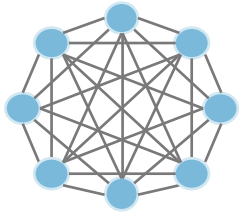
- Spatial distribution of network elements


Star


Tree


Ring


Bus


Full Mesh

Network classification (I)

Distance	Utilization	Classification
1 m	System	Multiprocesseur – Computer
10 m	Local	**LAN** (Local Area Network)
100 m	Building	
1 km	Campus	
10 km	City	**MAN** (Metropolitan Area Network)
100 km	Country	**WAN** (Wide Area Network)
1’000 km	Continent	
10’000 km	Planet	GAN (Global Area Network)

Network classification (II)

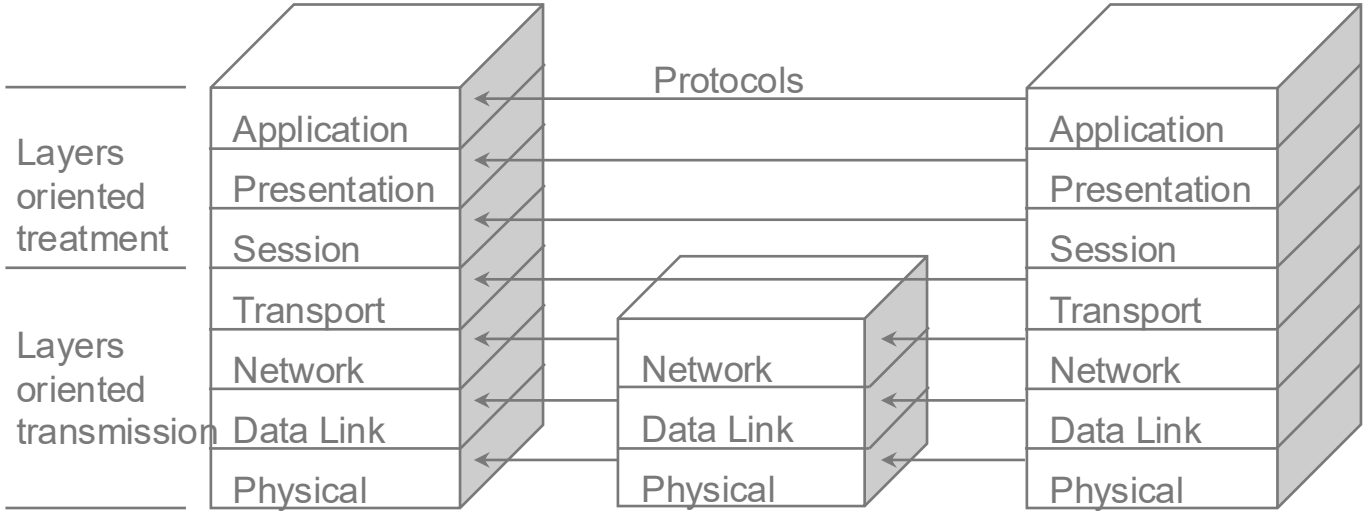
LAN (*Local Area Network*)

MAN (*Metropolitan Area Network*)

WAN (*Wide Area Network*)

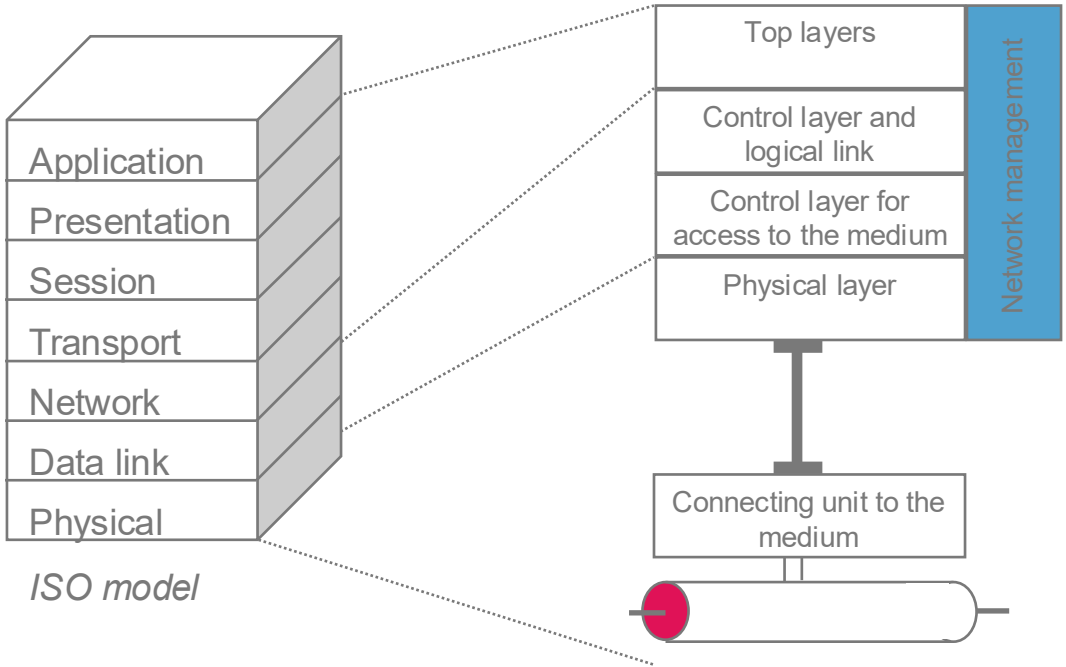
Category	LAN	MAN	WAN
Full-Form	Local Area Network.	Metropolitan Area Network.	Wide Area Network.
Span	Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as country or continent.
Ownership	LAN's ownership is private. A Local Area Network (LAN) is a secure and private network that can be owned by various institutions such as hospitals, schools, offices, and more.	MAN's ownership can be private or public. A Metropolitan Area Network (MAN) can exist as either a public or private network, and it is commonly owned by numerous businesses and telecommunications companies.	While WAN also might not be owned by one organization. A Wide Area Network (WAN) is not typically owned exclusively by a single company. It can be either privately or publicly owned.
Bandwidth	The bandwidth in LAN is very high.	Transmission speed is average.	WAN bandwidth ican be quite limited.
Propagation delay	Propagation delay is short.	Moderate propagation delay.	Long propagation delay in a WAN.
Congestion	Less congestion in LAN.	More impoprtant congestion in MAN.	Highest potential for congestion.
Design & Maintenan	LAN's design and maintenance are easy.	Design and maintenance are more difficult than LAN.	WAN's design and maintenance most challenging.
Fault tolerance	Easy way to have fault tolerance.	Less fault tolerance.	Costs and complexity impact the general availability of fault tolerance.

ISO reference model



The ISO model was proposed by ISO in 1983. Note that the ISO model is a theoretical reference model that does not apply perfectly to IT networks. In practice, the Internet model has imposed itself during the past few years. The ISO model arguably remains the best abstraction base (ISO 7498-1, ITU X.200).

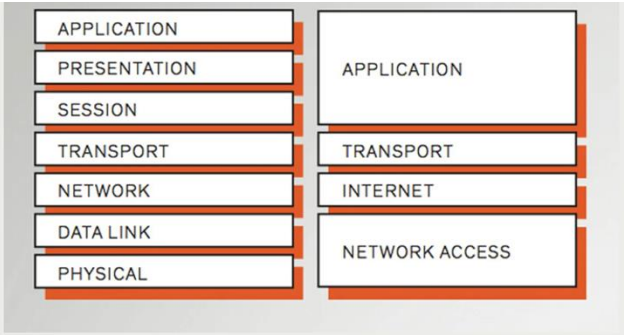
ISO 7498-1 vs. IEEE 802.x comparison



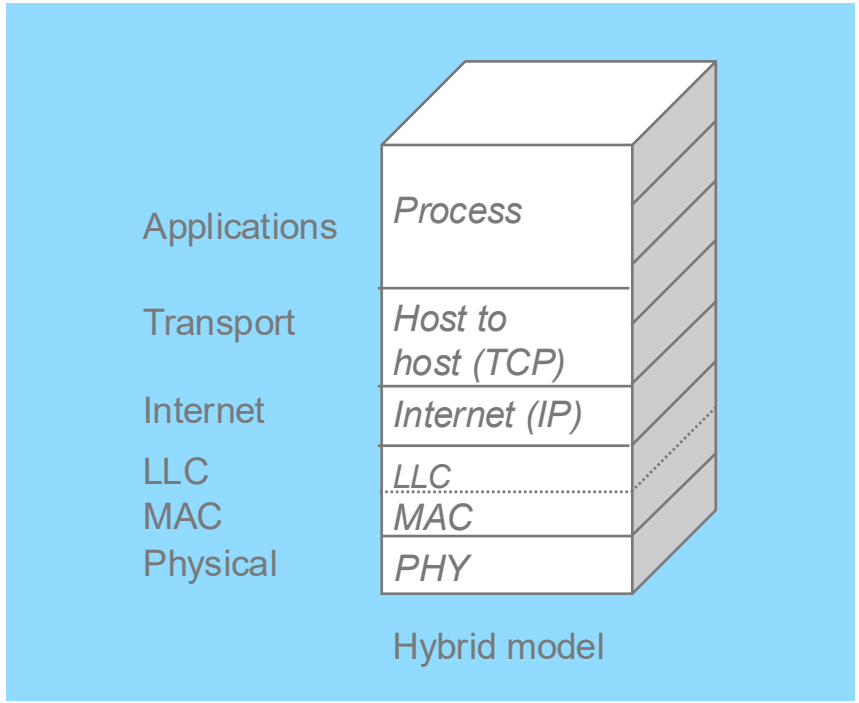
Note that there is no absolute identity of functions and boundaries

The Hybrid Model

Pragmatic layered model much used today, combining the IEEE and Internet models



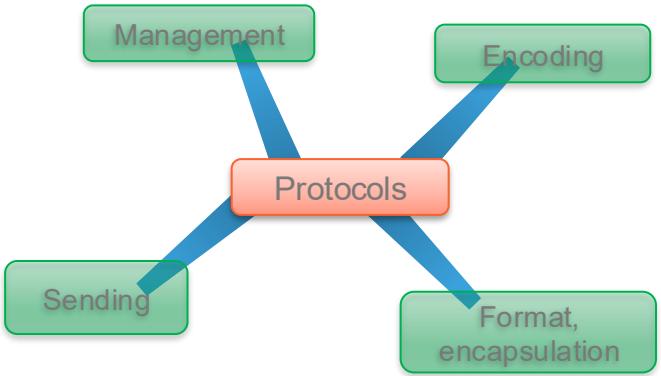
A layered approach: The OSI reference model (left column) divides computer communications into seven distinct layers, from physical media in layer 1 to applications in layer 7. Though less rigid, the TCP/IP approach to networking can also be construed in layers, as shown on the right.

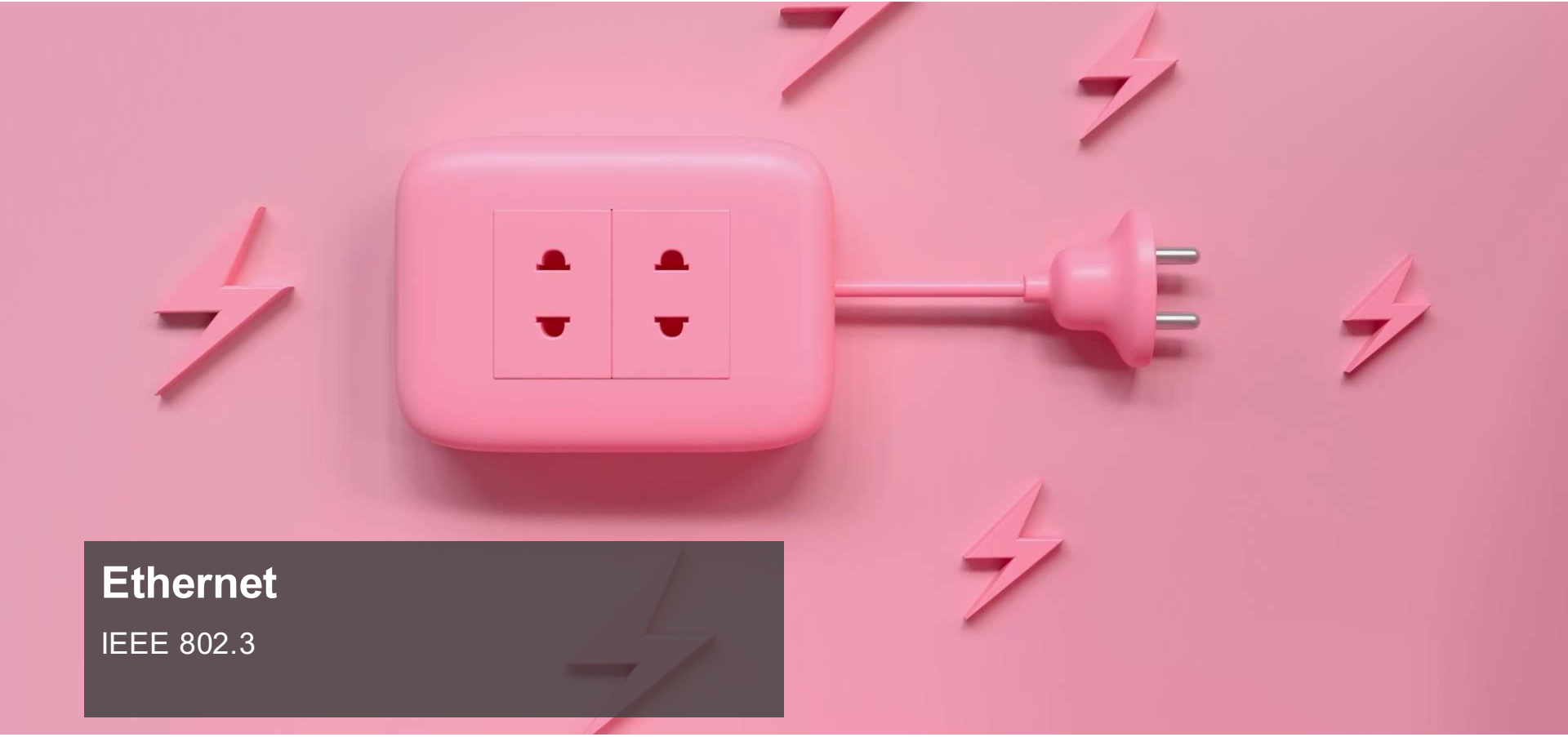


Source (and interesting read): https://spectrum.ieee.org/osi-the-internet-that-wasnt

“Standards”: rules to communicate

- Establish **rules** to communicate:
  - Identify sender and receiver
  - Common language and grammar
  - Speed and time management of the exchange
  - Confirmation or acknowledgment of exchanges
- Message Encoding
  - Process of converting information into another acceptable form
- Format, encapsulation and size of messages
- Messages management
  - Access methods
  - Flow control
  - Timer
- Option for sending messages
  - Unicast
  - Multicast
  - Broadcast





Ethernet

IEEE 802.3

Transparent Bridging: basic principle

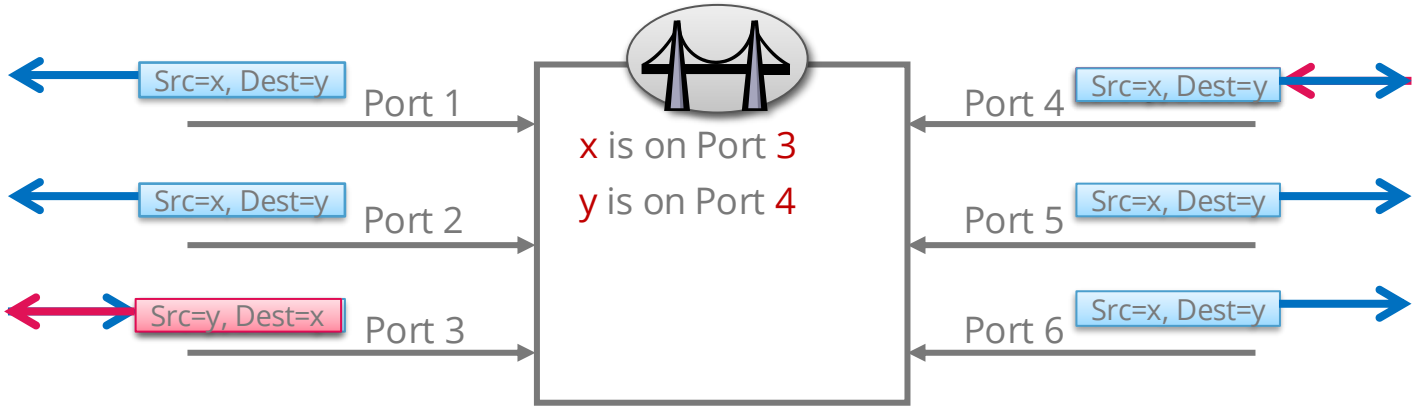
A transparent *Bridge* has five tasks to perform:

1. In case of doubt, to transfer all the arriving frames, in particular *broadcast* frames, to all the **other** ports (*flooding*).
2. To find out stations' MAC addresses based on the passing frames' **source addresses** and thus create a *bridging* table, associating a port with each known MAC address (*learning*).
3. To transfer the frames whose destination addresses are not in the segment from where the frames arrive to the exit port corresponding to this destination (*forwarding*).
4. To block frames where the destination is in the same segment as that from where the frames arrive
5. To avoid loops using the spanning tree's algorithm .

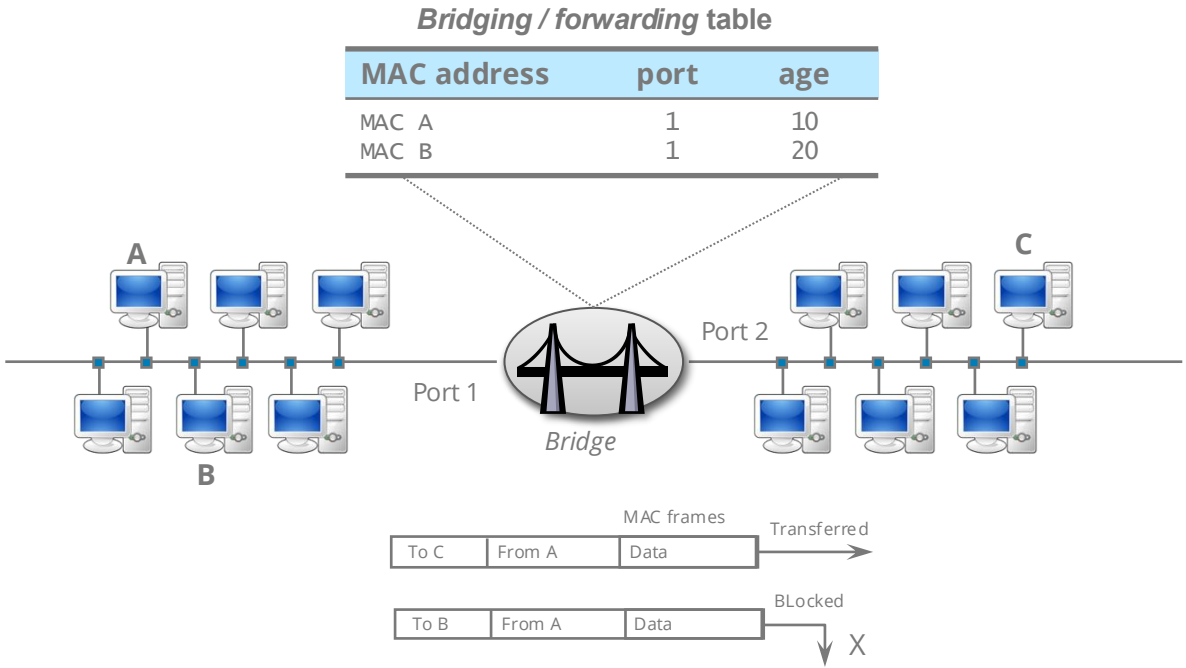
Frame Forwarding

- The forwarding table is automatically filled

  The source address of a frame arriving on a port indicate which hosts are accessible on that port.



Transparent bridging: frame forwarding

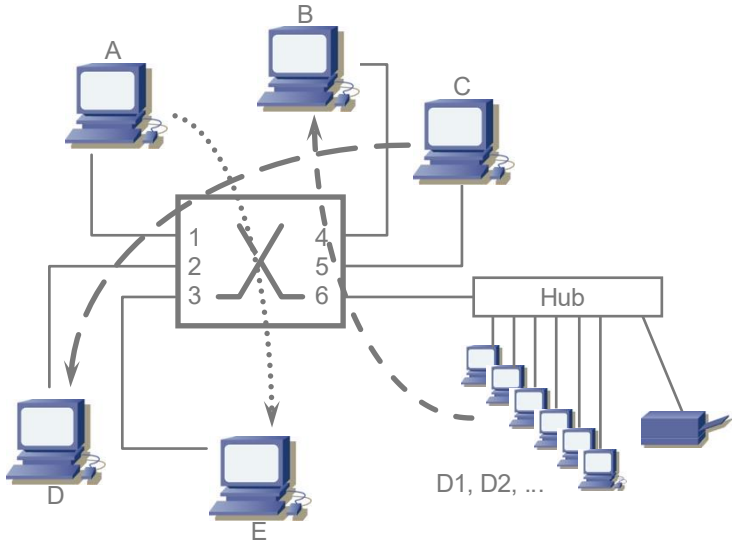


Switch Modes of Functioning

Cut-through

If station A sends a frame to station E, the *Switch* decodes the address of destination E as quickly as possible at access 1 and transmits the frame without delay (*"cut-through"*) uniquely to segment 3.

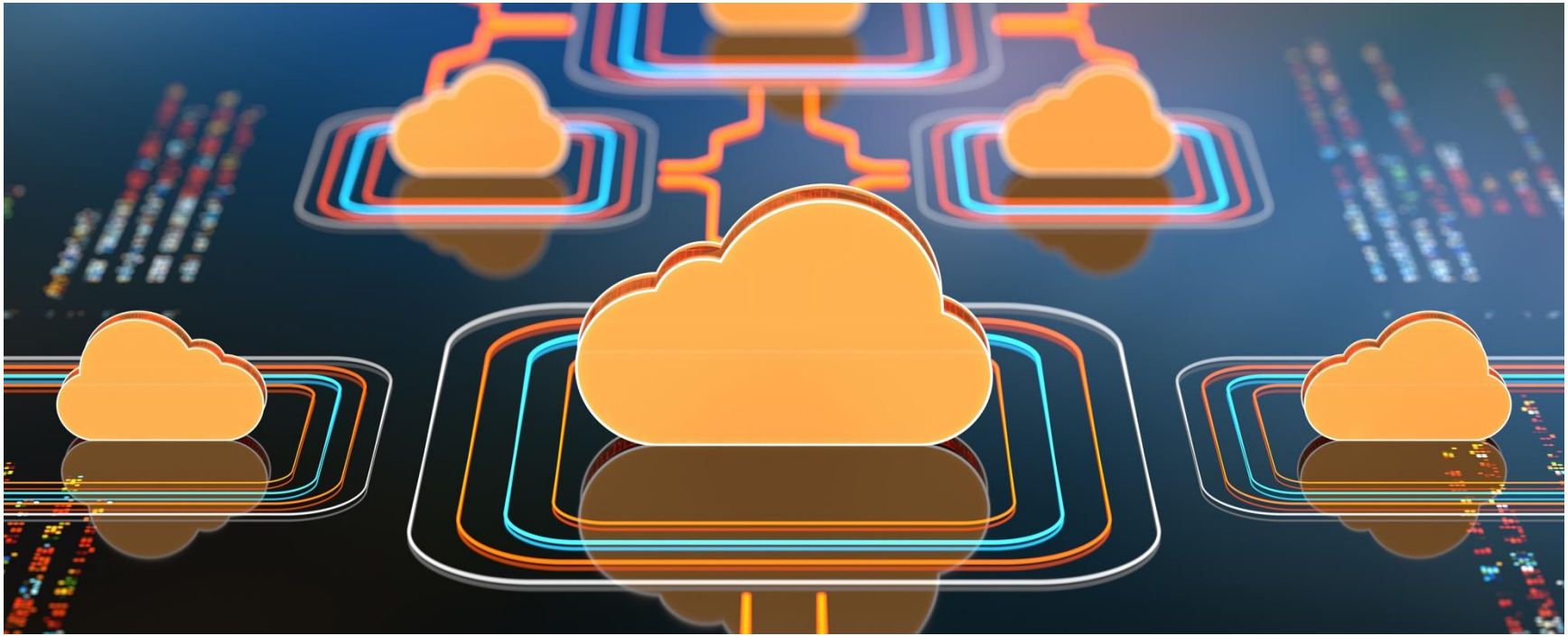
Note that it is not possible to perform an error control before forwarding the frame on.



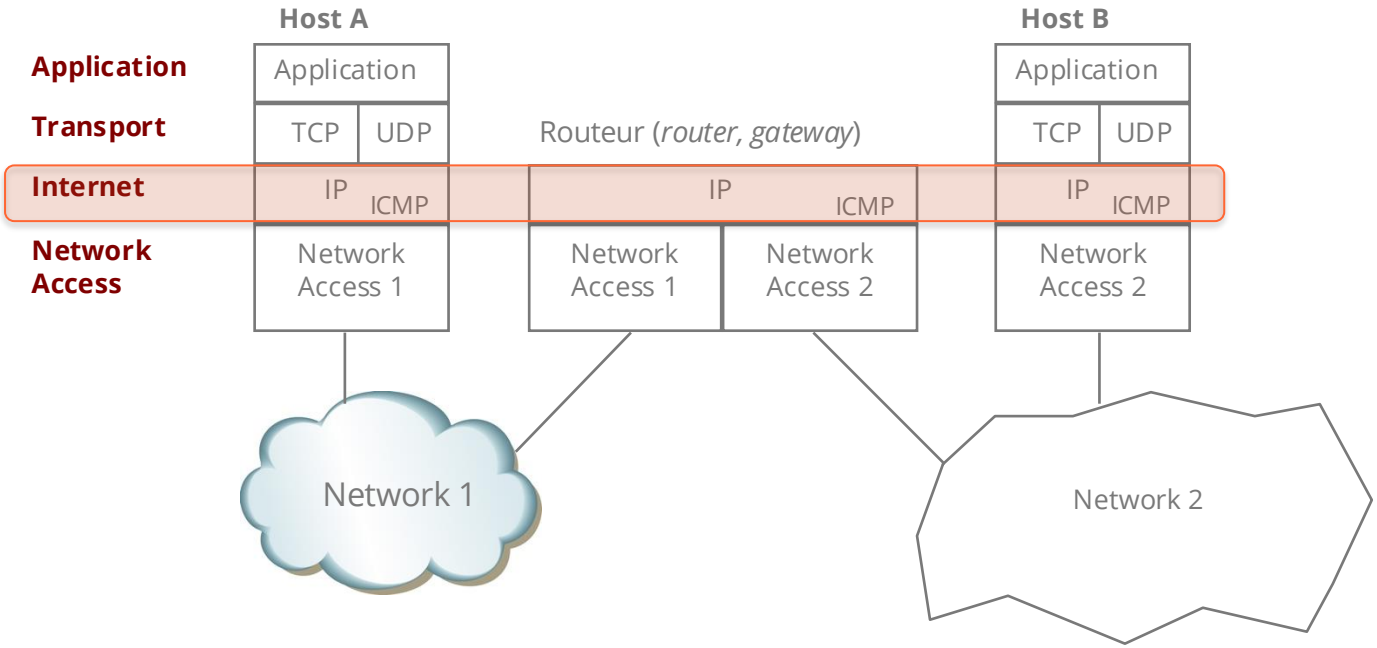
Store & forward

The frame is memorized in full before being transmitted,
which permits the elimination of frames containing errors.
The price to pay is increased transmission delay.

IP Protocol

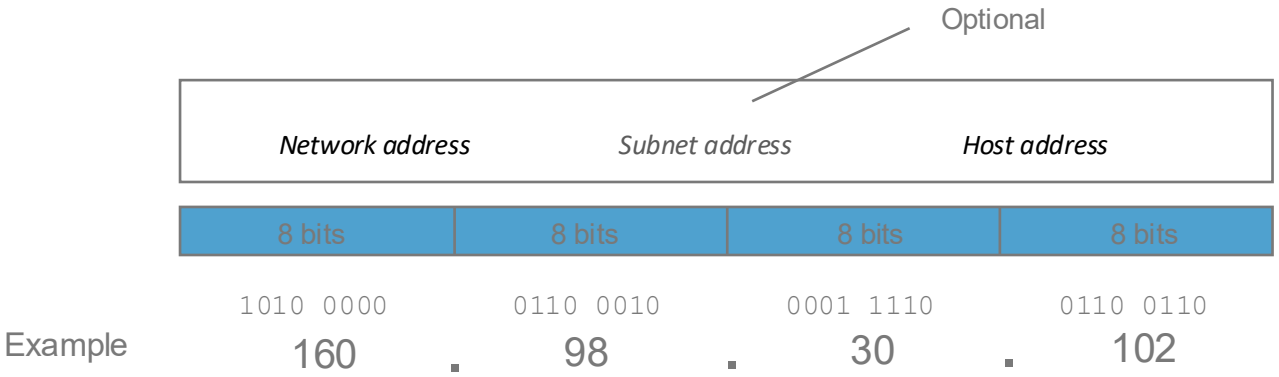


TCP/IP Architecture



IP addressing

An IP address (version 4 - RFC 791, Sept. 1981) is made up of 32 bits organized hierarchically from left to right in 2 or 3 variable-sized sections:

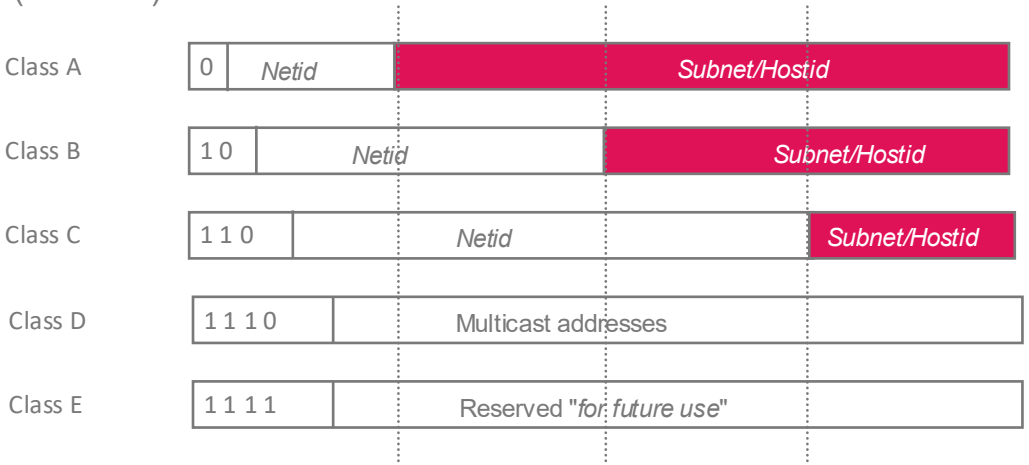


IP addresses are written in the form of 4 decimal numbers separated by points, the "*dotted decimal notation*". Each number represents the equivalent decimal of a binary byte.

The minimum value of a byte is 0 (0b0000'0000), the maximum, 255 (0b1111'1111).

