University of Applied Sciences and Arts
of Southern Switzerland
SUPSI

Course I4051

Telematica, Crittografia e Sicurezza

Angelo Consoli
SUPSI-DTI , Lugano-Viganello 2021/22

Course outline

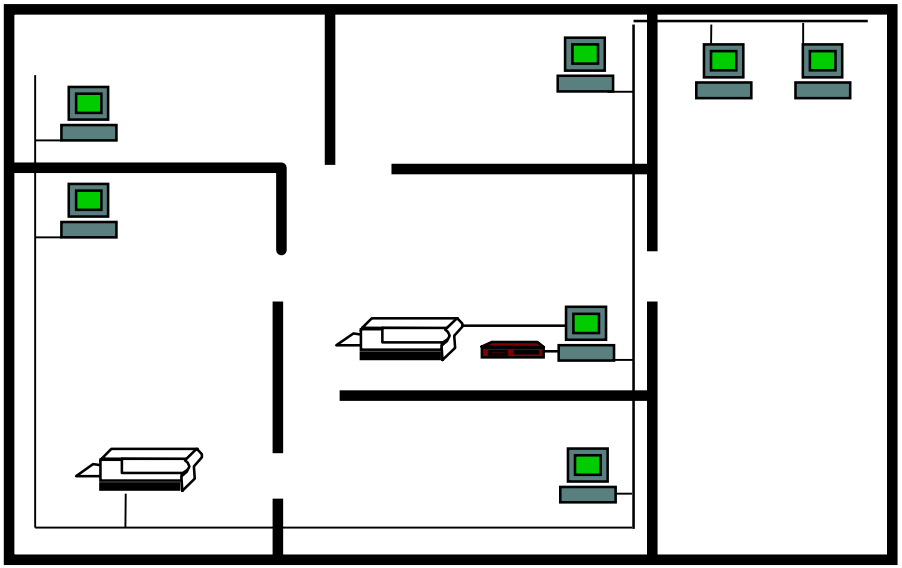
- General terms
- Local networks and distributed networks: architectures
- The justification of standards. Standardization bodies.
- The OSI reference model
- Local Area Networks (LAN): characteristics, infrastructures
- Wide Area Networks (WAN): characteristics, infrastructures
- Introduction to the most important network protocols
- Understanding data communication networks
- Intro to high performance networks and boardband technologies
- From protocols to applications

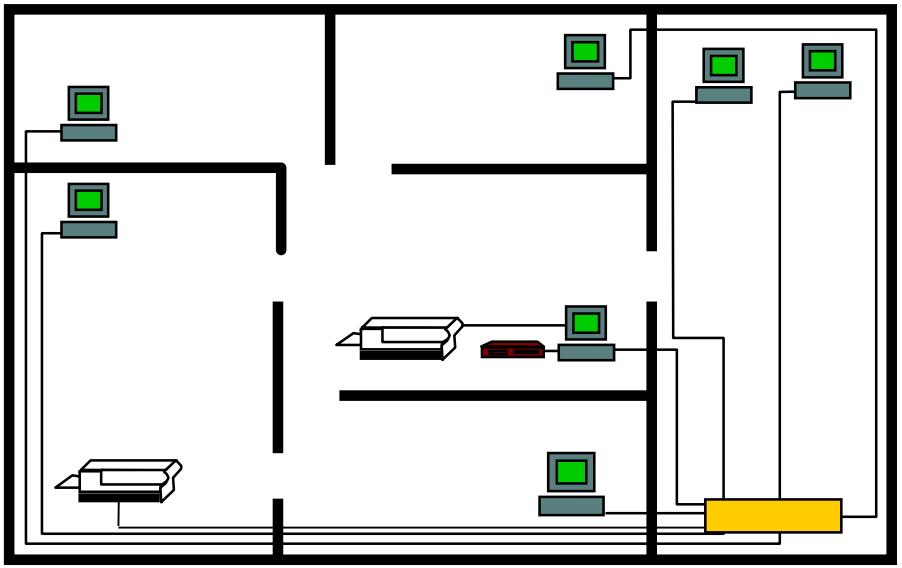
Computer networks: definitions

- **LAN** local **a**rea **n**etwork
- **MAN** **m**etropolitan **a**rea **n**etwork
- **WAN** **w**ide **a**rea **n**etwork
- **GAN** **g**eographical **a**rea **n**etwork

- **BAN** **b**ody **a**rea **n**etwork
- **PAN** **p**ersonal **a**rea **n**etwork
- **CAN** **c**ar **a**rea **n**etwork
- **SAN** **s**torage **a**rea **n**etwork

What is a LAN, how it works

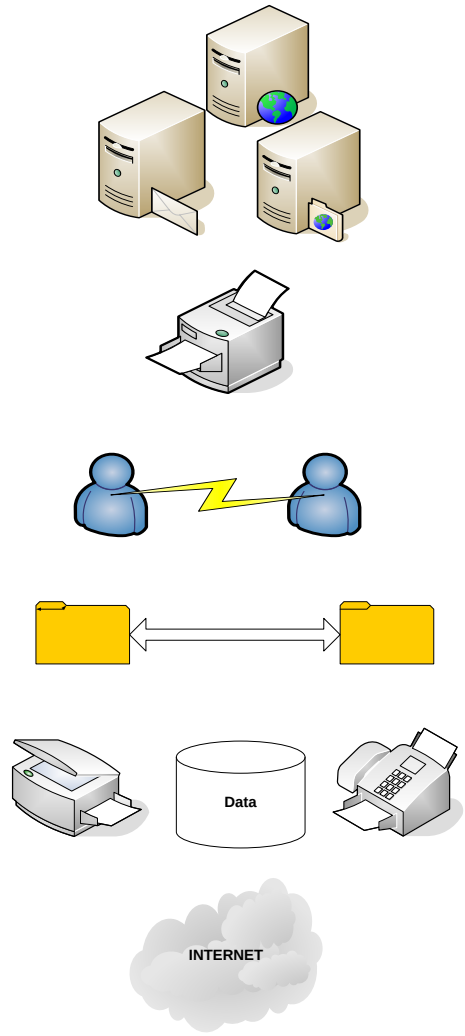




A LAN is a network of nodes (computer and other infrastructures) locally interconnected (in a geographically limited area)

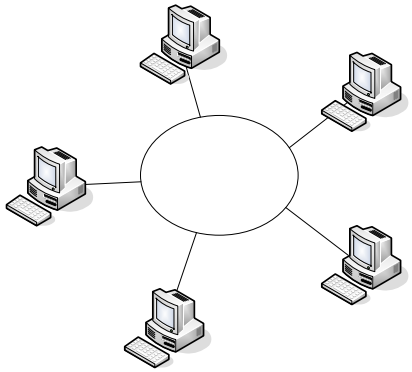
Benefits of a LAN

- File and document sharing
- File transfer
- Email
- Sharing of infrastructures:
  - printers,
  - scanners,
  - fax,
  - external connectivity,
  - …
- Centralized backups
- Shared/Centralized corporate database and data structures

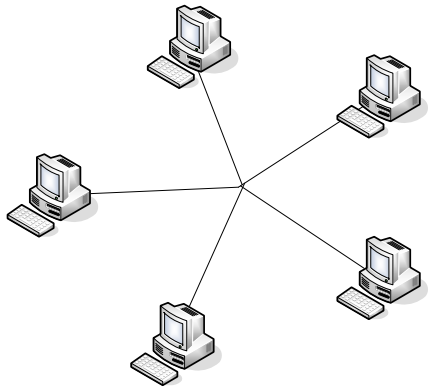


Computer Networks: reference architectures

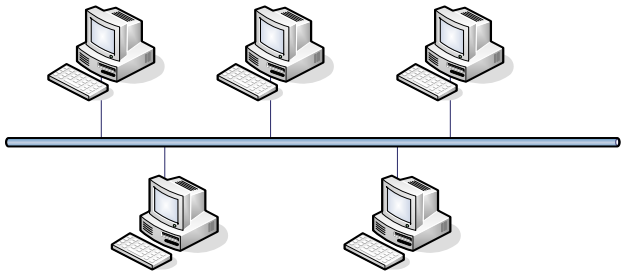
Extremely important: distinguishing between logical and physical level !



Ring



Star



Bus

Standardization bodies

ISO	International Organization for Standardization (ISO) {e.g. The OSI reference model}
ANSI	American National Standards Institute {e.g. FDDI}
EIA	Electronic Industries Association {e.g. RS232C}
IEEE	Institute of Electrical and Electronic Engineers {e.g. IEEE 802.3}
ITU-T	International Telecommunication Union Telecommunication Standardization Sector, also known by its old name CCITT {e.g. X.25}
IAB	Internet Architecture Board {e.g. TCP/IP, SNMP}
IETF	Internet Engineering Task Force (The IETF is supervised by the Internet Society Internet Architecture Board (IAB)
IANA	Internet Assigned Numbers Authority

Justification for the use of standards

- Standards guarantee generalized dissemination of new technologies
- Standards allow interconnection of heterogeneous systems
- Standards allow independence from specific vendors and products
- They allow creation of new products through combination of existing building blocks
- Standards guarantee interfacing of different universal solutions at both electrical and mechanical level
- The standardization may cover several aspects, among them:
  - Hardware level / electrical level
  - Mechanical level
  - Operating logic of infrastructures, systems and subsystems
- We distinguish among: *de facto standards and de jure standards*

ITU-T main standardization categories

Alphanumeric categories refer to standard groups:

- **V – serie:**
  data communication over switched phone lines (e.g. V.34)

- **X – serie:**
  data comunication over dedicated phone lines (e.g. X.400)

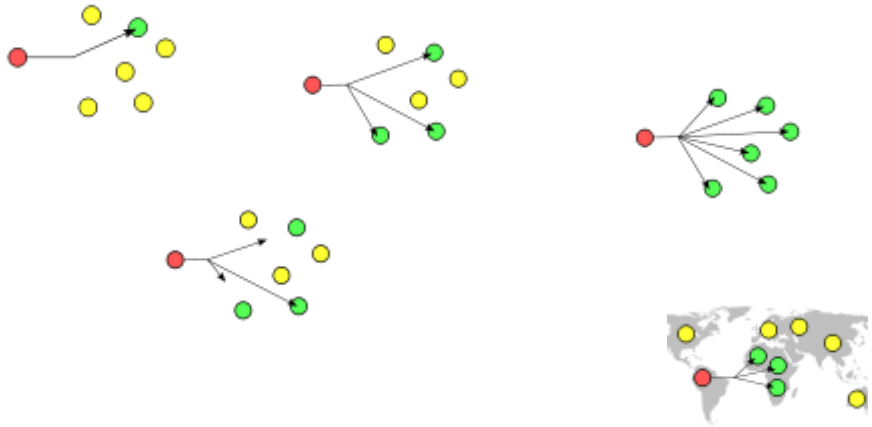
- **I – serie:**
  digital telephone system, ISDN (eg.. I.430)

Basic concepts (I)

- **Communication mode:**
  - Synchronous communication
  - Asynchronous communication
- **Connection mode:**
  - Point–to–point communication
  - Multipoint communication
- **Communication options:**
  - simplex
  - half–duplex
  - full–duplex
- **Interface types:**
  - DTE (Data Terminal Equipment)
  - DCE (Data Communication Equipment)

Basic concepts (II)

- **Services can be:**
  - *connection-oriented*
    - Creation of a connection;
    - Data transfer/exchange;
    - Release of the connection.
  - *connectionless*
    - Sending/transfer of data without establishing a connection among the communication nodes
- **Communication options:**
  - *unicast*
  - *multicast*
  - *broadcast*
  - *anycast*
  - *geocast*



Basic concepts (III)

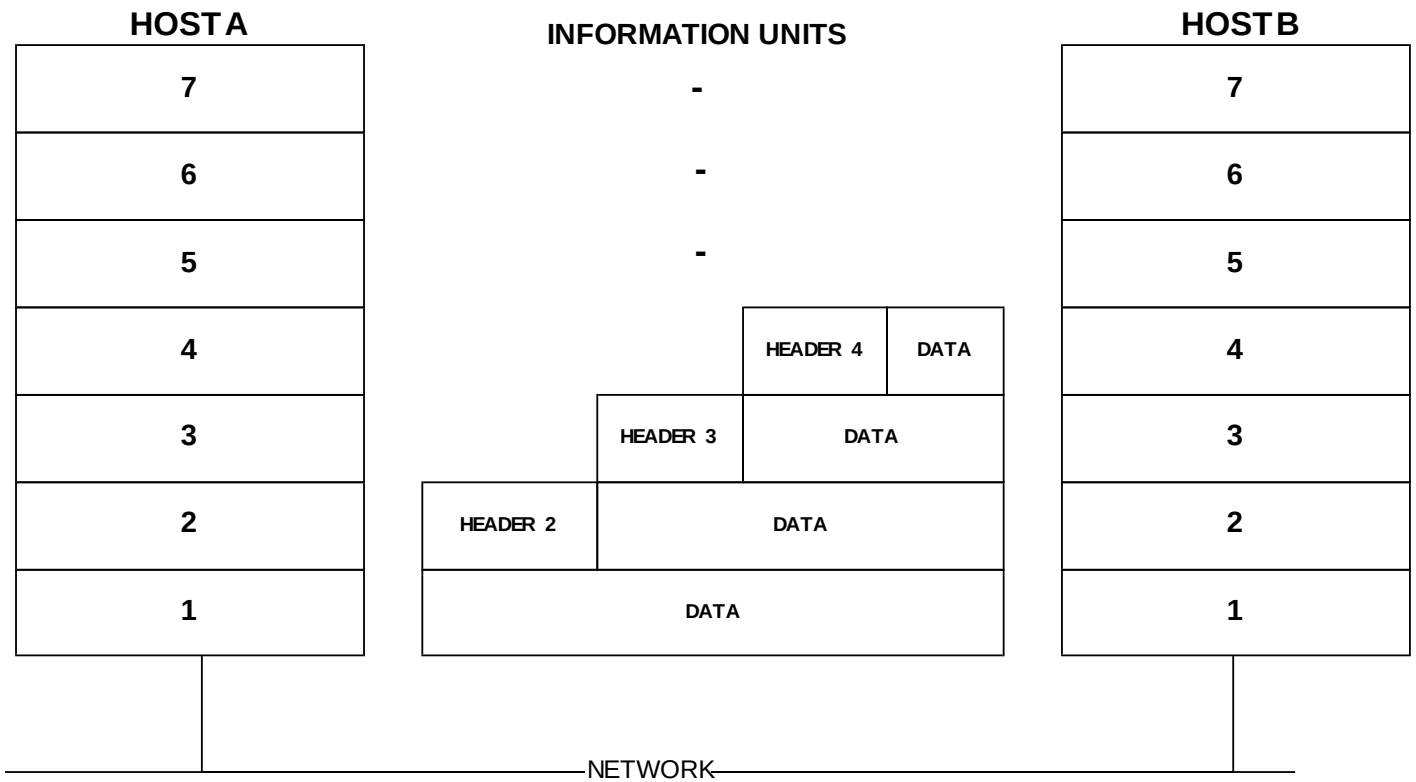
- **Services can be:**
  - Reliable
    - This type of service guarantee that all data is correctly sent to the due recipient.
    - Usually a confirmation message (*acknowledgement*) is necessary from the recipient side.
    - Reliability introduces an *overhead* that may be considered undesirable.
  - Not reliable

If a specified level doesn't offer a relaiable service, if reliability is needed this feautre can be provided by aupper layer

The OSI reference model

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

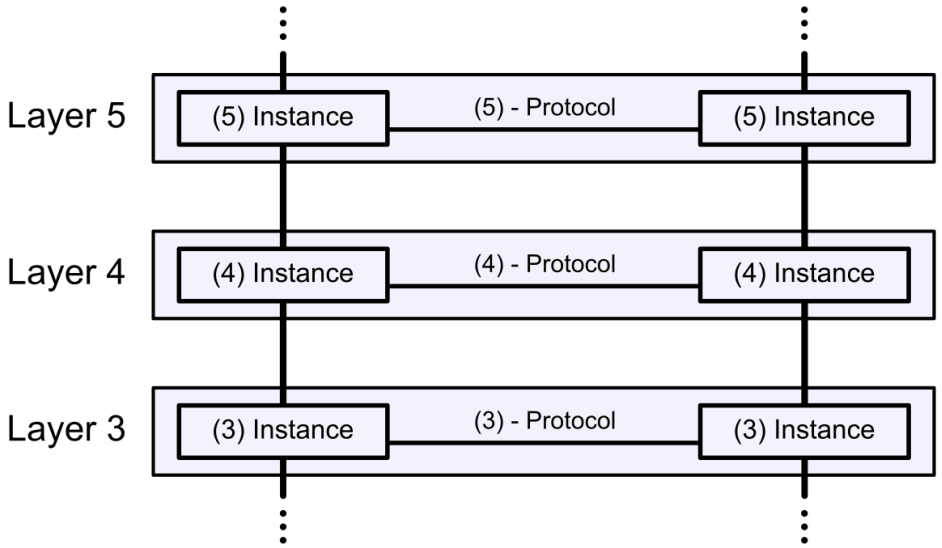
Information flow among levels



Each level adds information about the nature of data from/to the upper level

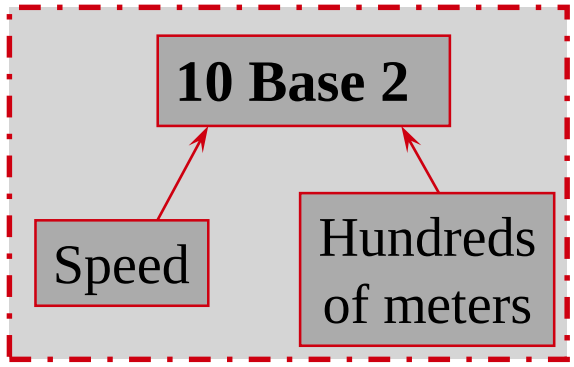
Relation between protocol and services

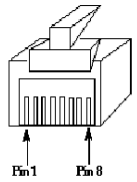
- Protocols define the methodology of an interaction, the layering of i.e. telecommunication protocol refer to the distinguishable sections within a protocol.
- Following the OSI model, the layers have an end to end check with the corresponding opposite layer.
- A service is delivered from the lower to the upper layer.
- The implementation of a service is not regulated, provided the service is delivered according to standards.



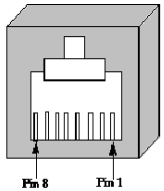
OSI Layer 1: Physical Layer: (I)

- **Cpper cables:**
  - 10 Base 5: thick coax, yellow cable
  - 10 Base 2: thin coax, BNC, RG58, 50 Ohm
  - 10 Base-T: twisted pair (RJ45)
    - UTP (Unshielded Twisted Pair)
    - STP (Shielded Twisted Pair)
  - AUI cable (Attachment Unit Interface)
  - Some standard cables:
    - UART / serial cable,
    - USB
    - Parallel cable,
    - Null-modem cable,
    - cross-over cable,
    - IEEE488 (GPIB)
  - Proprietary (non standard) cables

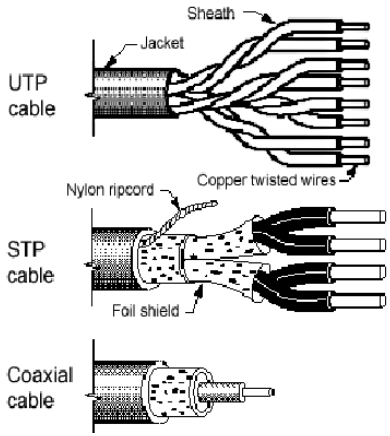




RJ-45 Jack Plug

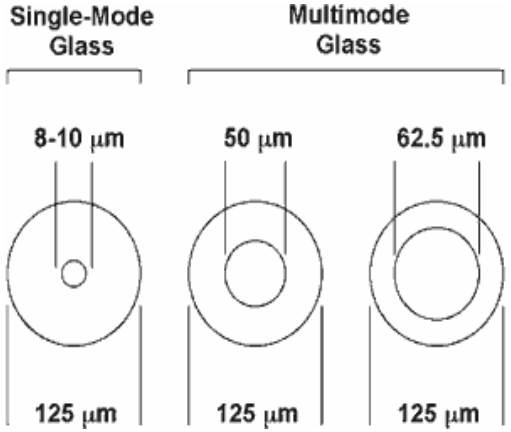


RJ-45 Jack Face



Physical layer: transmission media (II)

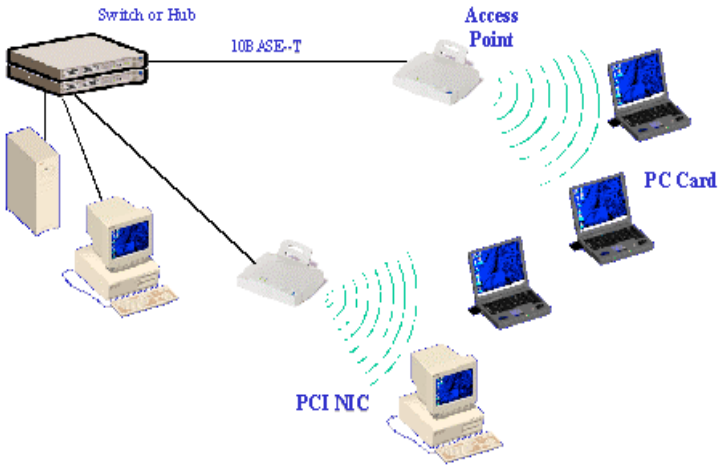
- **Optical fiber:**
  - Single/Mono Mode
  - Multi Mode



- **Wireless (radio frequency)**
  - Several Frequencies
  - Several standards

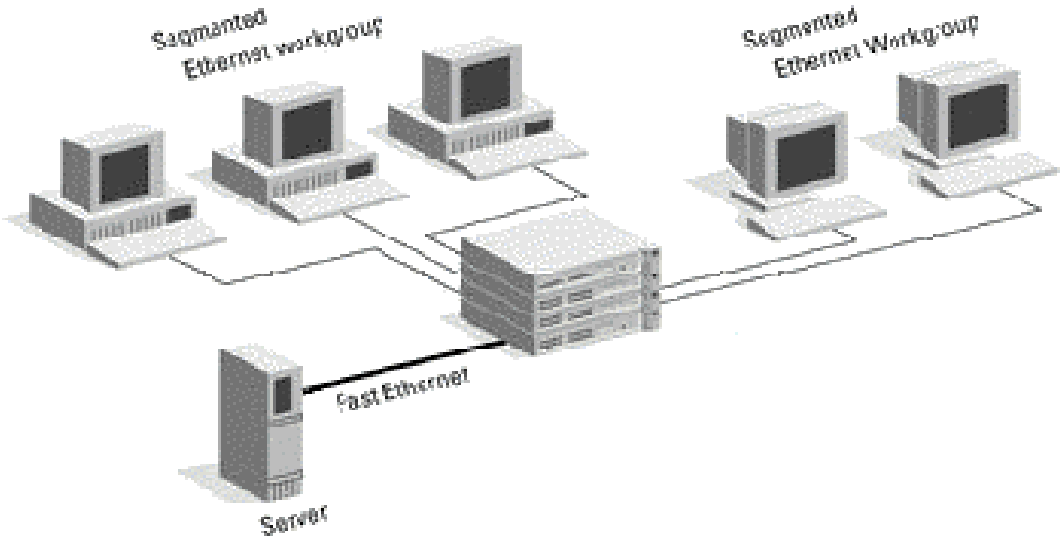
- **Infrared**

- **Other media ...**

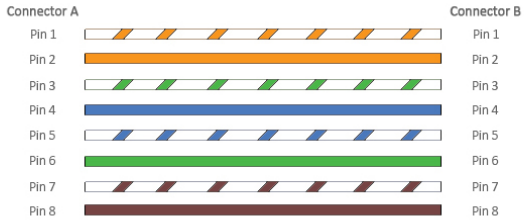


Physical layer: universal cable

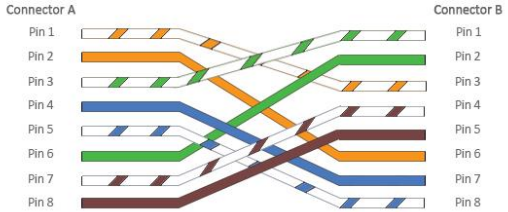
- Cabling standards:
  - ANSI: EIA/TIA 568 and TSB36 e TSB40
  - ISO/IEC DIS 11801.