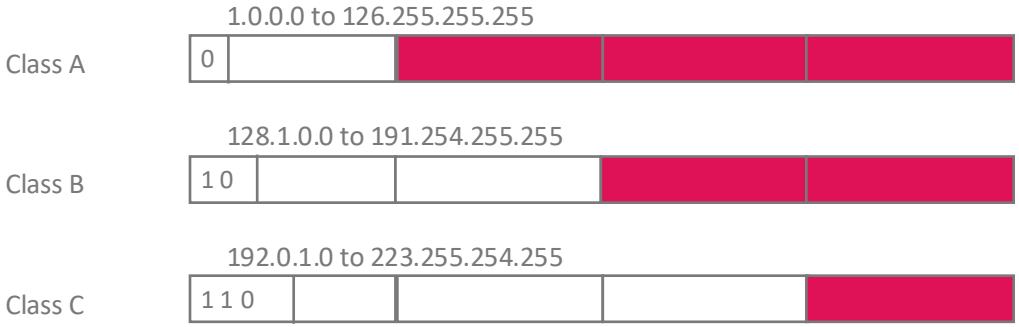
IP address classes (1)

Originally, the IP addressing space of 0.0.0.0 to 255.255.255.255 was strictly divided into "classes". IP supports 5 classes of address, called A, B, C, D and E. The first three are point-to-point addresses (*unicast*), class D is intended for point to multipoint (*multicast*) and class E is "reserved for future use"



Class A: 7 bits for the network (1-126), 24 bits for the *subnets*/stations
Class B: 14 bits for the network (128.1-191.254), 16 bits for the *subnets*/stations
Class C: 21 bits for the network (192.0.1-223.255.254), 8 bits for the *subnets*/stations
Class D: (224.0.0.0-239.255.255.255)
Class E: (240.0.0.0-255.255.255.254)

IP address classes (2)



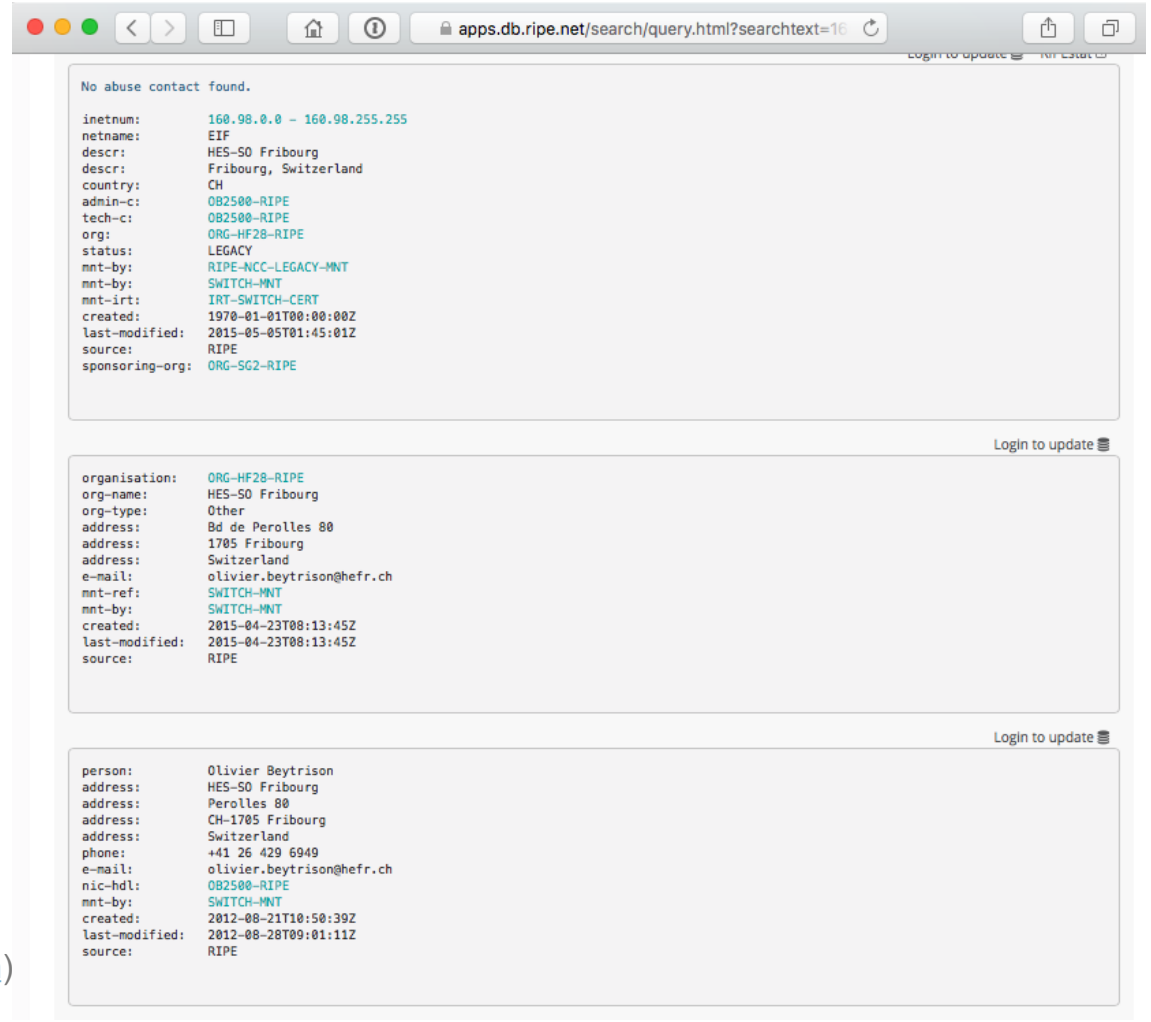
Class A: 126 networks with 16'777'214 stations each (0 and 127 reserved)
Class B: 16'382 networks, each with 65'534 stations
Class C: 2,097,150 networks, each with 254 stations

Conventions:

- An IP address with *Hostid* = **0** designates the network/subnet. An address with *Hostid* = **255** designates a *broadcast* on the network/subnet.
- Address 255.255.255.255 is blocked by the routers (*all ones broadcast*).
- Addresses **127.**X.X.X indicate a *loopback* (local loop) in the source station (frequently 127.0.0.1). Allows testing without passing via the network.
- Address 0.0.0.0 is the default address for the stations and the path to the *backbone* for the routers

Whois? 160.98

https://www.ripe.net
(or https://apps.db.ripe.net/db-web-ui/fulltextsearch)



Private and reserved addresses

Internet (RFC 1918) has reserved three blocks of IP addresses for "private networks". These addresses are destined for "watertight" networks not connected to the Internet. If they are released accidentally, they will be identified as such by routers

"Class A"	10.0.0.0 - 10.255.255.255
"Class B"	172.16.0.0 - 172.31.255.255
"Class C"	192.168.0.0 - 192.168.255.255

IPv4 reserved addresses (RFC 3330)

0.0.0.0/8	*"This" Network*	*[RFC1700, page 4]*
10.0.0.0/8	***Private-Use Networks***	***[RFC1918]***
14.0.0.0/8	*Public-Data Networks*	*[RFC1700, page 181]*
24.0.0.0/8	*Cable Television Networks*	*--*
39.0.0.0/8	*Reserved but subject to allocation*	*[RFC1797]*
127.0.0.0/8	***Loopback***	***[RFC1700, page 5]***
128.0.0.0/16	*Reserved but subject to allocation*	*--*
169.254.0.0/16	***Link Local****	
172.16.0.0/12	***Private-Use Networks***	***[RFC1918]***
191.255.0.0/16	*Reserved but subject to allocation*	*--*
192.0.0.0/24	*Reserved but subject to allocation*	*--*
192.0.2.0/24	*Test-Net*	
192.88.99.0/24	*6to4 Relay Anycast*	*[RFC3068]*
192.168.0.0/16	***Private-Use Networks***	***[RFC1918]***
198.18.0.0/15	*Network Interconnect Device Benchmark Testing*	*[RFC2544]*
223.255.255.0/24	*Reserved but subject to allocation*	*--*
224.0.0.0/4	*Multicast*	*[RFC3171]*
240.0.0.0/4	*Reserved for Future Use*	*[RFC1700, page 4]*

* Used by hosts in a watertight network. Obtained by auto-configuration (e.g. DHCP server not found)

Possible masks

The decimal values of **possible mask** bytes are as follows:

Mask byte	Decimal value
1000'0000	128
1100'0000	192
1110'0000	224
1111'0000	240
1111'1000	248
1111'1100	252
1111'1110	254
1111'1111	255

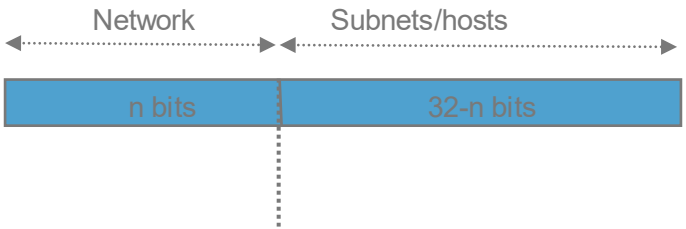
Note: masks are also frequently indicated by the number n of bits at "**1**" by **/n**.
For example, the mask of a class C address is /24. We speak of "*slash notation*", "CIDR *notation*" or " ***prefix***".

CIDR: *Classless Inter-Domain Routing*

Classful and *Classless*

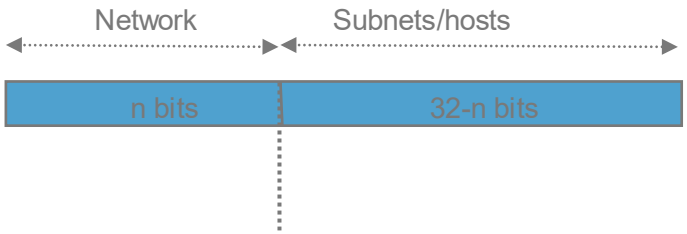
By extending the concept of *supernetting*, the CIDR can liberate classes:

Classful: respects classes A, B and C



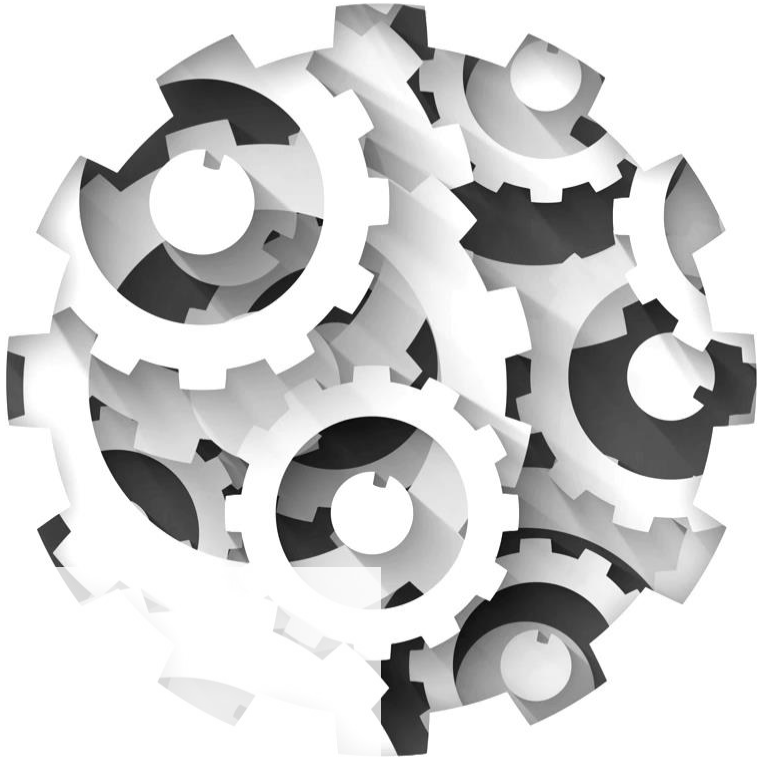
- Allocation of addresses as practiced up until the middle of the '90s
- Simple to administer
- Very quickly wastes addresses since there is no granularity as a function of the demanding network's size

Classless: ignores classes A, B and C

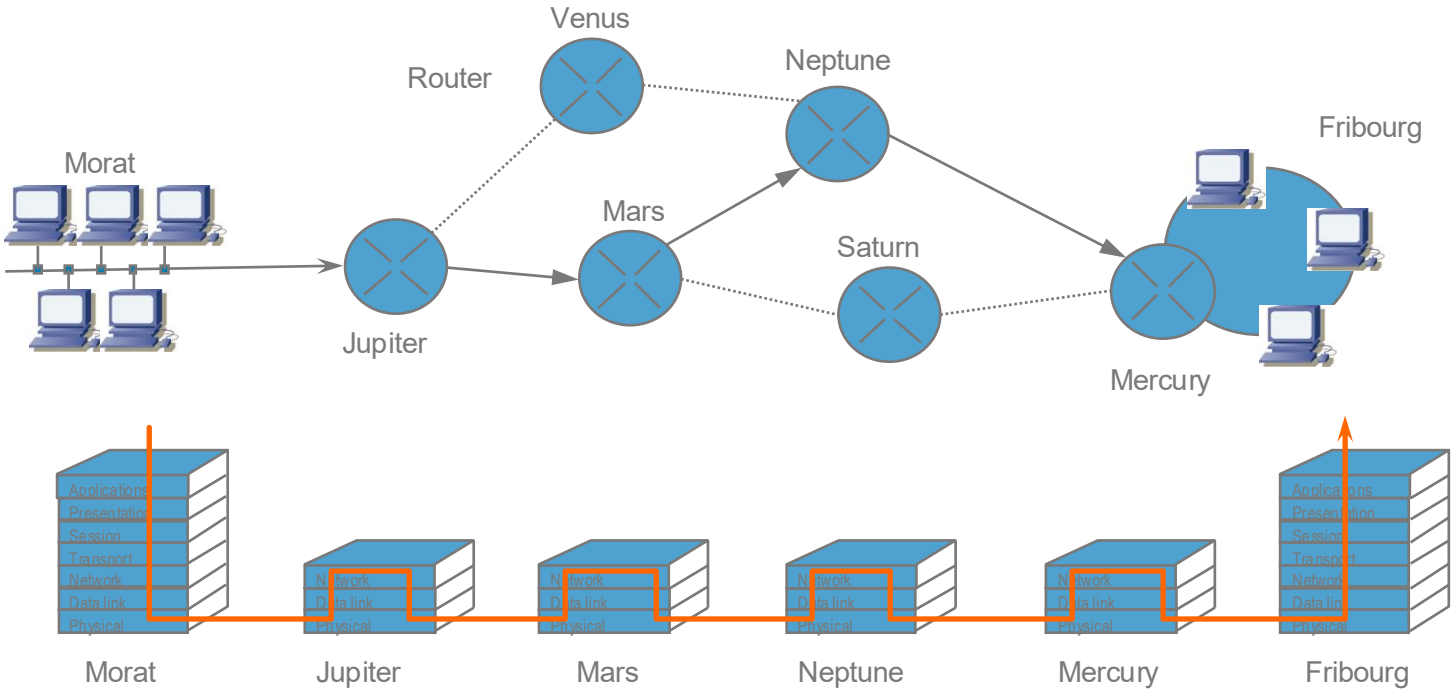


- Allocation of addresses through ISPs
- Network address from 3 to 32 bits
- Network addresses may be aggregated to form a "super address", which requires only one routing entry
- More complicated to administer
- Optimises address utilisation

Routing



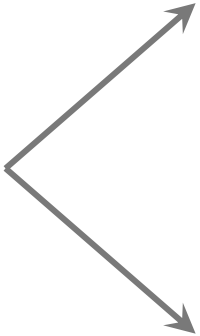
Routing



Routing: Transportation of packets from one end of a network to the other at the network layer level by selecting the path. Allows the interconnection of different networks.

Router operations (1)

Router functions

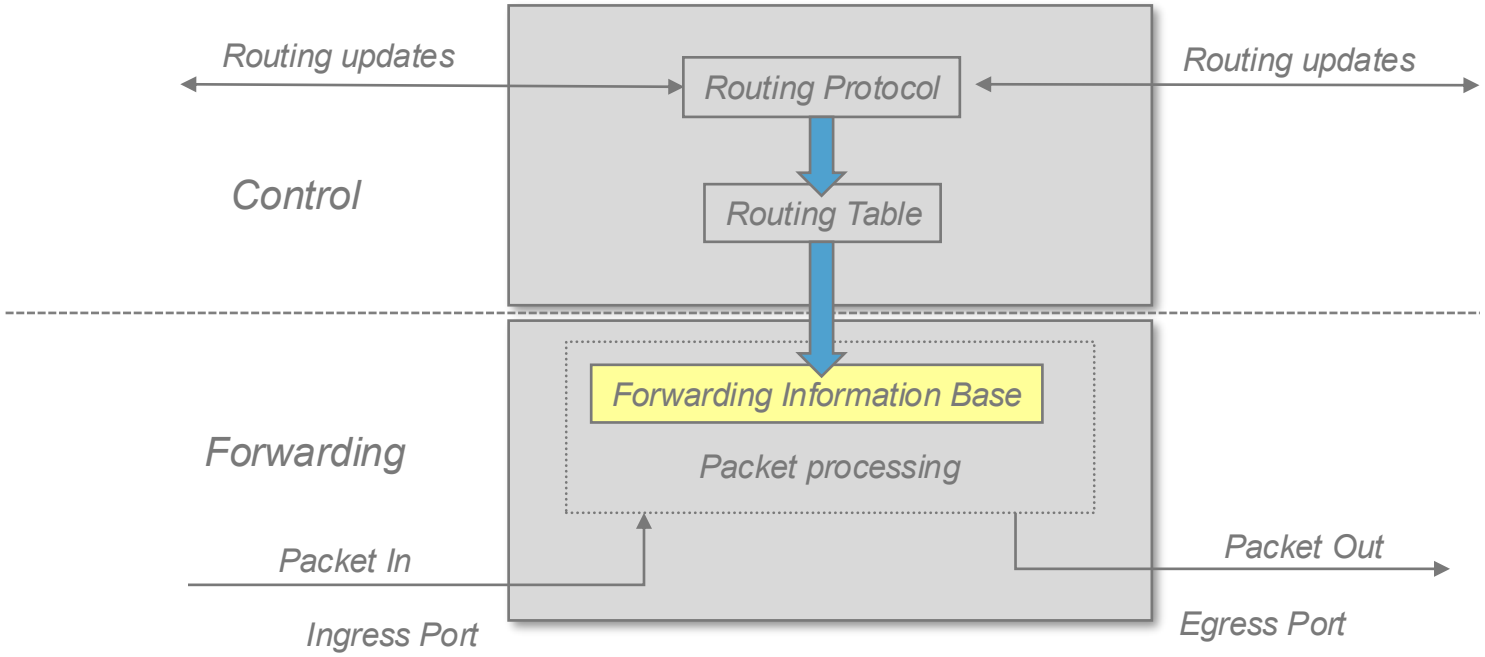


Management of the routing table (*control, control plane*). The routing table (*cache*) indicates the path to follow through the network by giving the address of the next router if the destination network is not connected directly. This routing table is either configured manually or established and managed by exchanging information about the network topology with other routers (routing protocol). Essentially SW.

Transfers (*forwarding, data plane*): Choice of the egress port as a function of the *Net prefix* based on the transport table (*Forwarding Information Base*) extracted from the routing table. The transport table gives the egress port and the address of the next router directly as a function of the *Net Prefix*.

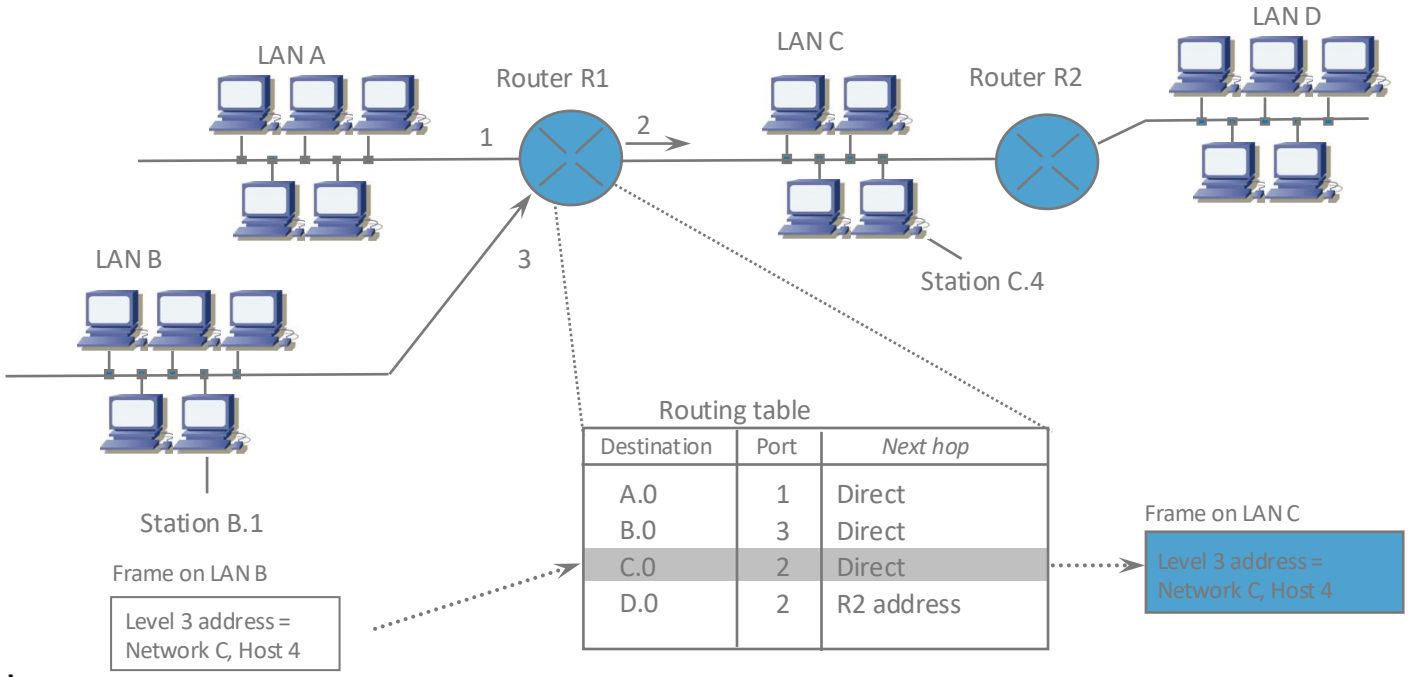
Modification of the packet header, if necessary. With IP, the time to live field must be incremented backwards and the error control field recalculated. Transmission of the packet via the egress port chosen. Essentially HW.

Router operations (2)



Routing table

Hosts: B.1, C.4, …
Networks/*Subnets:* A.0, B.0, C.0, D.0

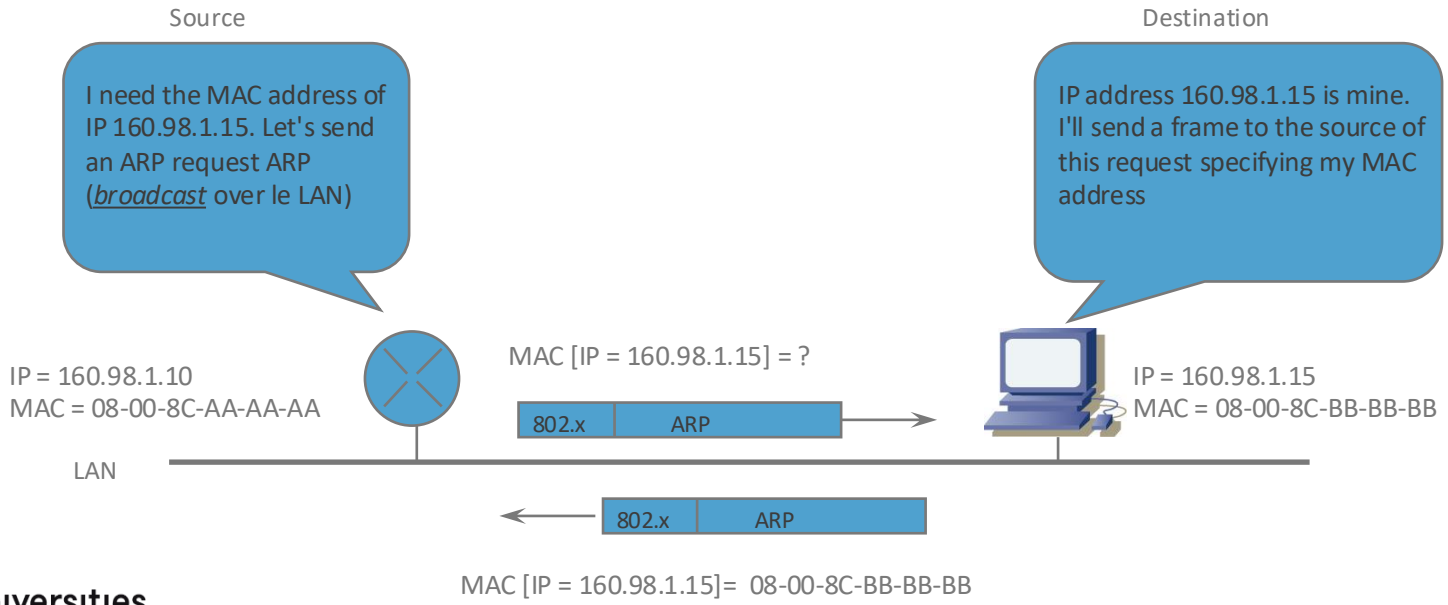


Direct, Indirect and Default Routing

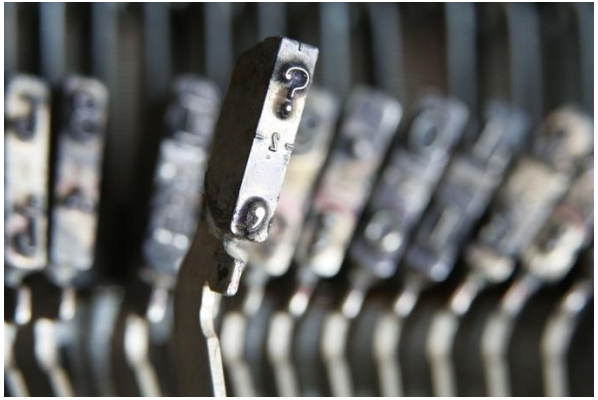
Direct	Routing to a destination that resides on the same network (same subnet as the egress port is connected on)
Indirect	Routing to a destination that resides on a remote network, using a table that specify the first router to use to reach this destination.
Default	Indirect routing through a default router (destination address is not found in the routing table of the source host). Identified with the IP address : 0.0.0.0

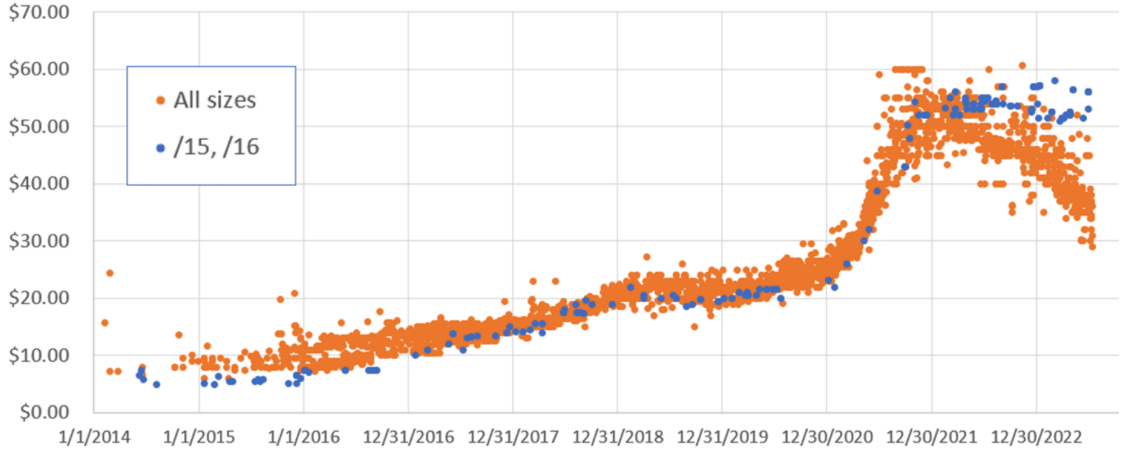
ARP (Address Resolution Protocol)

Address Resolution Protocol (ARP, RFC 826): to find the MAC address based on the IP address when the source and destination are on the **same** *subnet*



Why IPv4?



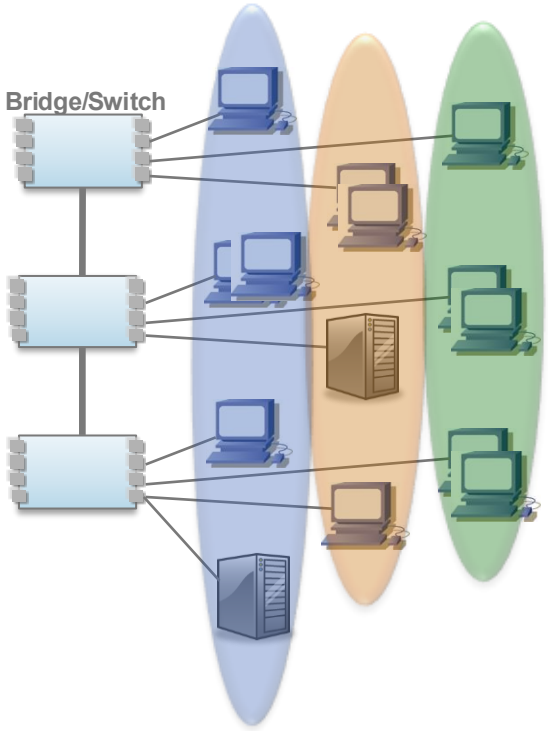


Source : https://circleid.com/posts/20230817-ipv4-prices-supply-and-demand-in-2023 (data by IPv4.Global)

Virtual LAN : Definition

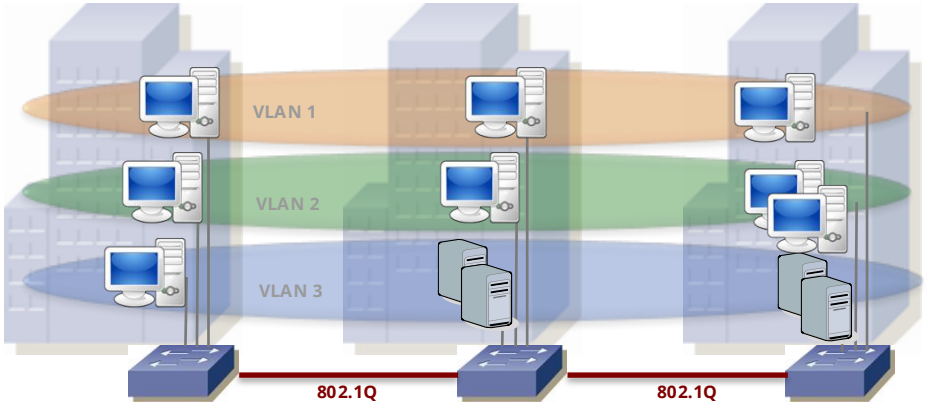
A **VLAN** (*Virtual Local Area Network*) could be define as:

- Group of hosts that are not sharing a physical medium, but that have the impression to do it. (Physical location of host is distributed)
- Hosts are connected trough *switches* that support Virtual LANs
- Hosts are communicating through the use of MAC addresses, without crossing a router
- The different VLANs are separated by routers
- A broadcast frame is sent to all stations of a VLAN (limited diffusion)
- Modern design has 1 VLAN = 1 IP Subnet



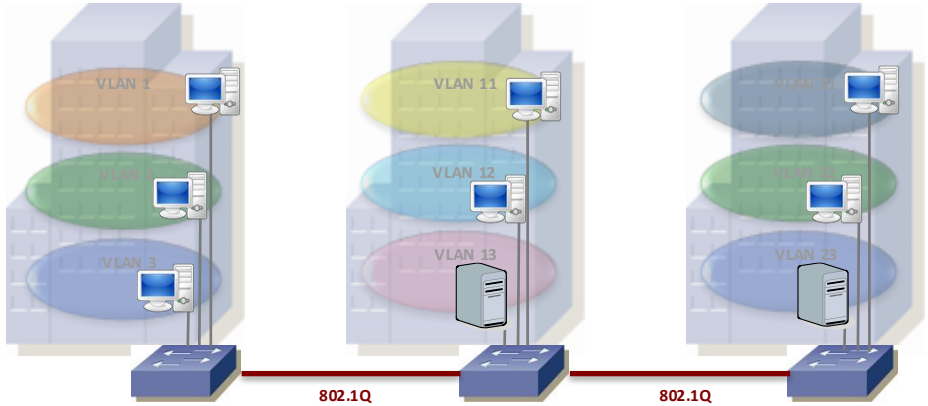
End-to-End VLANs

- Each VLAN is distributed geographically throughout the network.
- Users are grouped into each VLAN regardless of the physical location, theoretically easing network management.
- As a user moves throughout a campus, the VLAN membership for that user remains the same.



Local VLANs

- Create local VLANs with physical boundaries in mind rather than job functions of the users.
- Local VLANs exist between the access and distribution layers.
- Traffic from a local VLAN is routed at the distribution and core levels.
- Spanning tree is used only to prevent inadvertent loops in the wiring closet.
- One to three VLANs per access layer switch recommended.

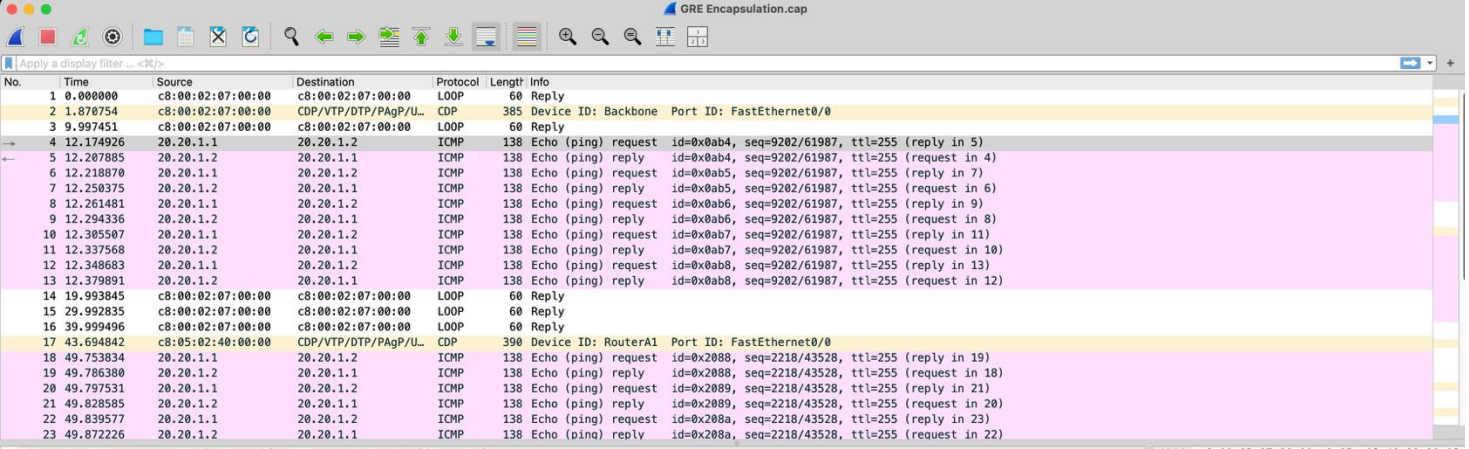


Advantages and disadvantages of VLANs

- ↗ *Broadcasts* stay inside a VLAN, better bandwidth usage
- ↗ Users and hosts are not grouped based on their physical location (LAN cabling), but on a logical base (functions, organization, protocols, IP Subnets, etc.). Changes are then simplified
  - → Grouped by virtual organization.
- ↗ **Security**: by isolating a group of users, we can more easily check the access to network resources.
- ↗ Cost: we use all the ports of all switches !
- ↘ VLAN Management could be complex : standards knowledge, trainings, etc.
- ↘ Administration protocols used by the control plane (supervision and configuration protocols) are consuming bandwidth
- ↘ On layer 3 VLANs, address attribution with DHCP could be problematic
- ↘ Cohabitation of proprietary standards (ISL, VTP, ..) and official standards (802.1Q, 802.1P,…) could also be problematic

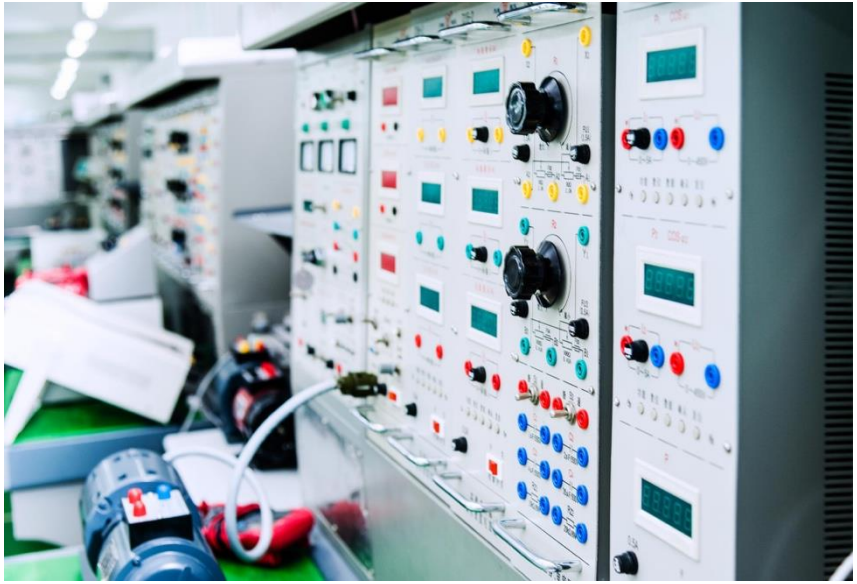
Wireshark

As well as *tshark* (or *tcpdump* or…)




```
ubuntu@ip-172-31-26-215:~/working$ tshark -r dnscat2.pcap -T fields -E header=y
 -e ip.src -e ip.dst -e ip.proto -e udp.dstport -e ip.len -e frame.time_delta_d
isplayed ip.dst==165.227.88.15 | head -20
ip.src  ip.dst  ip.proto        udp.dstport     ip.len  frame.time_delta_displa
yed
192.168.88.2    165.227.88.15   17      53      89      0.000000000
192.168.88.2    165.227.88.15   17      53      89      1.074819358
192.168.88.2    165.227.88.15   17      53      89      1.084471967
192.168.88.2    165.227.88.15   17      53      89      1.078728781
192.168.88.2    165.227.88.15   17      53      89      1.069749570
192.168.88.2    165.227.88.15   17      53      89      1.077714934
192.168.88.2    165.227.88.15   17      53      89      1.076642909
192.168.88.2    165.227.88.15   17      53      89      1.070790122
192.168.88.2    165.227.88.15   17      53      89      1.071048506
192.168.88.2    165.227.88.15   17      53      89      1.064914560
192.168.88.2    165.227.88.15   17      53      89      0.093778795
192.168.88.2    165.227.88.15   17      53      89      0.961346162
192.168.88.2    165.227.88.15   17      53      89      1.062188142
192.168.88.2    165.227.88.15   17      53      89      1.065854491
192.168.88.2    165.227.88.15   17      53      89      1.075033821
192.168.88.2    165.227.88.15   17      53      89      1.066068845
192.168.88.2    165.227.88.15   17      53      89      1.063321512
192.168.88.2    165.227.88.15   17      53      89      1.071506357
192.168.88.2    165.227.88.15   17      53      89      1.058017495
ubuntu@ip-172-31-26-215:~/working$
```

Role of Communication



Facilitating Information Flow

Communication technology enables seamless information flow between different systems and devices, improving efficiency in operations.

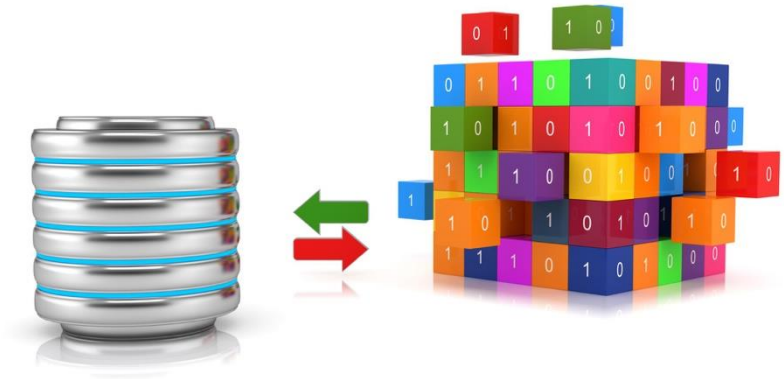
Enhancing Decision-Making

Effective communication technology supports better decision-making by providing real-time data and insights for operators and managers.

Promoting Operational Continuity

Reliable communication systems are essential for maintaining operational continuity, minimizing downtime, and ensuring productivity.

IT vs OT Needs



Focus Areas of IT

IT primarily deals with data management, business processes, and ensuring the integrity of information systems.

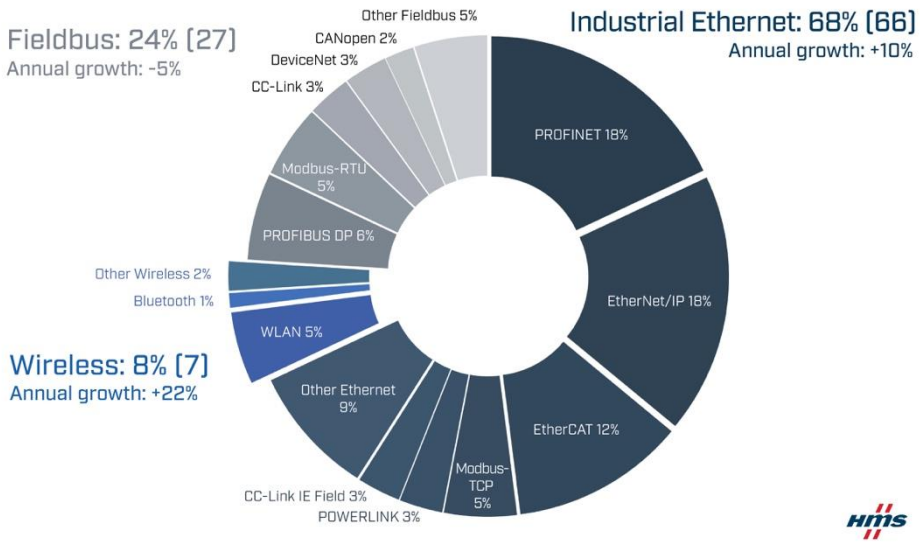
Focus Areas of OT

OT is focused on operational efficiency, safety and real-time performance in industrial settings ensuring smooth operations.

Importance of Understanding Differences

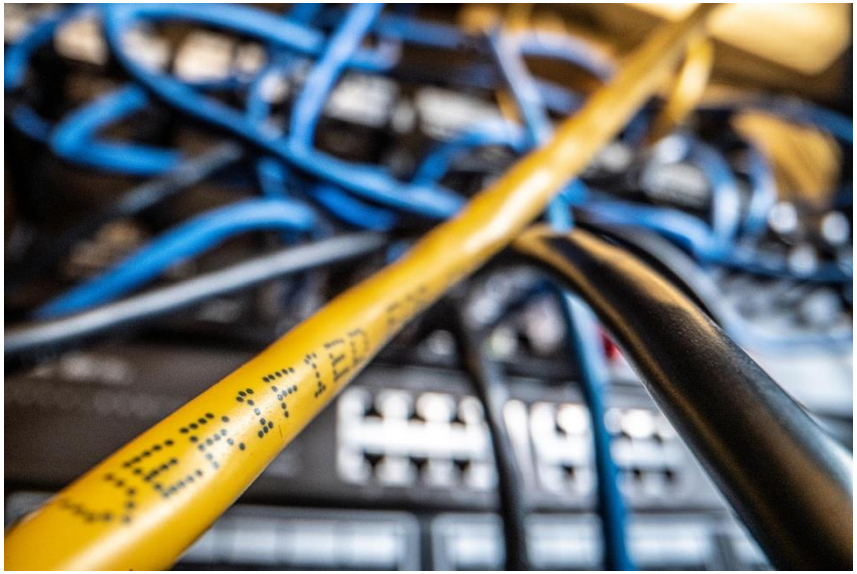
Recognizing the differences between IT and OT is crucial for implementing suitable communication technologies in OT environments.

Core Communication Technologies in OT



Source: https://www.hms-networks.com/

Wired Communication



Reliability of Wired Connections

Wired communication technologies, such as Ethernet, provide reliable connections essential for maintaining stability in data transfer.

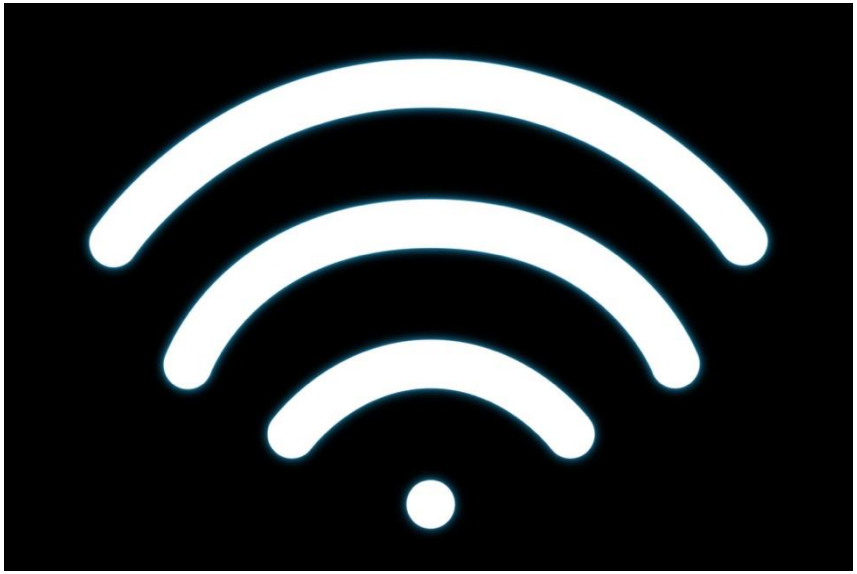
Speed of Data Transfer

Wired technologies are favored for their high-speed capabilities, crucial for real-time communication in industrial operations.

Importance in Industrial Settings

In industrial settings, wired communication is vital for ensuring stable and efficient operations, especially in real-time data scenarios.

Wireless Communication



Flexibility and Mobility

Wireless communication technologies enhance flexibility and mobility, allowing devices to connect without physical constraints.

Wi-Fi, Zigbee, WirelessHART and 5G Protocols

Protocols like Wi-Fi and Zigbee simplify installation and scalability in various applications, facilitating seamless connectivity.

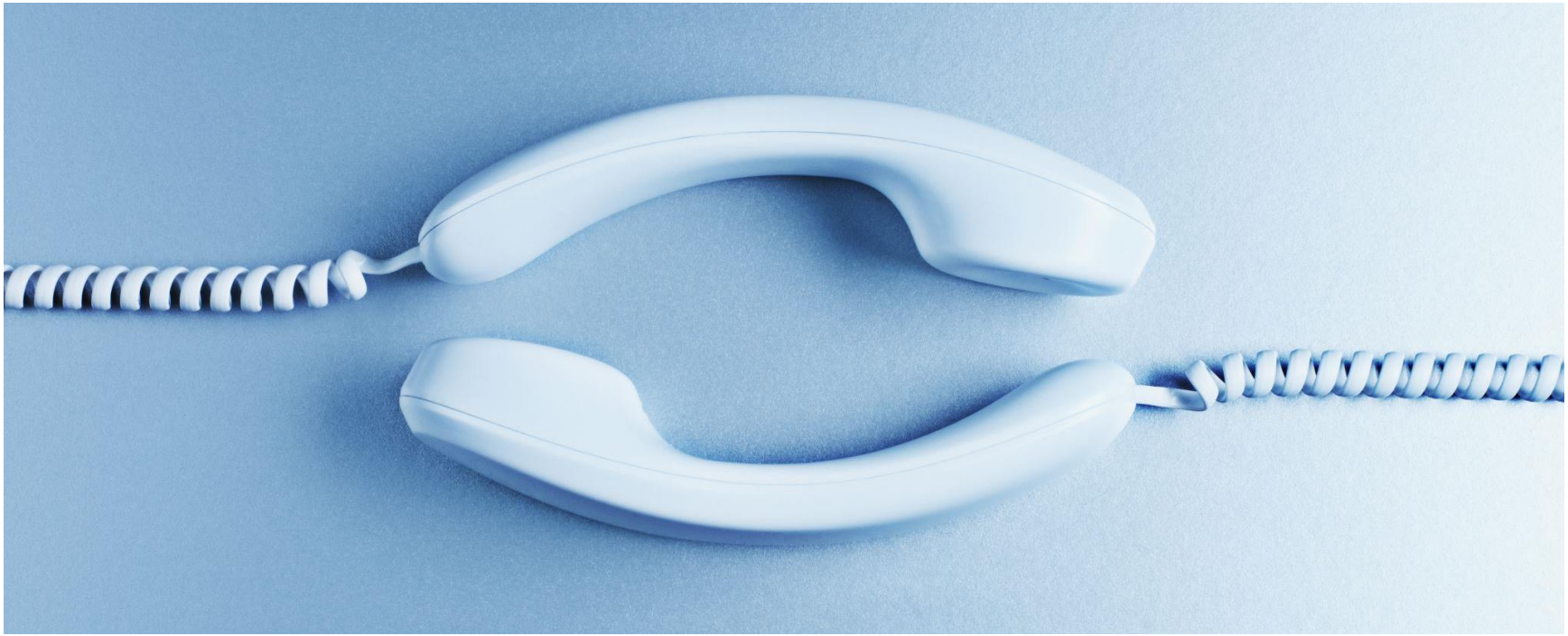
Interference and Security Challenges

Careful implementation of wireless technologies is critical to mitigate potential interference and security risks in operations.

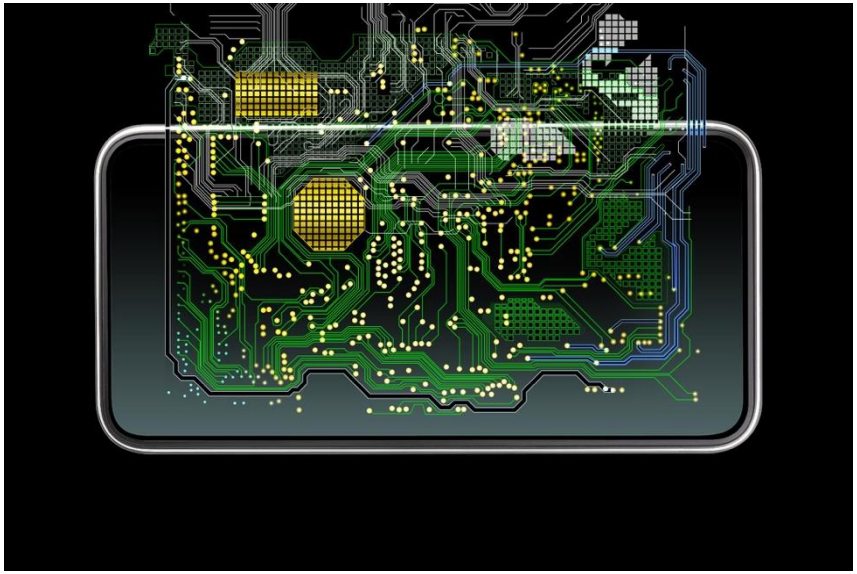
Requirements

- Determinism, Scalability, Reliability and Availability
- Latency
- Time synchronization
- Open Standards and Interoperability
- Security

Real-Time and Deterministic Communication in OT



Importance of Real-Time Communication



Timely Data Processing

Real-time communication is essential for timely data processing, ensuring that information is accurately and quickly transferred.

Control Actions in OT

Effective control actions in Operational Technology (OT) environments rely heavily on real-time communication to maintain system integrity.

Precision and Rapid Response

Applications requiring precise timing and rapid response, such as safety-critical operations, depend on robust real-time communication.

Quality of Service (QoS)

Prioritizing Network Traffic

QoS mechanisms are designed to prioritize network traffic, ensuring that critical data receives the bandwidth it requires for timely transmission.

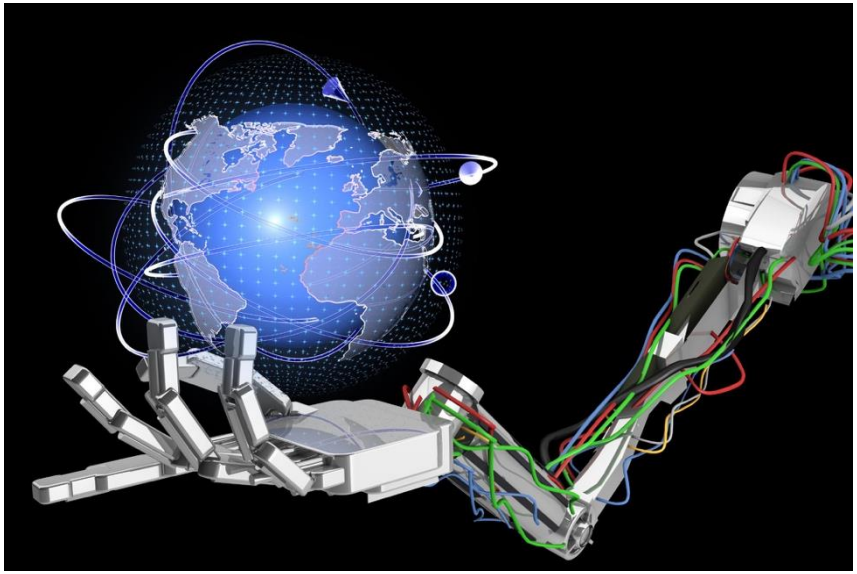
Minimizing Delay

Implementing QoS helps in minimizing delays for time-sensitive communications, which is crucial for operational effectiveness.

Operational Efficiency

QoS in operational technology (OT) communications is vital for maintaining overall operational efficiency and productivity.

Integration with RTOS



Efficient Task Management

Integrating RTOS with communication technologies enhances task management efficiency, essential for critical applications requiring timely processing.

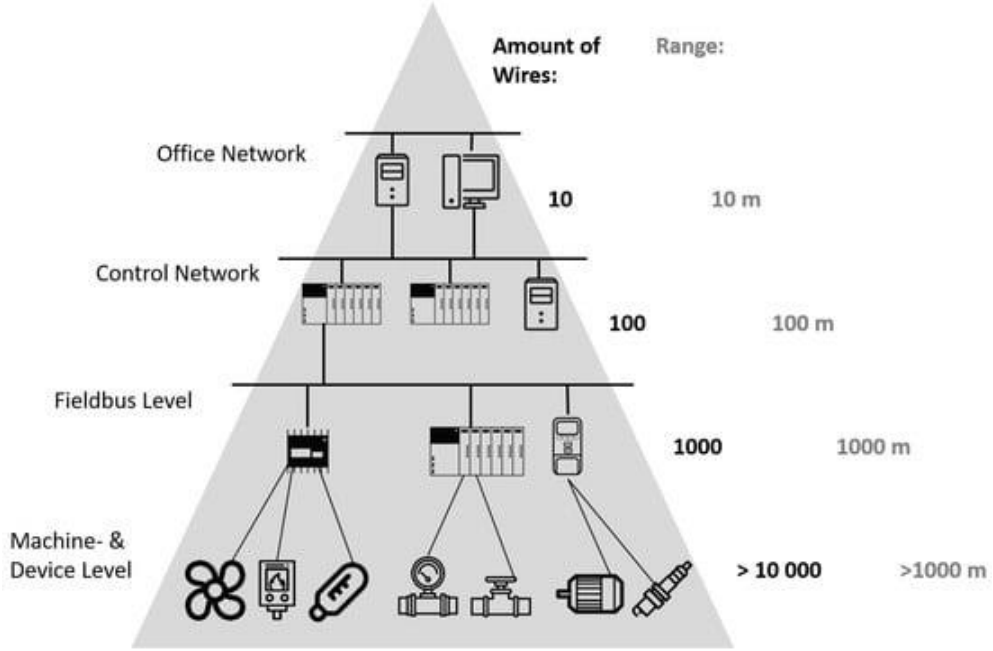
Resource Allocation

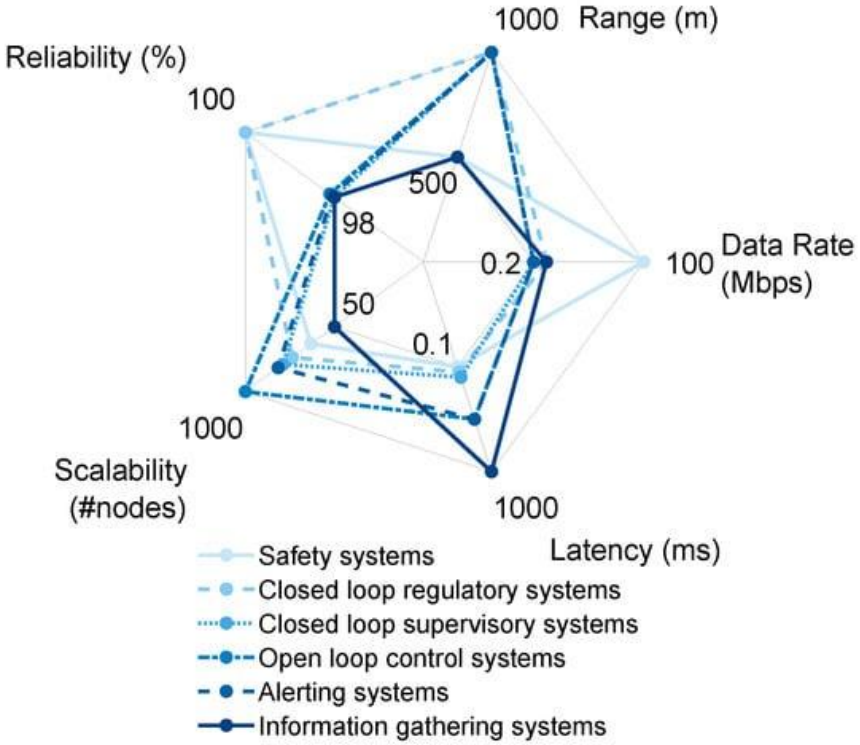
This integration optimizes resource allocation in operational technology environments, ensuring that resources are used effectively.

Real-Time Performance

The combination of communication technologies and RTOS is vital for applications that demand high real-time performance and reliability.

A 10000 feet overview





swissuniversities

Source: https://www.mdpi.com/1424-8220/20/2/488

A 10000 feet overview

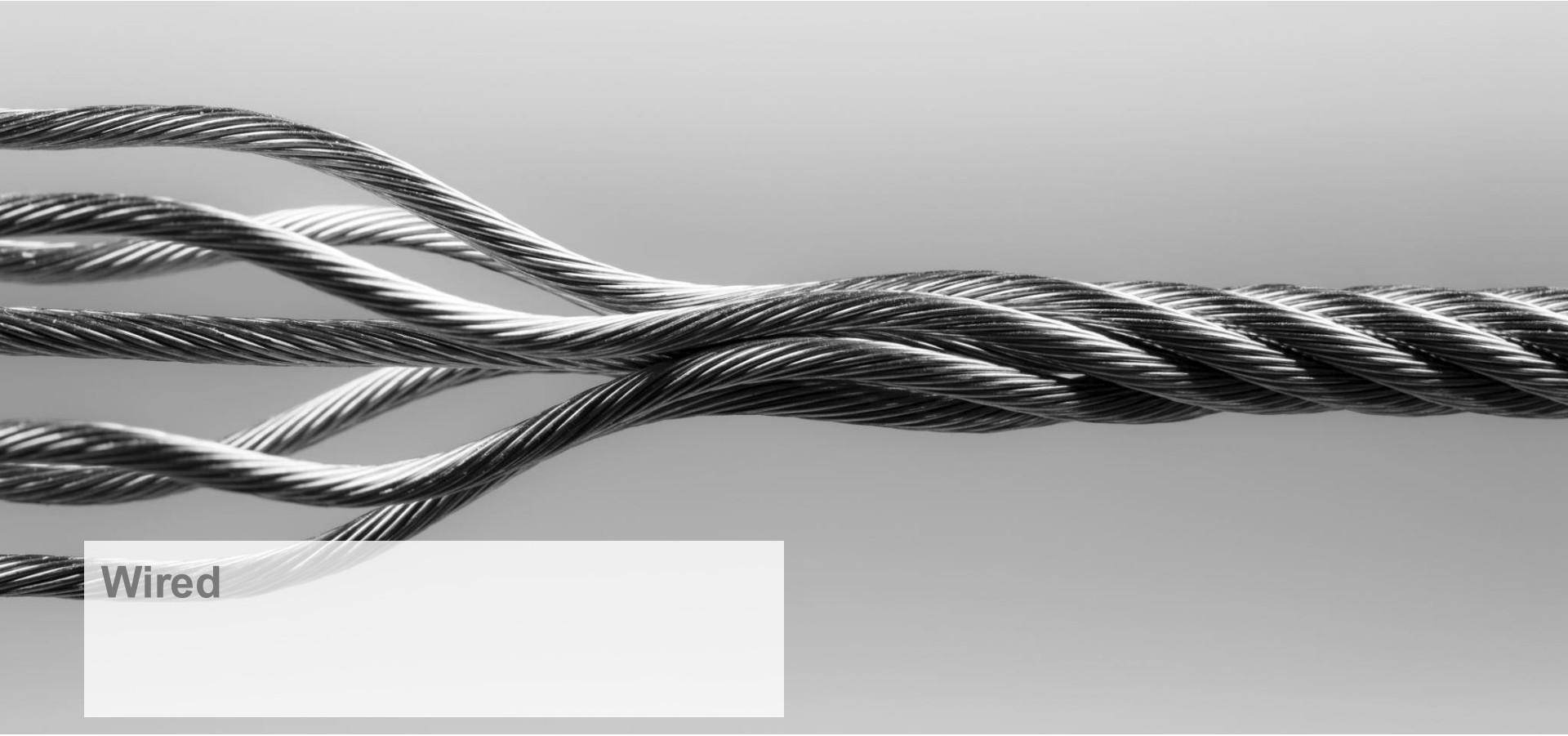
	Scenario Class	References	Predictability Requirement	Latency Requirement	Bandwidth Requirement	Wireless Communication
I	Autonomous Vehicles & Mobile Robots	[1, 9–13]	high	medium	variable	essential
II	Remote Control of Machines	[14–18]	high	high	low	not necessary
III	Sensor Data Analysis & Monitoring	[7, 19–22]	low	low	high	not relevant
IV	Worker Safety & Hazard Protection	[23–26]	high	high	low	not necessary
V	Task Offloading	[27–31]	medium	medium	high	not relevant
VI	Industrial Wearable Systems & Augmented Reality	[32–37]	low	medium	high	essential

	Security	Determinism	Bandwidth		Relevant Scenarios I	II	III	IV	V	VI
Fieldbuses										
CAN	E	10 ms	1 Mbps	[48, 49]	✗	✓	✗	✓	✗	✗
CAN-FD	E	100 μs	5 Mbps	[50]	✗	✓	✗	✓	✗	✗
Modbus	E	10 ms	115 kbps	[49]	✗	✓	✗	✓	✗	✗
PROFIBUS	E	10 ms	12 Mbps	[49, 51]	✗	✓	(✓)	✓	(✓)	✗
Wired network										
Modbus TCP	E	45μs (ideal conditions)	100 Mbps	[52]	✗	(✓)	✓	✓	✓	✗
PROFINET	E	10-100 ms	1 Gbps	[53]	✗	(✓)	✓	(✓)	✓	✗
EtherNet/IP	E	1-2 ms	1 Gbps	[54]	✗	✓	✓	✓	✓	✗
TSN CBS	E,A	2 / 50 ms	40 Gbps	[55]	✗	(✓)	✓	✓	✓	✗
EtherCAT	E	34 μs	10 Gbps	[56]	✗	✓	✗	✓	(✓)	✗
TTEthernet	E,A	low, μs (offline schedule)	1 Gbps	[55]	✗	✓	✓	✓	(✓)	✗
TSN ST	E,A	100 μs	40 Gbps	[55]	✗	✓	(✓)	✓	(✓)	✗
Wireless network										
WirelessHART	I,C,A	10 ms	250 kbps	[57]	✓	(✓)	✗	(✓)	✓	✗
ISA 100.11a	I,C,A	10 ms	250 kbps	[57]	✓	(✓)	✗	(✓)	✓	✗
Bluetooth 5.0	I,C,A	10-100 ms	48 Mbps	[58]	✗	✗	✓	✗	(✗)	(✓)
WLAN 6	I,C,A	1 ms (ideal conditions)	9.6 Gbps	[59, 60]	(✓)	✗	✓	✗	(✓)	✓
5G eMMB	I,C,A	10-100 ms	10 Gbps	[60]	✗	✗	✓	✗	(✓)	(✓)

Source: https://ieeexplore.ieee.org/abstract/document/10317890

Security

1. ***External:*** The protocol relies on external security measures.
2. ***Integrity:*** Messages are accompanied by robust checksums to detect modification.
3. ***Confidentiality:*** Each message is encrypted using a secret known only to authorized parties.
4. ***Secure Authentication and Authorization:*** Each node on the system must be securely identified before being granted access to the network.