Patch Cable/Straight Through Cable
Wring Scheme

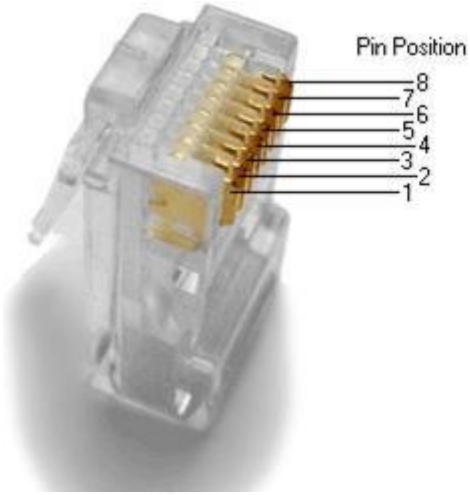


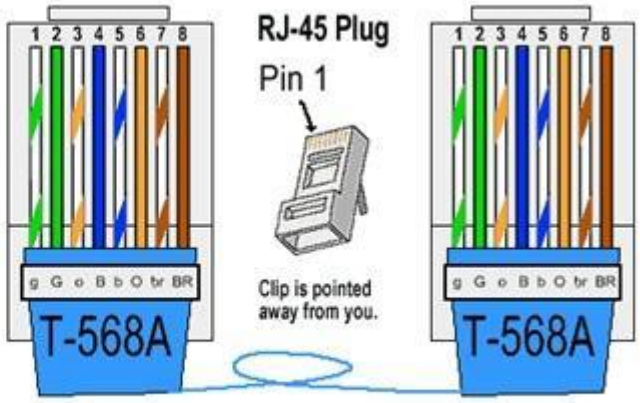
Crossover Cable Wring Scheme



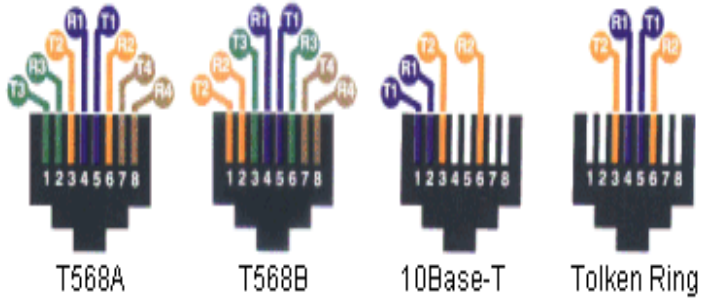
Physical layer: universal cable

Cavo	Frequenza (MHz)
Cat 3	16
Cat 4	20
Cat 5	100
Cat 6	250
Cat 7	600

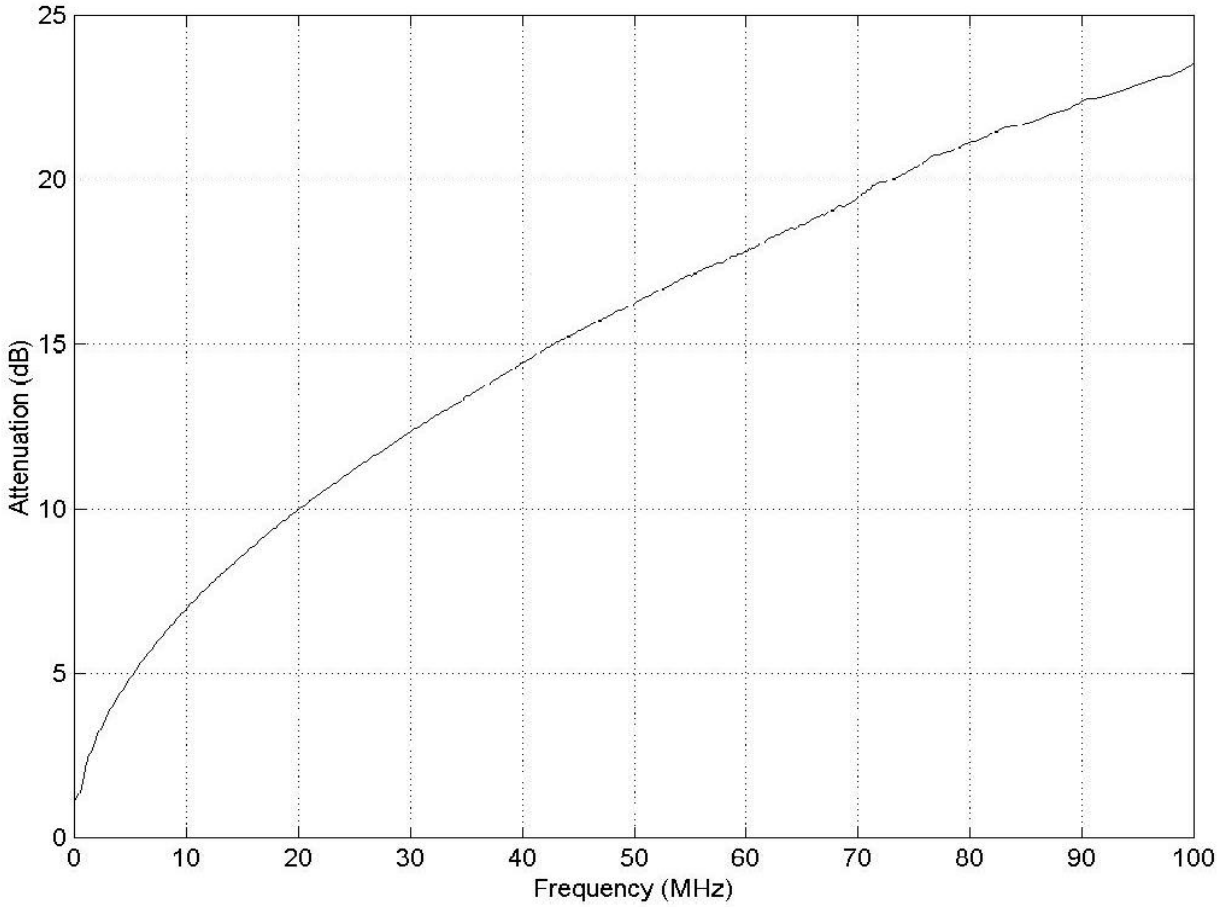




	Category 3	Category 5	Category 5e	Category 6	Category 6a	Category 7
Cable Type	UTP	UTP	UTP	UTP or STP	STP	S/FTP
Max. Data Transmission Speed	10 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10,000 Mbps	10,000 Mbps
Max. Bandwidth	16 MHz	100 MHz	100 MHz	250 MHz	500 MHz	600 MHz



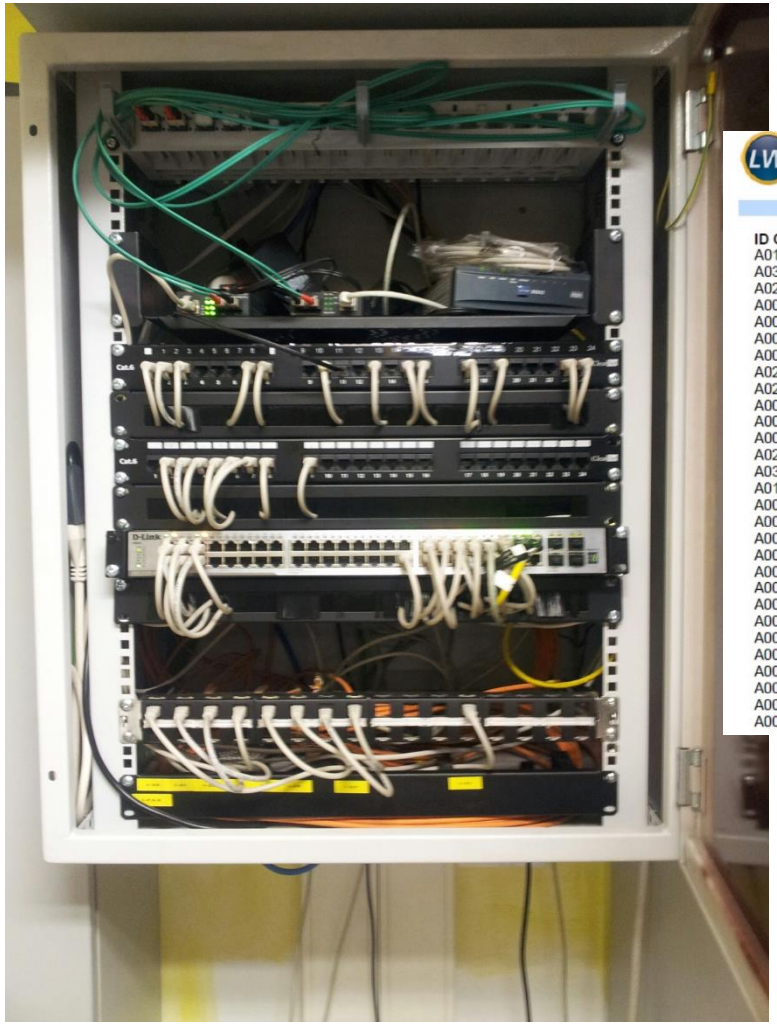
Physical layer: trasmission of segnals over cupper wire



Physical layer: infrastructures

- Network Interface Card (NIC)
- Repeater, Hub
- Media converter
- Transceiver
- MAU – Media Attachment Unit
- Multiport Transceivers
- Vampirs
- Patch Panel

Universal cabling and reports

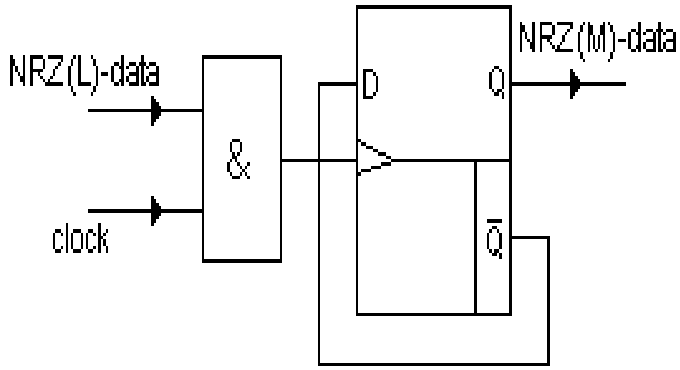


LINKWARE™ PC
CABLE TEST MANAGEMENT SOFTWARE

ID Cavo	Sommario	Limite di test	Lunghezza	Spazio Limite	Data / Ora
A010	PASSATO	ISO11801 Channel Class E	45 ft	2.5 dB (NEXT)	09/26/2015 11:35 AM
A030	PASSATO*	ISO11801 Channel Class E	45 ft	0.5 dB (NEXT)	09/26/2015 11:39 AM
A028	PASSATO*	ISO11801 Channel Class E	45 ft	0.7 dB (NEXT)	09/26/2015 11:42 AM
A003	PASSATO*	ISO11801 Channel Class E	67 ft	0.6 dB (NEXT)	09/26/2015 11:47 AM
A005	PASSATO	TIA Cat 5 Ch (TSB-95)	96 ft	11.2 dB (NEXT)	09/26/2015 11:51 AM
A006	PASSATO	TIA Cat 5 Ch (TSB-95)	96 ft	9.9 dB (NEXT)	09/26/2015 11:59 AM
A004	PASSATO	TIA Cat 5 Ch (TSB-95)	96 ft	9.1 dB (NEXT)	09/26/2015 12:01 PM
A026	PASSATO	TIA Cat 5 Ch (TSB-95)	95 ft	10.0 dB (NEXT)	09/26/2015 12:05 PM
A027	PASSATO	TIA Cat 5 Ch (TSB-95)	66 ft	15.2 dB (NEXT)	09/26/2015 12:08 PM
A002	PASSATO	TIA Cat 5 Ch (TSB-95)	46 ft	13.2 dB (NEXT)	09/26/2015 12:09 PM
A007	FALLITO	TIA Cat 5 Ch (TSB-95)	57 ft	6.3 dB (NEXT)	09/26/2015 12:13 PM
A008	PASSATO	TIA Cat 5 Ch (TSB-95)	67 ft	13.2 dB (NEXT)	09/26/2015 12:13 PM
A029	PASSATO	TIA Cat 5 Ch (TSB-95)	65 ft	11.5 dB (NEXT)	09/26/2015 12:15 PM
A031	PASSATO	TIA Cat 5 Ch (TSB-95)	67 ft	13.3 dB (NEXT)	09/26/2015 12:17 PM
A013	PASSATO	TIA Cat 5 Ch (TSB-95)	73 ft	8.9 dB (NEXT)	09/26/2015 12:19 PM
A009	PASSATO	TIA Cat 5 Ch (TSB-95)	68 ft	10.5 dB (NEXT)	09/26/2015 12:20 PM
A00	PASSATO	TIA Cat 5 Ch (TSB-95)	65 ft	11.1 dB (NEXT)	09/26/2015 12:23 PM
A0033	PASSATO	TIA Cat 5 Ch (TSB-95)	65 ft	9.3 dB (NEXT)	09/26/2015 12:25 PM
A0015	PASSATO	TIA Cat 5 Ch (TSB-95)	53 ft	14.3 dB (NEXT)	09/26/2015 12:27 PM
A0021	PASSATO	TIA Cat 5 Ch (TSB-95)	66 ft	8.6 dB (NEXT)	09/26/2015 12:33 PM
A0023	PASSATO	TIA Cat 5 Ch (TSB-95)	76 ft	12.3 dB (NEXT)	09/26/2015 12:43 PM
A0022	PASSATO	TIA Cat 5 Ch (TSB-95)	75 ft	11.7 dB (NEXT)	09/26/2015 12:44 PM
A0017	PASSATO	TIA Cat 5 Ch (TSB-95)	79 ft	11.5 dB (NEXT)	09/26/2015 12:45 PM
A0018	PASSATO	TIA Cat 5 Ch (TSB-95)	96 ft	11.8 dB (NEXT)	09/26/2015 12:46 PM
A0012	PASSATO	TIA Cat 5 Ch (TSB-95)	162 ft	9.6 dB (NEXT)	09/26/2015 12:47 PM
A0019	PASSATO	TIA Cat 5 Ch (TSB-95)	201 ft	13.0 dB (NEXT)	09/26/2015 12:52 PM
A0024	PASSATO	TIA Cat 5 Ch (TSB-95)	201 ft	13.6 dB (NEXT)	09/26/2015 12:53 PM
A0011	PASSATO	TIA Cat 5 Ch (TSB-95)	161 ft	9.4 dB (NEXT)	09/26/2015 12:55 PM
A0016	PASSATO	TIA Cat 5 Ch (TSB-95)	26 ft	18.7 dB (NEXT)	09/26/2015 01:02 PM

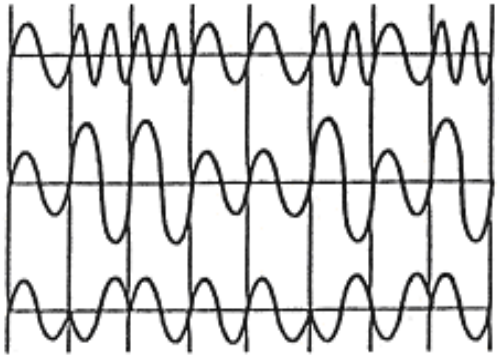
Information transmission (I)

- Direct signal transmission
- Signal modulation transmission
- Base band coding transmission
  - NRZ e RZ codes
  - Phase coding codes
  - Multilevel codes
  - Polar and unipolar coding



Information transmission (II)

- **Digital signal conversion to analog (modem)**
  - Amplitude modulation (ASK)
  - Frequency modulation (FSK)
  - Phase modulation (PSK)
  - Quadrature modulation (QAM)



- **Multiplexing:** multiple channel communication on the same shared medium:
  - techniques:
    - Time division multiplexing (TDM)
    - Frequency division multiplexing (FDM)
    - Wavelength division multiplexing (WDM)
    - Orthogonal frequency division multiplexing (OFDM)

OSI Level 2: data link layer

- It must guarantee to its upper layer a link without errors.
- It must manage how a machine/device access a network.
- It works on hardware addressing with elements that can be identified on this level (e.g. NIC, Bridge, Switch, …) e.g. MAC address ethernet: 08-00-2B-CA-CC-98
- It manages framing (data packets sorting)
- Error detection (checksums, parity bits)
- Error correction (e.g. Hamming code)
- It is able to solve shared media communication conflicts.

What can cause trasmission errors

- Johnson–Nyquist noise (thermal noise): electronic noise generated by the electrons in copper conductor.
- Impulse noise (issues caused by a machine, either mechanical or electric, changing state).
- All physical measures that distinguish a signal (amplitude, propagation speed, phase) they vary according to frequency.
- Mutual interference (crosstalk).
- Echoes on the transmission lines
- Attenuation caused by transmission lines

Due the nature of errors, they tend to appear in a burst effect instead of being an isolated event

Data integrity checks

- **Parity**
  In terms of parity we distinguish even and odd parity, this calculation is based on the bit states MARK or SPACE
  - VRC (vertical redundancy checking)
  - BCC (block check character)
  - SRC (spiral redundancy checking)
  - Interleaving

- **CRC (Cyclic Redundancy Checking)**
  This method is based on the fundamental theory that if a **integer number** of *n* digits is divided by a **prime number**, the **remainder** of the division will be an unique number valid for all *n* digits integer number. Prime number example:

CRC-16: $X^{16} + X^{15} + X^{2} + 1$

CRC-CCITT: $X^{16} + X^{12} + X^{5} + 1$

Error checks (I)

- VRC

Bit position #	#1	#2	#3	#4	#5
1	0	1	0	1	1
2	1	0	0	1	0
3	0 → 1	0	1	1	0
4	0	1 → 0	1	1	1
5	0	0 → 1	0	1	1
6	0	0	0	1	0
7	1	1	1	1	1
Parity Odd	1 → (0)	0 → (0)	0	0	1

Error checks (II)

- BCC

Bit position #	#1	#2	#3	#4	#5	Block parity char
1	0	1	0	1	1	0
2	1	0	0	1	0	1
3	0	0 → 1	1	1 → 0	0	1 → (1)
4	0	1 → 0	1	1 → 0	1	1 → (1)
5	0	0	0	1	1	1
6	0	0	0	1	0	0
7	1	1	1	1	1	0
Parity Odd	1	0 → (0)	0	0 → (0)	1	1

Error checks (III)

- SRC

Bit position #	#1	#2	#3	#4	#5	#6	#7	#8	#9	Block parity char
1	0	1	1	1	0	0	0	0	1	0
2	1	1	1	0	0	0	1	1	1	1
3	1	0	0	0	0	1	0	1	0	0
4	0	0	0	1	0	1	0	1	0	0
5	0	1	0	1	1	0	1	1	0	1
6	1	1	0	0	1	0	1	0	0	0
7	0	0	1	0	1	0	1	0	1	0
8	1	1	1	1	0	0	0	0	0	1

Error checks (IV)