Wired

Fieldbus

" A fieldbus is a member of a family of industrial digital communication networks used for real-time distributed control. Fieldbus profiles are standardized by the International Electrotechnical Commission (IEC) as IEC 61784/61158.

A complex automated industrial system is typically structured in hierarchical levels as a distributed control system (DCS).

In this hierarchy the upper levels for production managements are linked to the direct control level of programmable logic controllers (PLC) via a non-time-critical communications system (e.g. Ethernet).

The fieldbus links the PLCs of the direct control level to the components in the plant of the field level such as sensors, actuators, electric motors, console lights, switches, valves and contactors and replaces the direct connections via current loops or digital I/O signals. The requirement for a fieldbus are therefore
time-critical and cost sensitive.

Since the new millennium a number of fieldbuses based on Real-time Ethernet have been established. These have the potential to replace traditional fieldbuses in the long term. "

Source: https://en.wikipedia.org/wiki/Fieldbus

Fieldbus

Section	Title
IEC 61158-1	Overview and guidance for the IEC 61158 series
IEC 61158-2	Physical Layer specification and service definition
IEC 61158-3	Data Link Service definition
IEC 61158-4	Data Link Protocol specification
IEC 61158-5	Application Layer Service definition
IEC 61158-6	Application Layer Protocol specification
IEC 61158-7	Network management

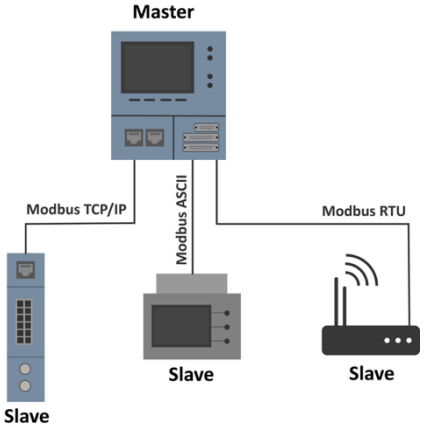
Section	Description
IEC 61784-1	Communication Profiles (CP) for continuos and discrete manufacturing on Fieldbus
IEC 61784-2	Additional CPs for 802.3 utilization in manufacturing

Communication Profile Families	Based on	Brand name
CPF-3	Fieldbus	Profibus
CPF-5	Fieldbus	World-FIP
CPF-12	Ethernet 802.3	EtherCAT
CPF-13	Ethernet 802.3	Ethernet PowerLink
CPF-15	Ethernet 802.3	Modbus

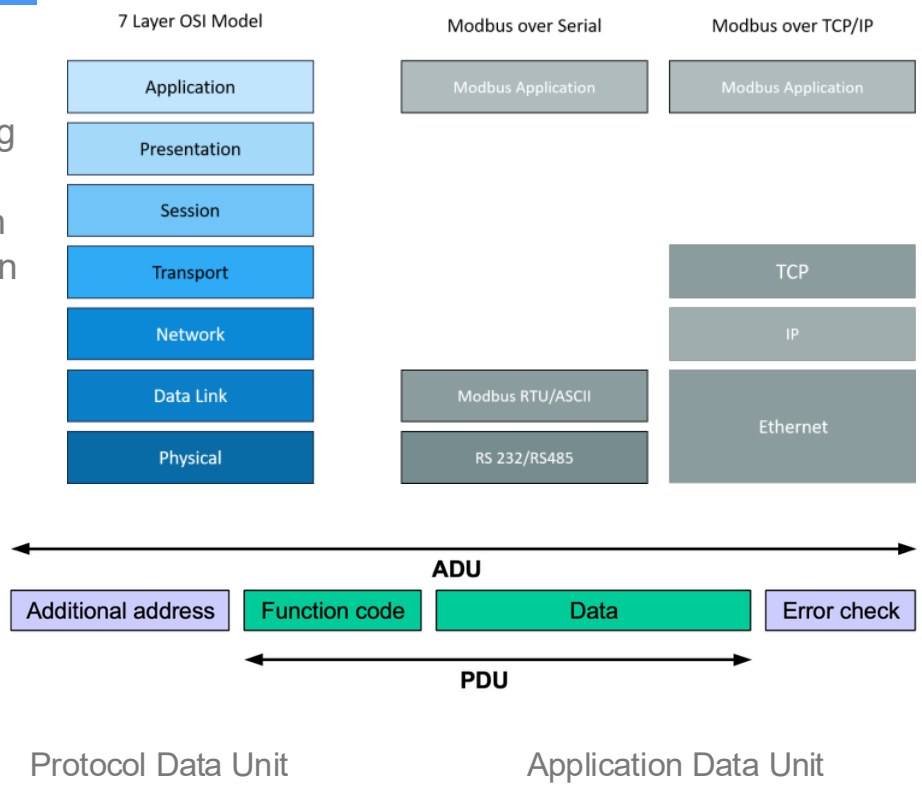
The Fieldbus War: History or Short Break Between Battles?

MODBUS (I)

- One of the de facto standards for connecting a wide range of devices, including sensors, actuators, and controllers, in industries such as manufacturing, energy, and transportation
- Simple client server protocol that operates with limited computing resources

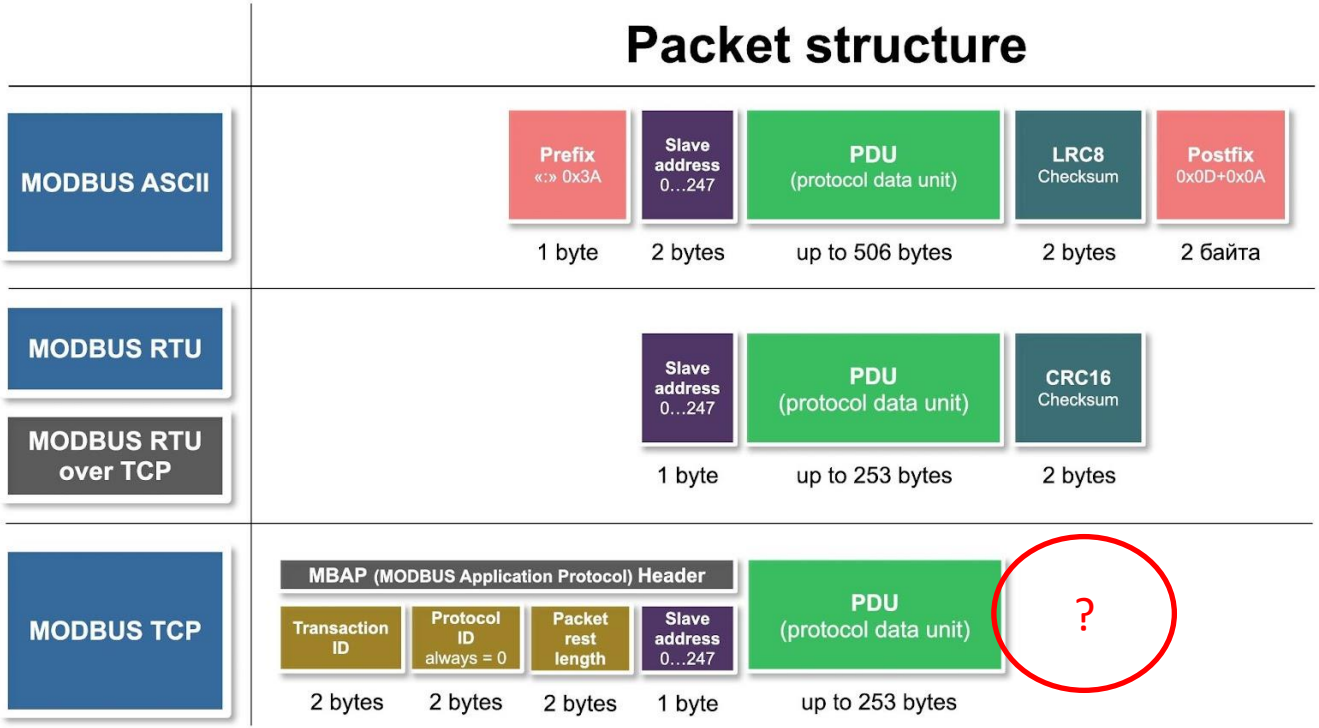


Source: https://www.dewetron.com/news/what-is-modbus-and-how-does-it-work/



Source: https://www.modbus.org/

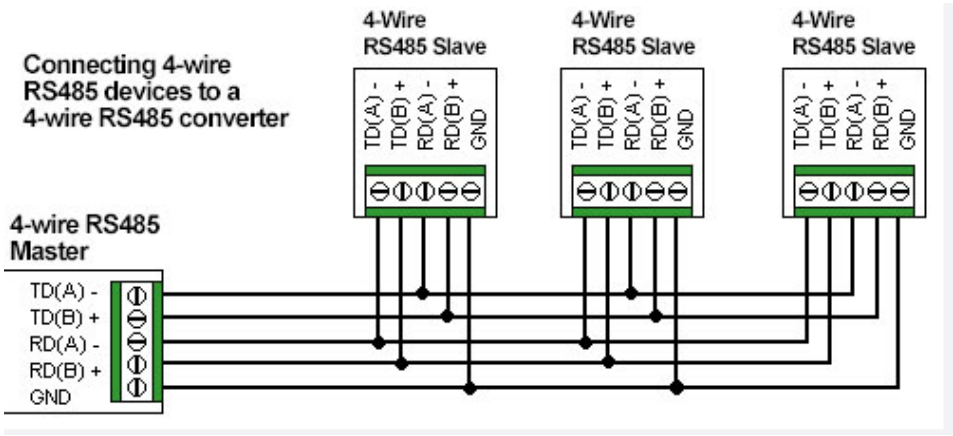
MODBUS (IV)



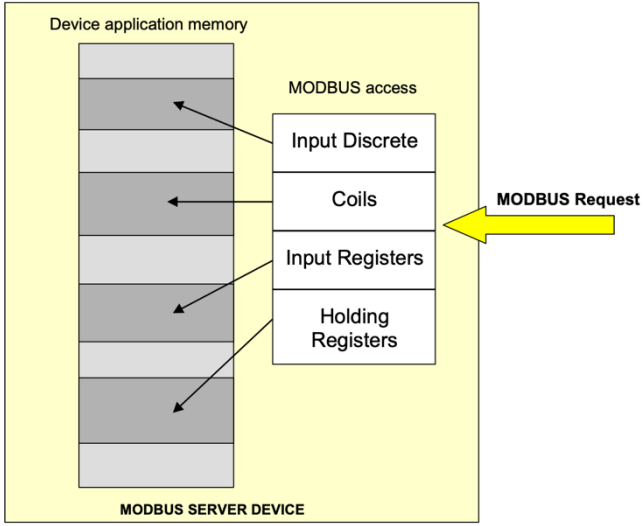
Source: https://hackaday.io/project/190514-diy-modbus-tcprtu-gateway-with-wifi/details

MODBUS (II)

Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.



Source : https://www.se.com/au/en/faqs/FA213223/



Source: https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

MODBUS (III)

Request

Function code	1 Byte	**0x01**
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of coils	2 Bytes	1 to 2000 (0x7D0)

Response

Function code	1 Byte	**0x01**
Byte count	1 Byte	**N***
Coil Status	**n** Byte	n = N or N+1

Request

Function code	1 Byte	**0x02**
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of Inputs	2 Bytes	1 to 2000 (0x7D0)

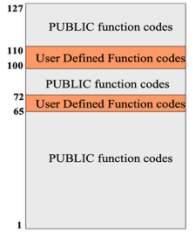
Response

Function code	1 Byte	**0x02**
Byte count	1 Byte	**N***
Input Status	**N*** x 1 Byte	

***N** = Quantity of Inputs / 8 if the remainder is different of 0 ⇒ N = N+1

Error

Error code	1 Byte	**0x82**
Exception code	1 Byte	01 or 02 or 03 or 04



Function Code	Name	Description
0	0	No address information is present
1	Read Coils	Read the status of discrete coils in a device
2	Read Discrete Inputs	Read the status of input registers in a device
3	Read Multiple Registers	Read the status of multiple holding registers in a device
16	Write Multiple Registers	Write a series of holding registers in a device
4	Read Input Registers	Read the status of multiple input registers in a device
5	Write Single Coil	Write a single coil in a device
6	Write Single Register	Write a single register in a device
7	Read Exception Status	Read information about the last exception
15	Write Multiple Coils	Can be used to set multiple coil values in a single go
20	Read File Record	Read a file record information
21	Write File Record	Write a file record information
22	Mask Write Register	Write a holding register after applying AND & OR masks
23	Read/Write Multiple Registers	Performs a write after read operation
24	Read FIFO	Reads from the device FIFO
43	Read Device Identification	Fetch information about the device including vendor name, product code, versions etc.

Source: https://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

MODBUS (V)

No Safety, No Realtime

Advantages

- Simplicity: its relative simplicity and ease of implementation, makes it accessible to developers and engineers with varying levels of expertise.
- Interoperability: open standard protocol supported by a wide range of devices from different manufacturers.
- Cost-Effectiveness: typically requires minimal hardware and software resources.
- Flexibility: supports various communication media, including serial (RS-232, RS-485) and Ethernet networks.
- Wide Adoption: has been around for several decades and is widely adopted in the industrial automation industry resulting in a large community of developers, engineers and vendors providing ample resources and support.

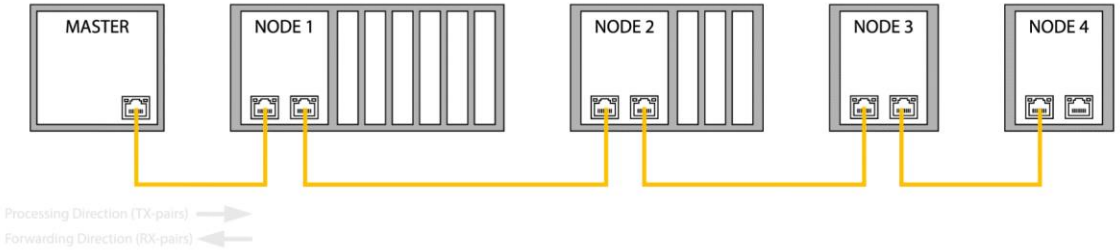
Disadvantages

- Limited Bandwidth: is a serial communication protocol and may have limited bandwidth compared to newer protocols designed for Ethernet networks. This limitation can impact data transmission, especially in large-scale systems.
- No Built-in Security or Redundancy: does not include built-in security features such as encryption or authentication.
- Limited Error Handling: it includes basic error checking mechanisms such as CRC (Cyclic Redundancy Check), it may not be sufficient to detect and recover from more complex communication errors.
- Limited Address Space: Modbus uses a 16-bit address space, imposing limitations on the number of devices and data points that can be addressed in a network
- No Support for Complex Data Types: supports simple data types such as integers and floating-point without native support for complex data structures.
- Polling Overhead: communication typically relies on polling mechanisms, consuming network bandwidth and not suited for high-speed or real-time applications.

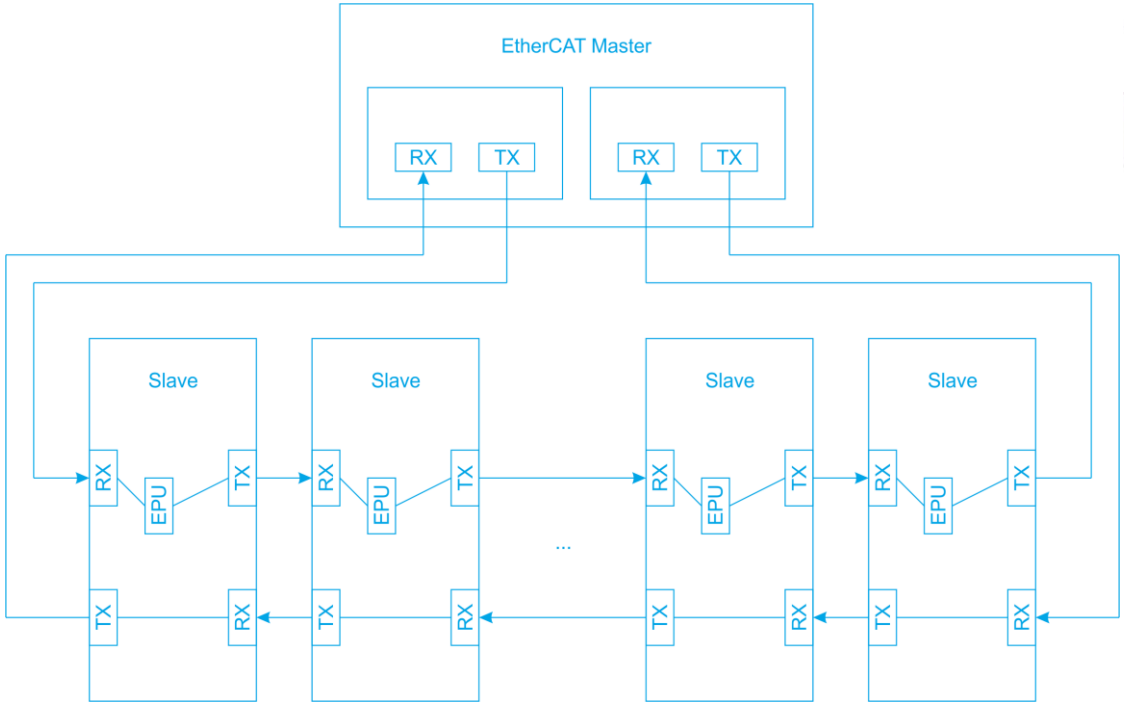
A Real-Time Alternative

EtherCAT (I) – A Fieldbus

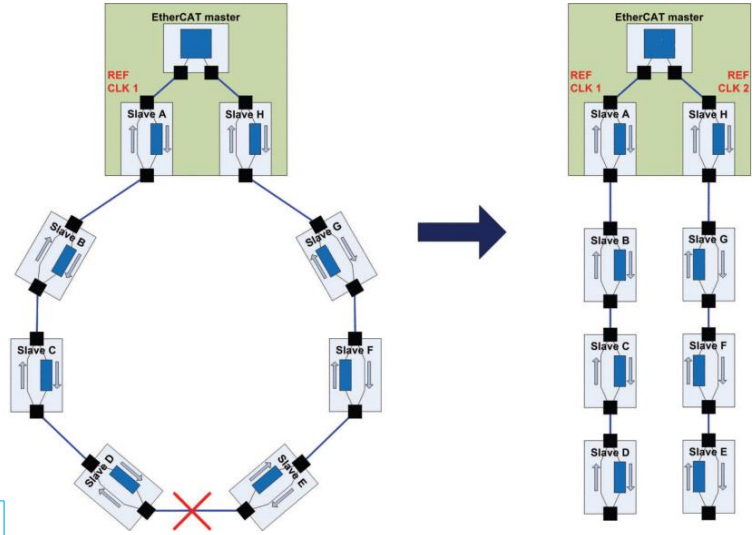
- Ethernet for **C**ontrol **A**utomation **T**echnology
- A real-time Ethernet solution
- Topology agnostic
- Support up to 2^{16} devices (65k)
- Synchronization through Distributed Clocks
- IEC 61158



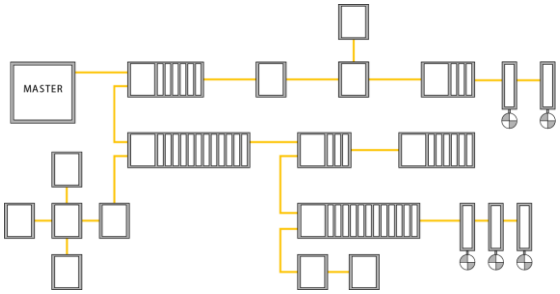
EtherCAT (II)



Source: https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_io_intro/1446583307.html&id=



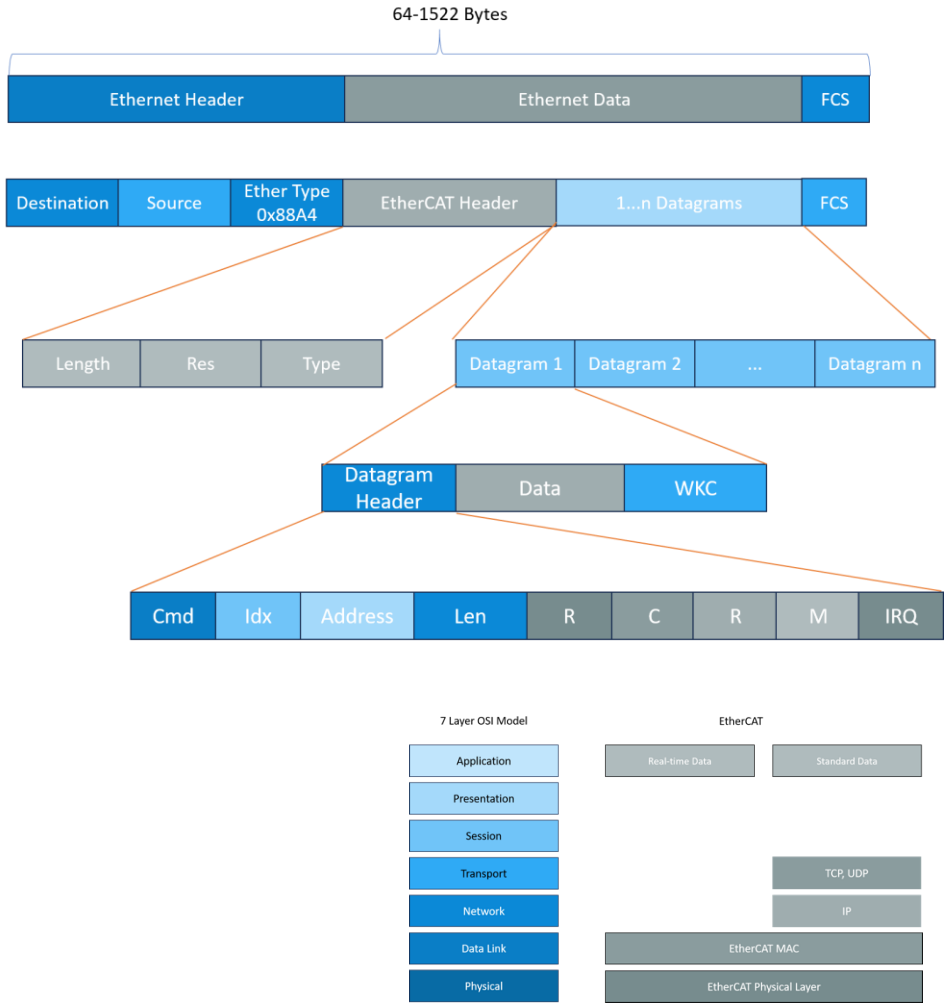
Source : https://ieeexplore.ieee.org/document/5551386



Source: https://www.acontis.com/en/what-is-ethercat-communication-protocol.html

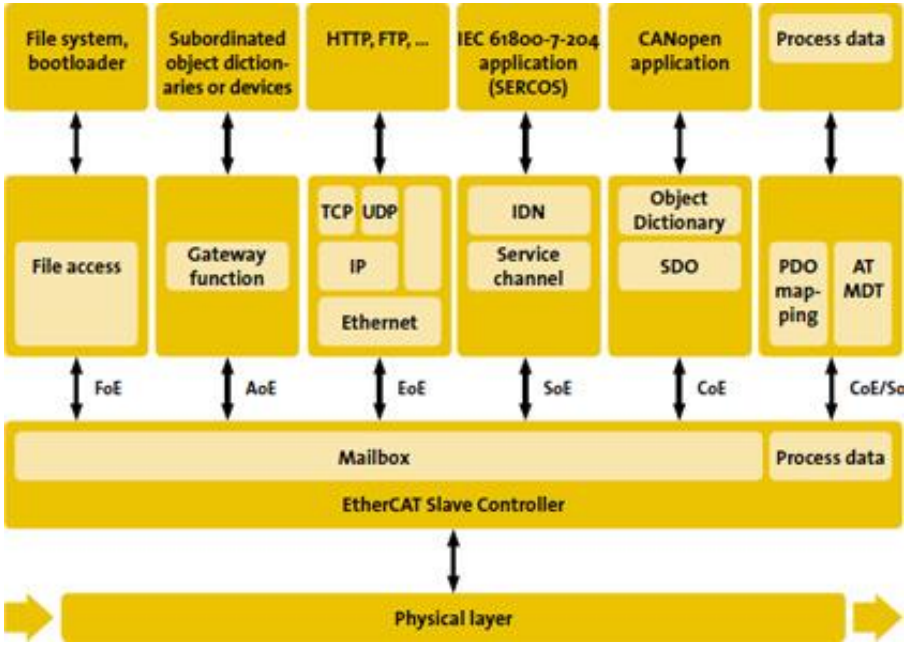
EtherCAT (III)

Field	Data type	Value/Description
Cmd	BYTE	EtherCAT command type
Idx	BYTE	The index is a numerical identifier used by the master to identify duplicates or lost datagrams. The EtherCAT slaves should not change the index.
Address	BYTE[4]	Address: auto-increment, configured station address or logical address
Len	11 bits	Length of the data following within this datagram
R	3 bits	Reserved, 0
C	1 bit	Circulating frame: 0: Frame does not circulate 1: Frame has circulated once
M	1 bit	Multiple EtherCAT datagrams 0: Last EtherCAT datagram 1: At least one further EtherCAT datagram follows
IRQ	WORD	EtherCAT event request register of all slave devices combined with a logical OR
Data	BYTE[n]	Data to be read or written
WKC	WORD	Working Counter



Source: https://www.embien.com/industrial-insights/comprehensive-guide-to-the-ethercat-protocol

EtherCAT (IV)



- Cyclic
  - Can access data (R, W)
  - See EtherCAT command types

Cmd	Abbreviation	Name	Description
1	APRD	Auto Increment Read	A slave increments the address. A slave writes the data it has read to the EtherCAT datagram if the address received is zero.
2	APWR	Auto Increment Write	A slave increments the address. A slave writes data to a memory area if the address received is zero.
3	APRW	Auto Increment Read Write	A slave increments the address. A slave writes the data it has read to the EtherCAT datagram and writes the newly acquired data to the same memory area if the received address is zero.
4	FPRD	Configured Address Read	A slave writes the data it has read to the EtherCAT datagram if its slave address matches one of the addresses configured in the datagram.
5	FPWR	Configured Address Write	A slave writes data to a memory area if its slave address matches one of the addresses configured in the datagram.

- Acyclic
  - Different profiles may be used as per application needs

  See image on the left

CoE: CANopen over EtherCAT, SoESERCOS over EtherCAT, FoE: File over EtherCAT, EoE: Ethernet over EtherCAT, AoE: ADS over EtherCAT

EtherCAT (IV) - Comparison

	ETHERNET	ETHERCAT
Common Physical and Data Link Layers	Yes	Yes
International Standard	IEEE-802.3	IEC 61158
Deterministic Timing	No	Yes
Master/Slave Operation	No	Yes
Ring-based Topology	Not required	Yes
Optimized for real-time control	No	Yes
Optimized to avoid data collisions	No	Yes

Source: https://dewesoft.com/blog/what-is-ethercat-protocol

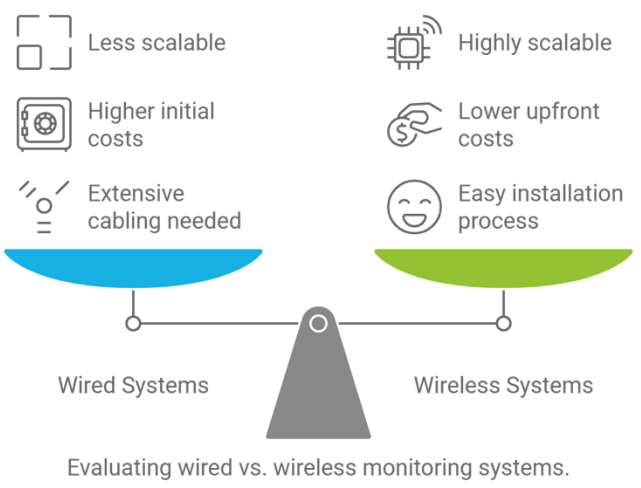
Advantages

- **Real-Time Communication**: Microsecond-level communication cycles support high-speed real-time control.
- **Cost-Efficiency**: Built on standard Ethernet hardware.
- **Scalability**: Supports networks with a wide range of node counts.
- **Flexible Topologies**: Adapts to diverse application needs with multiple topology options.
- **High Reliability**: Redundancy features ensure system robustness.

Challenges

- **Complex Network Design**: Large-scale systems require careful network design and planning.
- **Device Compatibility**: Only devices supporting EtherCAT protocols are compatible.
- **Integration and Debugging**: The real-time and high-efficiency nature of EtherCAT can require advanced tools and expertise for system integration and debugging.

Wireless



Evaluating wired vs. wireless monitoring systems.