- Interleaving

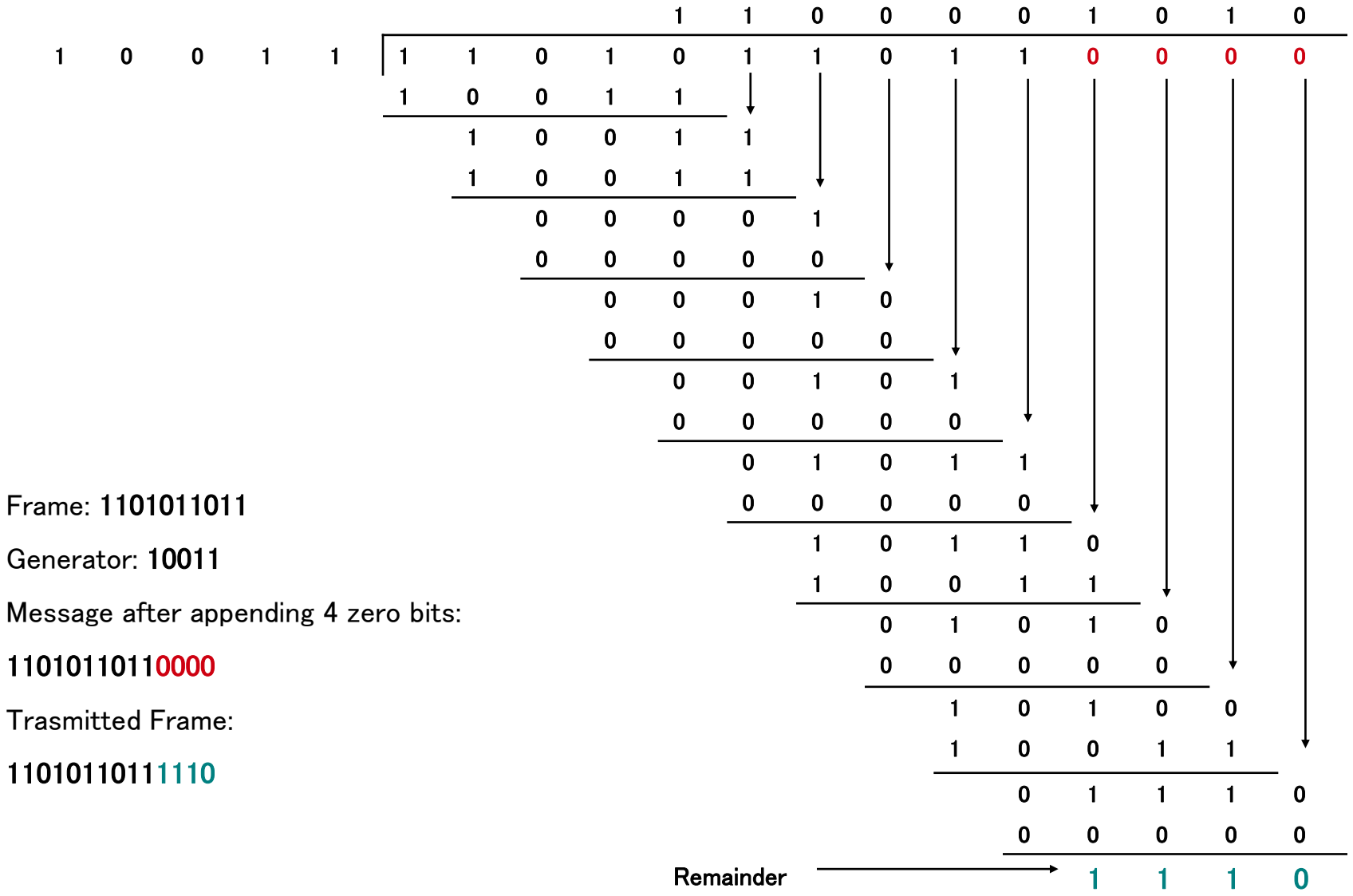
Original Characters

A 12345678	B 12345678	C 12345678	D 12345678	E 12345678	F 12345678	G 12345678	H 12345678

Interleaved Characters

ABCDEFGH 11111111	ABCDEFGH 22222222	ABCDEFGH 33333333	ABCDEFGH 44444444	ABCDEFGH 55555555	ABCDEFGH 66666666	ABCDEFGH 77777777	ABCDEFGH 88888888

CRC calculation



Frame: 1101011011

Generator: 10011

Message after appending 4 zero bits:

11010110110000

Trasmitted Frame:

11010110111110

Error detection & error correction

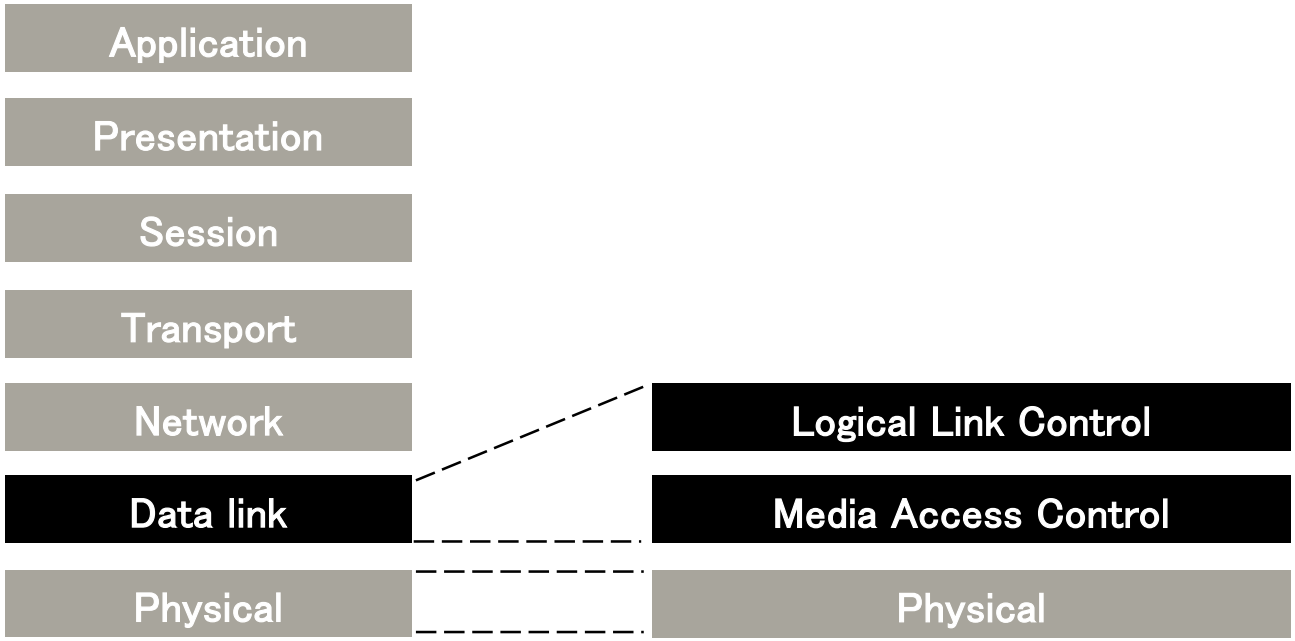
- **Hamming code (1950)**
  - Hamming distance *d*: number of difference bits between two words (*d* bits are needed to convert one word to the other).
  - Over a *m* bit transmission: 2^m possible words can be found, but since some bits are used for parity checks not all word will be used.
  - A distance *d* allows to detect *d-1* bit(s) errors.
  - A distance *d* allows to correct $x < INT(\frac{d-1}{2})$ bit(s) error.
  - Hamming code is able to correct isolated bits, to correct burst errors is possible to transmit information over a matrix so to split the burst on more transmitted words.

Errors Detection

- Hamming Code

Char	Dec	Hex	Symbol	Hamming Code										
				k1	k2	b1	k3	b2	b3	b4	k4	b5	b6	b7
M	77	4D	1001101	0	1	1	1	0	0	1	0	1	0	1
e	101	65	1100101	0	0	1	1	1	0	0	0	1	0	1
s	115	73	1110011	1	0	1	0	1	1	0	0	0	1	1
s	115	73	1110011	1	0	1	0	1	1	0	0	0	1	1
a	97	61	1100001	1	0	1	1	1	0	0	1	0	0	1
g	103	67	1100111	0	1	1	1	1	0	0	1	1	1	1
e	101	65	1100101	0	0	1	1	1	0	0	0	1	0	1

Data link layer: the OSI & IEEE standards



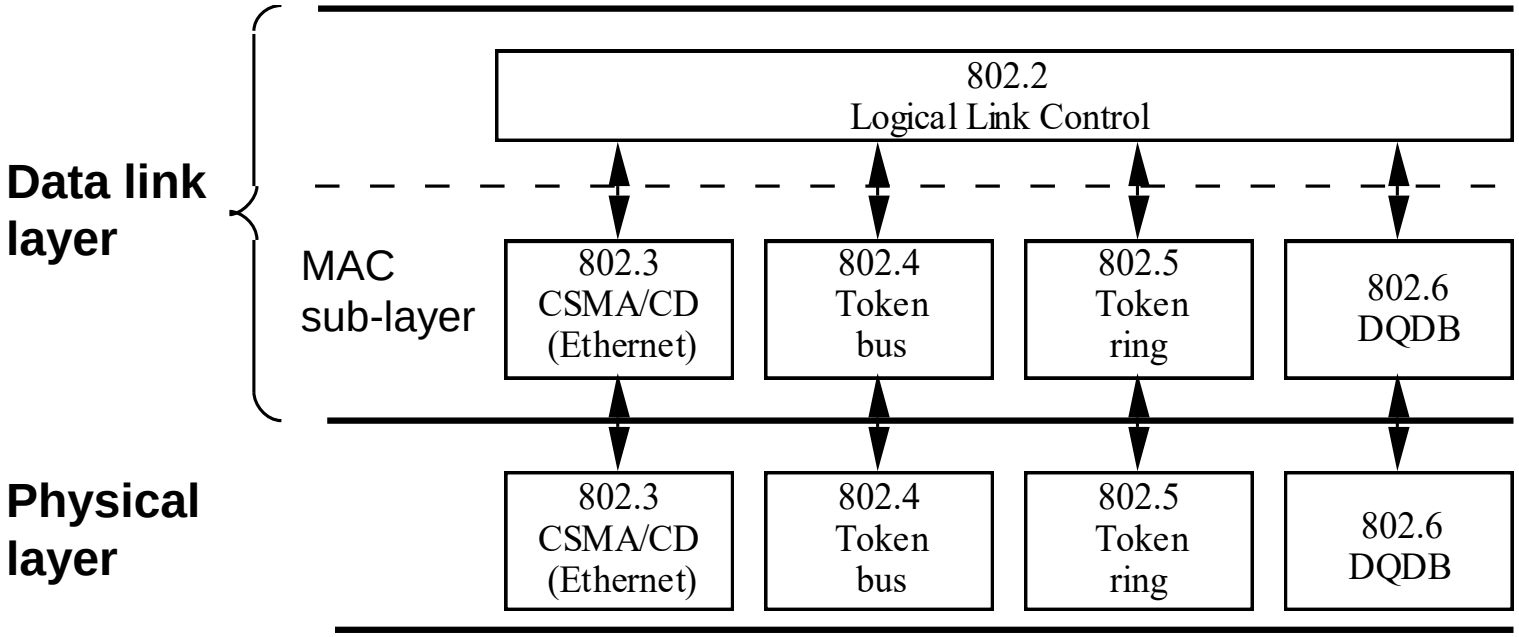
OSI	IEEE	
8802.1	802.1	Documentation, Management, Interconnection
8802.2	802.2	Logical Link Control
8802.3	802.3	Carrier Sense Multiple Access/Collision Detection (Bus Tecn.)
8802.4	802.4	Token Passing Using Bus Topology
8802.5	802.5	Token Passing using Ring Topology
…	…	Altri standard (802.11, 802.14, …)

Some IEEE 802.xx standards

- IEEE 802.1 Higher layer LAN protocols
- IEEE 802.2 Logical link control
- IEEE 802.3 Ethernet
- IEEE 802.4 Token bus (outdated)
- IEEE 802.5 Token Ring
- IEEE 802.6 Metropolitan Area Network (discountined)
- IEEE 802.7 Broadband TAG (discountined)
- IEEE 802.8 Fiber Optic TAG (discountined)
- IEEE 802.9 Integrated Services LAN (discountined)
- IEEE 802.10 Interoperable LAN Security (discountined)
- IEEE 802.11 Wireless local area network
- IEEE 802.12 demand priority
- IEEE 802.13 (not used)
- IEEE 802.14 Cable modem
- IEEE 802.15 Wireless personal area network
- IEEE 802.16 Broadband wireless access
- IEEE 802.17 Resilient packet ring
- IEEE 802.18 Radio Regulatory TAG
- IEEE 802.19 Coexistence TAG
- IEEE 802.20 Mobile Broadband Wireless Access
- IEEE 802.21 Media Independent Handoff
- IEEE 802.22 Wireless Regional Area Network

MAC e LLC sub-layers

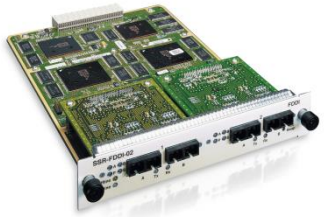
- The different standards at data link level differ at the MAC xub-layer.
- The LLC sub-layer makes the data link service for the upper layers transparent to the media used for the communication.

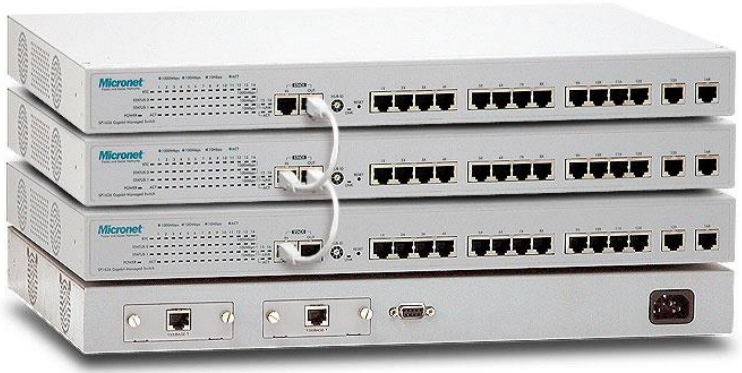


Data link layer

- Protocols active on this layer:
  - CSMA/CD
  - Ethernet
  - Token Ring
  - FDDI
  - DQDB
  - SLIP
  - PPP
  - ISDN
- Typical infrastructures:
  - Switch
  - Bridge (old concept)
  - Access point

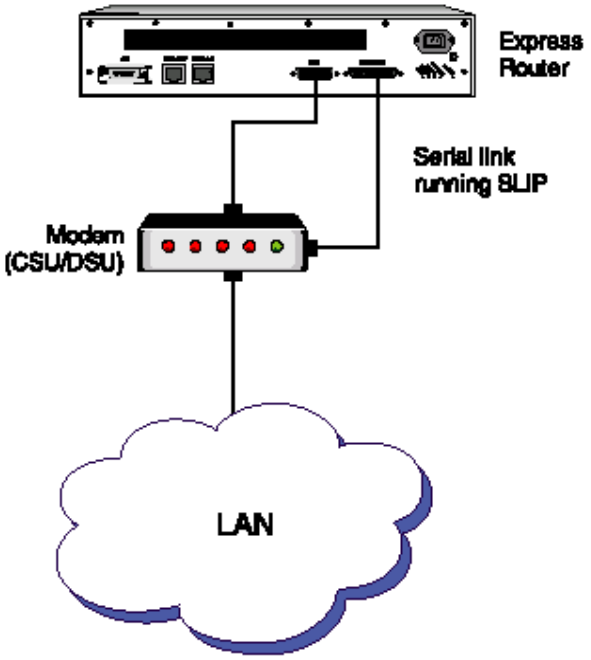






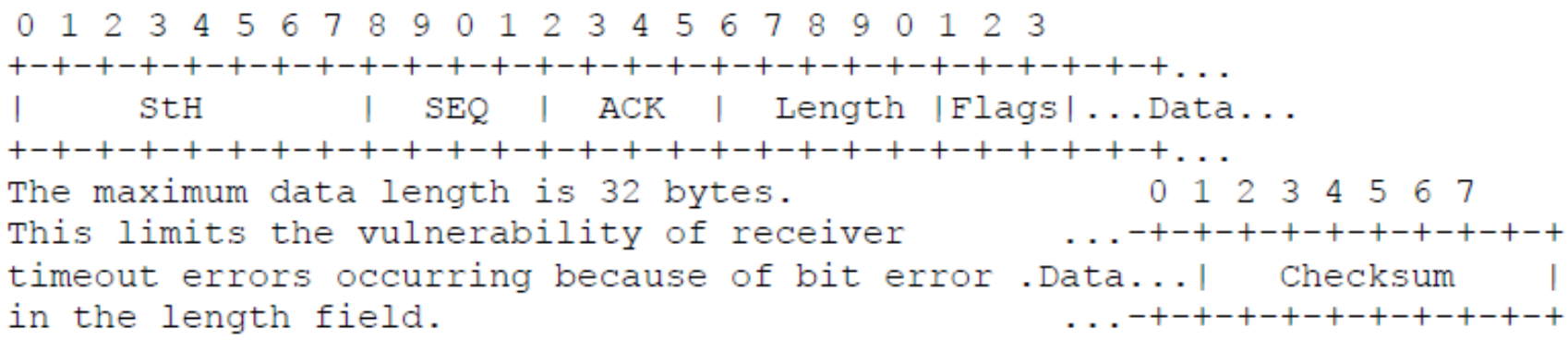
Serial Line Internet Protocol (SLIP)

- SLIP is considered the originating point-to-point protocol for TCP/IP traffic, it is still used by some ISP.
- SLIP adopts a special end-of-character (0xC0), this is used at the start and at the end of each IP datagram as a packet delimiter.
- The ≪escape≫ character is not the same as ESC of the American Standard Code for Information Interchange (ASCII).



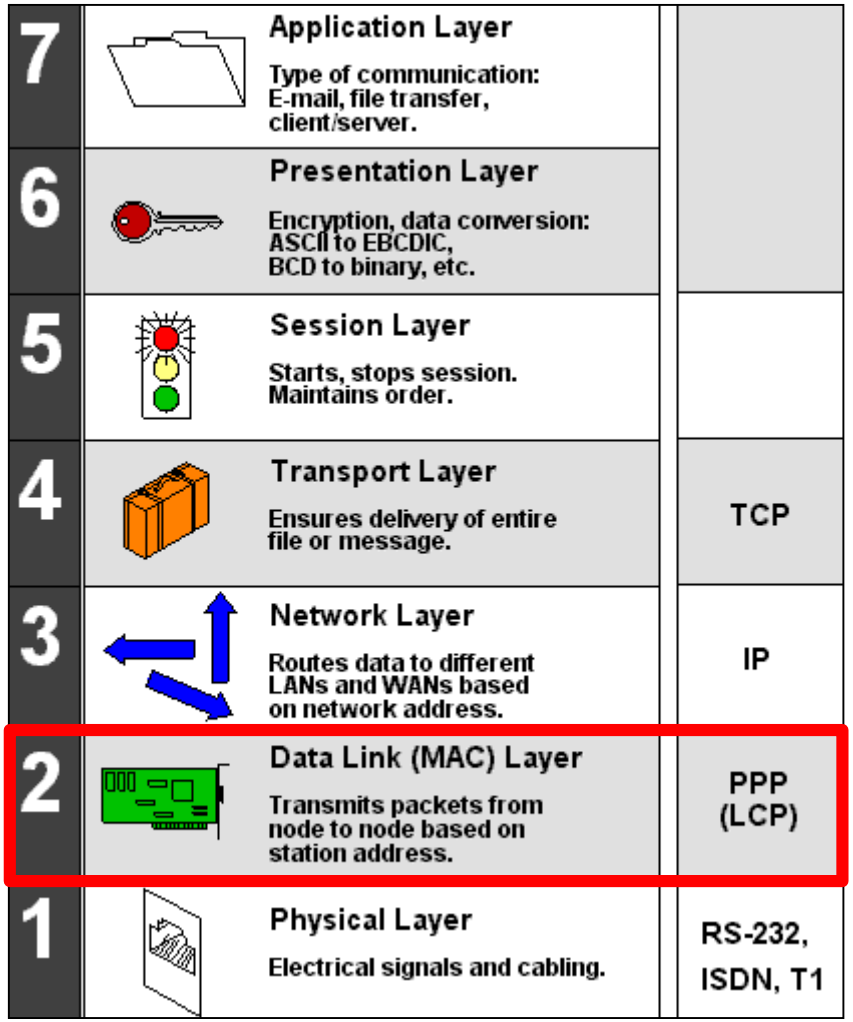
Serial Line Internet Protocol (SLIP)

- The protocol is specified in RFC 1055. The maximum datagram size of a SLIP datagram is 1066 bytes
- RFC 1144 is another RFC developed to avoid compressions of IP and TCP headers transmitted over a SLIP channel.
- This modified version is called Compressed SLIP (C-SLPI).



Point-to-Point Protocol (PPP)

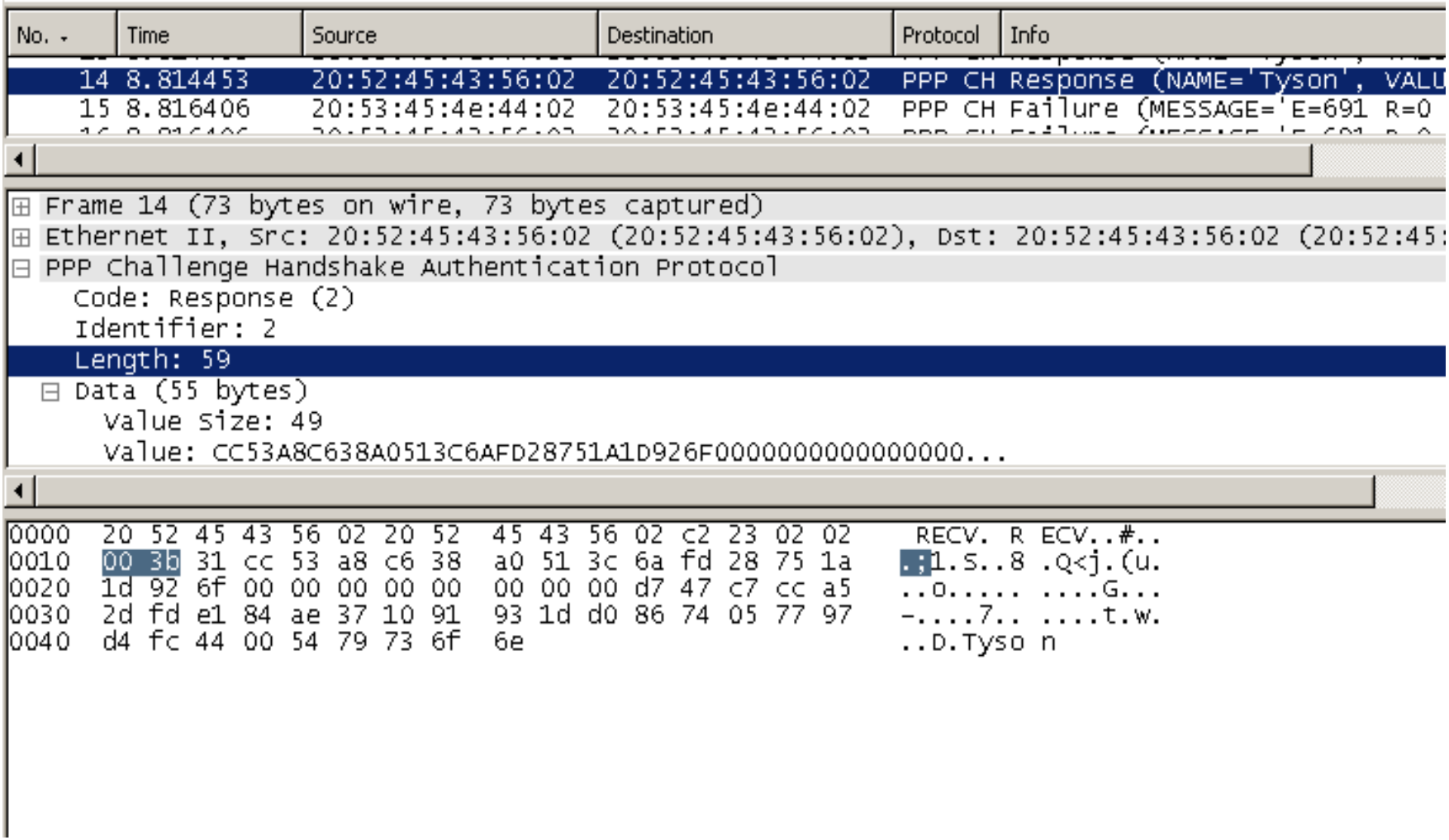
- Point–to–point protocol (PPP) foresees encapsulation service for data link WAN similar to what it is used in LAN configuration.
- PPP is specified in RFC 1661, the specification includes the following characteristics:
  - Encapsulation methods supporting multiple concurrent protocols modules on the same link.
  - A specialized protocol, Link Control Protocol (LCP) is used to negotiate any point–to–point.



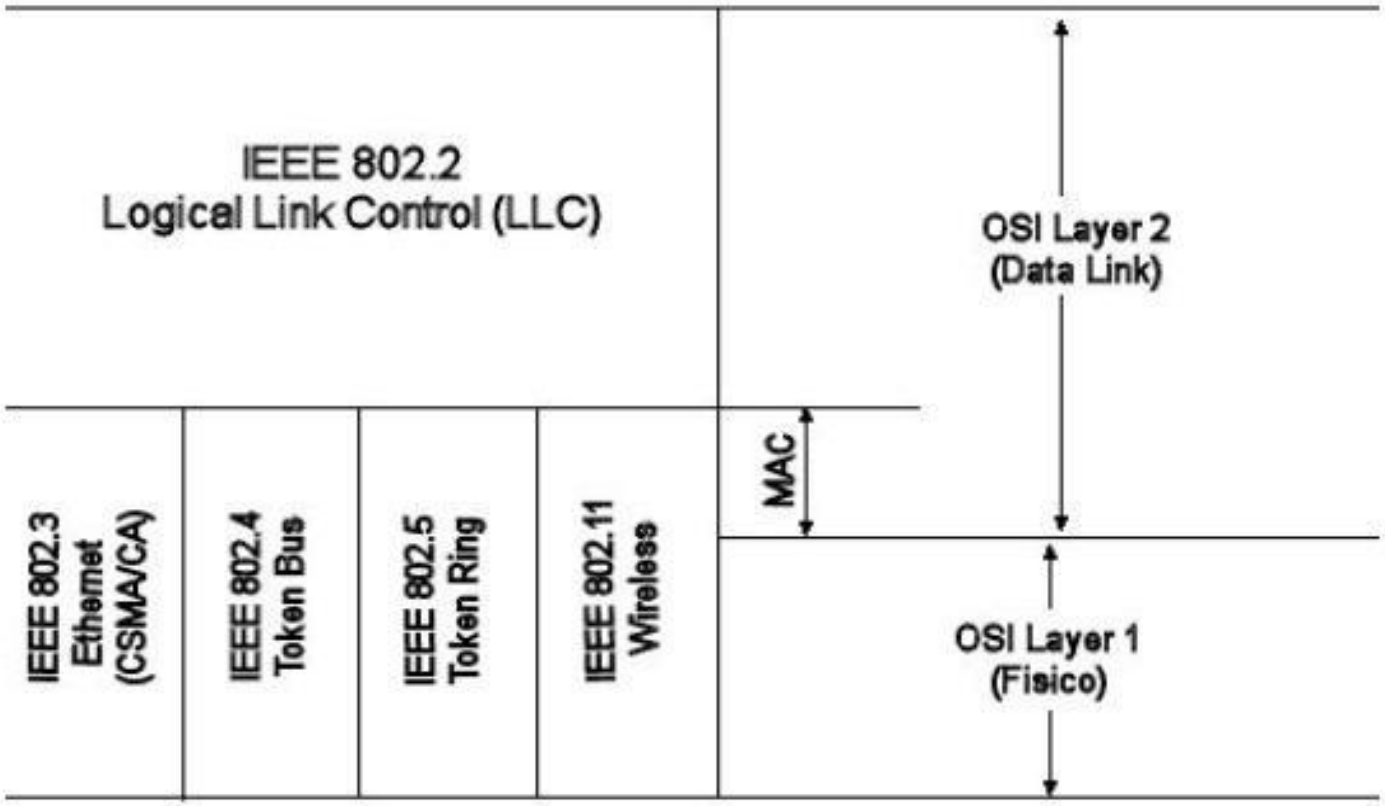
Point-to-Point Protocol (PPP)

- The PPP frames support addressing information such as link control or other HDLC derivate, despite this most implementation of PPP use a short version that skips unnecessary information.
- PPP header's field include:
  - *Flag*
  - *Protocol identifier*
  - *Frame Check Sequence (FCS)*
- Considering PPP is used along side synchronous technologies, such as T1/E1, Integrated Services Digital Network (ISDN), DSL or Synchronous Optical Network (SONET) a technique to switch bits much faster and more efficient is applied. This is a main difference with asynchronous technologies.
- PPP maximum packet size: 1500 bytes. This feature is perfectly compatible with Ethernet based networks.

PPP Handshake



IEEE 802.xx


IEEE 802.2
Logical Link Control (LLC)
IEEE 802.3
Ethernet
(CSMA/CA)
IEEE 802.4
Token Bus
IEEE 802.5
Token Ring
IEEE 802.11
Wireless
MAC
OSI Layer 2
(Data Link)
OSI Layer 1
(Fisico)

CSMA/CD Protocol (IEEE802.3)

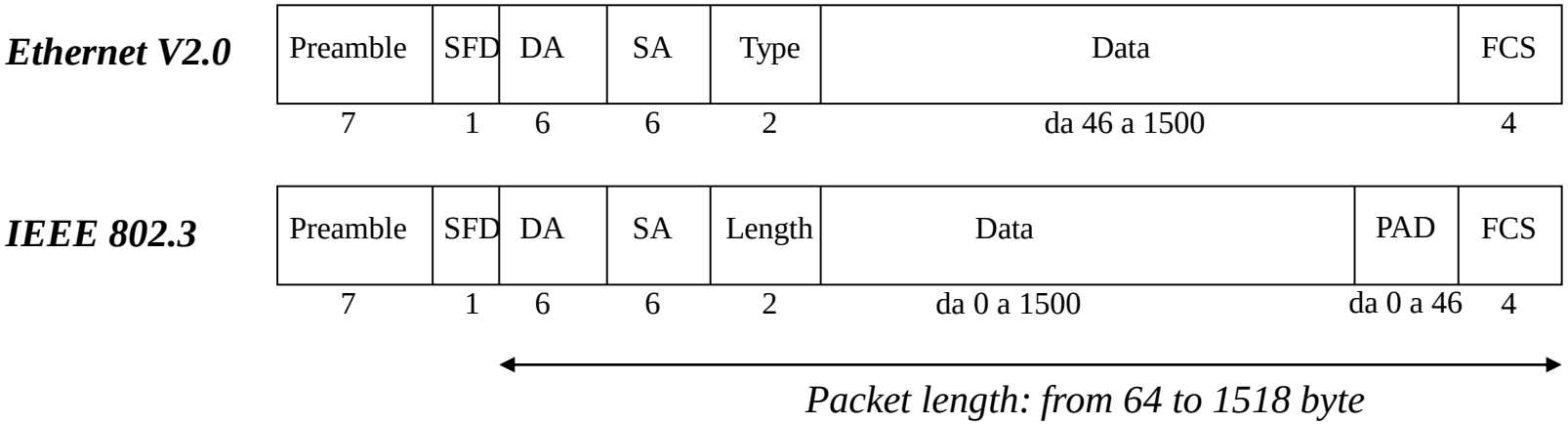
- The IEEE 802.3 standard specifies the protocol CSMA/CD
- Native speed: 10Mbps
- Mechanism process:
  - CS: Carrier Sense: each nodes listen the network for activity.
  - MA: the network is shared among all nodes.
  - CD: even during transmission the components are actively listening on the network to detect collision. In case a collision is detected:
    - The node detecting the collision send a jammer signal that resets the all network.
    - Each node recovers connectivity after a random interval.
    - Each node listen to the network.
    - The transmitting node re-transmits data if no activity is detected, otherwise it waits.

Ethernet Protocol

- Logical bus
- Physical star, or bus
- Uses CSMA/CD
- 10 Mbps
- UTP or STP, coax, or fiber cable
- Standard: IEEE 802.3
- Old LAN technology

Ethernet and IEEE802.3

- The ethernet protocol and the CSMA/CD standard simply differ by 2 bytes in the frame:



- When a packet is received the card checks the 2 bytes:
  - content > 1500 → Ethernet packet
  - content < 1500 → 802.3 packet, the protocol type is encapsulated in the information handled by the LLC level.

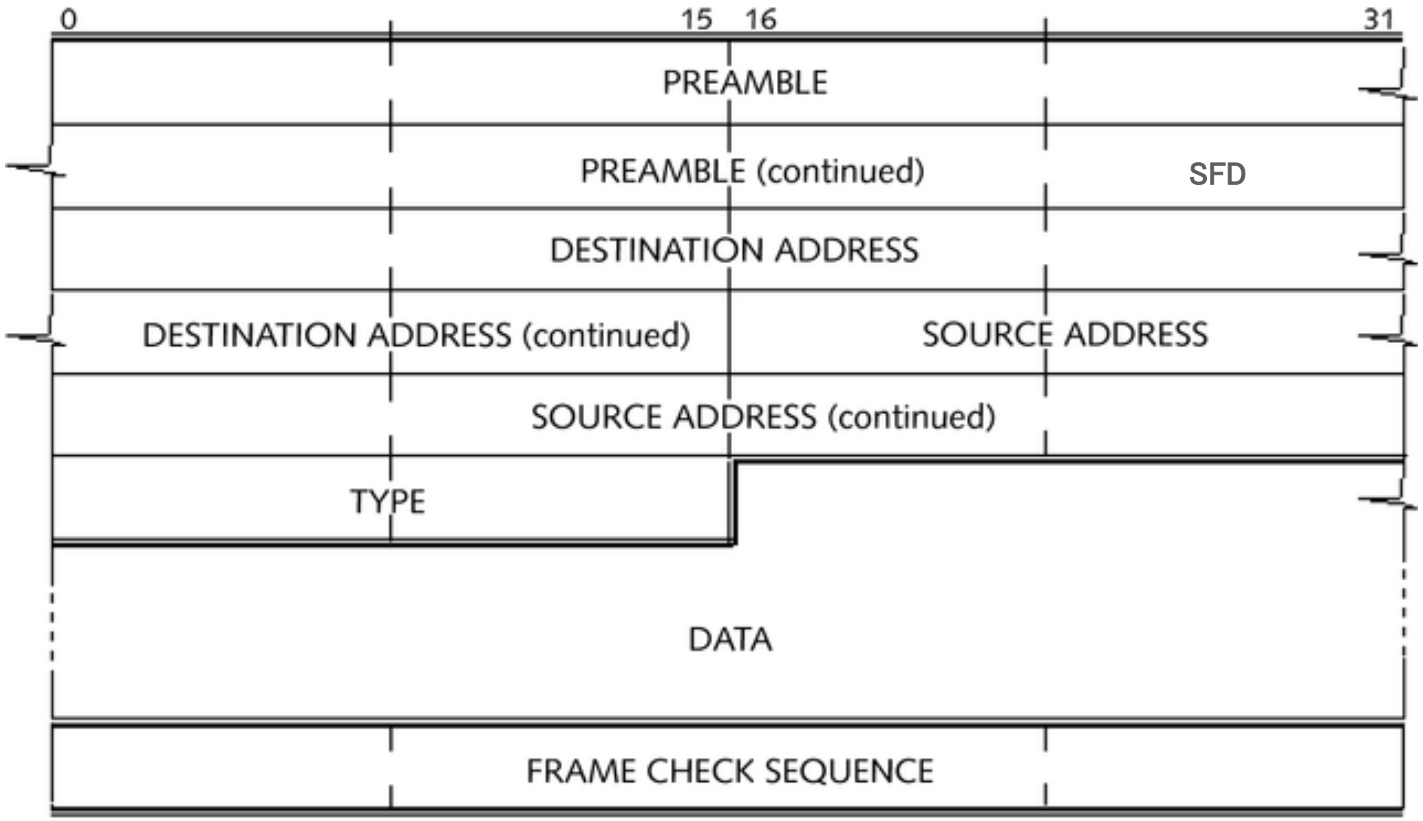
Ethernet Frame Types

- The Ethernet II frame type is the de facto standard frame type used for IP datagram transmissions over Ethernet networks
- The Ethernet II frame has a protocol identification field (the Type field) that contains the value 0x0800 to identify the encapsulated protocol as IP
- Before an IP datagram is transmitted onto the media, the data link driver puts the leading frame onto the datagram
- If a frame does not meet the minimum frame size of 64 bytes, the driver must pad the Data field
- The Ethernet NIC performs a Cyclical Redundancy Check (CRC) procedure on the contents of the frame, and places a value at the end of the frame in the Frame Check Sequence field
- Finally, the NIC sends the frame, led by a preamble, which is a leading bit pattern used by the receiver to correctly interpret the bits as ones and zeroes

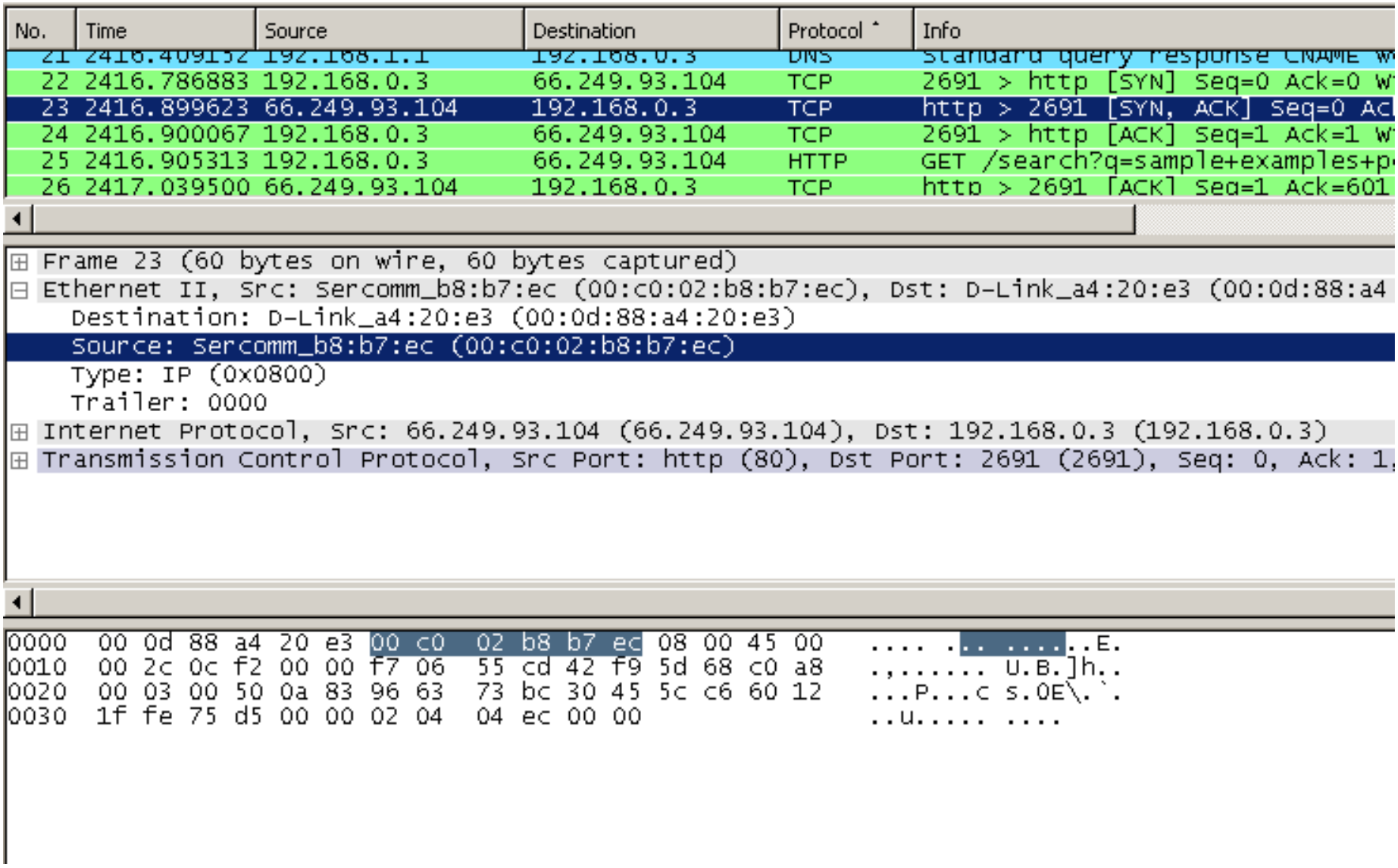
Ethernet II Frame Structure

- The Ethernet II frame type consists of the following values, fields, and structure:
  - Preamble
  - Start Frame Delimiter
  - Destination Address field
  - Source Address field
  - Type field
  - Data field
  - Frame Check Sequence field

Ethernet II Frame Structure



Frame Structure: Layer 2



Ethernet Frame Types

- There are three Ethernet frame types that TCP/IP can use:
  - Ethernet II
  - Ethernet 802.2 Logical Link Control (LLC)
  - Ethernet 802.2 Sub-Network Access Protocol (SNAP)

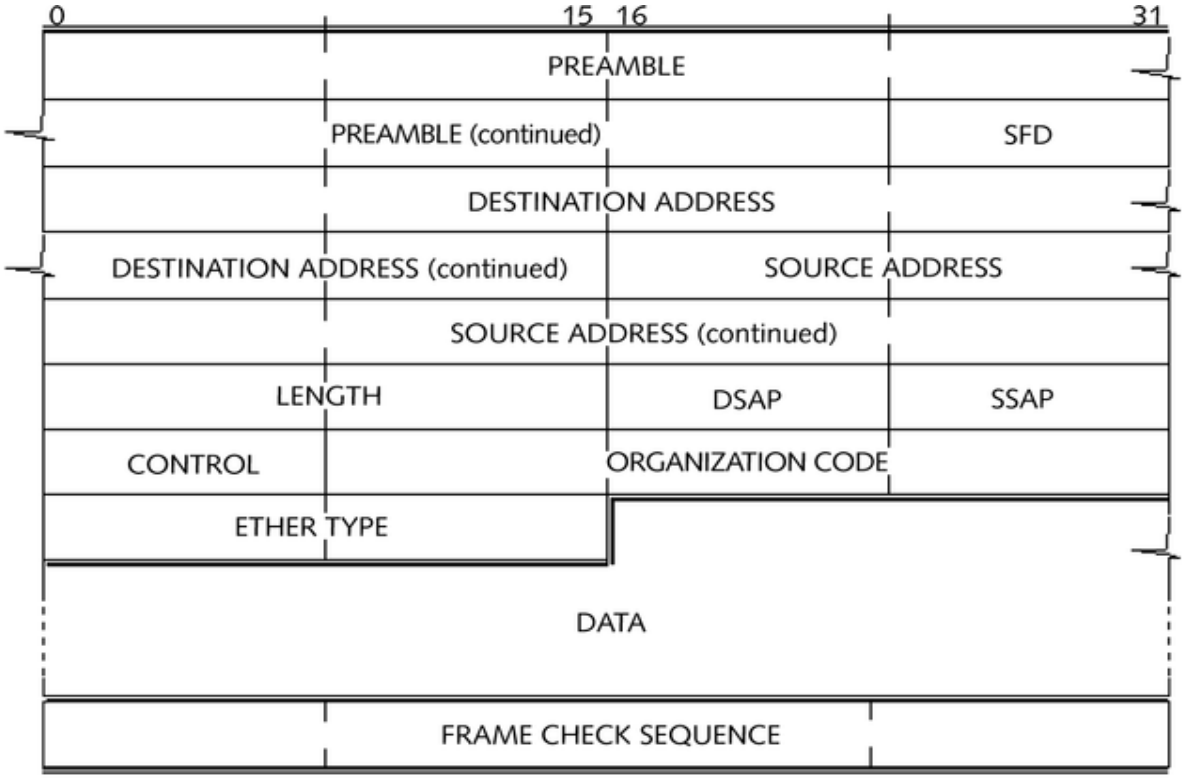
Ethernet 802.2 LLC Frame Structure

- The Ethernet 802.2 LLC frame type consists of the following fields:
  - Preamble
  - Start Frame Delimiter (SFD) field
  - Destination Address field
  - Source Address field
  - Length field
  - Destination Service Access Point (DSAP) field
  - Source Service Access Point (SSAP) field
  - Control field
  - Data field
  - Frame Check Sequence (FCS) field