Source: https://www.packetpower.com/blog/wired-vs-wireless-monitoring-systems

Critical Factors

- Limited energy capacity
- Hardware resource constraints
- Dynamic network
- Node deployment
- Sensor Location
- Fault tolerance
- Latency
- Data aggregation
- Scalability

	Bluetooth	WiFi	Zigbee	6LoWPAN	IrDA
Nominal range	10m	100m	100m	100m	1m
Nominal Tx power	-20 to 10 dBm	15 to 20 dBm	-25 to 0 dBm	-25 to 0 dBm	approx. 40 mW
Typical power consumption	Less than 10 mW (BLE)	250 mW	250 mW	250 mW	10 mW

Source: http://www.jestr.org/downloads/Volume13Issue1/fulltext101312020.pdf

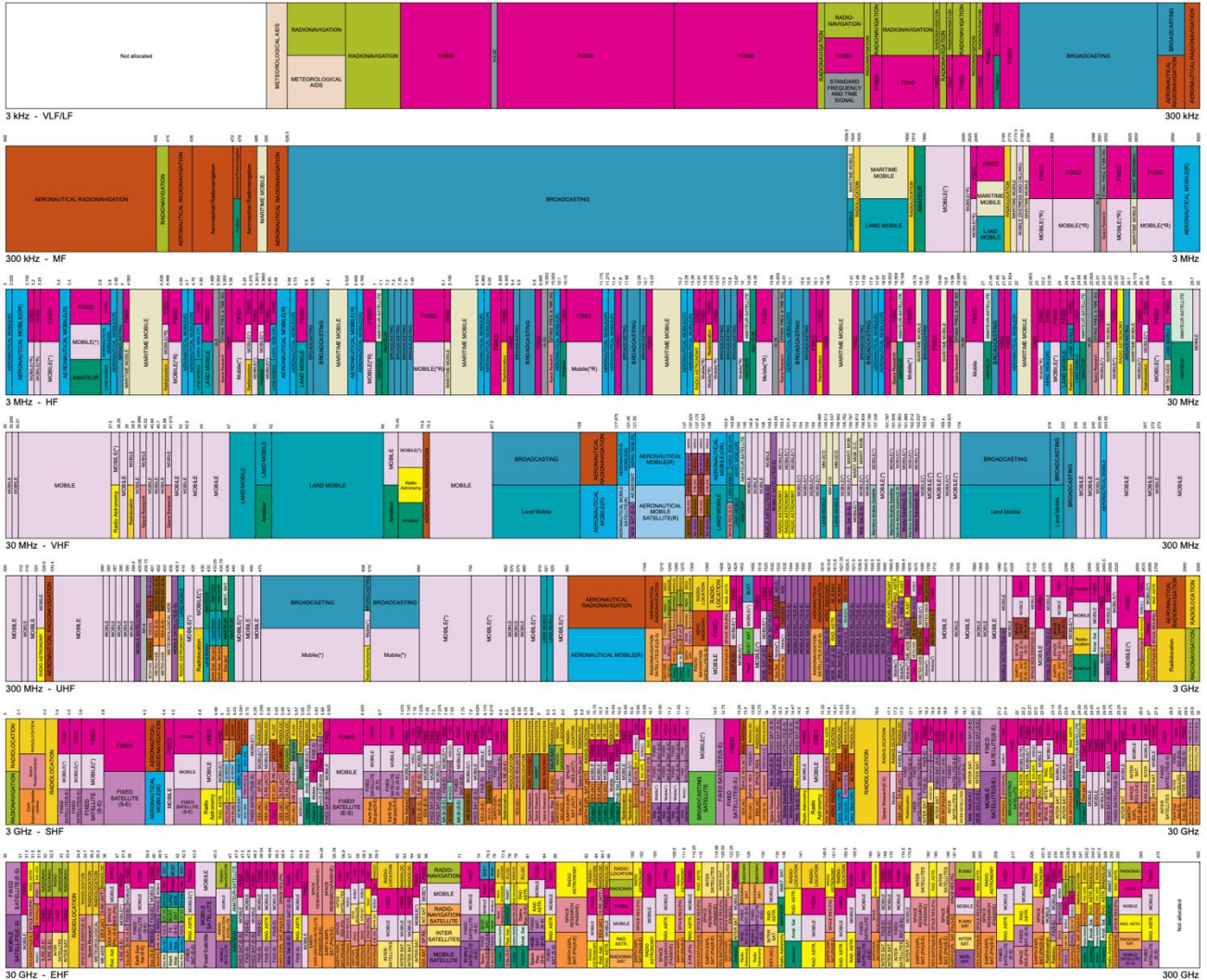
FREQUENCY ALLOCATIONS

NaFZ 2025

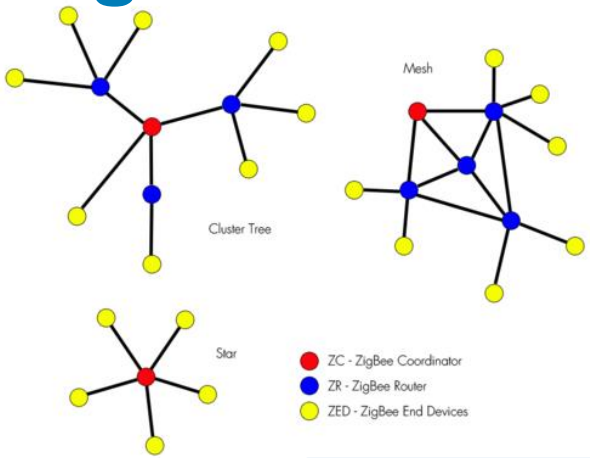
Source: https://www.bakom.admin.ch/bakom/en/homepage/frequencies-and-antennas/national-frequency-allocation-plan.html

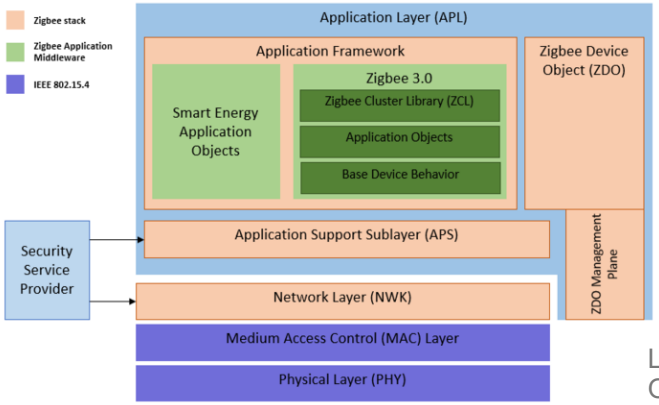
RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL AIDS
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE EXCEPT AERONAUTICAL
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE



Zigbee





- Zigbee® is an IEEE 802.15.4-based communication protocol used to create wireless personal area networks (WPAN) certified by Connectivity Standards Alliance
- Roles
  - Coordinator (ZC): This is the first node to be started. It is responsible for forming the network by allowing other nodes to join the network through it. Once the network is established, the coordinator has a routing role. In a centralized network, every Zigbee mesh network must have one and only one coordinator.
  - Router (ZR): This is a node with a routing capability that is also able to send and receive data. It also allows other nodes to join the network. A Zigbee mesh network can have multiple routers.
  - End device (ZED): This is a node that is only capable of sending and receiving data; it has no routing capability. A Zigbee mesh network can have multiple end devices. End devices can also be sleepy end devices (SED), allowing very-low-power consumption.

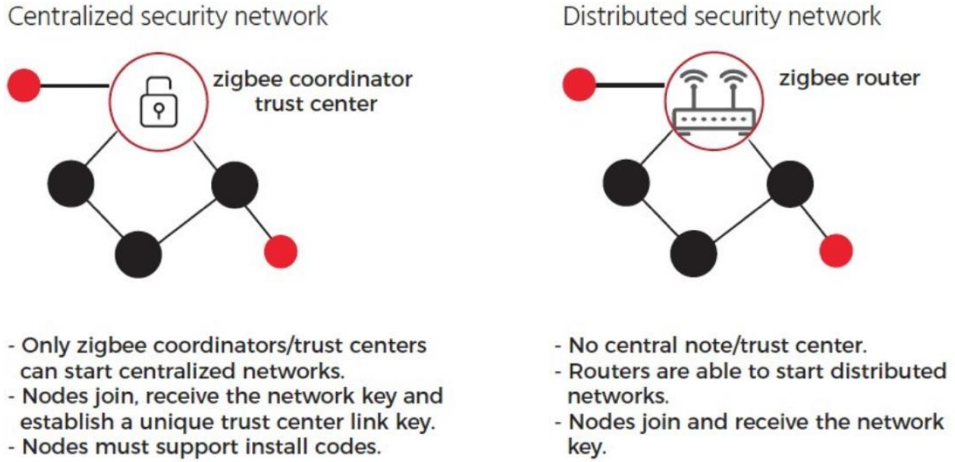
Logo source: https://upload.wikimedia.org/wikipedia/commons/1/1e/Zigbee_logo.svg
Others: https://wiki.st.com/stm32mcu/wiki/Connectivity:Introduction_to_Zigbee

Zigbee (II)

Characteristics

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation
- Extremely low-duty cycle
- 3 frequency bands with 27 channels
- 128-bit symmetric keys (link + network keys)

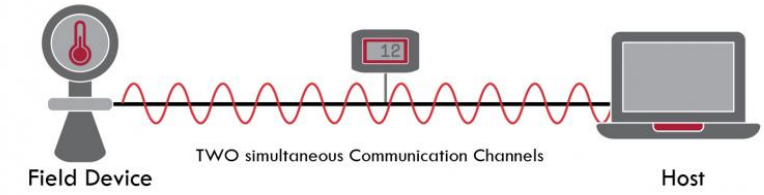
Frequency Band (MHz)	Frequency Range (MHz)	Modulation Technique	Bit Rate (Kbps)	Country	Number of Channels
868	868-868.6	BPSK	20	Europe	1
915	902-928	BPSK	40	USA and Australia	1-10, 13 (North America)
2400	2400-2483.5	OQPSK	250	Worldwide	16



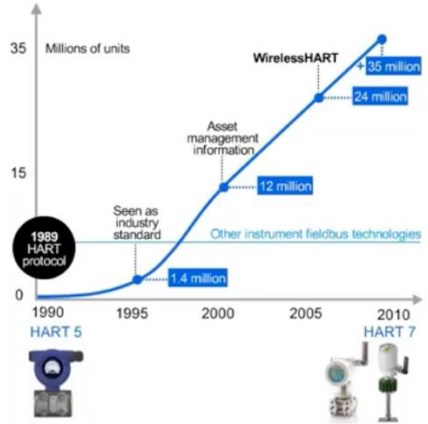
Frequency source: https://www.everythingrf.com/community/zigbee-frequency-bands
Security network source: https://research.kudelskisecurity.com/2017/11/08/zigbee-security-basics-part-2/

WirelessHART (I)

- HART (Highway Addressable Remote Transducer)
- Bi-directional industrial field communication protocol
- Used to communicate between field devices and host systems
- The global installed base of HART-enabled devices is 20 million
- Wired HART provides two simultaneous channels, one analogue, the other digital



- WirelessHART (Released in Sept. 2007)
- Wireless extension of HART Standards
- The first open wireless communication standard for industrial process control applications
- Now IEC62591
- Backward compatibility



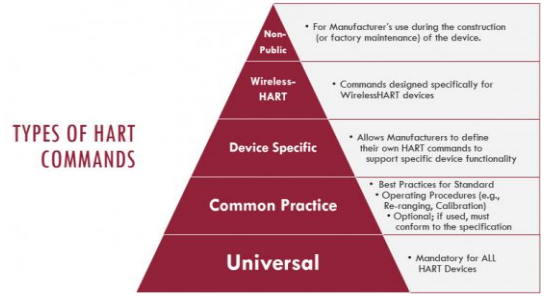
Source: https://www.fieldcommgroup.org/technologies/hart/hart-technology-explained

WirelessHART (II)

Characteristics

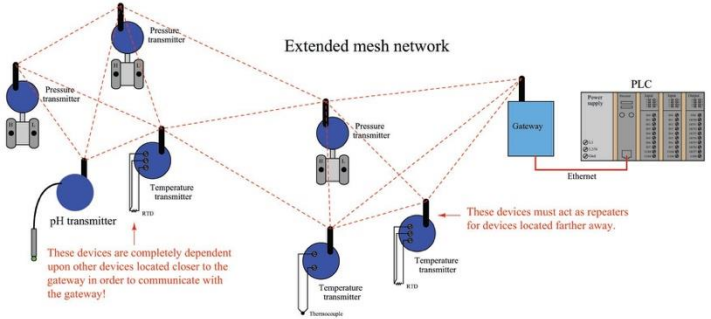
- Low Power Consumption
- Low Data Rate (up to 250 kbps)
- Mid-Range (up 225 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (in Theory))
- Cost and Implementation: WirelessHART aims for simple configuration and easy access to instrument data
- Extremely low-duty cycle.
- It uses 15 of the 16 channels defined by IEEE 802.15.4. WirelessHART employs frequency hopping.
- Time synchronised (1ms)
- Supports redundant data transmission

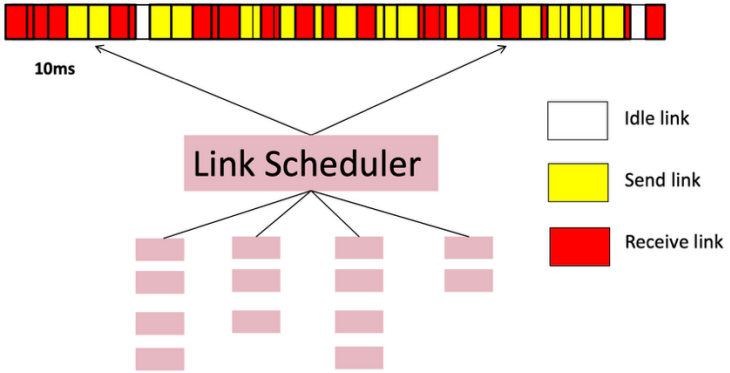
OSI Layer	HART	
Application	Command Oriented. Predefined Data Types and Application Procedures	
Presentation		
Session		
Transport	Auto-Segmented transfer of large data sets, reliable stream transport, Negotiated Segment sizes	
Network		Power-Optimized Redundant Path, Mesh to the edge Network
Data Link	A Binary, Byte Oriented, Token Passing, Master/Slave Protocol	Secure, Time Synched TDMA/ CSMA, Frequency Agile with ARQ
Physical	Simultaneous Analog & Digital Signaling 4-20mA Copper Wiring	2.4 GHz Wireless, 802.15.4 based radios, 10dBm Tx Power
	Wired FSK/PSK & RS 485	**Wireless 2.4 GHz**



Source: https://www.fieldcommgroup.org/technologies/hart/hart-technology-explained

WirelessHART (III)



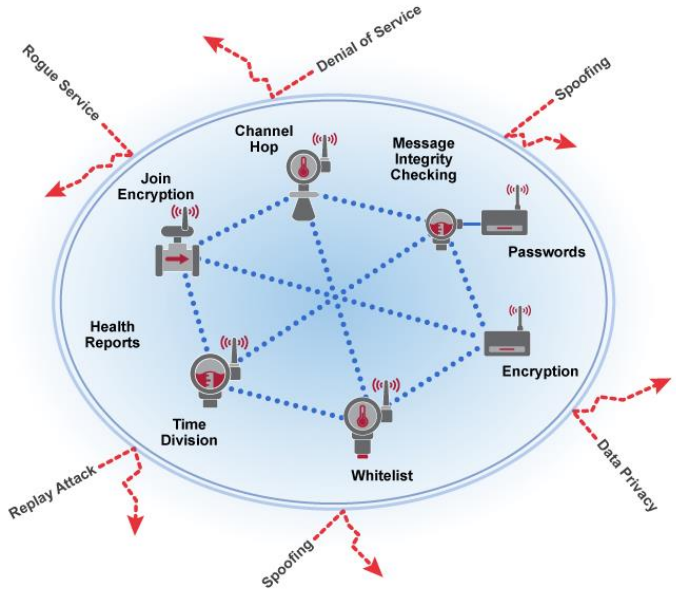


- Roles
  - Wireless field devices connected to process or plant equipment. This device could be a device with WirelessHART built in or an existing installed HART-enabled device with a WirelessHART adapter attached to it.
  - Gateways enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
  - A Network Manager is responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.
- Time Division Multiple Access (TDMA) grants 10ms response times.

Sources: https://instrumentationtools.com/wireless-hart-communication-protocol-overview/ and https://control.com/textbook/wireless-instrumentation/wirelesshart/

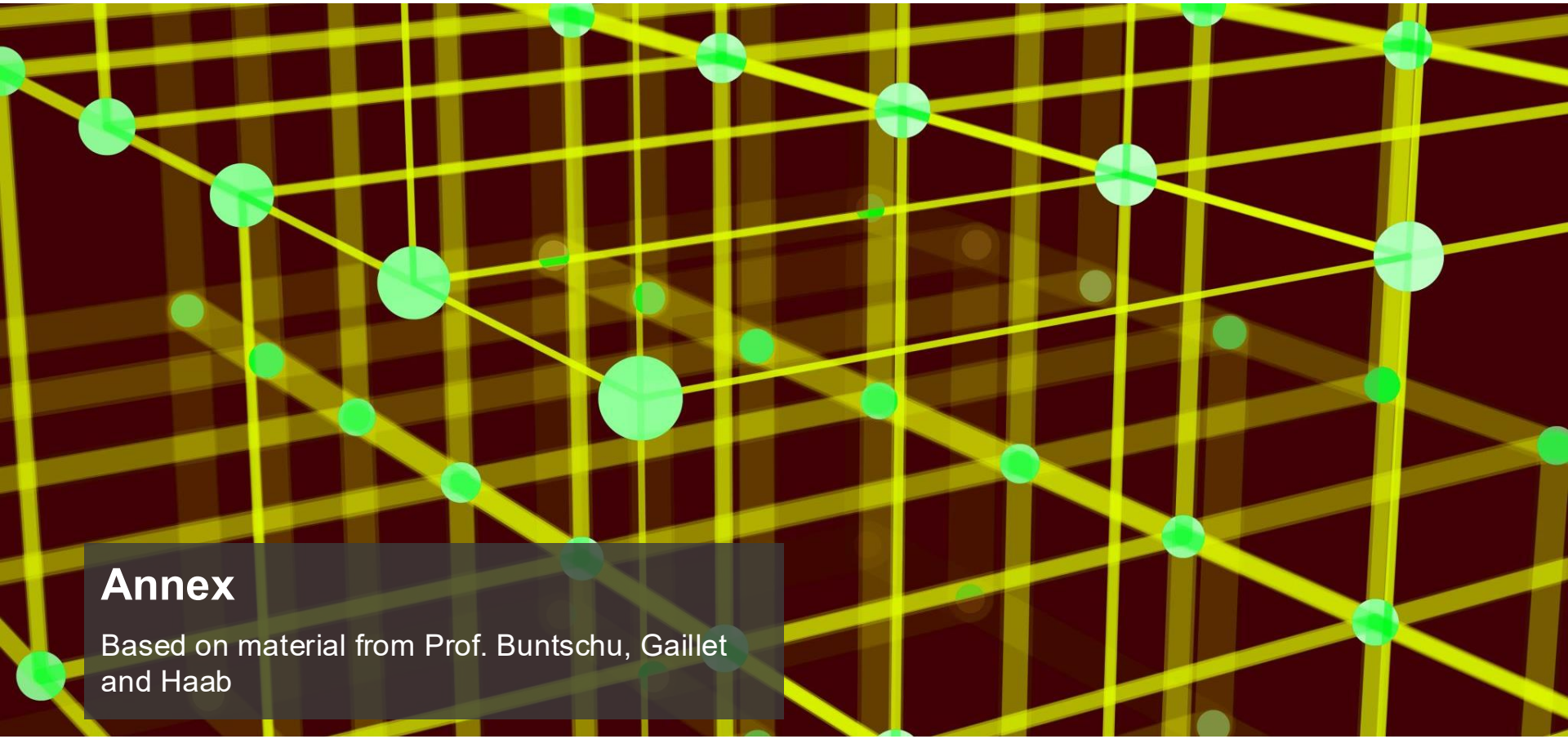
WirelessHART (II)

- Security



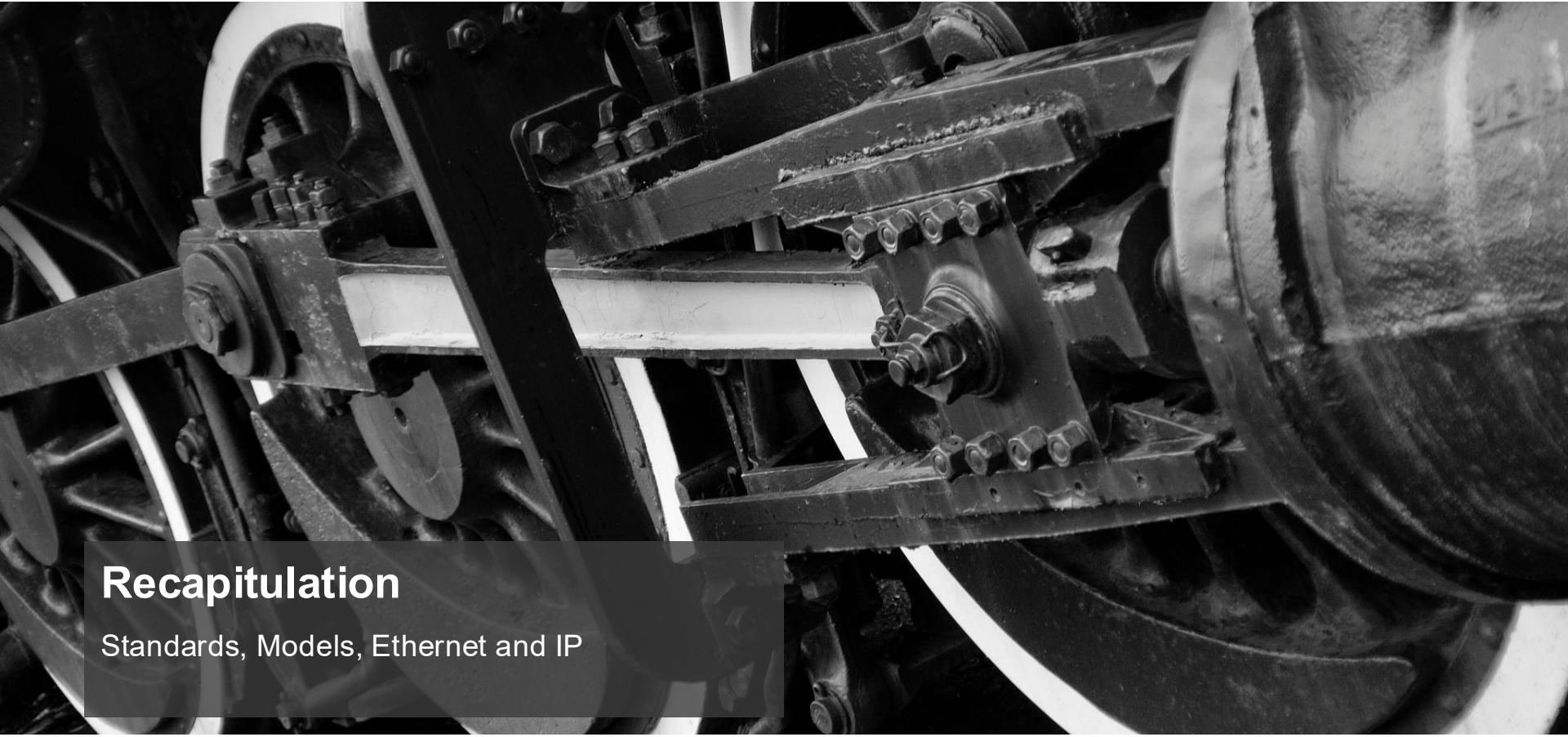
- Every message is end-to-end protected at the network layer
- Industry standard 128-bit AES encryption
- Unique encryption key for each message
- Rotate encryption keys used to join the network – automatic or on-demand
- Common network key is shared among all devices on a network to facilitate broadcast activity as needed
- The join key serves as authentication to the Security Manager that the device belongs to this network.
- Join keys can either be unique to each device or be common to a given network.


Which one is best?



Annex

Based on material from Prof. Buntschu, Gaillet and Haab

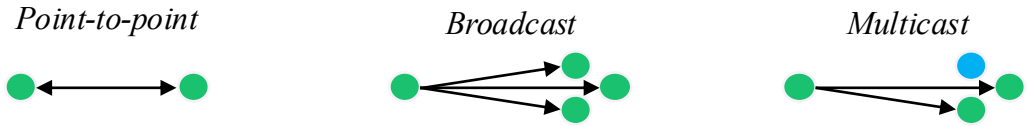


Recapitulation

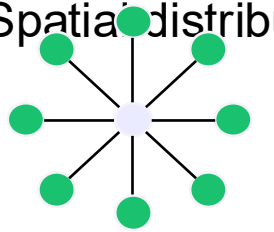
Standards, Models, Ethernet and IP

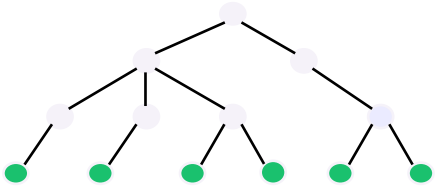
Topologies

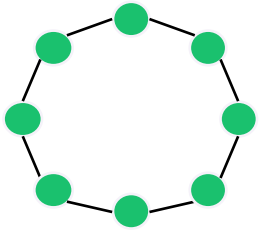
- Communication types

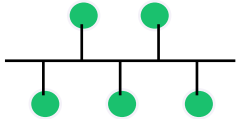


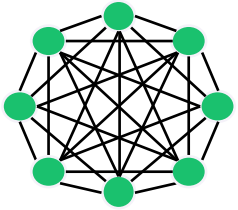
- Spatial distribution of network elements


Star


Tree


Ring


Bus


Full Mesh

Network classification (I)

Distance	Utilization	Classification
1 m	System	Multiprocesseur – Computer
10 m	Local	**LAN** (Local Area Network)
100 m	Building	
1 km	Campus	
10 km	City	**MAN** (Metropolitan Area Network)
100 km	Country	**WAN** (Wide Area Network)
1’000 km	Continent	
10’000 km	Planet	GAN (Global Area Network)

Network classification (II)

LAN (*Local Area Network*)

MAN (*Metropolitan Area Network*)

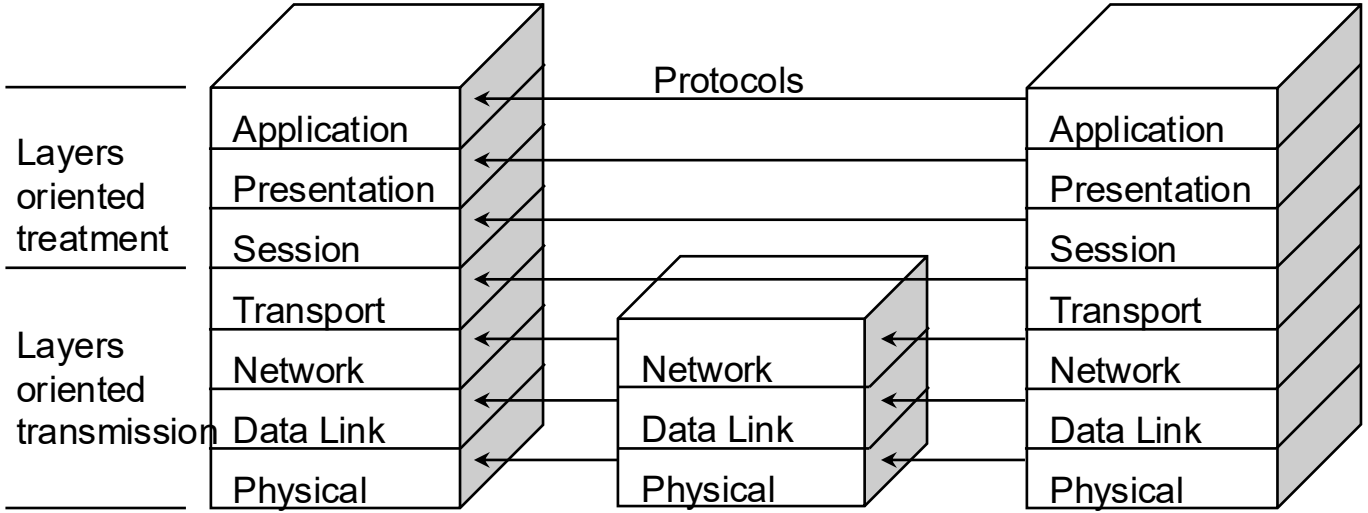
WAN (*Wide Area Network*)

Category	LAN	MAN	WAN
Full-Form	Local Area Network.	Metropolitan Area Network.	Wide Area Network.
Span	Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as country or continent.
Ownership	LAN's ownership is private. A Local Area Network (LAN) is a secure and private network that can be owned by various institutions such as hospitals, schools, offices, and more.	MAN's ownership can be private or public. A Metropolitan Area Network (MAN) can exist as either a public or private network, and it is commonly owned by numerous businesses and telecommunications companies.	While WAN also might not be owned by one organization. A Wide Area Network (WAN) is not typically owned exclusively by a single company. It can be either privately or publicly owned.
Bandwidth	The bandwidth in LAN is very high.	Transmission speed is average.	WAN bandwidth ican be quite limited.
Propagation delay	Propagation delay is short.	Moderate propagation delay.	Long propagation delay in a WAN.
Congestion	Less congestion in LAN.	More impoprtant congestion in MAN.	Highest potential for congestion.
Design & Maintenan	LAN's design and maintenance are easy.	Design and maintenance are more difficult than LAN.	WAN's design and maintenance most challenging.
Fault tolerance	Easy way to have fault tolerance.	Less fault tolerance.	Costs and complexity impact the general availability of fault tolerance.

Standardization

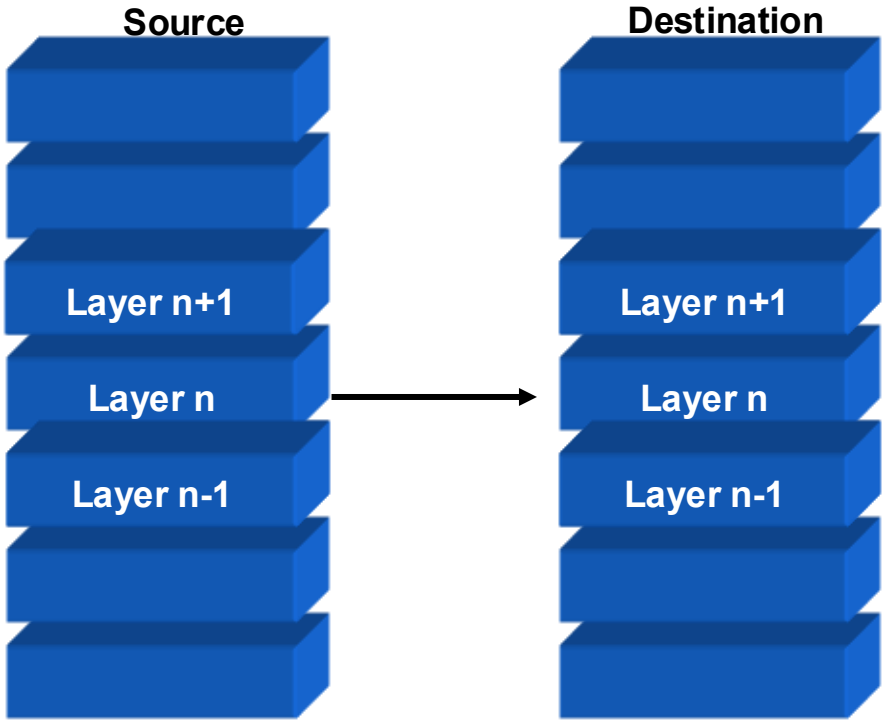
- **ISO** (*International Organization for Standardization*)
  - international standardization (excludes voice communications)
  - most important example: ISO basic reference model
- **ITU** (*International Telecommunication Union*)
  - international association for national operators of voice communication
  - ITU-T (Telecommunications, previously: CCITT)
  - ITU-R (Radio Communications, previously: CCIR)
  - examples: X.25, V.34, (B-)ISDN ATM
- **ETSI** (*European Telecommunication Standards Institute*)
  - harmonization of European national standards
- **IEEE** (*Institute of Electrical and Electronics Engineers*)
  - the world's largest professional association
  - standardization activities relating to electrical engineering and informatics
  - example: LAN/MAN 802.x standards (taken over by ISO IS 8802)

ISO reference model



The ISO model was proposed by ISO in 1983. Note that the ISO model is a theoretical reference model that does not apply perfectly to IT networks. In practice, the Internet model has imposed itself during the past few years. The ISO model arguably remains the best abstraction base (ISO 7498-1, ITU X.200).