Ethernet 802.2 LLC Frame Structure

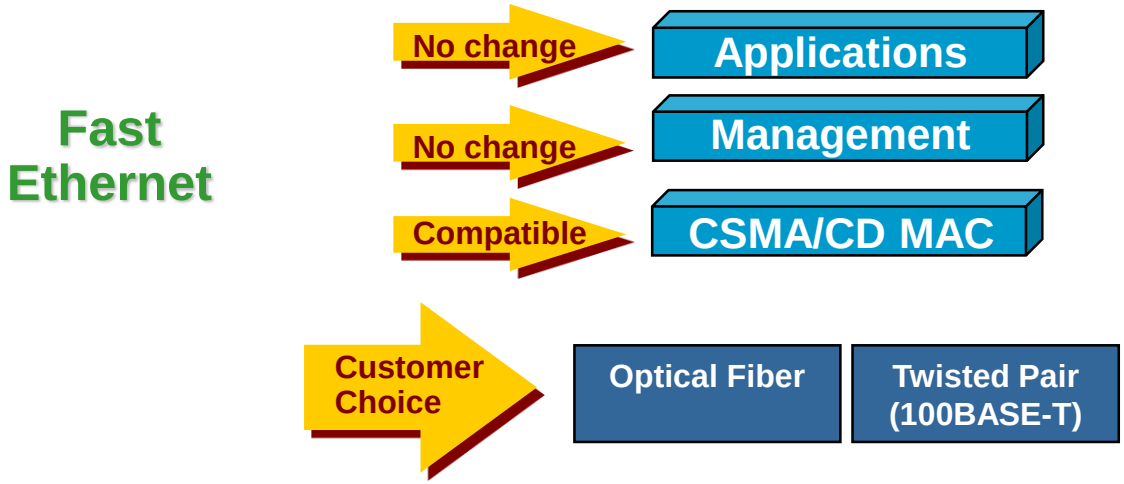
Ethernet SNAP Frame Structure

- The Registry entry ArpUseEtherSNAP must be set to 1 to enable use of the Ethernet 802.2 SNAP frame format for IP and ARP traffic over Ethernet



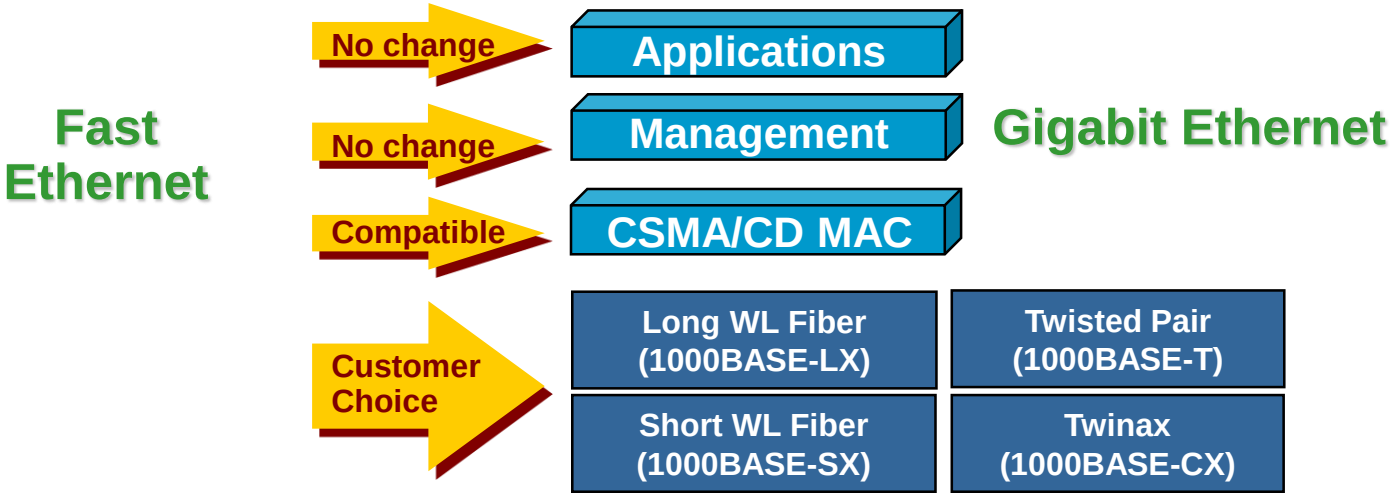
Fast Ethernet

- Like 10 Mbps Ethernet except:
  - 100 Mbps instead of 10 Mbps
  - UTP, STP, or fiber (no coax)
- Standard: IEEE 802.3u
- Old desktops connectivity standard



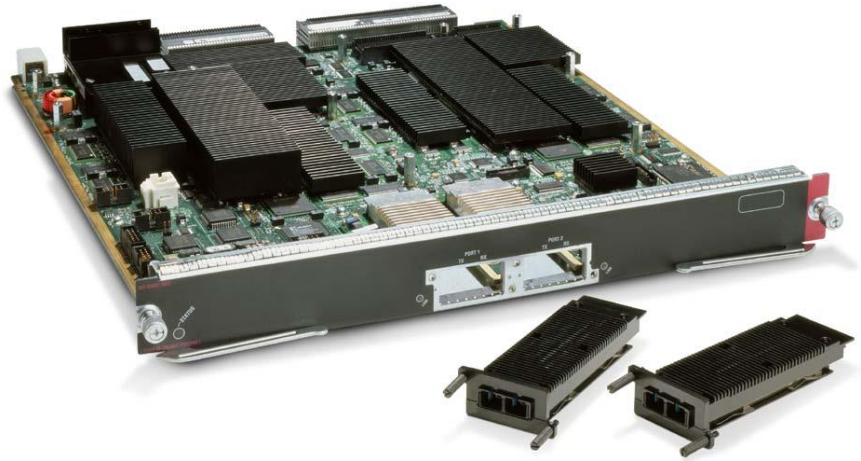
Gigabit Ethernet

- Easy migration without disruption
- 1000 Mbps
- Standard: IEEE 802.3z
- Low cost of ownership
- Scalability to high performance
- The last generation frame-based desktop technology



10 Gigabit Ethernet

- It is build with the same features and structure of 1 Gigabit Ethernet the only difference its a higher bitrate: 10 Gbps
- Very easy migration, no particular configuration is necessary to upgrade to this technology.
- This is envisaged to be the standard to be adopted by next generation backbones.
- Standard backbone technology.



	Cat 5e	Cat 6	Cat 6A / Cat7
100M	👍	👍	👍
1Gb	👍	👍	👍
2.5Gb	👍	👍	👍
5Gb	👍	👍	👍
10Gb	✋	👍	👍

100 Gigabit Ethernet

Cisco Nexus 7000 Series Switches 100 Gigabit Ethernet

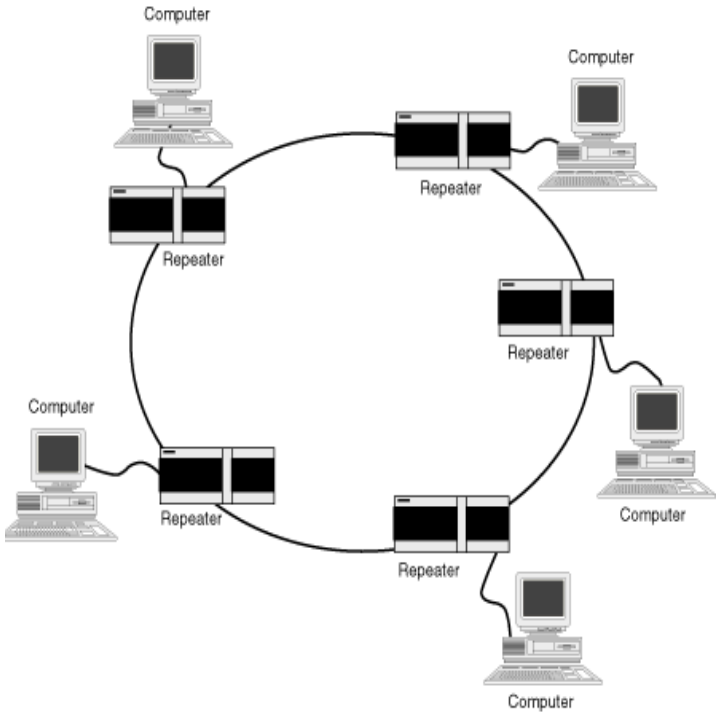
Dual Port Fiber 100 Gigabit Ethernet PCI Express Content Director Server Adapter Intel® Based

Token Ring (IEEE 802.5)

- IEEE 802.5 specifies:
  - The protocol, the media, physical connection, coding scheme.
- It operates at 16 Mbps
- Working principle:
  - When a machine wants to communicate it has to wait for free token, as soon as the machine gets a free token it loads the token with data.
  - The clearing process is expected to be done by the machine that originates the token, that will therefore empty it.
  - Other machines have to wait for the token to be free to communicate, however they can reserve the token to use it when it will be free.

Token Ring

- Logical ring, physical star
- Uses token passing
  - Station can only transmit when it has token
- 4 or 16 Mbps
- UTP, STP, or fiber cable
- Standard: IEEE 802.5
- Few "all-new" Token Ring installs today, but has large installed base



Token Ring Frame Types

- The IEEE 802.5 standard defines token ring networking.
- Token ring networks rely on a physical star network design architecture, although they use a logical ring transmission paths.
- On a token ring network, each token ring workstation acts as a repeater. It repeats each packet received back onto the network.
- There are two variants of token ring frames: Token Ring 802.2 LLC frames and Token Ring SNAP frames.

Token Ring Networks Are Physically Stars, But Logically Rings

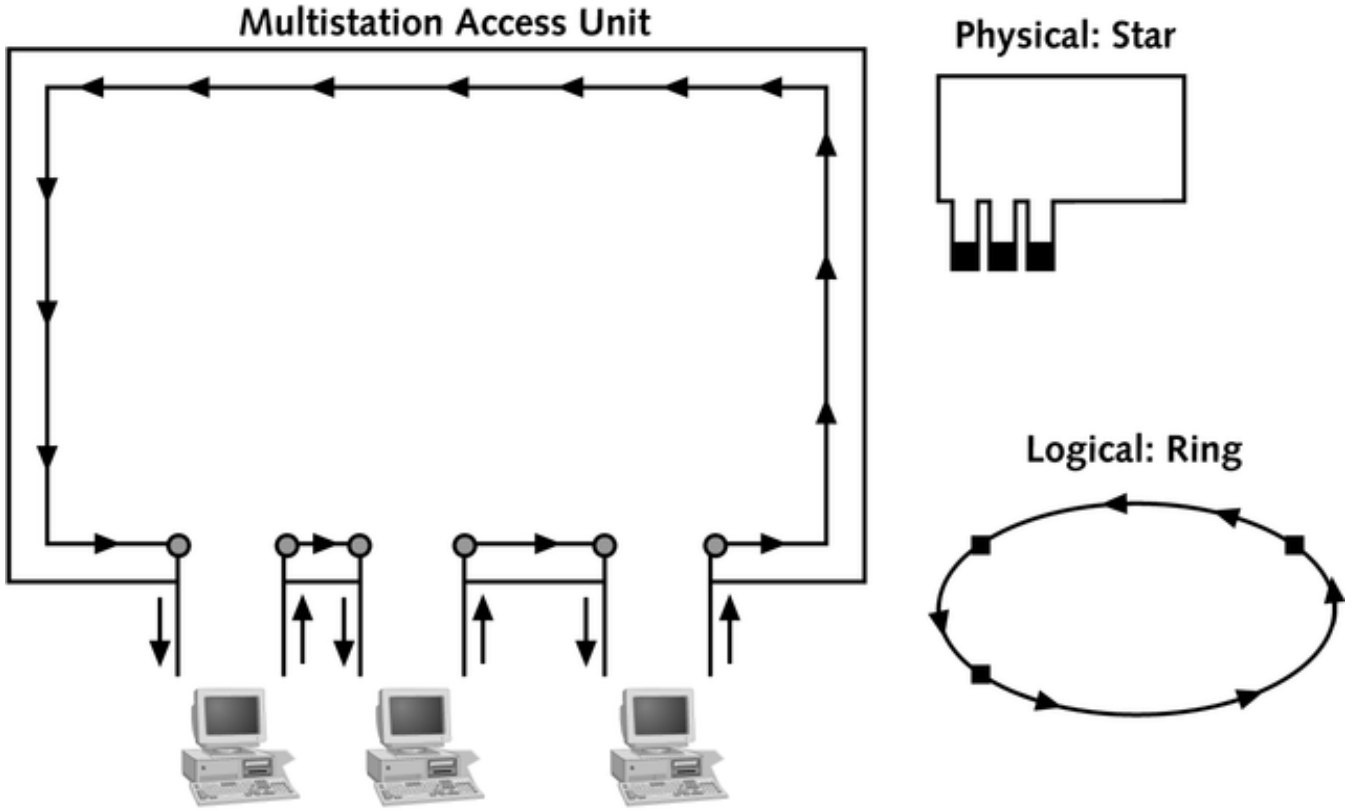
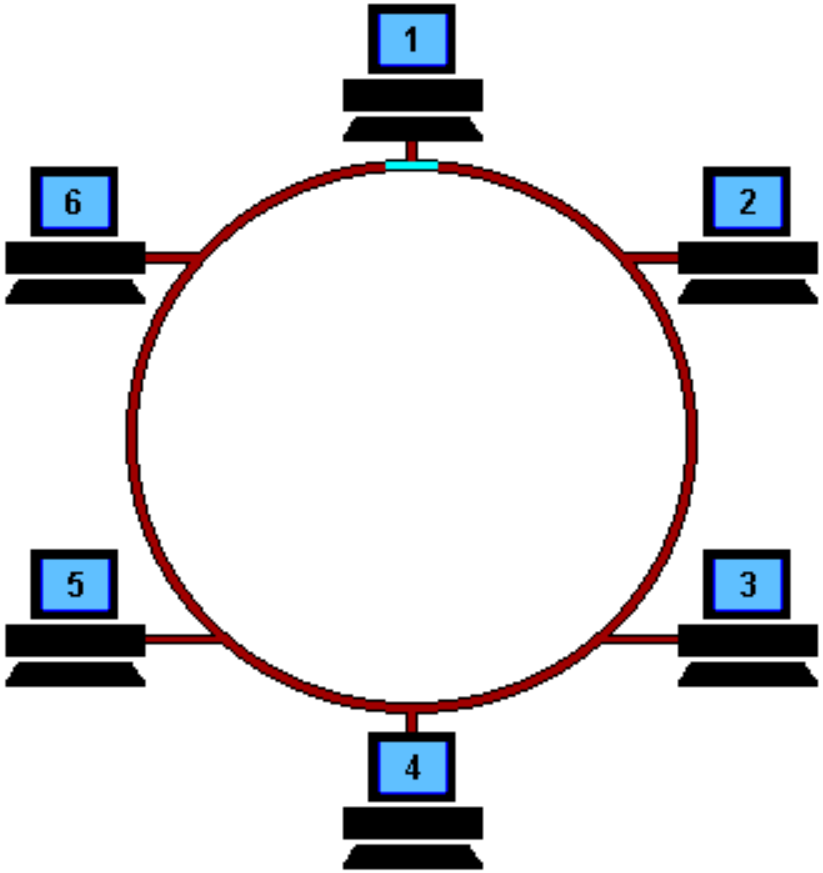


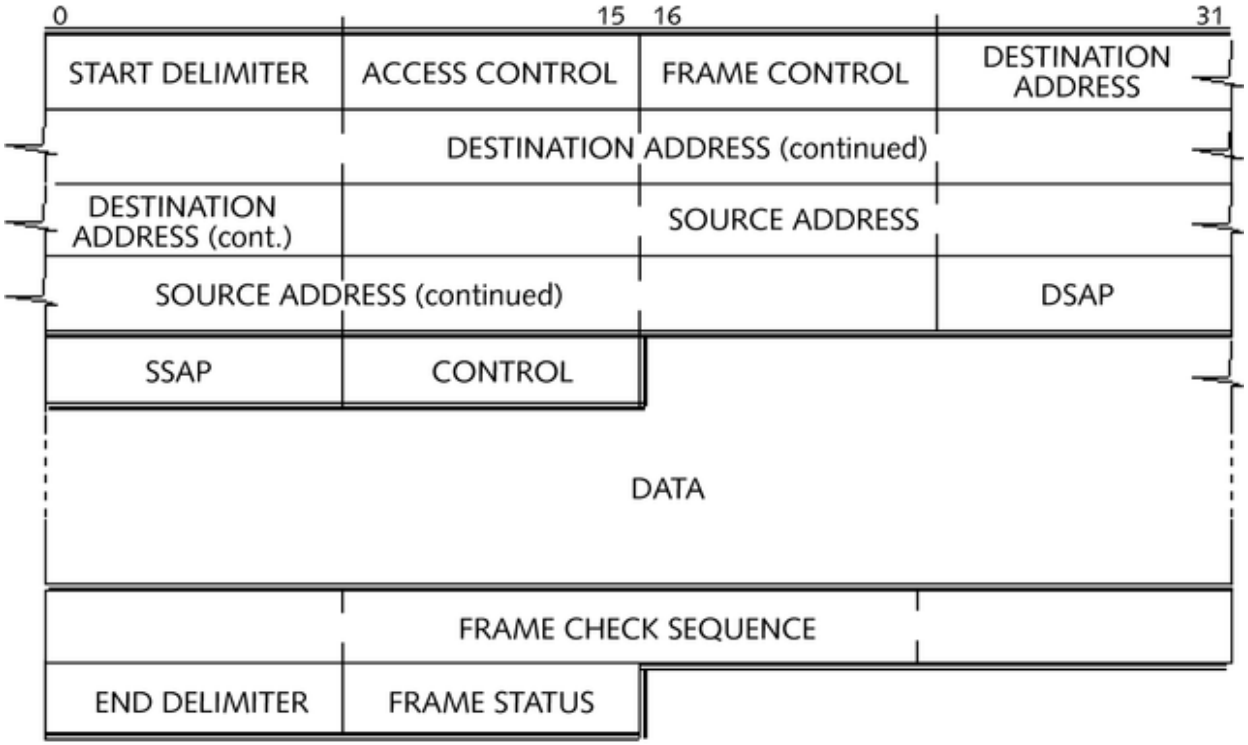
Figure 3-4 Token ring networks are physically stars, but logically rings

Token Ring



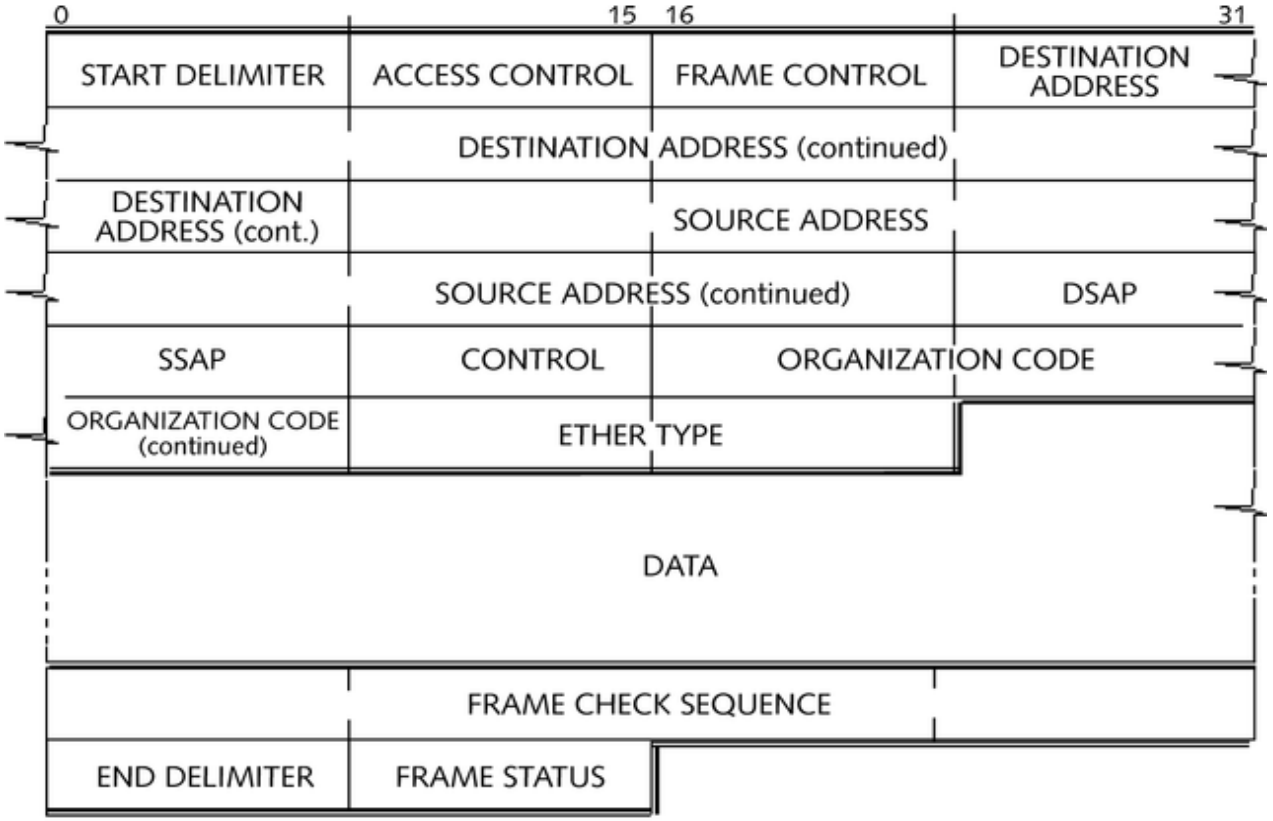
Token Ring 802.2 LLC Frame Format

- The standard Token Ring 802.2 LLC frames include the same LLC fields used by the Ethernet 802.2 LLC frame



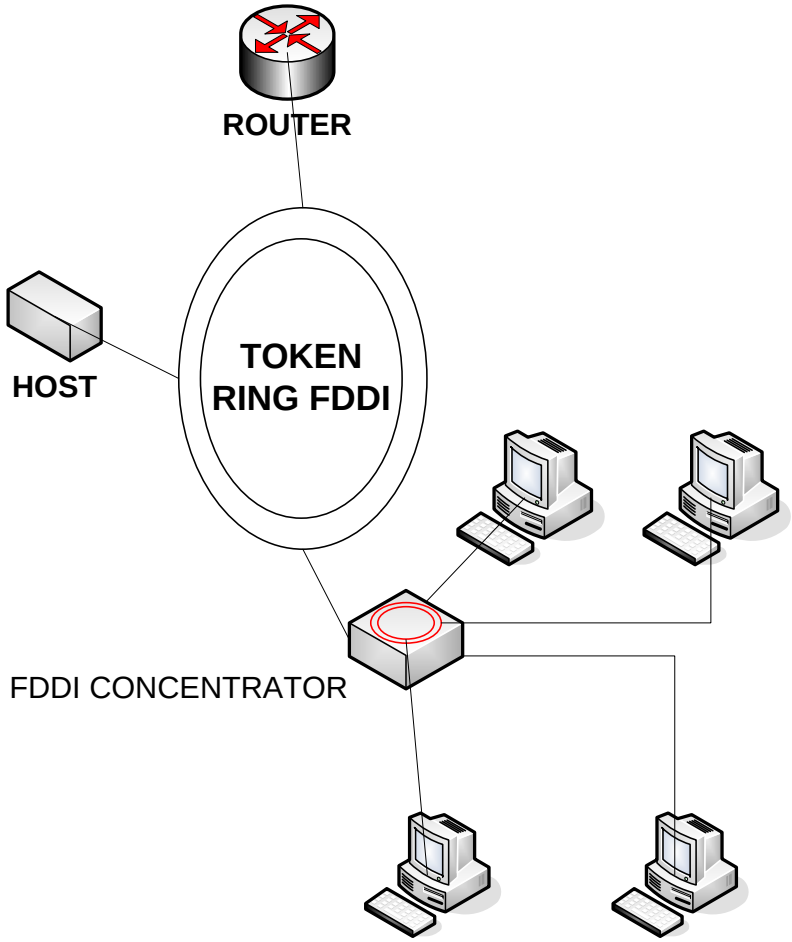
Token Ring SNAP Frame Format

- The Token Ring SNAP frame format expands the standard 802.2 LLC layer by adding an Organization Code field and an Ether Type field



FDDI
(Fiber Distributed Data Interface)

- Logical ring, physical ring, or star
- Dual counter-rotating rings
- 100 Mbps
- Standard: ISO 9314
- Fiber, UTP or STP
- Older backbone technology
- Was in place at many larger networks



Wireless LAN

- Connects to Existing Cable Infrastructure
  - Wireless NICs
  - Access Points
- Uses frequency bands around 2.4GHz and 5GHz
- Standard:

  IEEE 802.11a

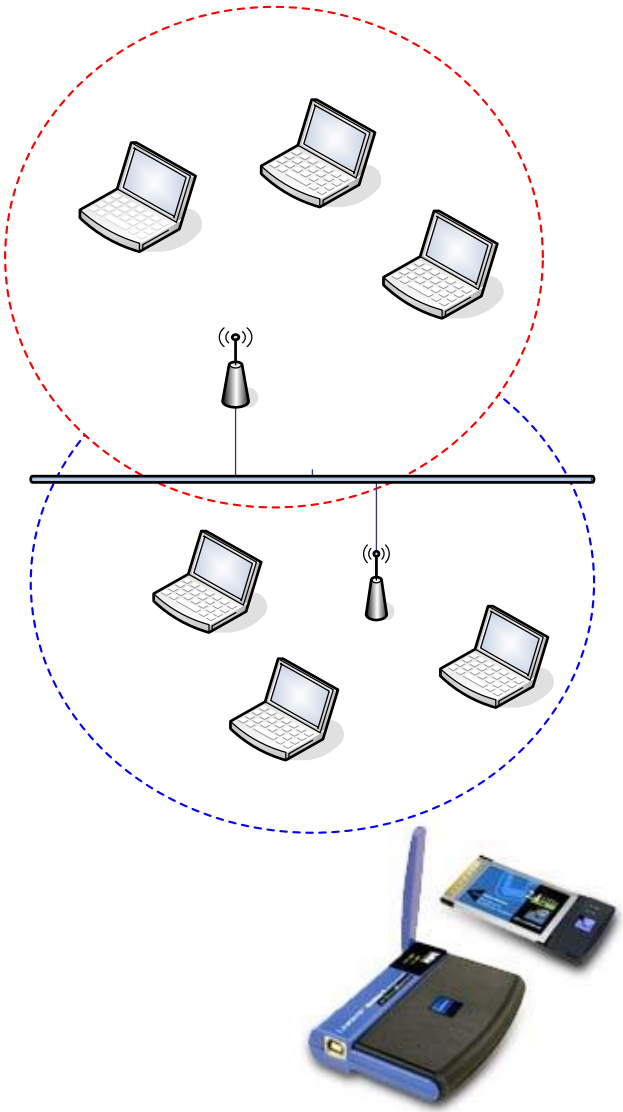
  IEEE 802.11b

  IEEE 802.11g

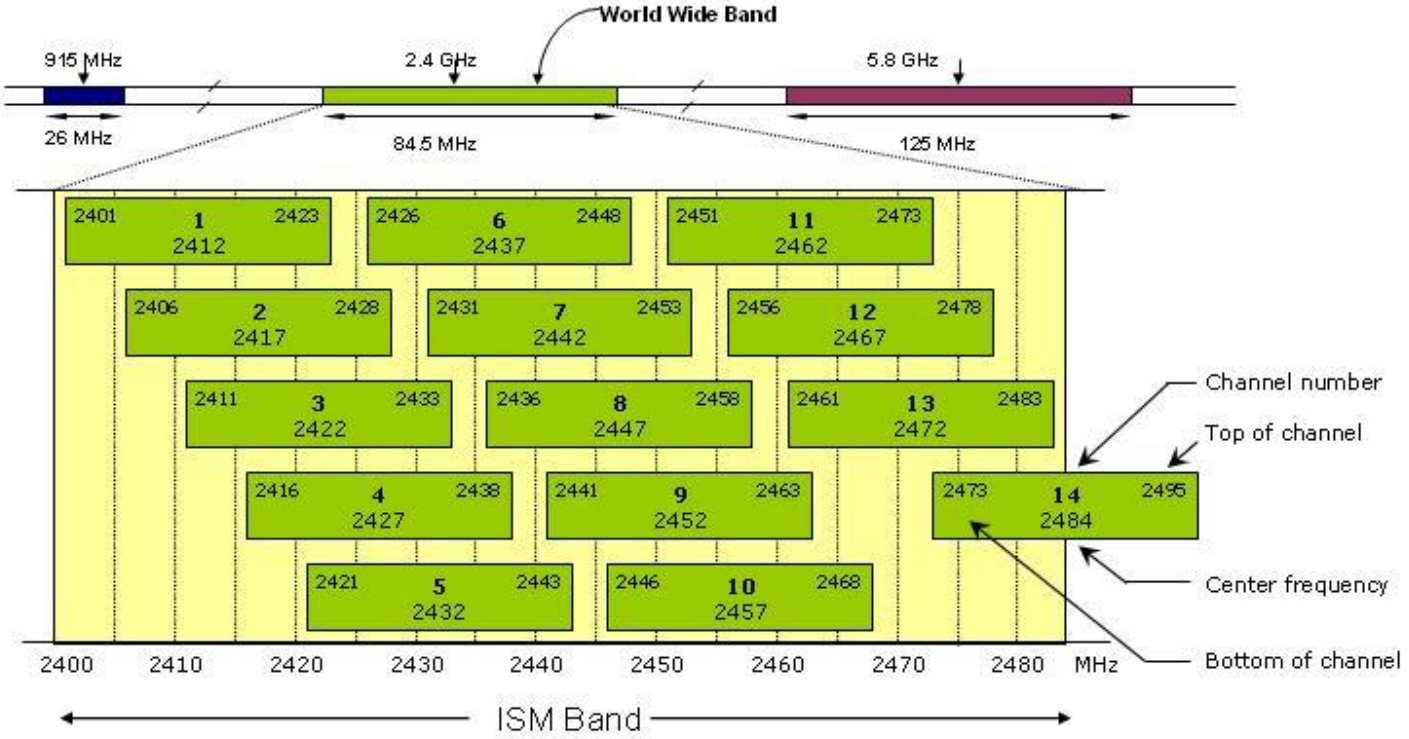
  IEEE 802.11n

  IEEE 802.11i

  …
- Bandwidth 11 Mbps, 54 Mbps, 300 Mbps
  Throughput: ? Mbps
- Two spread spectrum radio techniques allowed
  - Frequency Hopping (FH)
  - Direct Sequence (DS)

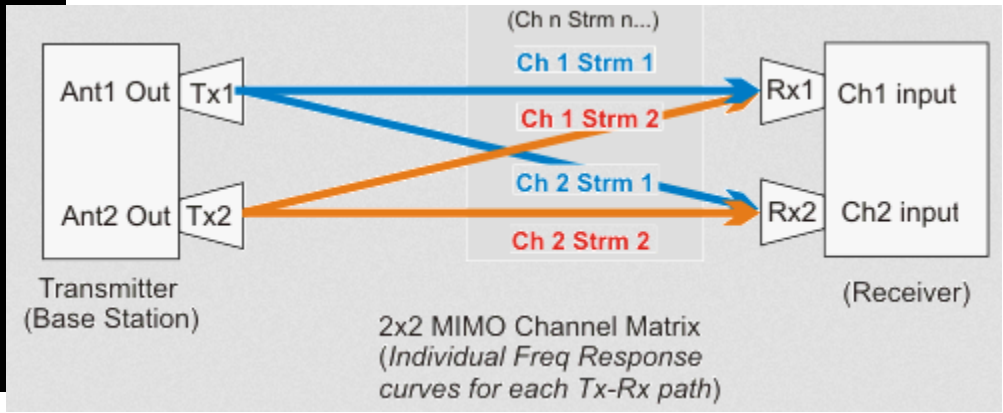


Wi-Fi



802.11n Maximum Supported Data Rates

	MIMO ANTENNAS	DUAL-STREAM MIMO	TRIPLE- STREAM MIMO
Single-Radio AP	2x2	300 Mbps	-
	3x3	300 Mbps	450 Mbps
Dual-Radio AP (aggregate data rates)	2x2	600 Mbps	-
	3x3	600 Mbps	900Mbps



Wireless LAN

Wireless standards

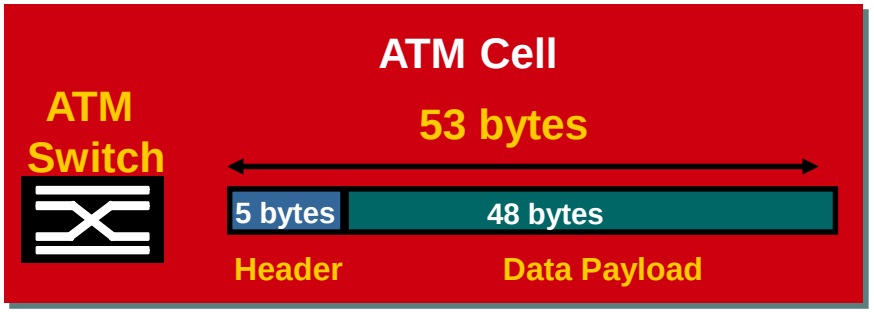
- IEEE 802.11-1997 – The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a – 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b – 5.5 Mbit/s and 11 Mbit/s, 2.4 GHz standard (1999)
- IEEE 802.11c – Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d – International (country-to-country) roaming extensions (2001)
- IEEE 802.11e – Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11f – Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g – 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h – Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i – Enhanced security (2004)
- IEEE 802.11j – Extensions for Japan (4.9–5.0 GHz) (2004)
- IEEE 802.11k – Radio resource measurement enhancements (2008)
- IEEE 802.11n – Higher Throughput WLAN at 2.4 and 5 GHz; 20 and 40 MHz channels; introduces MIMO to Wi-Fi (September 2009)
- IEEE 802.11p – WAVE-Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r – Fast BSS transition (FT) (2008)
- IEEE 802.11s – Mesh Networking, Extended Service Set (ESS) (July 2011)
- IEEE 802.11t – Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- IEEE 802.11u – Improvements related to Hotspots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)
- IEEE 802.11v – Wireless network management (February 2011)

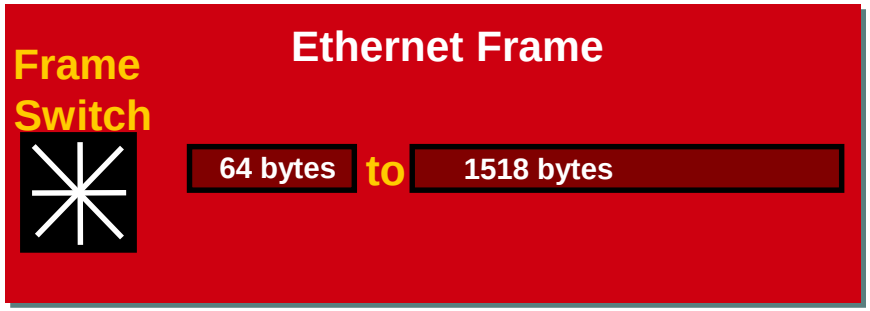
Wireless LAN

- Wireless security
  - **WEP – Wired Equivalent Privacy**
    - WEP uses RC4 encryption algorithms for security and CRC-32 to verify data integrity. WEP RC4 it is based on two keys, 40 bits and 104 bit.
    - When the vector is transmitted without encryption, 24 bit are added as padding to the packets.
  - **WPA – Wi-Fi Protected Access**
    - Data is encrypted using the block algorithm RC4 with a 128 bit key and a 48 bits initialization vector.
    - The Temporal Key Integrity Protocol (TKIP) dynamically changes the active key in-use, this procedure combined with the inizialization vector which is double than the one used in WEP, making this encryption standard more secure.
  - **WPA – Wi-Fi Protected Access 2**
    - WPA + AES 128 bit

ATM (Asynchronous Transfer Mode)

- 25, 155, 622 Mbps or 2.4 Gbps
- Cell-based vs. frame transmissions
  - 53 byte cells
- Negotiated service connection
  - End-to-end connections
  - Virtual circuits
- Switch-based
- Dedicated capacity
- Is NOT an IEEE-Standard





Choosing a LAN Technology

	Speed	Found In	Cost	Media
Ethernet	10 Mbps	Simple (old) LAN installations	low	Coax, STP, UTP, fiber
Fast Ethernet	100 Mbps	Workstations using old NICS or networking infrastructures	low	STP, UTP, fiber
Gigabit Ethernet	1 Gbps	Standard desktop communication and old Backbone systems	medium/low	STP, Fiber
Token Ring	4 or 16 Mbps	Infrastructures using IBM mainframes	medium	STP, UTP, fiber (between hubs)
FDDI	100 Mbps	Infrastructures requiring security and optical communication.	high	Fiber, CDDI-copper
ATM	25 Mbps-2.4Gbps	Backbone systems	high	STP, UTP, Fiber

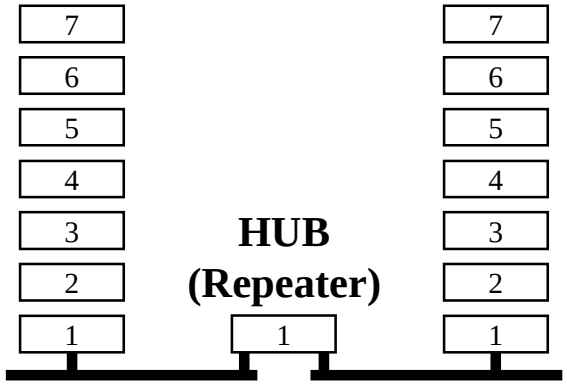
Charactersing attributes of a LAN

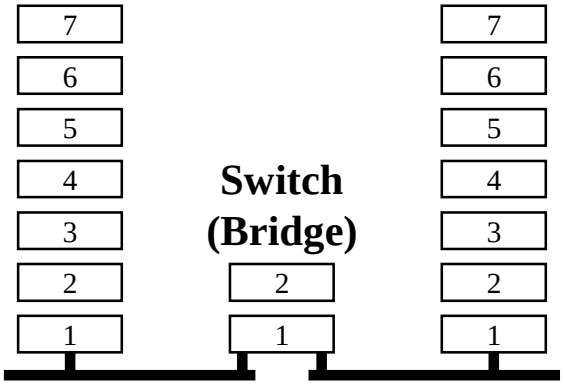
- Reliability (established technology).
- Flexibility (wide varity of applications).
- Modularity and standardized technology (independent from manufacturers)
- Extensibility
- Manageability
- Other qualifing characteristics/standards:
  - IEEE 802 standards
  - Universal cabling (EIA 568, ISO 11801)

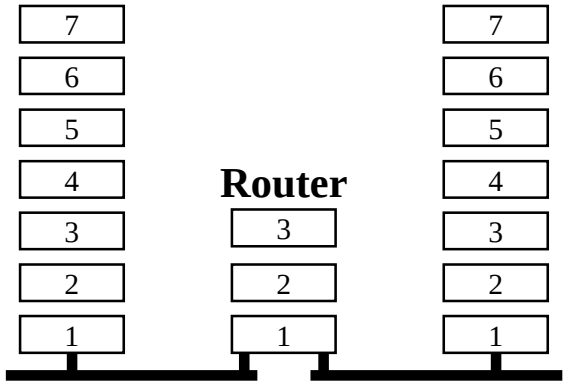
LAN: Systems' interconnection

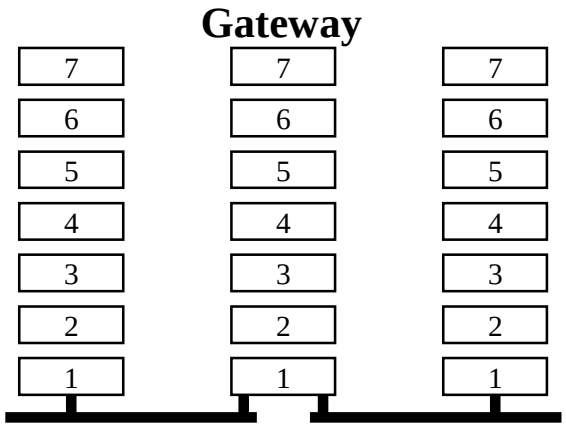
- Objective: interconnection of heterogeneous systems.
- Devices operating at different OSI layers should be distinguished.
- The following network infrastructures operating at different OSI layers should be known:
  - Repeater or Hub
  - Bridge or Switch or Wi-Fi Access Point
  - Router
  - Gateway
  - Firewall
  - …

Repeater, Bridge, Router, Gateway



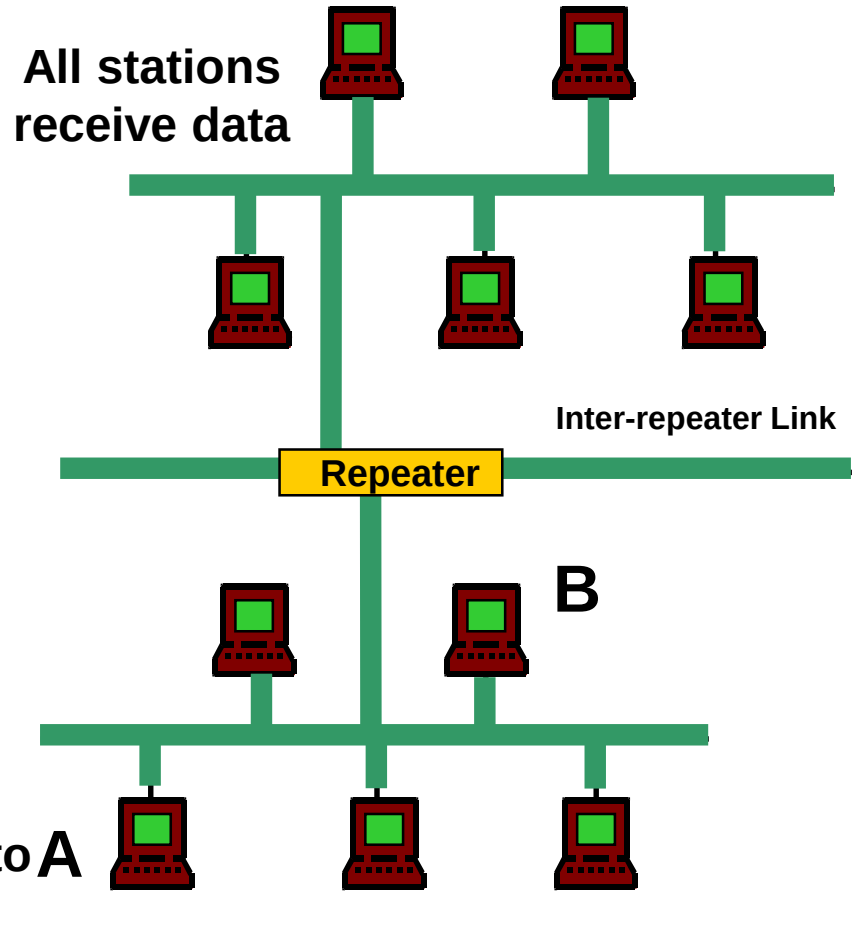






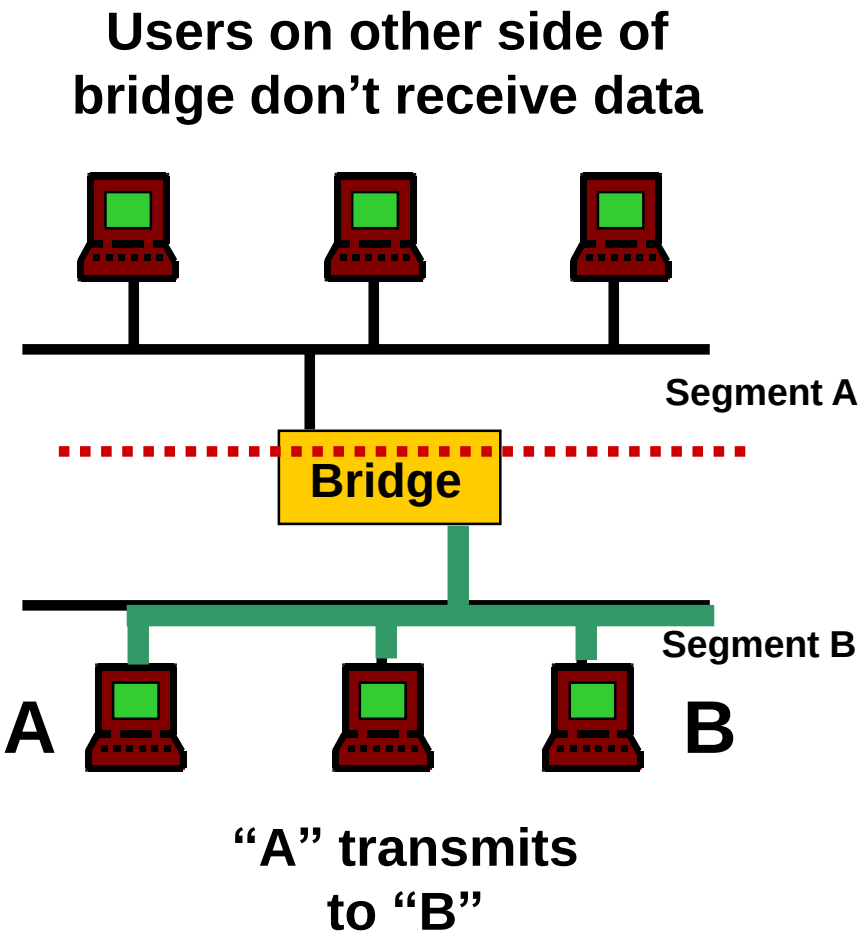
Repeaters o HUB

- Repeaters extend a LAN (enabling coverage of longer distances).
- Repeaters forward every data packet to every port.
- Repeaters regenerate the electrical signal that may be attenuated over distance.
- Repeaters detect collision and do not propagate them.