Principles of the layer model

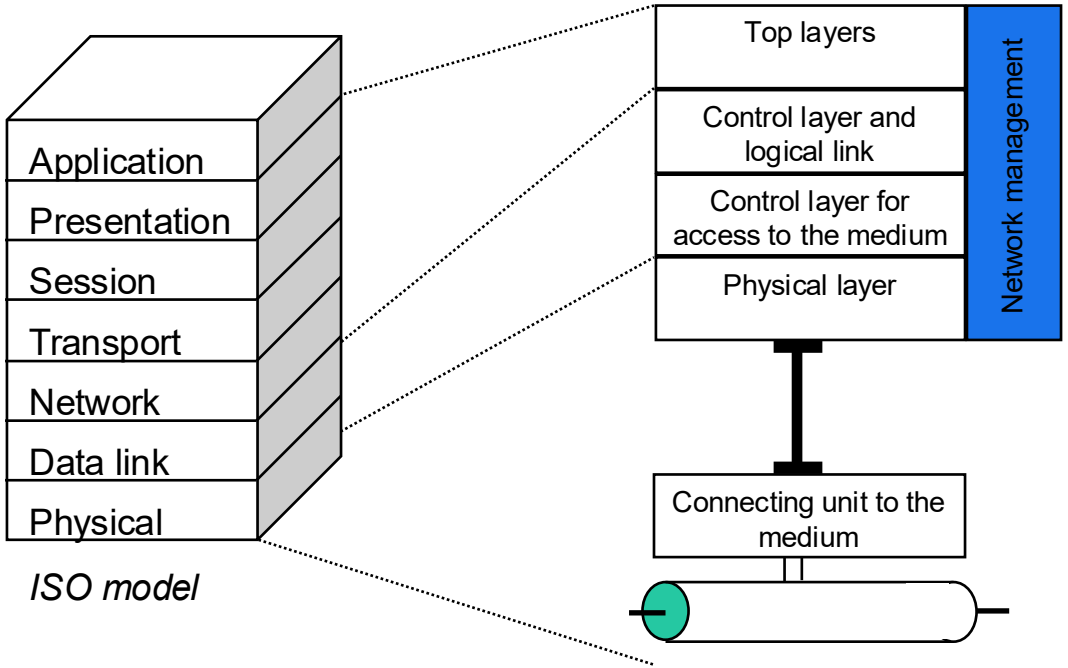


The objective of layer protocols is to simplify network description and design, and at the same time, interface normalization.

Each layer communicates horizontally with the corresponding layer at the same level.

Layer *n* at the destination receives exactly the same object as was sent by layer *n* at the source.

ISO 7498-1 vs. IEEE 802.x comparison



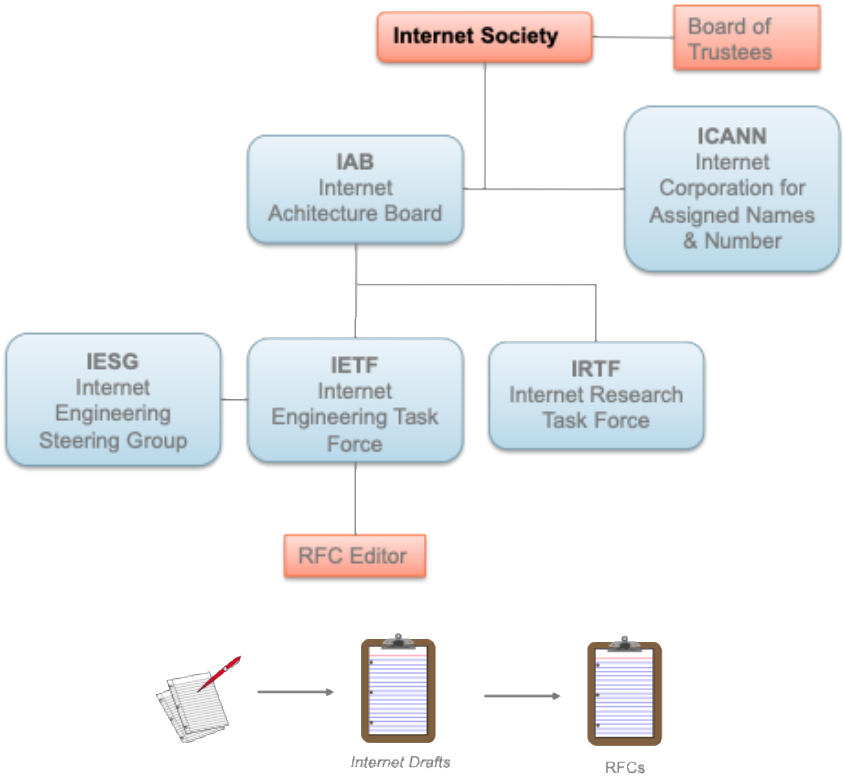
Note that there is no absolute identity of functions and boundaries

Internet Society

International, non-profit organisation run by a council (based on the *National Geographic Society*) model, founded 1992.

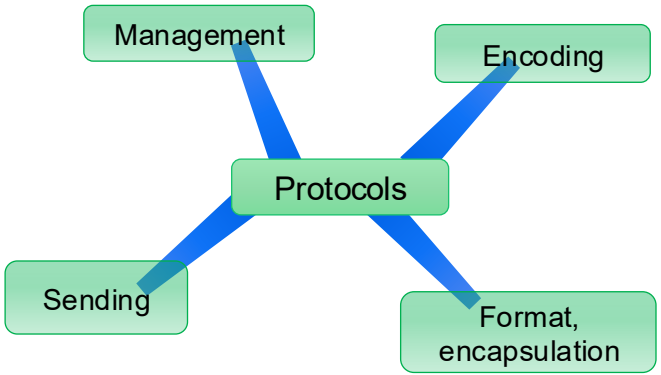
In the Internet Society, *the Internet Architecture Board* (IAB) is a forum and council that supervises the IETF (*Internet Engineering Task Force*) and the IRTF (*Internet Research Task Force*).

Amongst other activities, *the Internet Society* (ISOC, http://www.isoc.org) is at the origin of this "uncontrolled" network that is the Internet and at the base of the interoperability standards of the same name. The Internet tele informatic networks model defines a less rigorous and more pragmatic model than that of ISO.



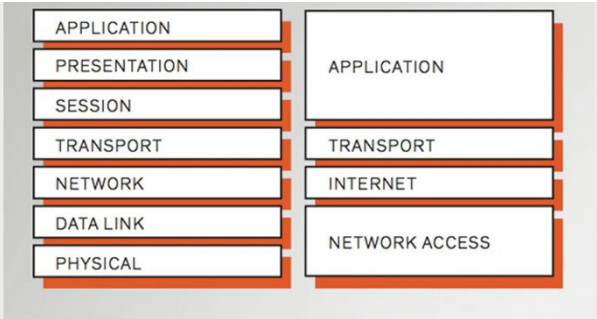
“Standards”: rules to communicate

- Establish **rules** to communicate:
  - Identify sender and receiver
  - Common language and grammar
  - Speed and time management of the exchange
  - Confirmation or acknowledgment of exchanges
- Message Encoding
  - Process of converting information into another acceptable form
- Format, encapsulation and size of messages
- Messages management
  - Access methods
  - Flow control
  - Timer
- Option for sending messages
  - Unicast
  - Multicast
  - Broadcast

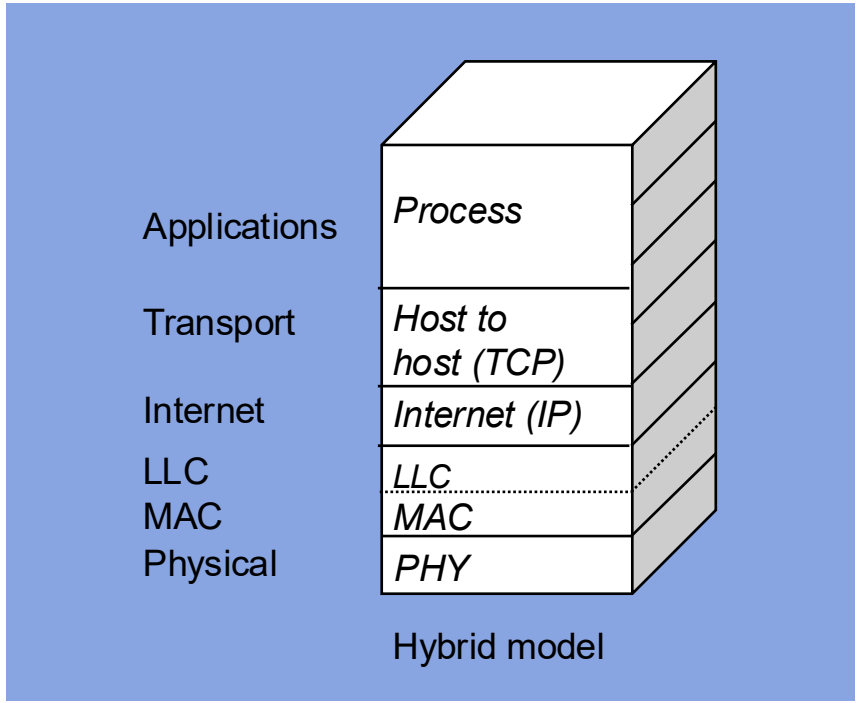


The Hybrid Model

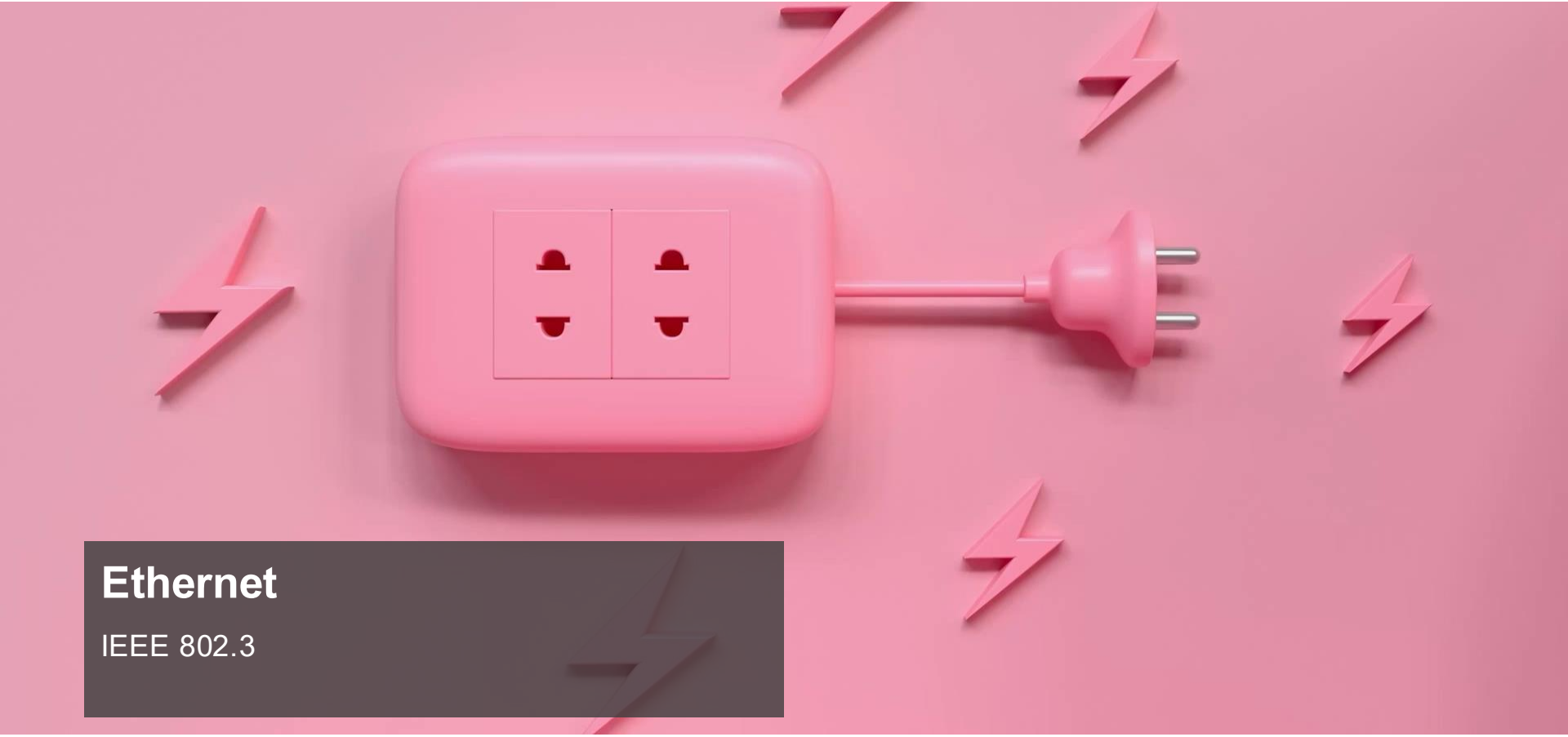
Pragmatic layered model much used today, combining the IEEE and Internet models



A layered approach: The OSI reference model (left column) divides computer communications into seven distinct layers, from physical media in layer 1 to applications in layer 7. Though less rigid, the TCP/IP approach to networking can also be construed in layers, as shown on the right.



Source (and interesting read): https://spectrum.ieee.org/osi-the-internet-that-wasnt

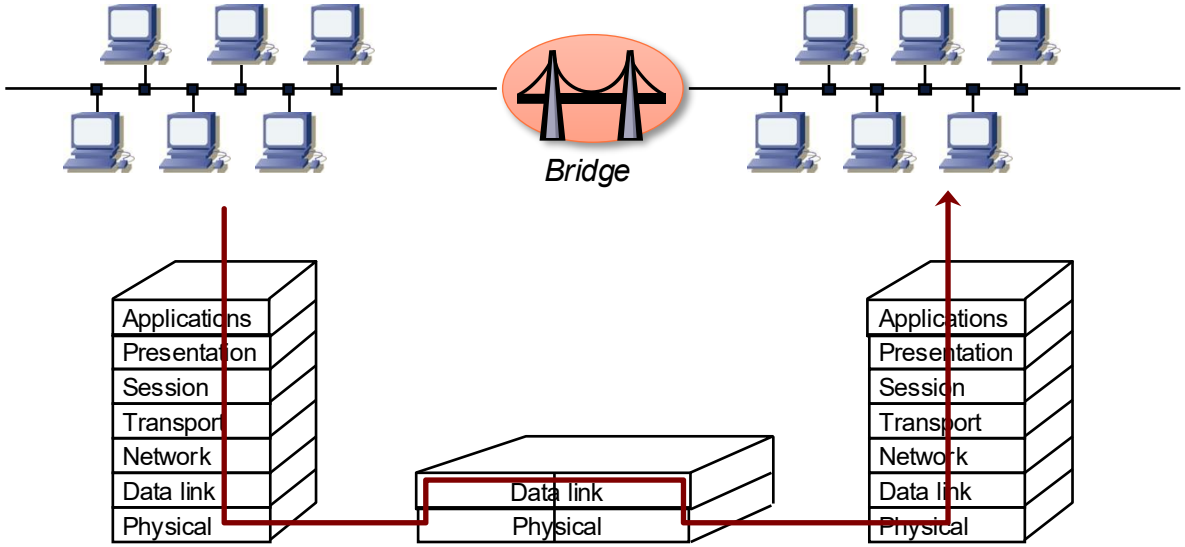


Ethernet

IEEE 802.3

Bridging

- A *Bridge* permits two or more LANs at the layer-2 level to be interconnected (MAC sub-layer). The *Bridge* filters traffic from the MAC address so as to avoid the propagation of needless traffic over the network. In general, but not always, a *Bridge* links networks of the same type
- The *Bridge* analyses the frames that pass, thus introducing a slight transfer delay.



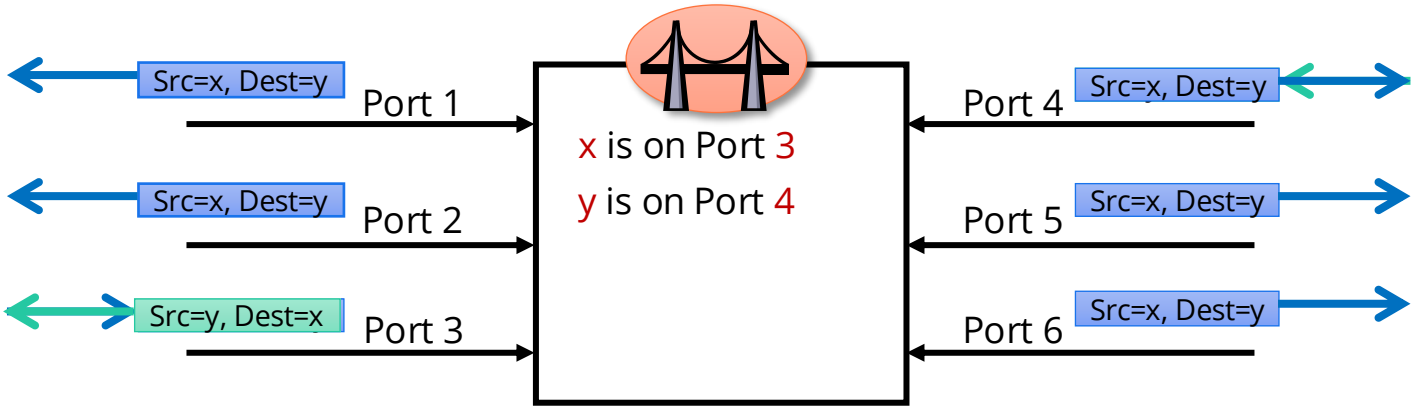
Transparent Bridging: basic principle

A transparent *Bridge* has five tasks to perform:

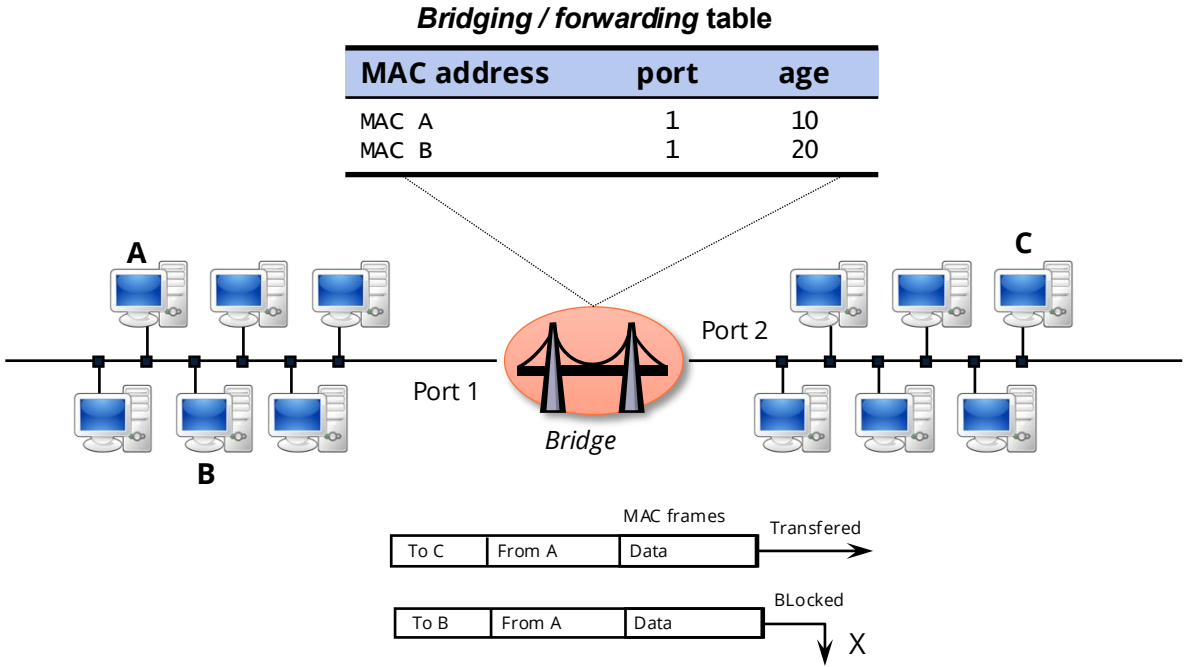
1. In case of doubt, to transfer all the arriving frames, in particular *broadcast* frames, to all the **other** ports (*flooding*).
2. To find out stations' MAC addresses based on the passing frames' **source addresses** and thus create a *bridging* table, associating a port with each known MAC address (*learning*).
3. To transfer the frames whose destination addresses are not in the segment from where the frames arrive to the exit port corresponding to this destination (*forwarding*).
4. To block frames where the destination is in the same segment as that from where the frames arrive
5. To avoid loops using the spanning tree's algorithm .

Frame Forwarding (3)

- The forwarding table is automatically filled
  - The source address of a frame arriving on a port indicate which hosts are accessible on that port.



Transparent bridging: frame forwarding

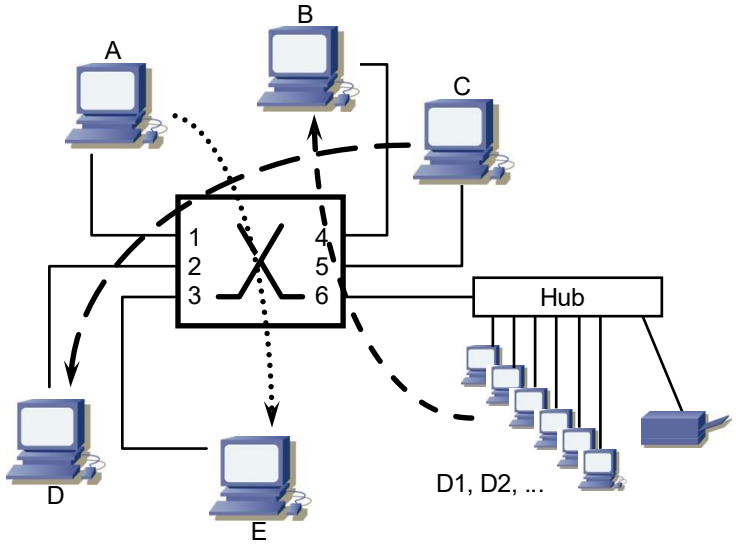


Switch Modes of Functioning

Cut-through

If station A sends a frame to station E, the *Switch* decodes the address of destination E as quickly as possible at access 1 and transmits the frame without delay (*"cut-through"*) uniquely to segment 3.

Note that it is not possible to perform an error control before forwarding the frame on.



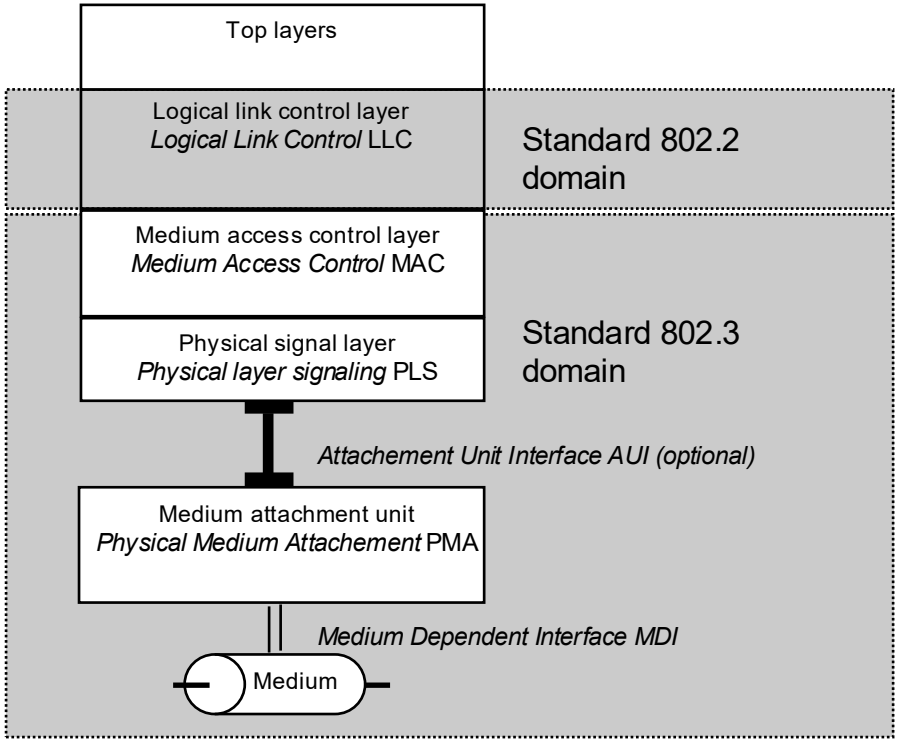
Store & forward

The frame is memorized in full before being transmitted, which permits the elimination of frames containing errors. The price to pay is increased transmission delay.

Reference model IEEE 802.3/ISO 8802/3

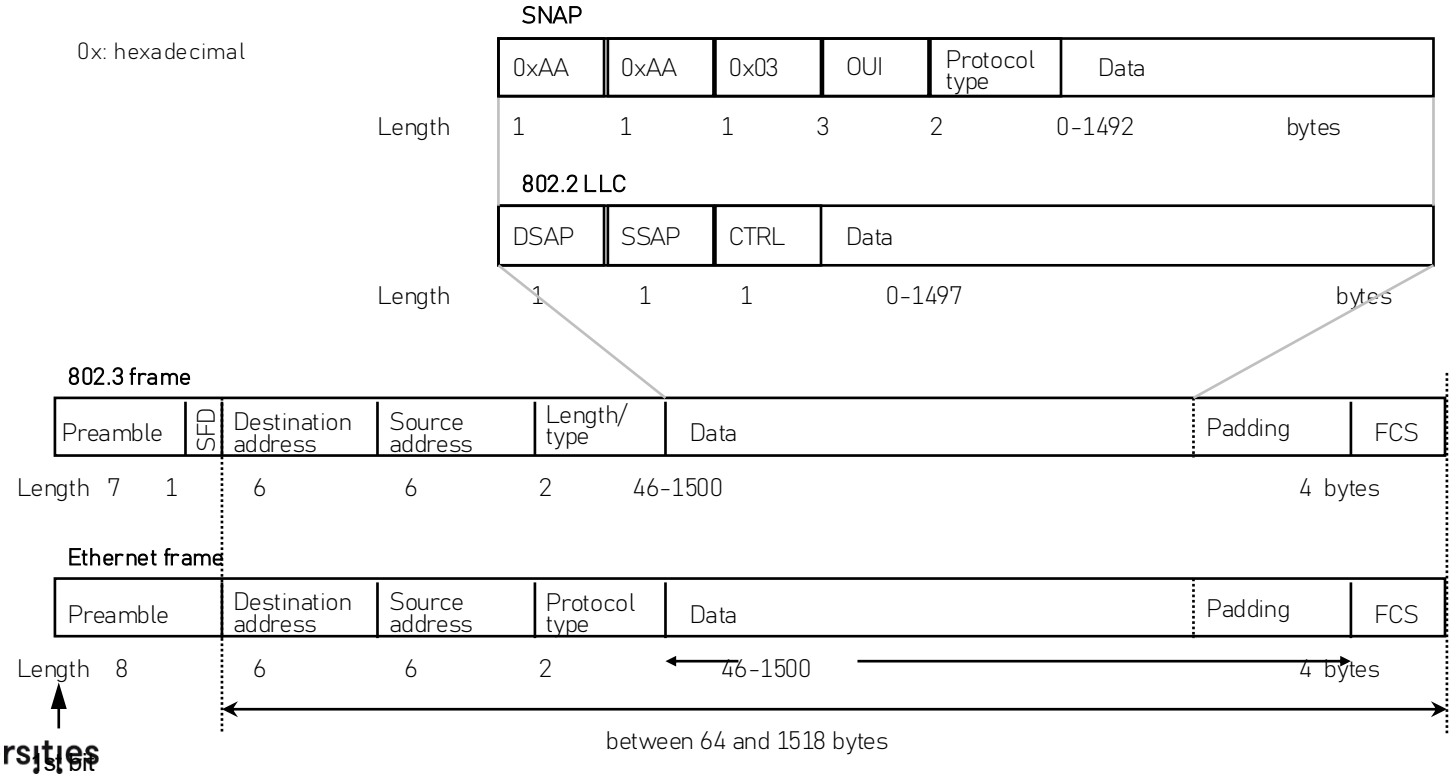
(1Mbit/s and 10Mbit/s)

It should be noted that the IEEE 802.3 standard does not define the interfaces between the network management plan and the MAC or physical layers



Note: this model corresponds to the IEEE 802.3 1993 revision without the 100Mbit/s and 1000Mbit/s variants

802.3 and Ethernet frames (1)



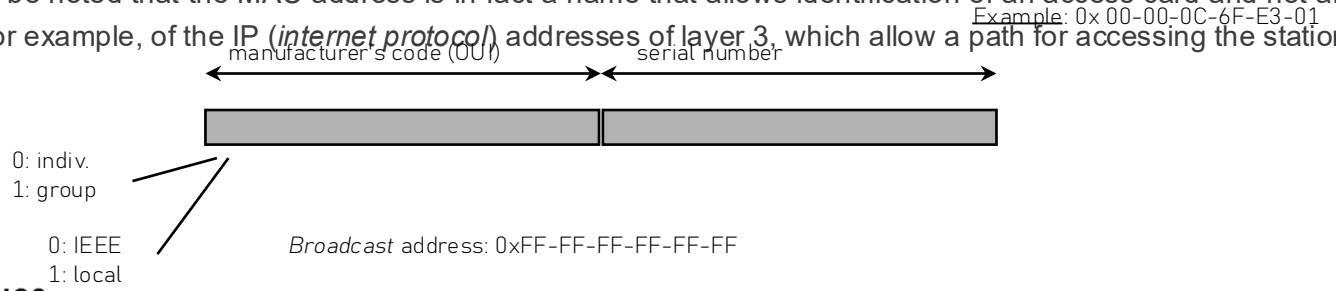
802.3 and Ethernet frames (2)

The 802.3 fields are sent over the medium with the **low-order** bit (LSB - least *significant bit, Little Endian*) of each byte first

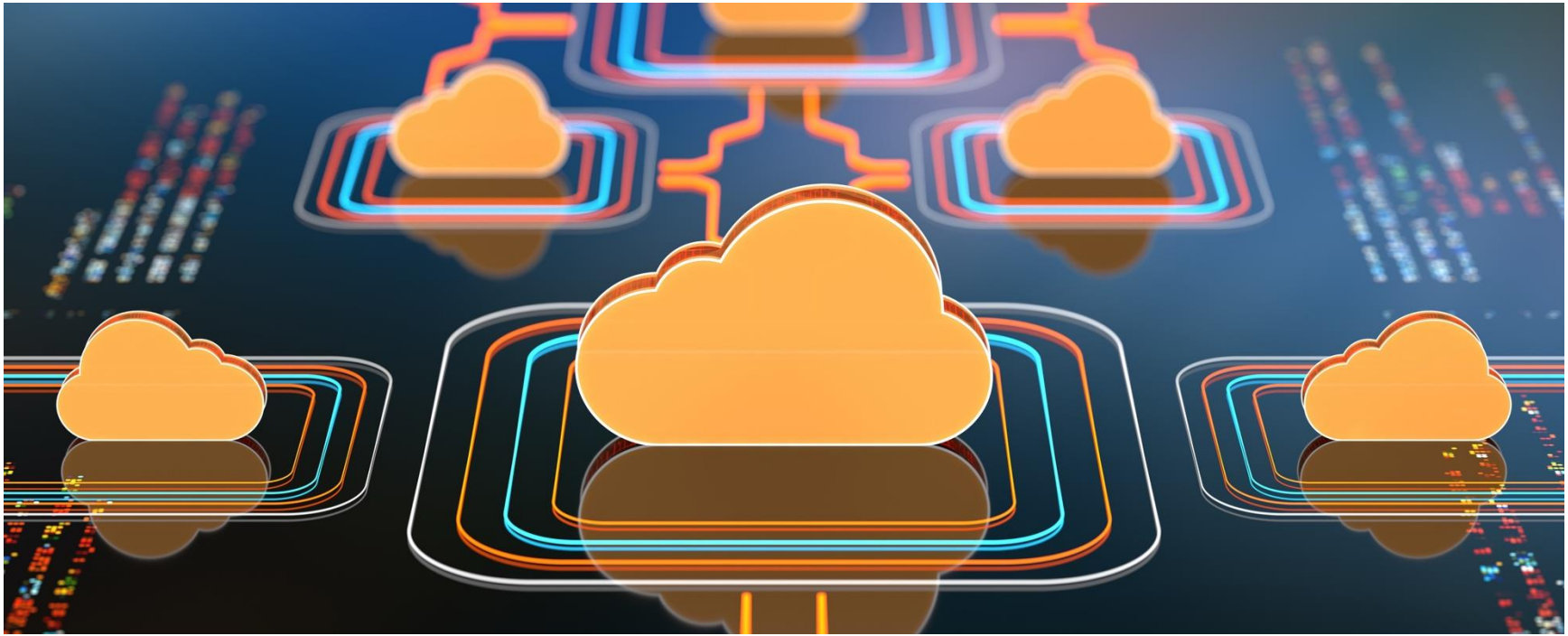
- **Preamble**: field used for frame delimitation is to supply a signal at 5MHz
  (802.3): 7 bytes of “10101010”
  (Ethernet): 62 bits of “10…“ and 2 bits “11” (*synch*)
- **SFD (*start frame delimiter)***:
  (802.3) frame delimitation 1 octet “10101011”
  Note: the 8 first bytes of 802.3 and Ethernet frames are thus identical
- **Source and destination addresses**: MAC addresses of 48 bits each
- **Protocol type**: (Ethernet) *type field*: is used to determine which protocol is used at the top layers. This code, also called *DIX code*, identifies the protocol of layer 3. The Ethernet frame does not have a length field. It is thus the role of the MAC layer to identify the end of the frame and the role of the top layers to determine the length of the data field.
- **Length/type**: (IEEE 802.3) gives the number of bytes in the data field. If the value of this field is superior to 0x0600 (1536), it is interpreted as being the protocol type.
- **Pad** : this field allows a minumum frame length of 64 bytes to be guaranteed (without preamble and without SFD)
- **FCS** (*frame check sequence*): error control sequence, allows detection of errors on the frame with a 32-degree polynomial. Protects from the first bit of the destination address to the last bit of the FCS.