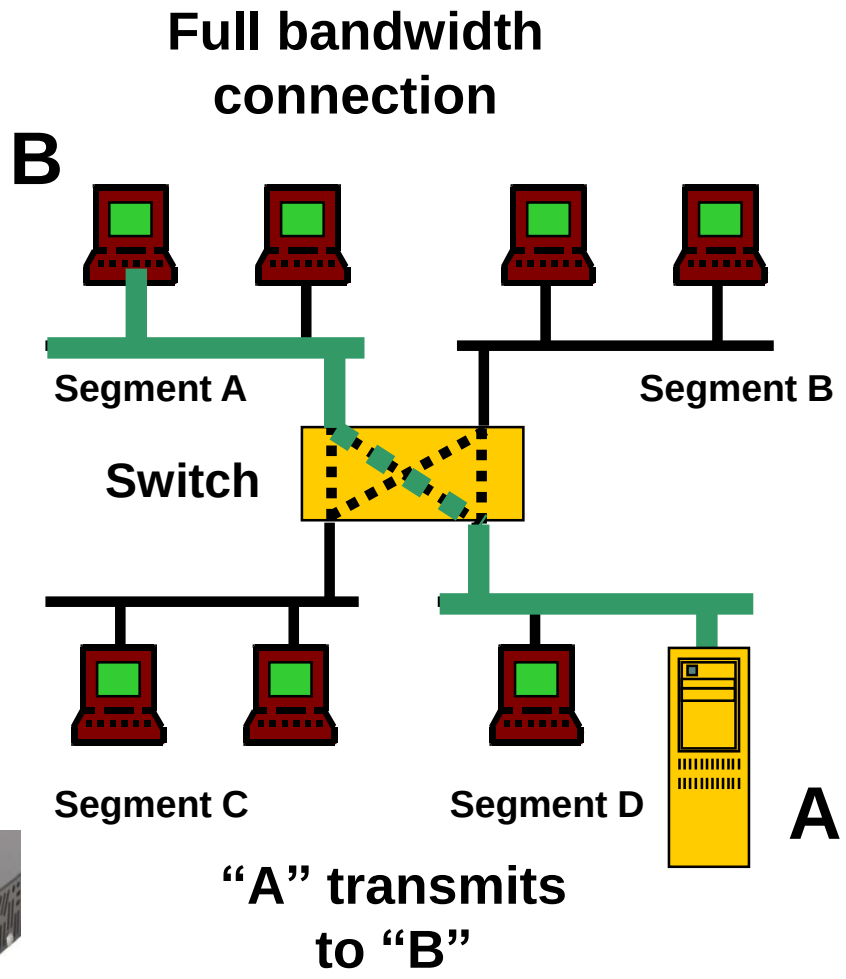
Internetworking Devices - Bridges

- Segments traffic and reduces congestion
- Keeps local traffic local
- Can connect similar LAN types
- Not used today for LAN performance needs



Internetworking Devices - Switches

- Segment traffic and reduce congestion
- Can be either frame or cell (ATM) based
- Significant performance increase
- Low cost and easy to use
- Desktop or backbone
- LAN only



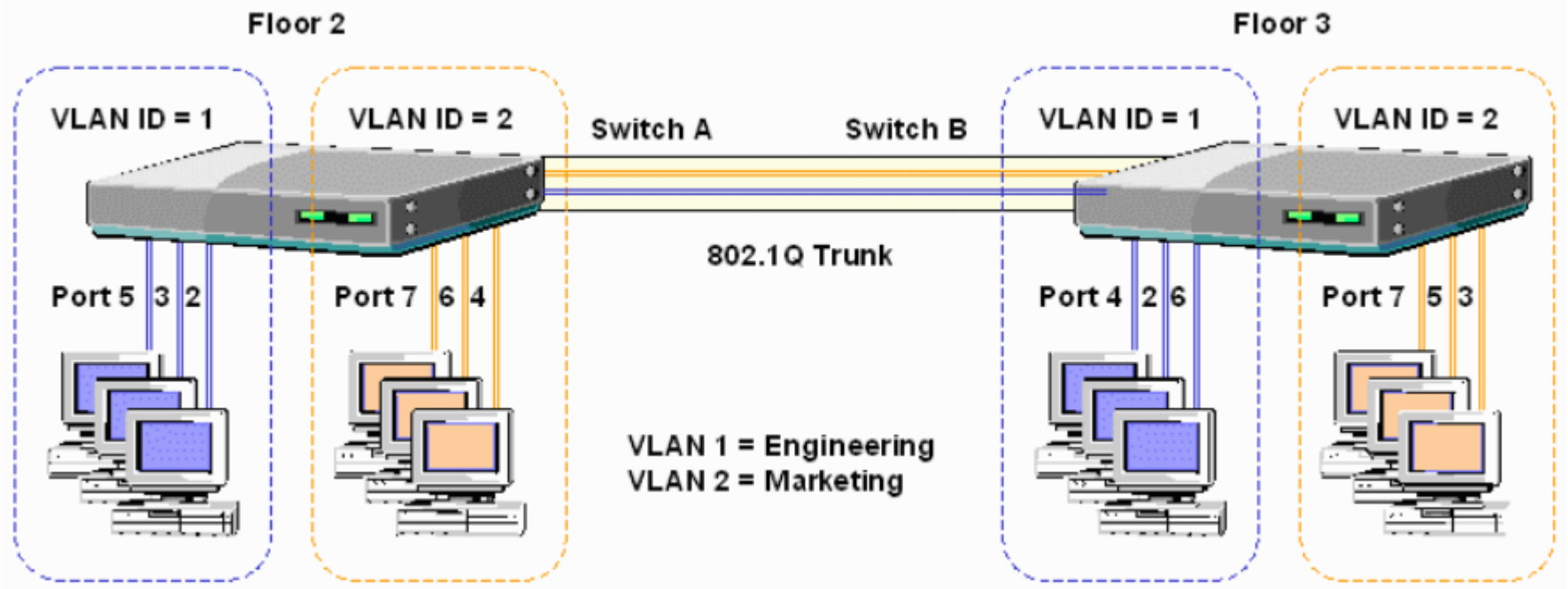
Bridge or level 2 switch (I)

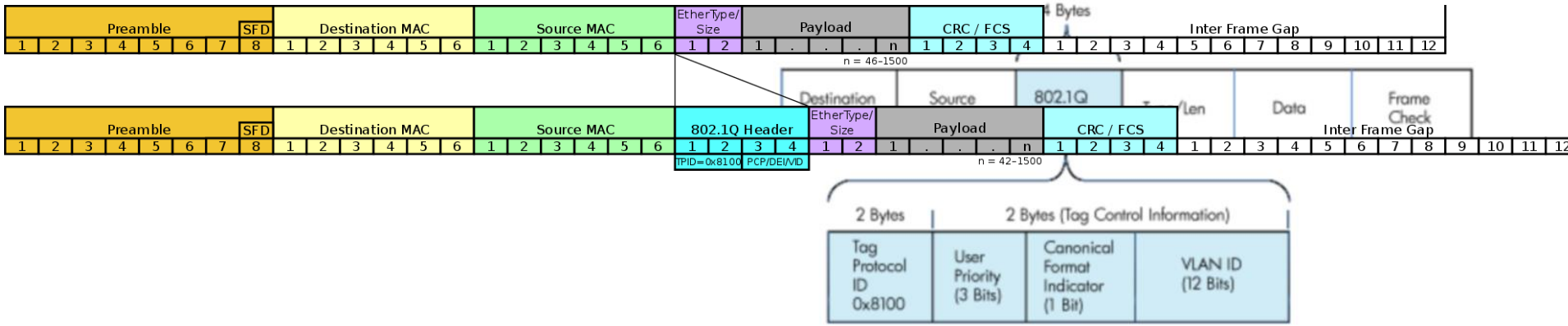
- They operate for same LAN topology (standard).
- They help reducing the traffic over the network.
- Each MAC address belonging to a LAN has to be unique.
  - e.g. : 00-2B-8C-42-5A-F1
- Level 2 doesn't allow routing.
- All stations see the network like a single LAN.
- Switches can learn and communicate topology information (spanning tree algorithm).
- Switching tables allow mapping of different MAC addresses on the different ports of the infrastructure.
- These infrastructures don't require particular initial setup. They operate normally. Some of them can be managed.

Switch topologies and technologies

- Not manageable (small or large switches)
- Manageable: this instrument allows being configured through standard management interfaces (serial/USB console; via ethernet (HTTPS, telnet, …))
  - VLAN
  - QoS
  - Limited layer 2 switching
  - Some switches include layer 3 switching
  - Anti ARP spoofing features
- Some switches offer PoE (power over ethernet) functionality
  - 802.3af (802.3at Type 1)
  - 802.3at Type 2

VLAN Trunk


Floor 2
Floor 3
VLAN ID = 1
VLAN ID = 2
Switch A
Switch B
VLAN ID = 1
VLAN ID = 2
802.1Q Trunk
Port 5 3 2
Port 7 6 4
Port 4 2 6
Port 7 5 3
VLAN 1 = Engineering
VLAN 2 = Marketing

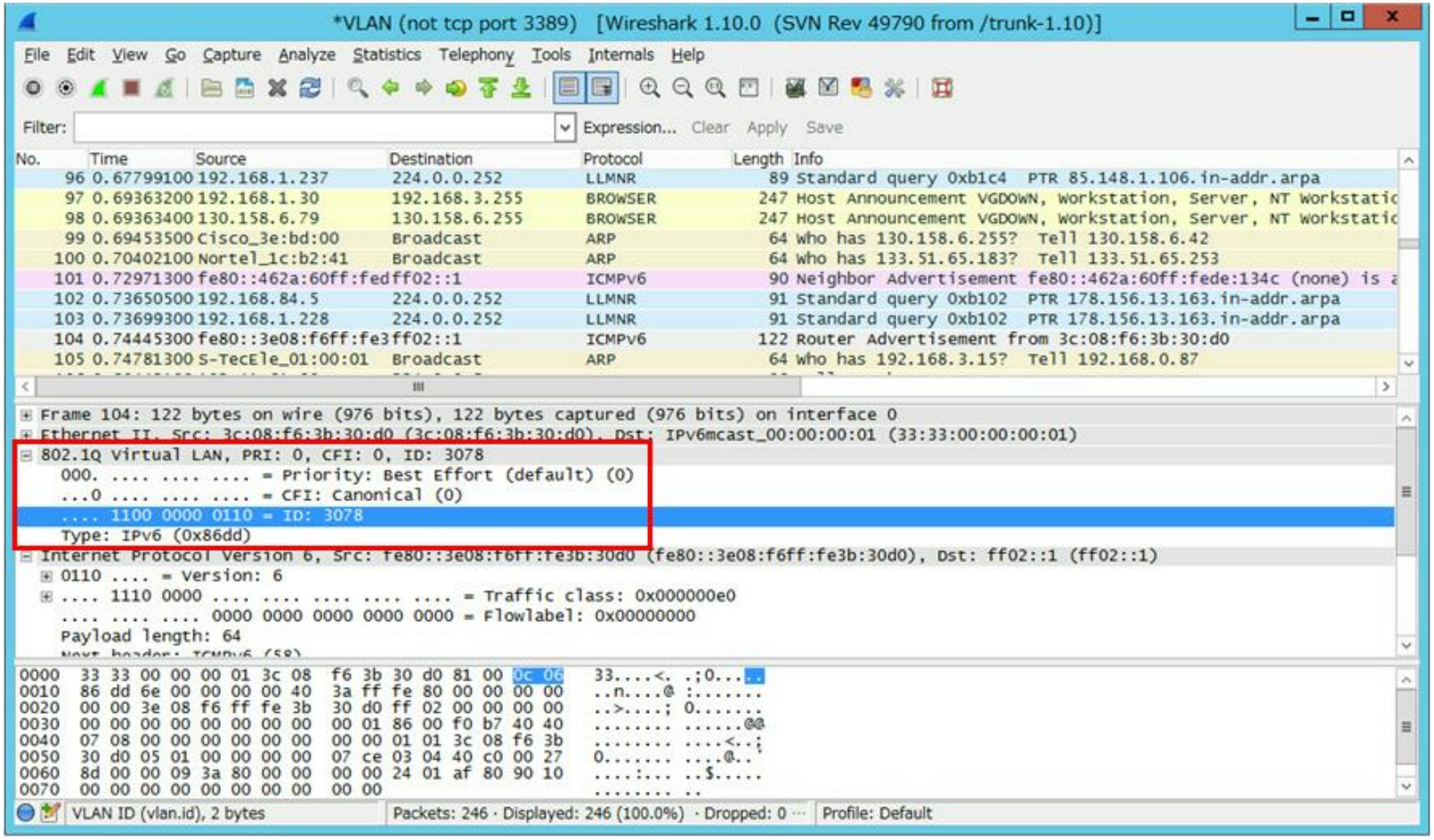

Preamble
SFD
Destination MAC
Source MAC
EtherType/ Size
Payload
CRC / FCS
4 Bytes
Inter Frame Gap
n = 46–1500
802.1Q Header
TPID=0x8100
PCP/DEI/VID
Destination
Source
802.1Q
Len
Data
Frame Check
n = 42–1500
2 Bytes
2 Bytes (Tag Control Information)
Tag Protocol ID 0x8100
User Priority (3 Bits)
Canonical Format Indicator (1 Bit)
VLAN ID (12 Bits)

VLAN Trunk

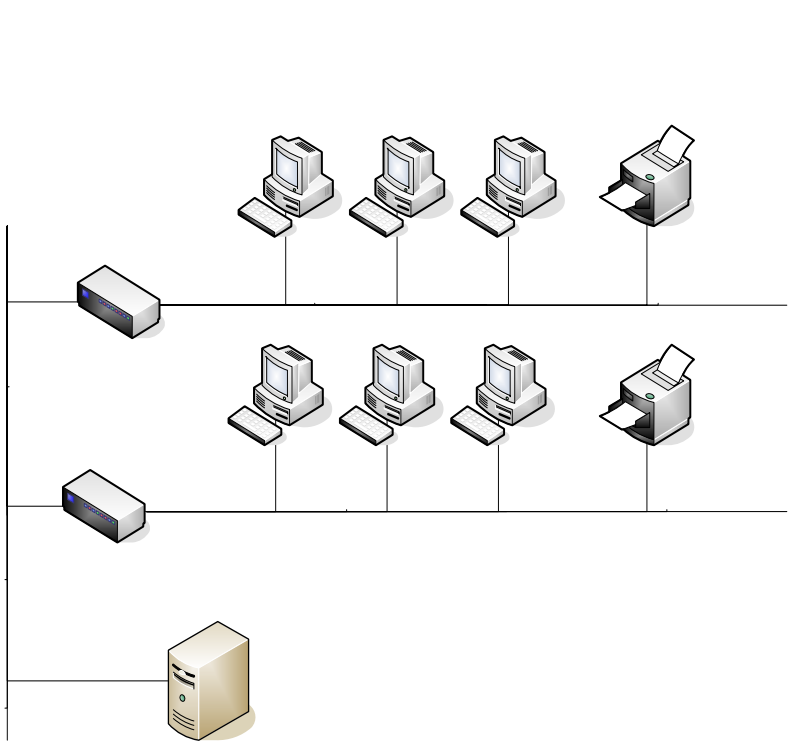
- Tag protocol identifier (TPID)
  - 16-bit field, set to **0x8100** to identify the frame as IEEE 802.1Q-tagged frame. Located at the same position as the EtherType field in untagged frames, thus used to distinguish the frame from untagged frames.
- Tag control information (TCI)
  - A 16-bit field containing the following sub-fields:
  - Priority code point (PCP)
    - A 3-bit field which refers to the IEEE 802.1p class of service and maps to the frame priority level. Different PCP values can be used to prioritize different classes of traffic.
  - Drop eligible indicator (DEI)
    - A 1-bit field. (formerly CFI[b]) May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.[6]
  - VLAN identifier (VID)
    - A 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs.

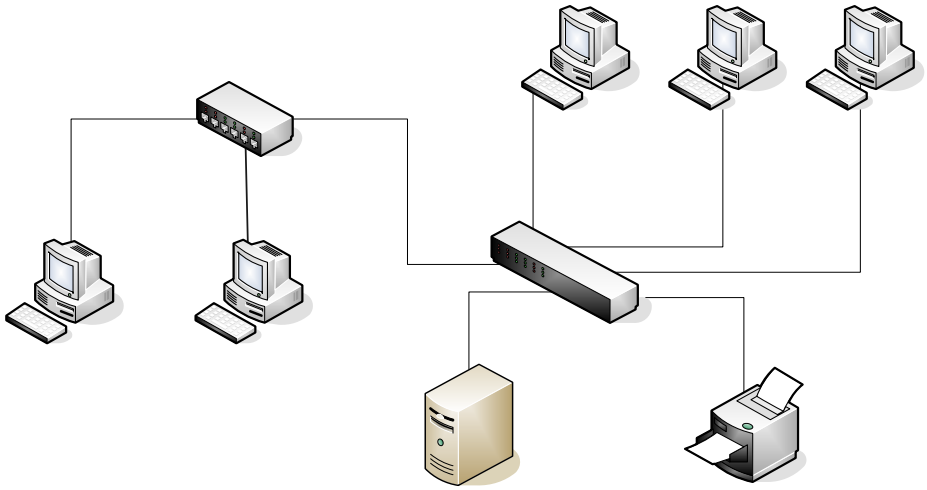
VLAN Tagging

- The IEEE 802.1Q protocol



Bridge or layer 2 switch (II)





OSI layer 3: IP address classes

- Original address classes regulating the internet: 8, 16 and 24 bit
  - Class A: 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh
    0 ··· 127 **2^24 host**
  - Class B: 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh
    128 ··· 191 **2^16 host**
  - Class C: 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh
    192 ··· 255 **2^8 host**
  - (n: network part, h: host part)

- Subnetting and supernetting
  - Subnetting: increase of the network mask, splitting a network in several sub-networks.
  - Supernetting: reduction of the number of bit in the network mask. This allows merging different neighbour networks.

Network mask (subnet mask)

- Consists of 4 bytes (32 bits):
  - The “1” indicate the network part of the IP address.
  - The “0” indicate the host part (variable part) of the IP address.

- Notation:
  - dotted quad
    - e.g.: 255.255.255.224
  - bit count: number of “1” bits starting from the left e.g.: /27

- Network part of the address: the one mapped to the “1” bits
  - E.g.: 193.5.15.167 / 24 => network address: 193.5.15.0
  - Exercise: 193.5.15.167 / 26 => network address: _____

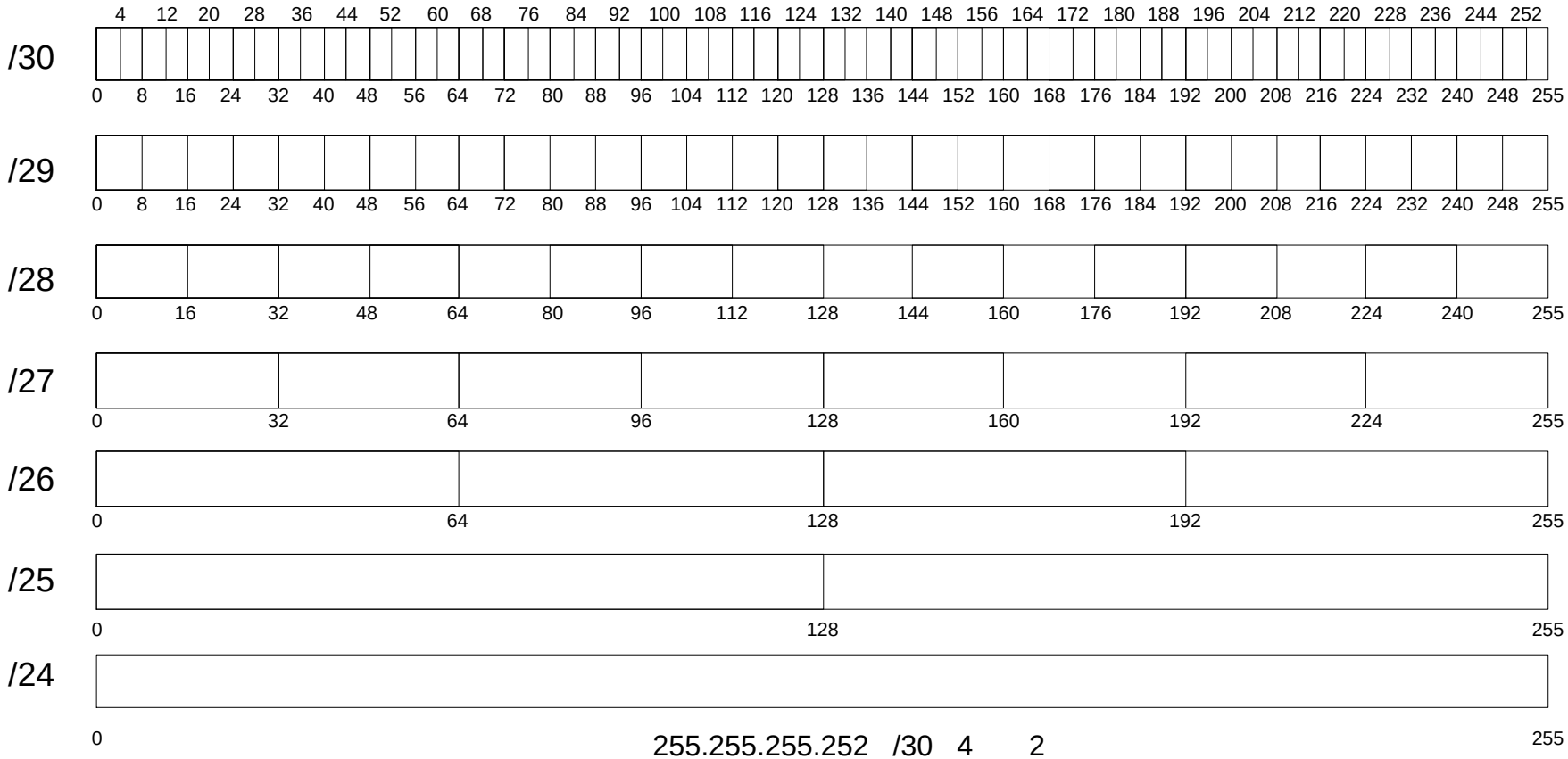
Network mask (subnet mask)