MAC addresses

- In order for each 802.3 network card to be identified, the MAC protocol defines an address called the MAC address. This address is attributed by the IEEE in a **unique fashion**. It can, however, sometimes be modified.
- The MAC address is normally indicated in 12-character hexadecimal form. The first six are attributed to a manufacturer or seller. This is the OUI code (*Organizationally Unique Identifier).* The last six are administered by the manufacturers (serial number).
- The first bit (on the medium, i.e. the last bit of the 1st byte) of the MAC address shows whether it is an individual address (0) or a group address (1). The second bit shows if it is a global address, administered by the IEEE (0) or if it is administered locally (1).
- In general, the MAC address is placed in a ROM memory. We speak here of a “burned-in address” (BIA).
- It should be noted that the MAC address is in fact a name that allows identification of an access card and not an address in the sense, for example, of the IP (*internet protocol*) addresses of layer 3, which allow a path for accessing the station to be found.



IP Protocol

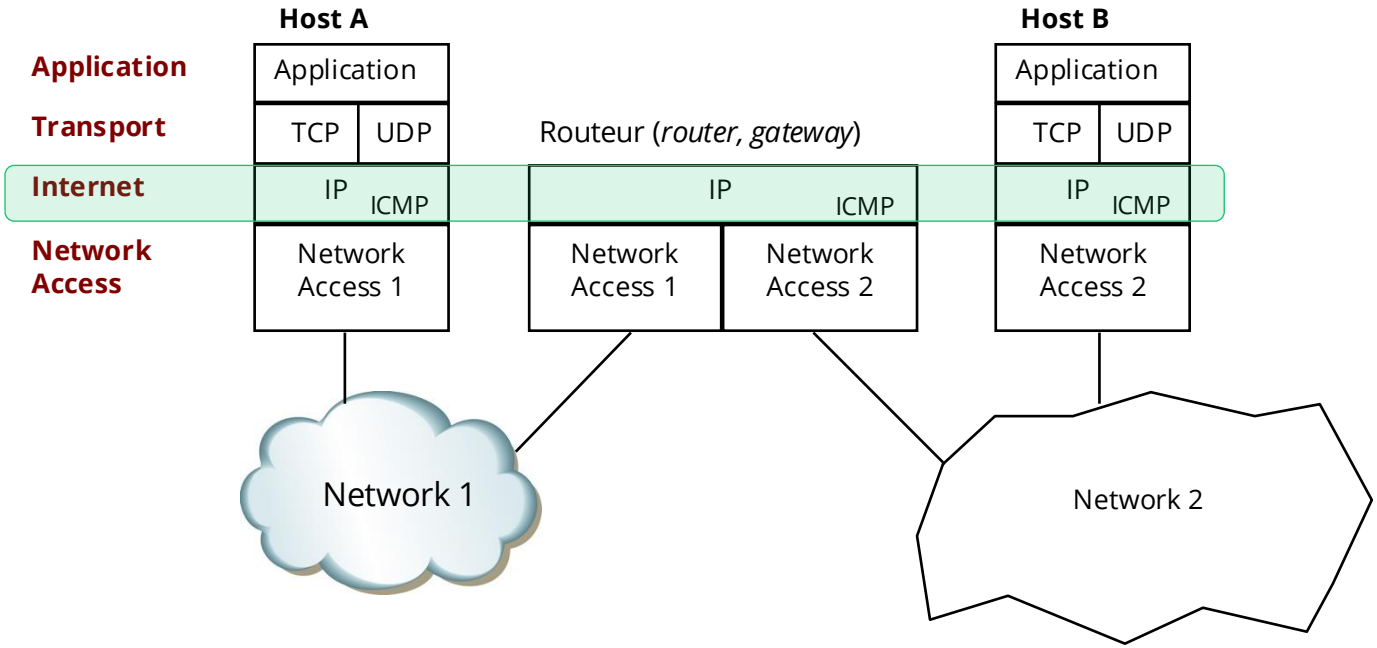


Introduction

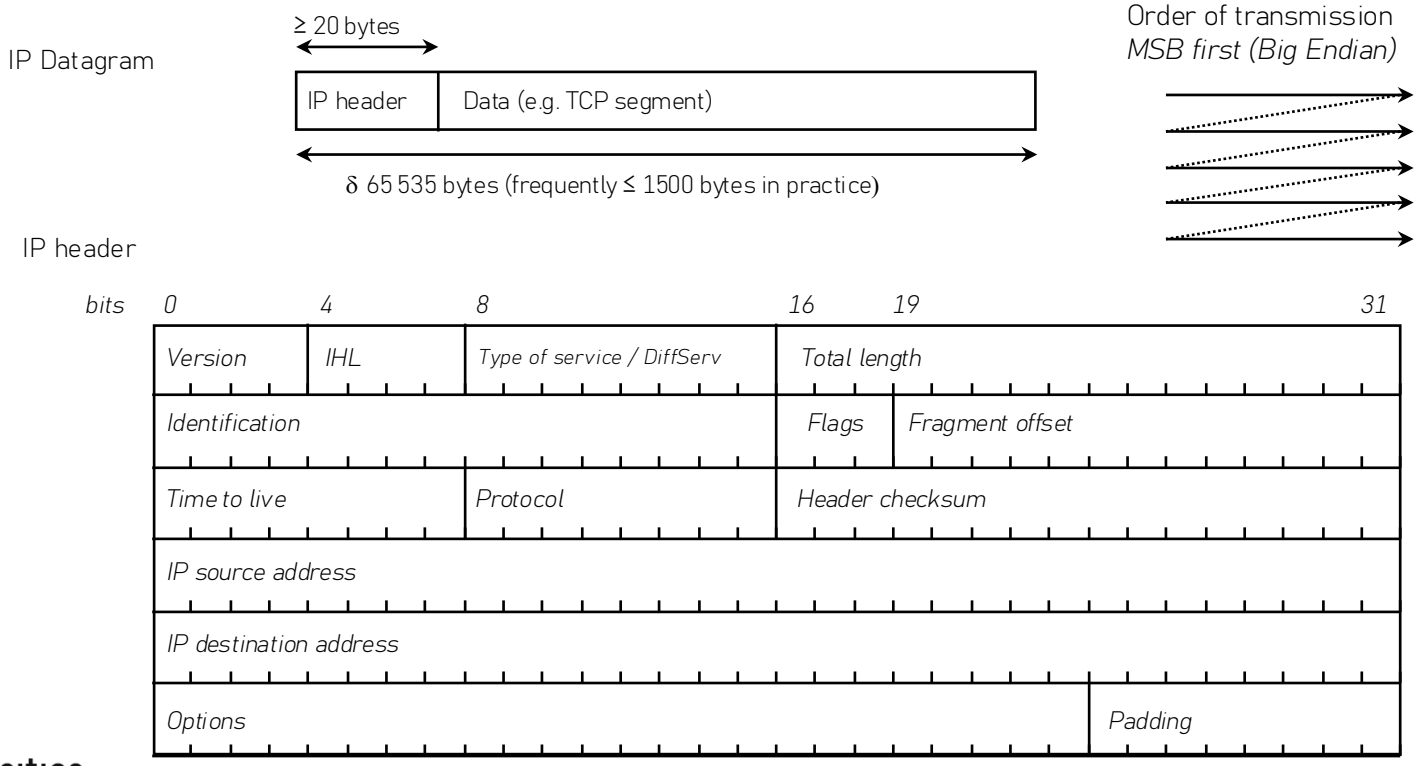
IP Protocol (IPv4, RFC 791, Sept. 1981)

- The IP protocol transports **datagrams** (independent packets) from a source station (*host*) to a destination station via networks interconnected by routers (originally, and still frequently, called *gateways*).
- The two basic functions of IP are **addressing** and **fragmentation** (little used)
- Each station, or its network connection, has an IP address. Every datagram contains the full source and destination IP addresses.
- The selection of a path through a network is called **routing**. Based on the destination IP address, routers use a routing algorithm to decide which egress port must be used and what equipment on this egress port has to be addressed.
- This protocol offers a non-guaranteed service without connection known as "*best effort*" between stations connected to the network. IP does not control errors in the data field nor provide acknowledgements confirming that the datagram arrived correctly at the destination.

TCP/IP Architecture



IP datagram format



IP datagram fields (1)

An IP datagram header is made up of a 20-byte obligatory part and a variable-length optional part. The field meanings are as follows:

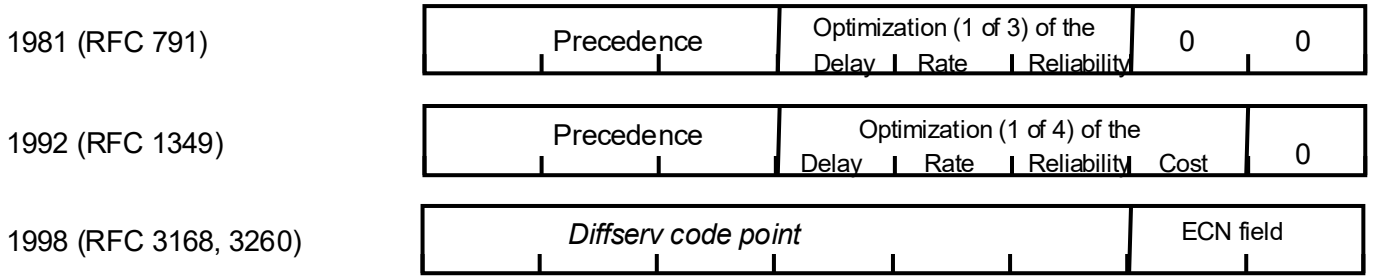
- **Version** [4 bits] permits identification of the IP protocol version (IPv4 = 0b0100).
- **Internet header length, IHL** [4 bits] gives the header length in 32-bit words (multiple of 4 bytes). Value from 5 to 15; 5 is the default value (no options).
- **Type of service** [8 bits] gives indications of the service required: precedence, delay, rate and reliability. For a long time, however, this field has neither been used or supported. It is therefore set at zero. For several years, this service quality field has been used for certain applications within the framework of *DiffServ* (RFC 2474, 3168 and 3260).
- **Total length** [16 bits] gives the length of the datagram (header and data) in **bytes**. Value from 20 to 65,535.
- **Identification** [16 bits] permits the datagram fragments to be reassembled (all the fragments of the same datagram have the same value for the identification field). May be provided by the superior layers or generated by the IP. Generally sequential.
- **Flags** [3 bits] serve for fragment management
  - → The first bit is always 0
  - → The second bit (**DF**, *do not fragment* = 1*, may fragment* = 0) serves to prevent possible fragmentation. Frequently used for diagnostic purposes (ICMP message sent if the size is too big)
  - → The third bit indicates whether or not the fragment is the last of a datagram (**MF**, *more fragments* = 1, *last fragment or single fragment = 0*)

IP datagram fields (2)

- **Fragment offset** [13 bits] allows the fragment to be situated in the datagram by indicating how many 8-byte data words have already been sent. Value from 0 to 8191.
- **Time to live** [8 bits] permits the number of nodes crossed (*hops*) to be counted by incrementing an 8-bit counter backwards. Frequently, incorrectly, indicated in seconds. Must be decreased by at least 1 at each router. The packet is eliminated if this field reaches 0.
- **Protocol** field [8 bits] allows the datagram to be directed to the right port for accessing the superior layers (1 for ICMP, 6 for TCP, 17 for UDP, etc.). See RFC 1700, replaced by http://www.iana.org/numbers.html.
- **Header checksum** [16 bits] allows the header integrity to be verified in order to avoid errors. Ones' complement (all the bits reversed) of the sum in ones' complement of the 16-bit header words (binary sum with reports and addition of *overflows* on the least significant bits). For the calculation, this field is set to zero. If the error control indicates that there are errors, the datagram is eliminated.
- **IP source address** [32 bits] identifies the source of the IP datagram.
- **IP destination address** [32 bits] identifies the destination of the IP datagram. **Option** fields [≤ 40 bytes of which 1 type byte and 1 length indication byte, TLV format (*type, length, value*)] are used to transport various types of information, such as identification of the nodes crossed or to force a routing path across the network (diagnostic or security). These fields are generally not used.
- **Padding** [1 to 3 bytes] completes a 32-bit word (multiple of 4 bytes).

Type of Service / DiffServ field

The signification and utilisation of the "type of service" has evolved over time. Originally, it defined the quality optimization criterion of the predominant routing. Since the routers did not support it, it fell into disuse. More recently, the requirements of service quality revived interest in this field, replacing it with the ***Diffserv*** code, indicating relative precedence, and a field allowing congestion signalling along the path.

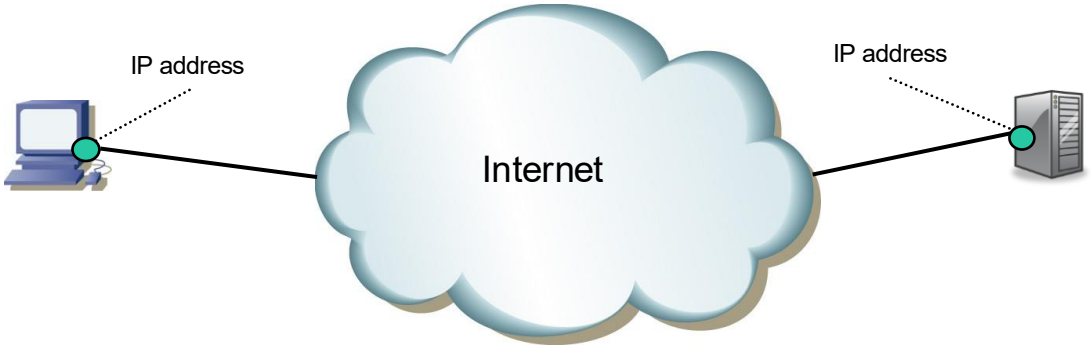


ECN field (*Explicit Congestion Notification*)

ECT (*Explicit congestion notification Capable Transport*): an indication that the TCP layer can react in case of congestion. ECN = 01 or 10 flagged by the two systems at the extremities (source and destination) to indicate that they support congestion indication.

CE (*Congestion Experienced*): ECN = 11 flagged by the server observing congestion along the path. The destination returns the **ECN echo flag** in its TCP acknowledgments to the source, which indicates to the source that it must reduce its congestion window by half.

Introduction



Each station (*host*), or rather its **connection** to the IPv4 Internet network has a unique 32-bit address called the **IP address**.

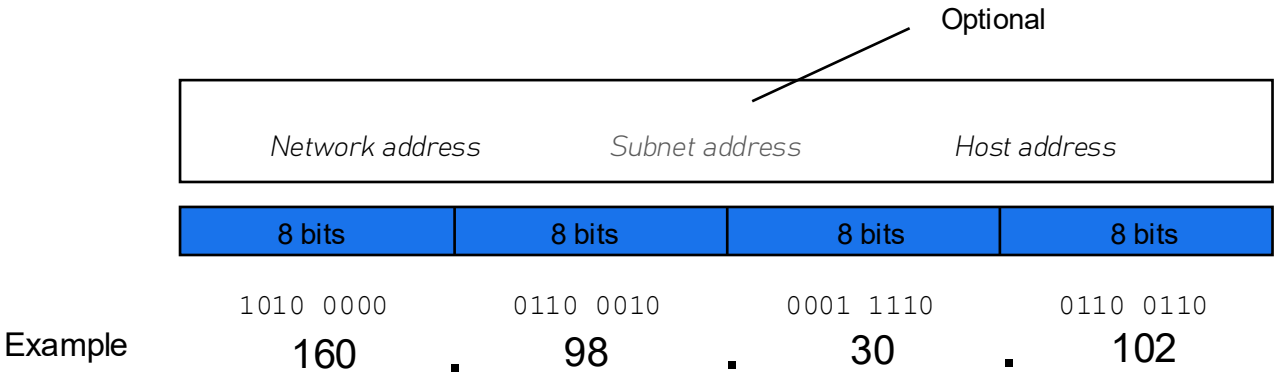
This address consists of a network part (*netid* or *netprefix*), which identifies the AS (***Autonomous System***): ISP (*Internet Service Provider*), organization or company and a part unique to the **station** (*hostid*), which identifies this station in the network.

The IP address is a global address and "partially hierarchical", which permits the destination to be found by passing via the routers.

This address is made up in such a way as to simplify routing. The Internet network permits routing of IP packets to the destination in a sure way by first using the network part of the address, then the part identifying the destination station in the destination network.

IP addressing

An IP address (version 4) is made up of 32 bits organized hierarchically from left to right in 2 or 3 variable-sized sections:

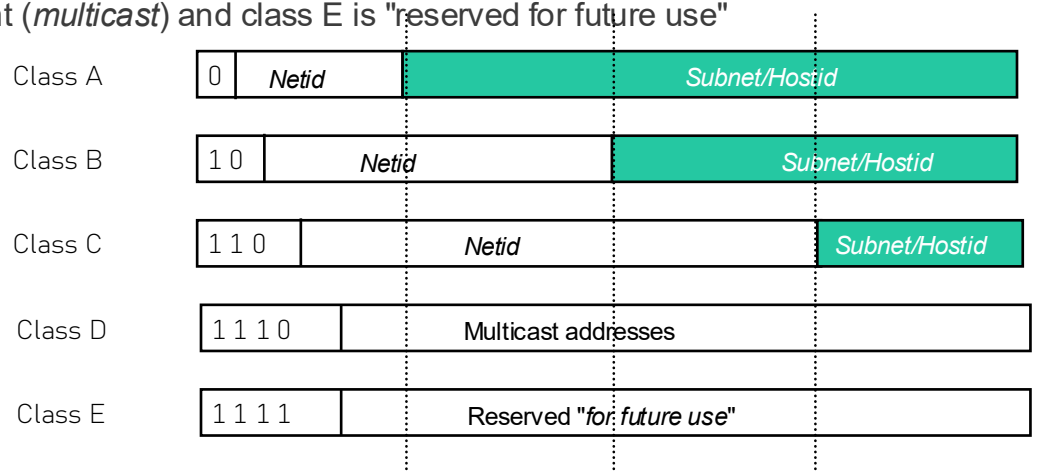


IP addresses are written in the form of 4 decimal numbers separated by points, the "*dotted decimal notation*". Each number represents the equivalent decimal of a binary byte.

The minimum value of a byte is 0 (0b0000'0000), the maximum, 255 (0b1111'1111).

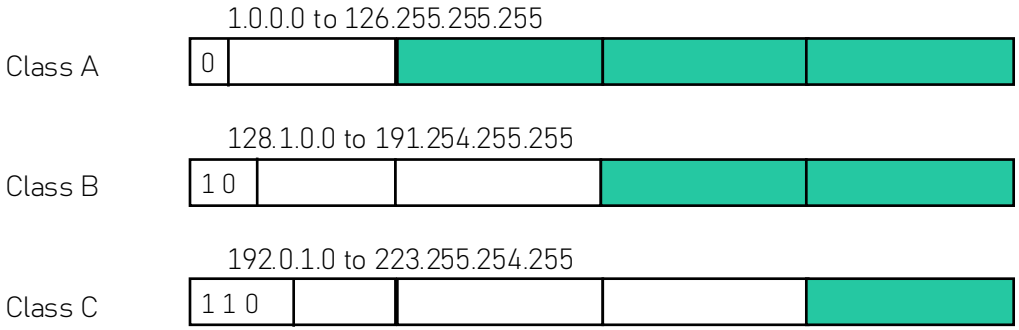
IP address classes (1)

Originally, the IP addressing space of 0.0.0.0 to 255.255.255.255 was strictly divided into "classes". IP supports 5 classes of address, called A, B, C, D and E. The first three are point-to-point addresses (*unicast*), class D is intended for point to multipoint (*multicast*) and class E is "reserved for future use"



Class A: 7 bits for the network (1-126), 24 bits for the *subnets*/stations
Class B: 14 bits for the network (128.1-191.254), 16 bits for the *subnets*/stations
Class C: 21 bits for the network (192.0.1-223.255.254), 8 bits for the *subnets*/stations
Class D: (224.0.0.0-239.255.255.255)
Class E: (240.0.0.0-255.255.255.254)

IP address classes (2)



Class A: 126 networks with 16'777'214 stations each (0 and 127 reserved)
Class B: 16'382 networks, each with 65'534 stations
Class C: 2,097,150 networks, each with 254 stations

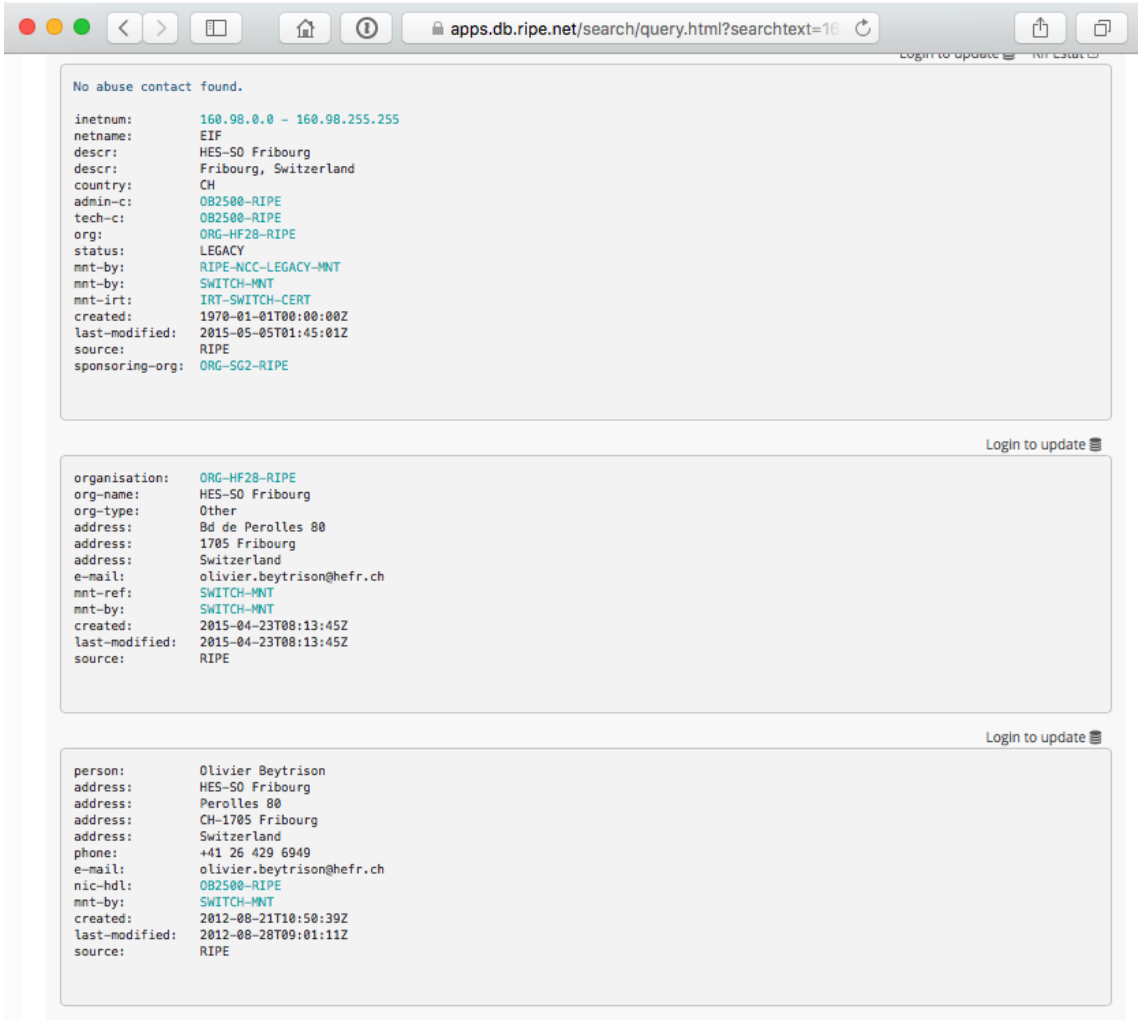
Conventions:

- An IP address with *Hostid* = 0 designates the network/subnet. An address with *Hostid* = 255 designates a *broadcast* on the network/subnet.
- Address 255.255.255.255 is blocked by the routers (*all ones broadcast*).
- Addresses 127.X.X.X indicate a *loopback* (local loop) in the source station (frequently 127.0.0.1). Allows testing without passing via the network.
- Address 0.0.0.0 is the default address for the stations and the path to the *backbone* for the routers

Evolution of IP addressing

- The objective of network/subnet/host address organization is to simplify routing by grouping all the hosts on the same LAN onto one subnet. Routing is then done uniquely by the prefix (network/subnet part). The network part of the address is attributed by IANA, one of its regional representatives or an ISP. The part of the address attributed to the subnet is managed by the network administrator
- The original idea of the Internet was to have 3 network categories: large (class A), medium (class B) and small (class C). Unfortunately, it quickly turned out that many networks needed a class B address and this division into classes led to a "waste" of addresses.
- Towards 1995, the **CIDR** (*Classless Inter-Domain Routing*) removed this strict division and allowed the allocation of variable length network addresses grouped through ISPs.
- Current estimations indicate that IP version 4 will run out of addresses in a few years. Note that numerous assigned IP addresses are not (yet) used.
- The extension of Internet addresses to 16 bytes was one of the main reasons for the new version of IP (IPv6). Current estimations predict that there will be a shortage of IPv4 addresses between 2014 and 2018.
- (for example, see the detailed analysis at *http://bgp.potaroo.net/tools/ipv4*).

Whois? 160.98



https://www.ripe.net

160.98 neighbors

160.091.0.0 Oak Ridge National Laboratory, NET-ORNL-NETB3 P.O. Box 2008 Oak Ridge, TN 3783 US

160.092.0.0 Axime S.A.NET-SEGINZ.I. - Rue de la Pointe 59133 SeclinFrance SEGIN 160.92.0.028-Aug-96.

160.093.0.0 New Jersey Department of Transportation NET-NJDOTCN 6001035 Parkway Ave.Trenton, NJ 08625 NJDOT 160.93.0.001-May-92.

160.094.0.0 University of Minnesota NET-UMN-OTHERNetworking ServicesComputer and Information Services University of Minnesota 130 Lind Hall 207 Church St SE Minneapolis MN 55455-0134USA UMN-OTHER 160.94.0.014-Oct-97.

160.095.0.0 Cummins Engine Co. NET-CUMMINS-FS 500 Jackson Street Columbus, IN 47201 CUMMINS-FS 160.95.0.029-Sep-94.

160.096.0.0 National Computer Board NET-NCB-SGNET71 Science Park Drive NCB Building SINGAPORE 0511 NCB-SGNET

160.097.0.0 Universita' della Calabria NET-CALUNIV Universita' della Calabria Dipartimento di Fisica Contrada Arcavata di Rende I-87036, (Cosenza)IT CALUNIV

160.098.0.0 ECOLE D'INGENIEURS FRIBOURGNET-EIF Perolles 80 CH-1705 Fribourg Switzerland EIF 160.98.0.016-Jun-98.

160.099.0.0 Univerzitet U Nisu NET-UNINET-NIS Rektorat Univerziteta u NisuTrg Bratstva i jedinstva 2,18000 Nis Yugoslavia UNINET-NIS

160.100.0.0 AIX Systems Support Centre, IBMUK) Ltd. Mountbatten House (MH2B7)Basing View Basingstoke Hampshire RG21 1EJUnited Kingdom

160.101.0.0 Teknekron Software Systems, Inc.NET-TSS530 Lytton Ave., Suite 301 Palo Alto, CA 94301 TSS160.101.0.002-May-95.

160.102.0.0 Chadron State College NET-CSCNET4Chadron State College Computer Center-Ann Burk1000 S. Main StreetChadron, NE 69337 CSCNET4160.102.0.021-Jul-93.

160.103.0.0 European Synchrotron Radiation Facility NET-ESRFNETESRF, B.P. 220 , 38043 Grenoble Cedex - France ESRFNET160.103.0.021-May-93.

160.104.0.0 Tadpole Technology, IncNET-TADPOLE137 Ditton Walk Cambridge CB5 8FNUK TADPOLE160.104.0.003-Nov-97.

160.105.0.0 No match

160.106.0.0 External Affairs and International NET-SIGNET3125 Sussex Drive Ottawa, Ontario Canada K1A 0G2 SIGNET3160.106.0.018-May-92.

160.107.0.0 Naval Air Systems Command Headquarters NET-NAVAIRHQ-NET Naval Air Systems Command HQ Information Management Department 7.222467 Millstone Road, Building 1490 Patuxent River, MD 20670 NAVAIRHQ-NET160.107.0.006-Apr-99.

160.108.0.0 Loral NET-NASA-SSCCPO Box 58487 Houston, TX 77258 NASA-SSCC160.108.0.019-May-92.

Private and reserved addresses

Internet (RFC 1918) has reserved three blocks of IP addresses for "private networks". These addresses are destined for "watertight" networks not connected to the Internet. If they are released accidentally, they will be identified as such by routers

"Class A"	10.0.0.0 - 10.255.255.255
"Class B"	172.16.0.0 - 172.31.255.255
"Class C"	192.168.0.0 - 192.168.255.255

IPv4 reserved addresses (RFC 3330)

0.0.0.0/8	"This" Network	[RFC1700, page 4]
10.0.0.0/8	**Private-Use Networks**	**[RFC1918]**
14.0.0.0/8	Public-Data Networks	[RFC1700, page 181]
24.0.0.0/8	Cable Television Networks	--
39.0.0.0/8	Reserved but subject to allocation	[RFC1797]
127.0.0.0/8	**Loopback**	**[RFC1700, page 5]**
128.0.0.0/16	Reserved but subject to allocation	--
169.254.0.0/16	**Link Local***	
172.16.0.0/12	**Private-Use Networks**	**[RFC1918]**
191.255.0.0/16	Reserved but subject to allocation	--
192.0.0.0/24	Reserved but subject to allocation	--
192.0.2.0/24	Test-Net	
192.88.99.0/24	6to4 Relay Anycast	[RFC3068]
192.168.0.0/16	**Private-Use Networks**	**[RFC1918]**
198.18.0.0/15	Network Interconnect Device Benchmark Testing	[RFC2544]
223.255.255.0/24	Reserved but subject to allocation	--
224.0.0.0/4	Multicast	[RFC3171]
240.0.0.0/4	Reserved for Future Use	[RFC1700, page 4]

* Used by hosts in a watertight network. Obtained by auto-configuration (e.g. DHCP server not found)

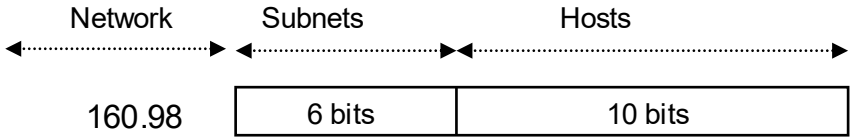
Sub-networks (*subnetting*)

Routing permits the organization of a network into different subnets (RFC 950), which correspond to point-to-point links or local networks separated by routers.

In class A/B/C or variable length addresses, it is possible to introduce optimum sized subnets for partitioning the network.

For creating subnets, addresses must be considered in binary form.

All combinations of bit numbers for the subnets and hosts are permitted, on condition that the total is equal to the number of bits allocated to the subnets/hosts in the class.



In the above example, there is a class B address in which 62 subnets have been created, each with 1022 hosts.

Subnet addresses formed uniquely of "0" or "1" are not recommended (the mask must be provided in order to avoid ambiguity in the network designation or the *broadcast*).

Possible masks

The decimal values of **possible mask** bytes are as follows:

Mask byte	Decimal value
1000'0000	128
1100'0000	192
1110'0000	224
1111'0000	240
1111'1000	248
1111'1100	252
1111'1110	254
1111'1111	255

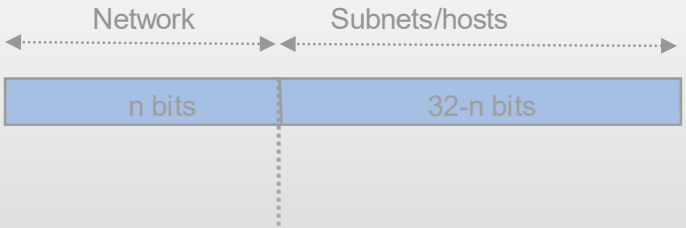
Note: masks are also frequently indicated by the number n of bits at "**1**" by **/n**.
For example, the mask of a class C address is /24. We speak of "*slash notation*", "CIDR *notation*" or " ***prefix***".

CIDR: *Classless Inter-Domain Routing*

Classful and *Classless*

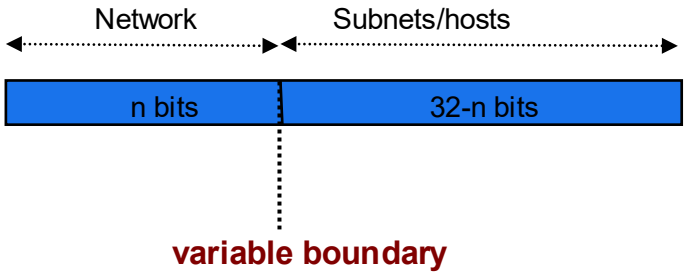
By extending the concept of *supernetting*, the CIDR can liberate classes:

Classful: respects classes A, B and C



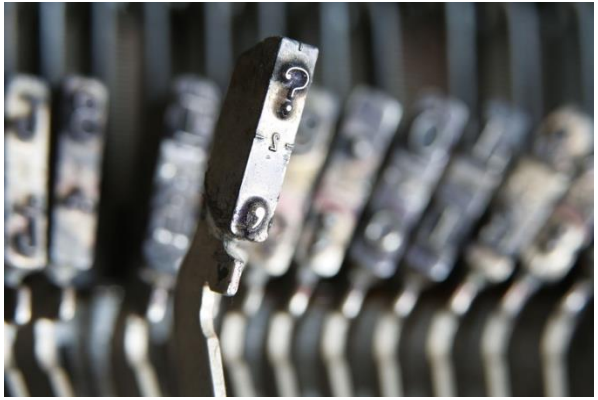
- Allocation of addresses as practiced up until the middle of the '90s
- Simple to administer
- Very quickly wastes addresses since there

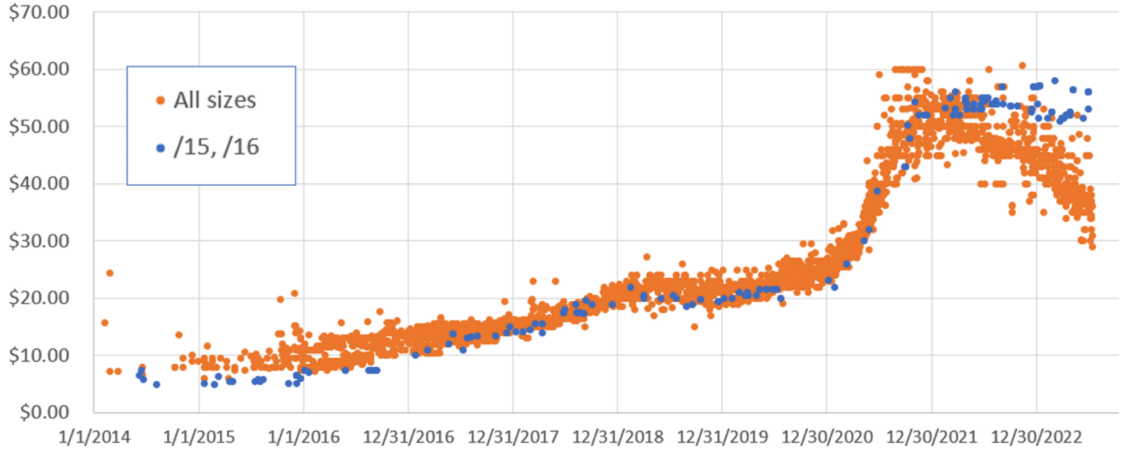
Classless: ignores classes A, B and C



- Allocation of addresses through ISPs
- Network address from 3 to 32 bits
- Network addresses may be aggregated to form a "super address", which requires only one routing entry
- More complicated to administer
- Optimises address utilisation

Why IPv4?

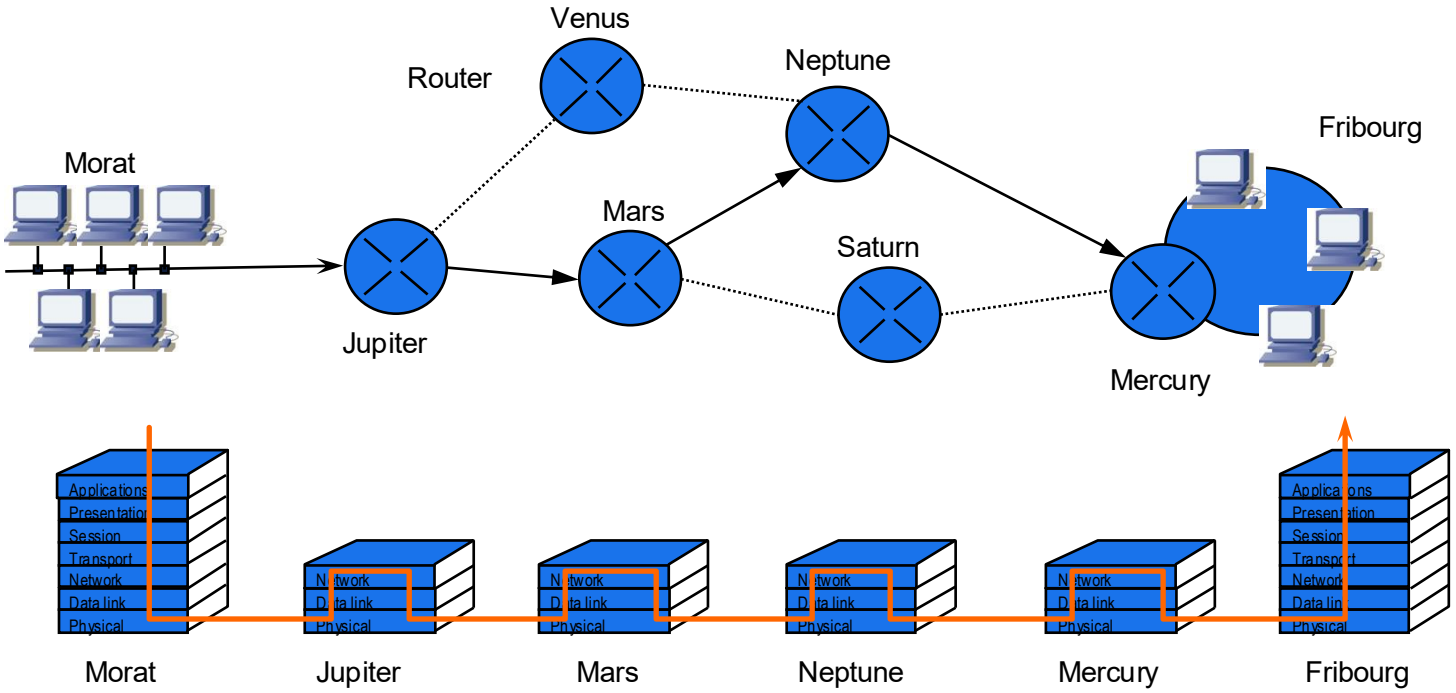




Source : https://circleid.com/posts/20230817-ipv4-prices-supply-and-demand-in-2023 (data by IPv4.Global)

Routing

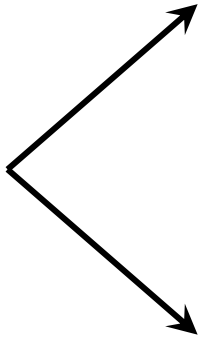
Routing



Routing: Transportation of packets from one end of a network to the other at the network layer level by selecting the path. Allows the interconnection of different networks.

Router operations (1)

Router functions

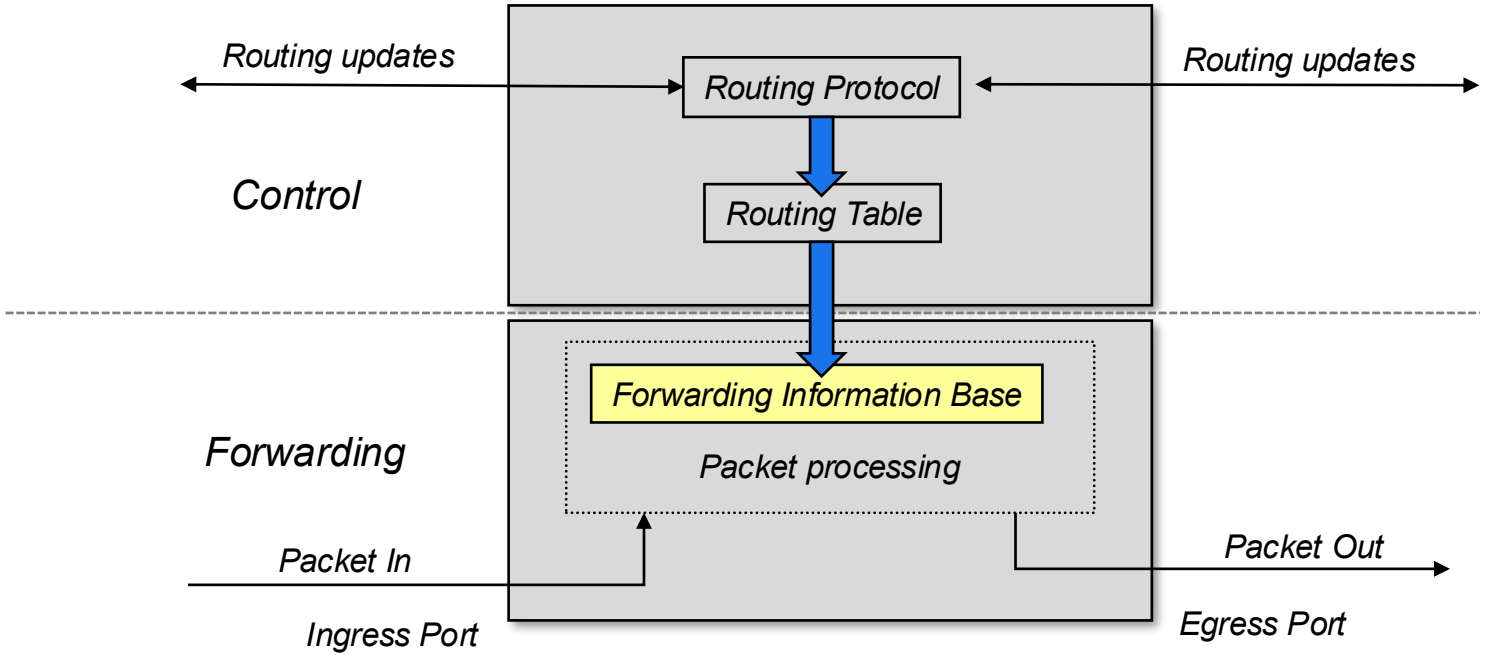


Management of the routing table (*control, control plane*). The routing table (*cache*) indicates the path to follow through the network by giving the address of the next router if the destination network is not connected directly. This routing table is either configured manually or established and managed by exchanging information about the network topology with other routers (routing protocol). Essentially SW.

Transfers (*forwarding, data plane*): Choice of the egress port as a function of the *Net prefix* based on the transport table (*Forwarding Information Base*) extracted from the routing table. The transport table gives the egress port and the address of the next router directly as a function of the *Net Prefix*.

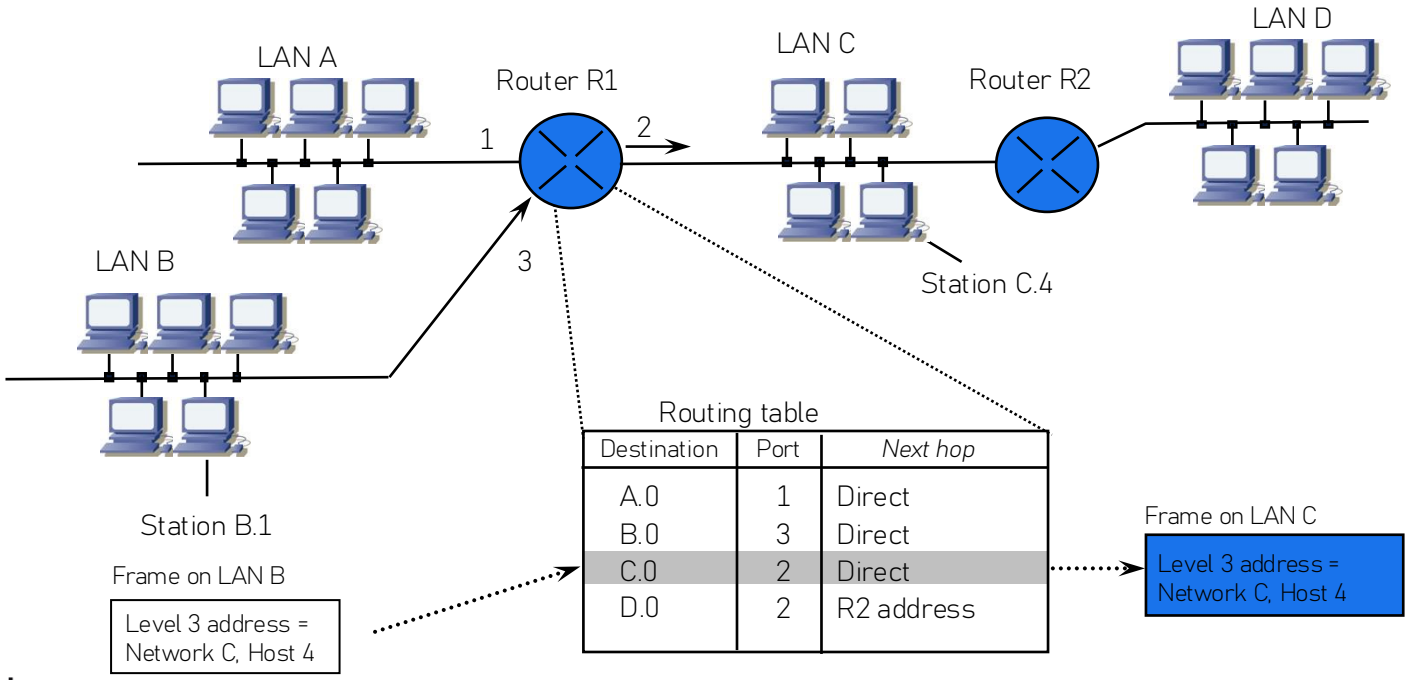
Modification of the packet header, if necessary. With IP, the time to live field must be incremented backwards and the error control field recalculated. Transmission of the packet via the egress port chosen. Essentially HW.

Router operations (2)



Routing table

Hosts: B.1, C.4, …
Networks/*Subnets:* A.0, B.0, C.0, D.0

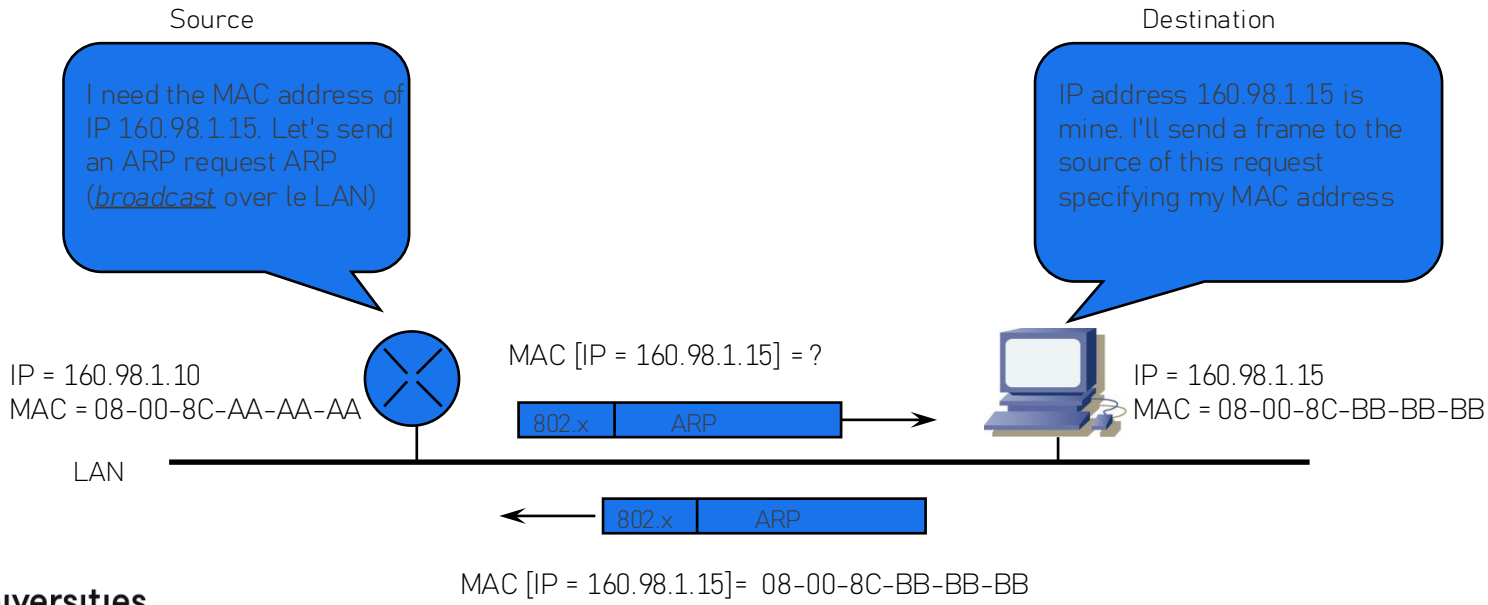


Direct, Indirect and Default Routing

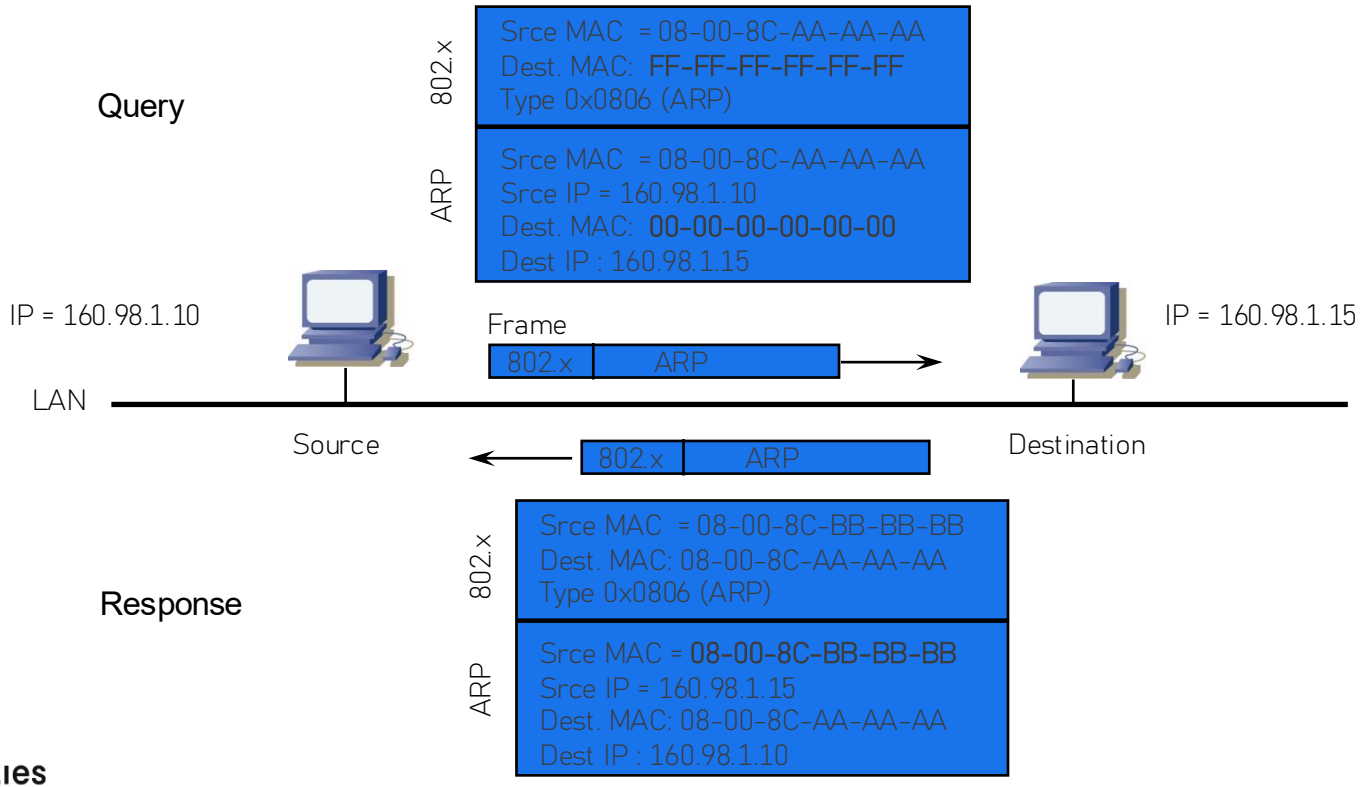
Direct	Routing to a destination that resides on the same network (same subnet as the egress port is connected on)
Indirect	Routing to a destination that resides on a remote network, using a table that specify the first router to use to reach this destination.
Default	Indirect routing through a default router (destination address is not found in the routing table of the source host). Identified with the IP address : 0.0.0.0

ARP (Address Resolution Protocol)

Address Resolution Protocol (ARP, RFC 826): to find the MAC address based on the IP address when the source and destination are on the **same** *subnet*



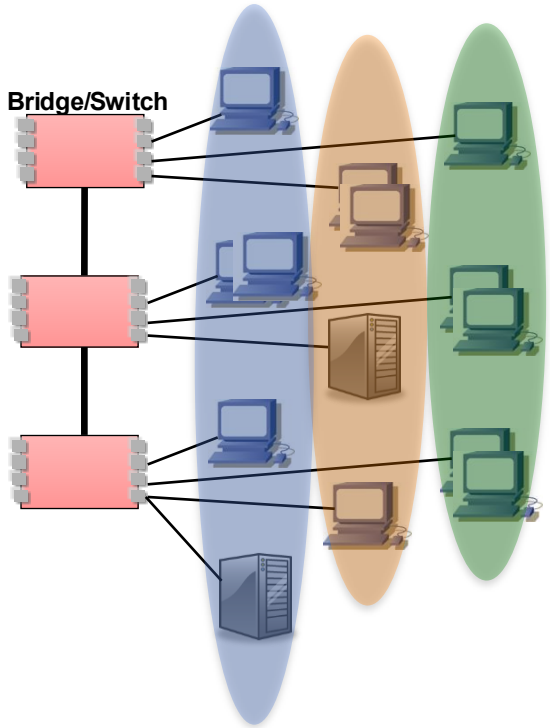
ARP frames


Query
802.x
Srce MAC = 08-00-8C-AA-AA-AA
Dest. MAC: FF-FF-FF-FF-FF-FF
Type 0x0806 (ARP)
ARP
Srce MAC = 08-00-8C-AA-AA-AA
Srce IP = 160.98.1.10
Dest. MAC: 00-00-00-00-00-00
Dest IP : 160.98.1.15
IP = 160.98.1.10
IP = 160.98.1.15
Frame
802.x
ARP
LAN
Source
Destination
802.x
ARP
Response
802.x
Srce MAC = 08-00-8C-BB-BB-BB
Dest. MAC: 08-00-8C-AA-AA-AA
Type 0x0806 (ARP)
ARP
Srce MAC = 08-00-8C-BB-BB-BB
Srce IP = 160.98.1.15
Dest. MAC: 08-00-8C-AA-AA-AA
Dest IP : 160.98.1.10

Virtual LAN : Definition

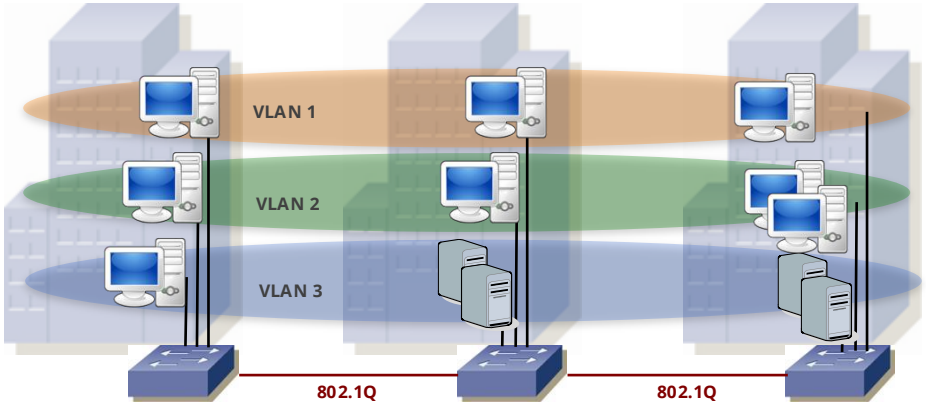
A **VLAN** (*Virtual Local Area Network*) could be define as:

- Group of hosts that are not sharing a physical medium, but that have the impression to do it. (Physical location of host is distributed)
- Hosts are connected trough *switches* that support Virtual LANs
- Hosts are communicating through the use of MAC addresses, without crossing a router
- The different VLANs are separated by routers
- A broadcast frame is sent to all stations of a VLAN (limited diffusion)
- Modern design has 1 VLAN = 1 IP Subnet



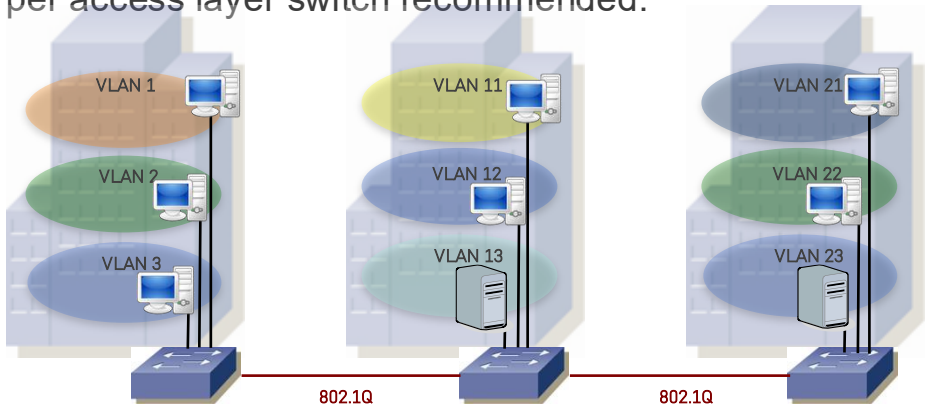
End-to-End VLANs

- Each VLAN is distributed geographically throughout the network.
- Users are grouped into each VLAN regardless of the physical location, theoretically easing network management.
- As a user moves throughout a campus, the VLAN membership for that user remains the same.



Local VLANs

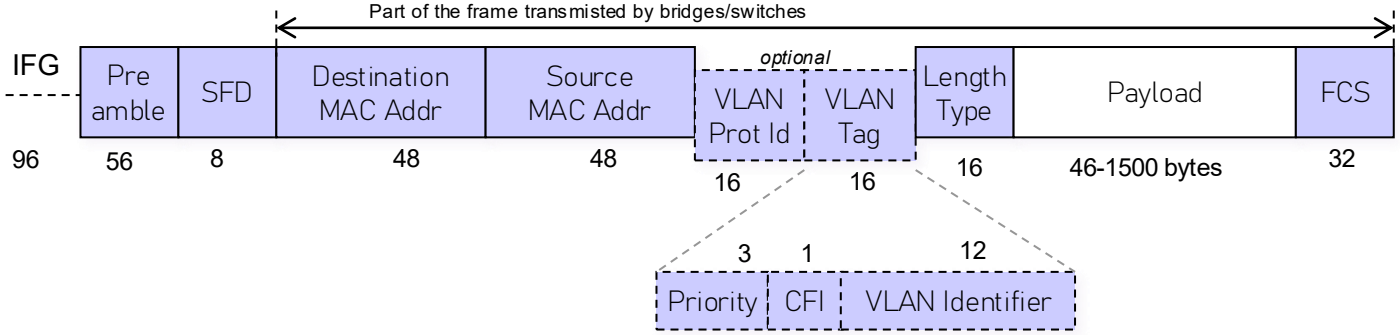
- Create local VLANs with physical boundaries in mind rather than job functions of the users.
- Local VLANs exist between the access and distribution layers.
- Traffic from a local VLAN is routed at the distribution and core levels.
- Spanning tree is used only to prevent inadvertent loops in the wiring closet.
- One to three VLANs per access layer switch recommended.



Advantages and disadvantages of VLANs

- ↗ *Broadcasts* stay inside a VLAN, better bandwidth usage
- ↗ Users and hosts are not grouped based on their physical location (LAN cabling), but on a logical base (functions, organization, protocols, IP Subnets, etc.). Changes are then simplified
  - → Grouped by virtual organization.
- ↗ **Security**: by isolating a group of users, we can more easily check the access to network resources.
- ↗ Cost: we use all the ports of all switches !
- ↘ VLAN Management could be complex : standards knowledge, trainings, etc.
- ↘ Administration protocols used by the control plane (supervision and configuration protocols) are consuming bandwidth
- ↘ On layer 3 VLANs, address attribution with DHCP could be problematic
- ↘ Cohabitation of proprietary standards (ISL, VTP, ..) and official standards (802.1Q, 802.1P,…) could also be problematic

IEEE 802.3 & 802.1Q : Frame format



Extension of the IEEE 802.3 frame:

- → **VLAN Protocol Id**: use with Ethernet = 0x8100
- → **VLAN Tag Priority**: 0..7 (default 0)
- → **VLAN Tag CFI** (Canonical Format Indicator) : 0 in the Ethernet networks (this flag is used with 802.1Q and the token-ring network)
- → **VLAN Tag VLAN Identifier** : 0..4095

Wireshark