- Possible netmasks, in dotted quad and bit count format:

...	/...	...	...
255.255.254.0	/23	512	510
255.255.255.0	/24	256	254
255.255.255.128	/25	128	126
255.255.255.192	/26	64	62
255.255.255.224	/27	32	30
255.255.255.240	/28	16	14
255.255.255.248	/29	8	6
255.255.255.252	/30	4	2

- Number of IPs = 256 − last byte in the Netmask

Subnet mask



255.255.255.252	/30	4	2
255.255.255.248	/29	8	6
255.255.255.240	/28	16	14
255.255.255.224	/27	32	30
255.255.255.192	/26	64	62
255.255.255.128	/25	128	126
255.255.255.0	/24	256	254

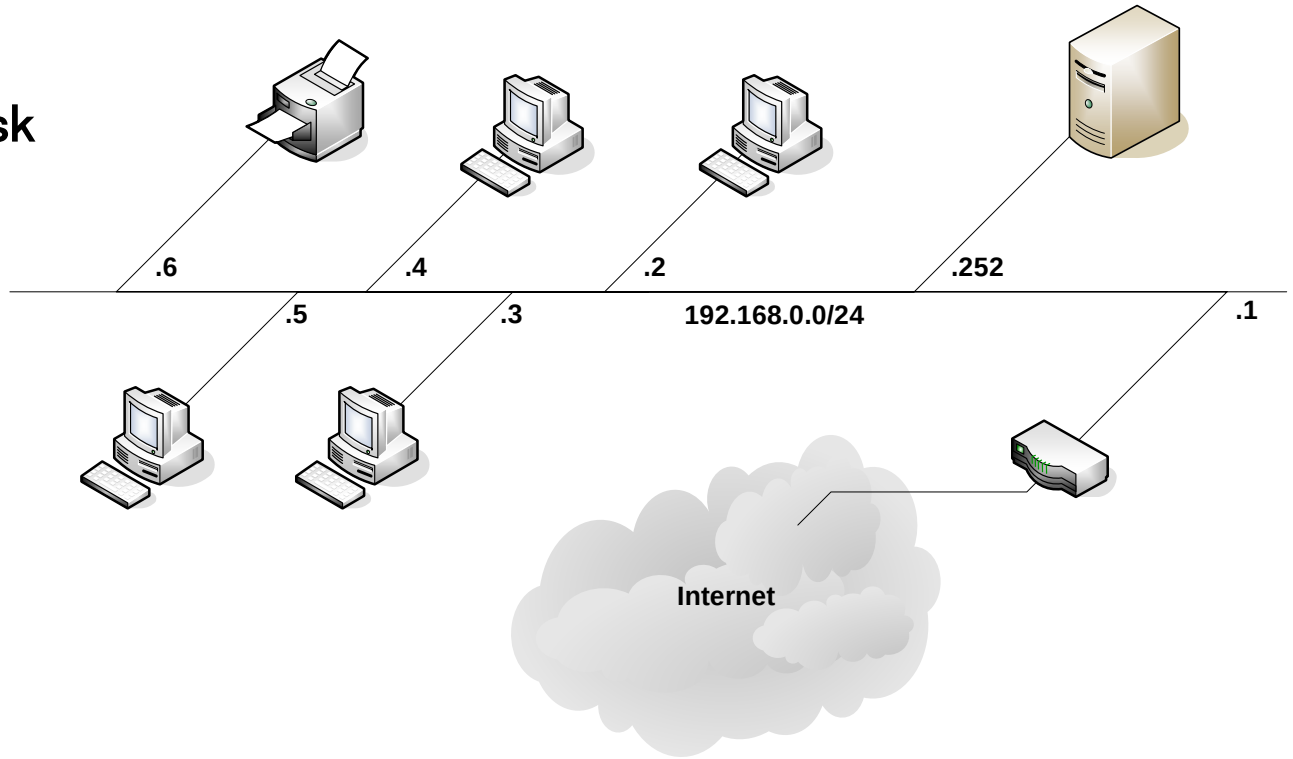
Special IP addresses

- **Special IP addresses**
  - Network address: first host address in the IP range (e.g. The host 0 in class C; 192.168.1.0
  - Broadcast address: last host address in the IP range (e.g. host 255 in class C networks; 192.168.1.255)
  - Loopback or Localhost: local host address
    - 127.0.0.0 , 127.0.0.1, 127.0.0. ....

- **Private IP addresses**
  - RFC 1918, these IP address classes cannot be used across the internet, they are reserved for use on private networks:
    - 10.0.0.0 .. 10.255.255.255 [10.0.0.0/8]
    - 172.16.0.0 .. 172.31.255.255 [172.16.0.0/12]
    - 192.168.0.0 .. 192.168.255.255 [192.168.0.0/16]

IP Configuration

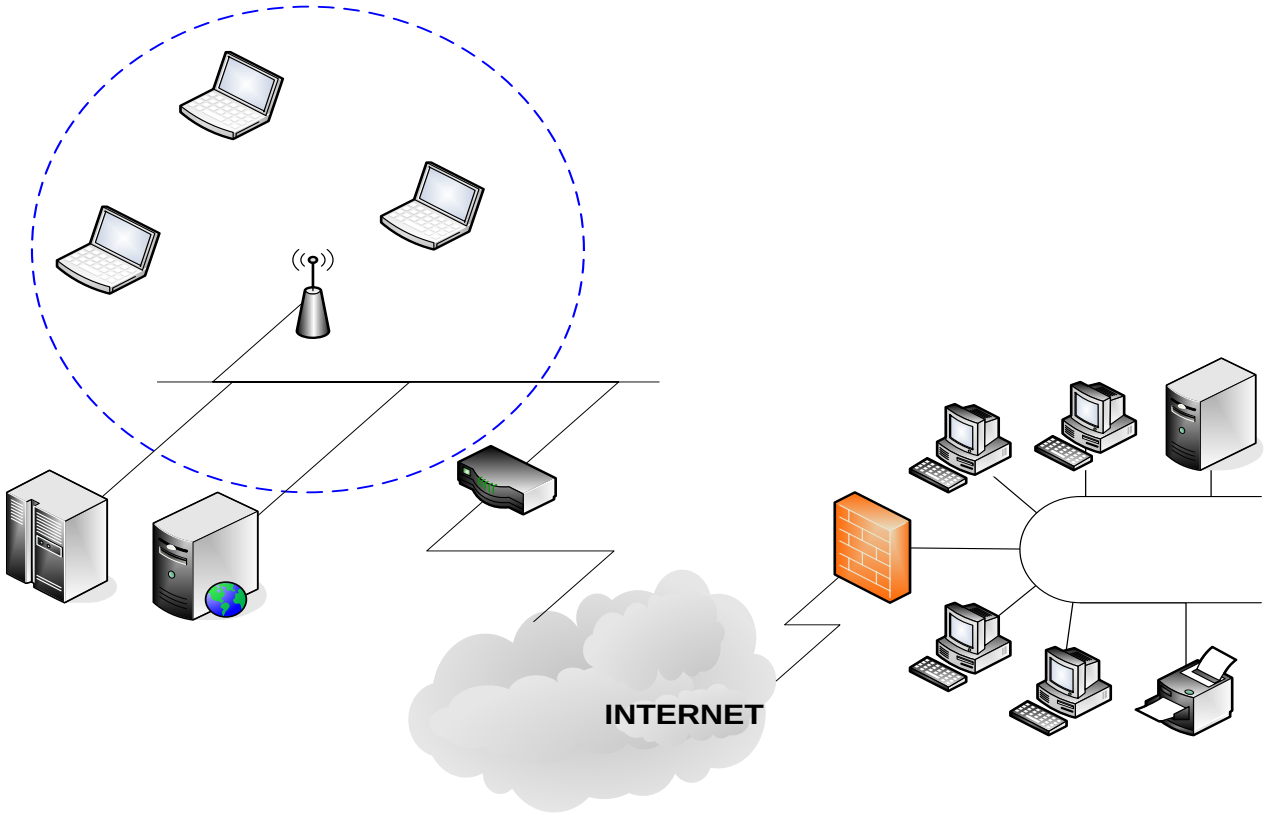
- In an IP based network, a node (device, host, network infrastructure, …) can act on the LAN (internal/private network) based on the following 2 parameters:
  - **IP Address**
  - **Subnet Mask**



- In order for a node communicate outside the LAN, it requires an additional parameter: the **Default Gateway**

Gateway

- A gateway connects 2 networks.
- It generally operates at OSI layer 3, but may also act on 4 to 7.
- It allows the interconnection of architectures, protocols, frames and addressing formats that may strongly differ from each other.

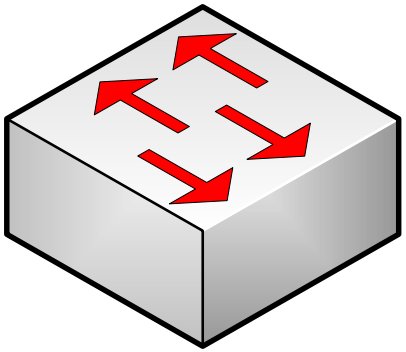


Routing

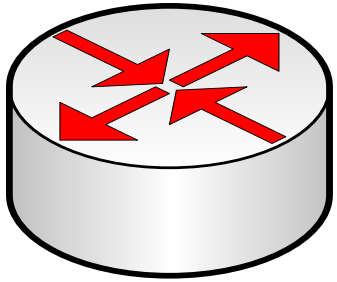
- A router is a network infrastructure carrying out routing decisions on frames.
- Routers operate at network level (OSI 3 layer).
- Routing decisions are done for each single packet.
- In order to be able to route packets, a router uses a routing table.
- A routing table contains information about:
  - (sub)networks (groups of contiguous IP addresses).
  - Parameters allowing the drouting decision to be taken, such as:
    - Distance vector
    - Bandwidth
    - Delay
    - …
  - Default route (if any).

Routing vs. Switching

- Symbol used for Network Switch



- Symbol used for Network Router



- A switch (or Layer 2 switch) connects **hosts** belonging to the same network
- A router connects different (**sub-)networks**
- A Layer 3 switch (also called routing switch) operates like a Layer 2 switch, but also has the functionality of a router. It may learn and interconnect hosts belonging to different networks.

Router or Layer 3 switch (I)

- They are able to manage layer 3 communication protocole as well as routing protocols.
- Some protocols may not permit routing (e.g. Netbeui)

- Some routers communicate using protocols :
  - To exchange routing information.
  - To transport data on the network.

- Routers use protocols to communicate with end-nodes :
  - To learn information from the connected networks.
  - To obtain the MAC address from the network address.
  - To gain information about possible network issues.

Router or layer 3 switch (II)

- It is possible to distinguish between:
  - **STATIC ROUTING**:
    - Each new network or route must be manually added, programmed and maintained on each routers.
  - **DYNAMIC ROUTING**:
    - It make use of routing table(s) and autonomously cares for routing and continuous update of the routing status and tebles.
    - The optimization of routing path is based on 2 principles:
      - "Distance vector" (metric system to calculate the path, number of hop, or number of networks between 2 end nodes).
      - "Link State" (it operates taking into account the current state of the path: bandwidth, link state such as delay and network congestion).

Router or layer 3 switch (III)

- Layer 3 switch:
  - They were firstly developed at the end of the 90'
  - They are based on ASIC technology that integrate routing principles in hardware solution.
  - They can be defined as "real routers":
    - They can determine a path and route networks.
    - They can check the integrity of a layer (the third).
    - They can check the time to live of a packet.
    - They allow the creation of security features for networks.

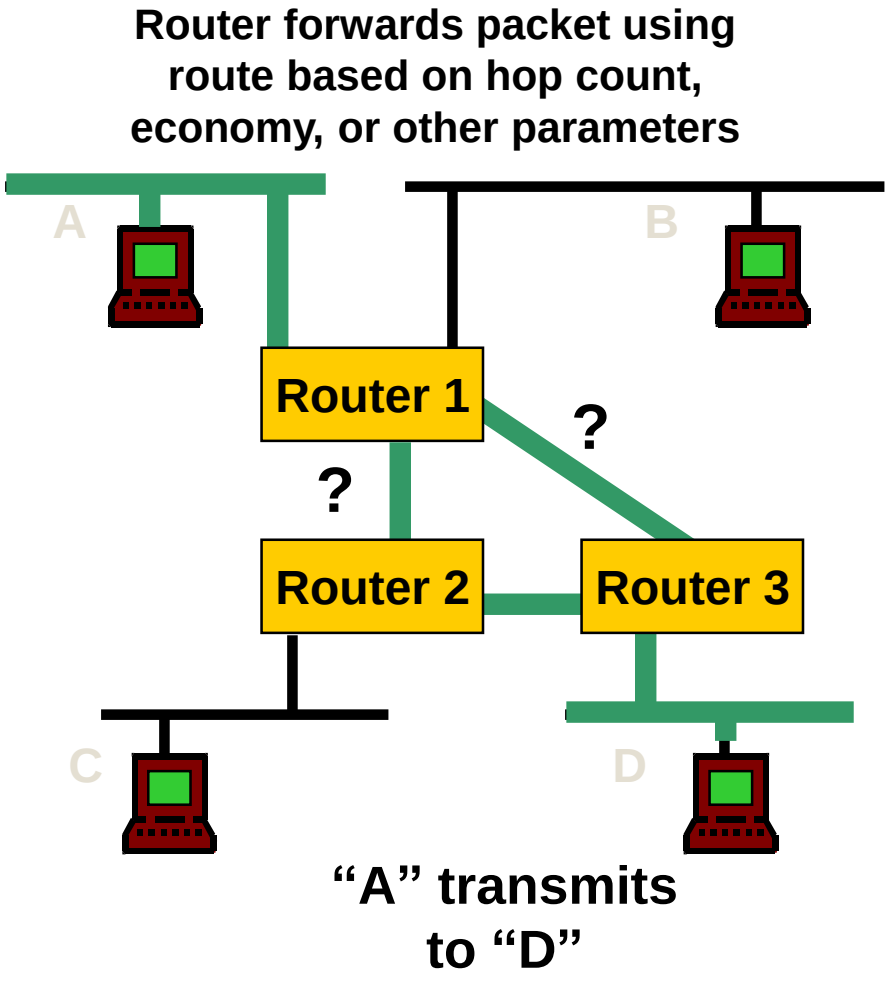
Router or layer 3 switch (IV)

Comparison table: router and layer 3 switch

Characteristics	**Layer 3 switch**	**Router**
It is able to route protocols such as IP, IPX, Appletalk, …	Yes	Yes
Subnet defintion	Layer 2 functionality	Hardware port
Forwarding architecture	Hardware	Software
Remote monitoring	Yes	Yes
Packets forward performances	High	Low
WAN support	No	Yes
Needed setup configuration	Minor	Major

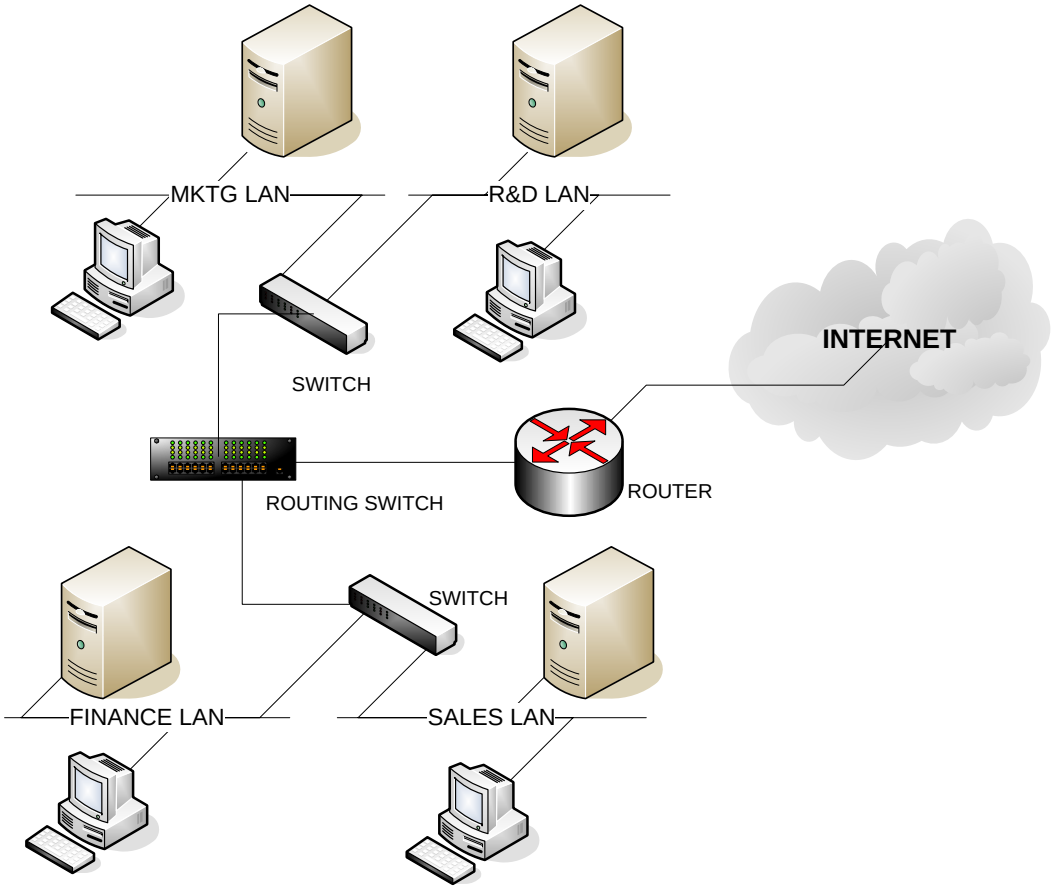
Internetworking Devices - Routers

- More expensive and complex than switches
- Protocol-dependent
- Can connect similar/different LAN types
- LAN or WAN use

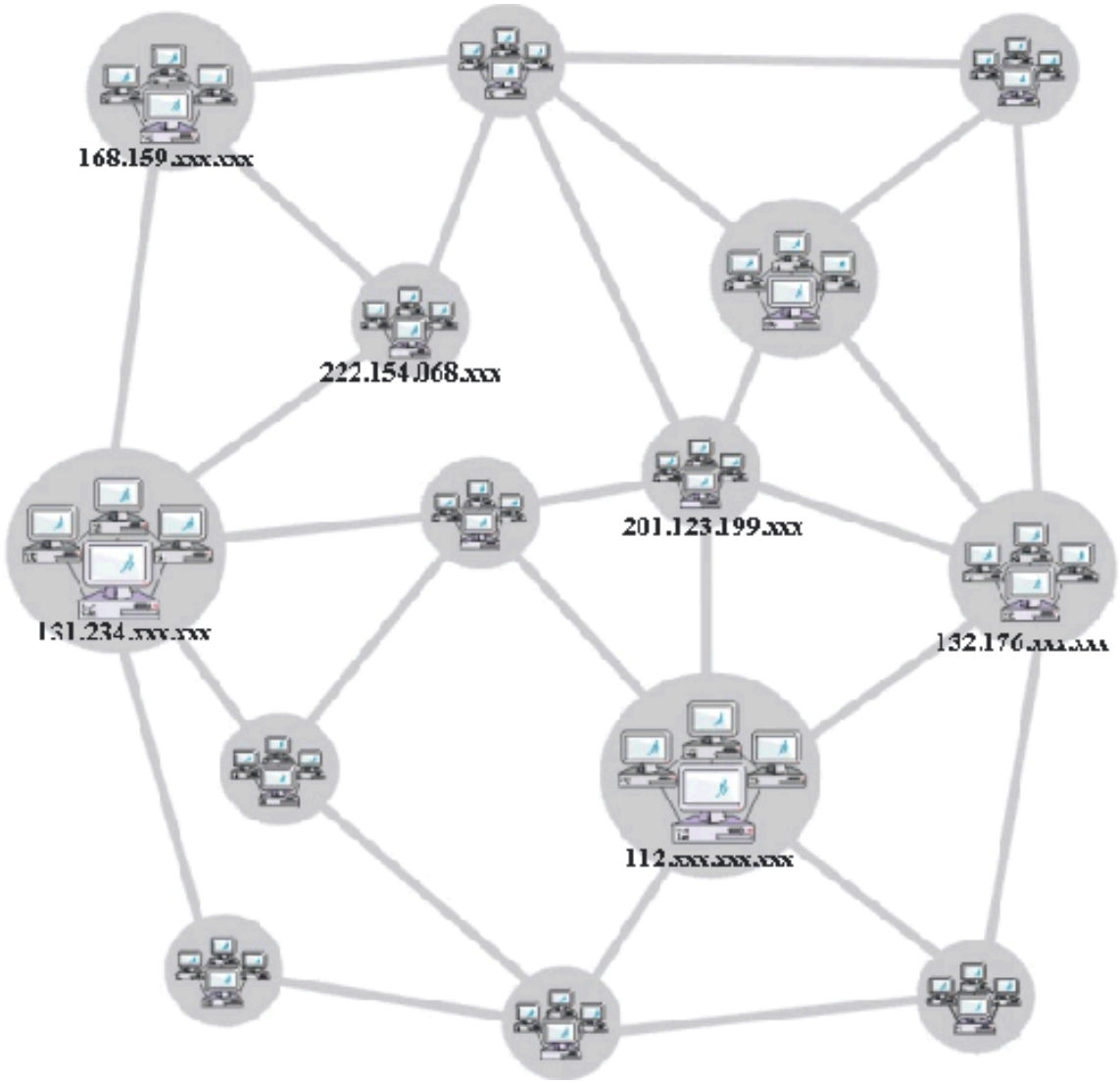


Routing Switches

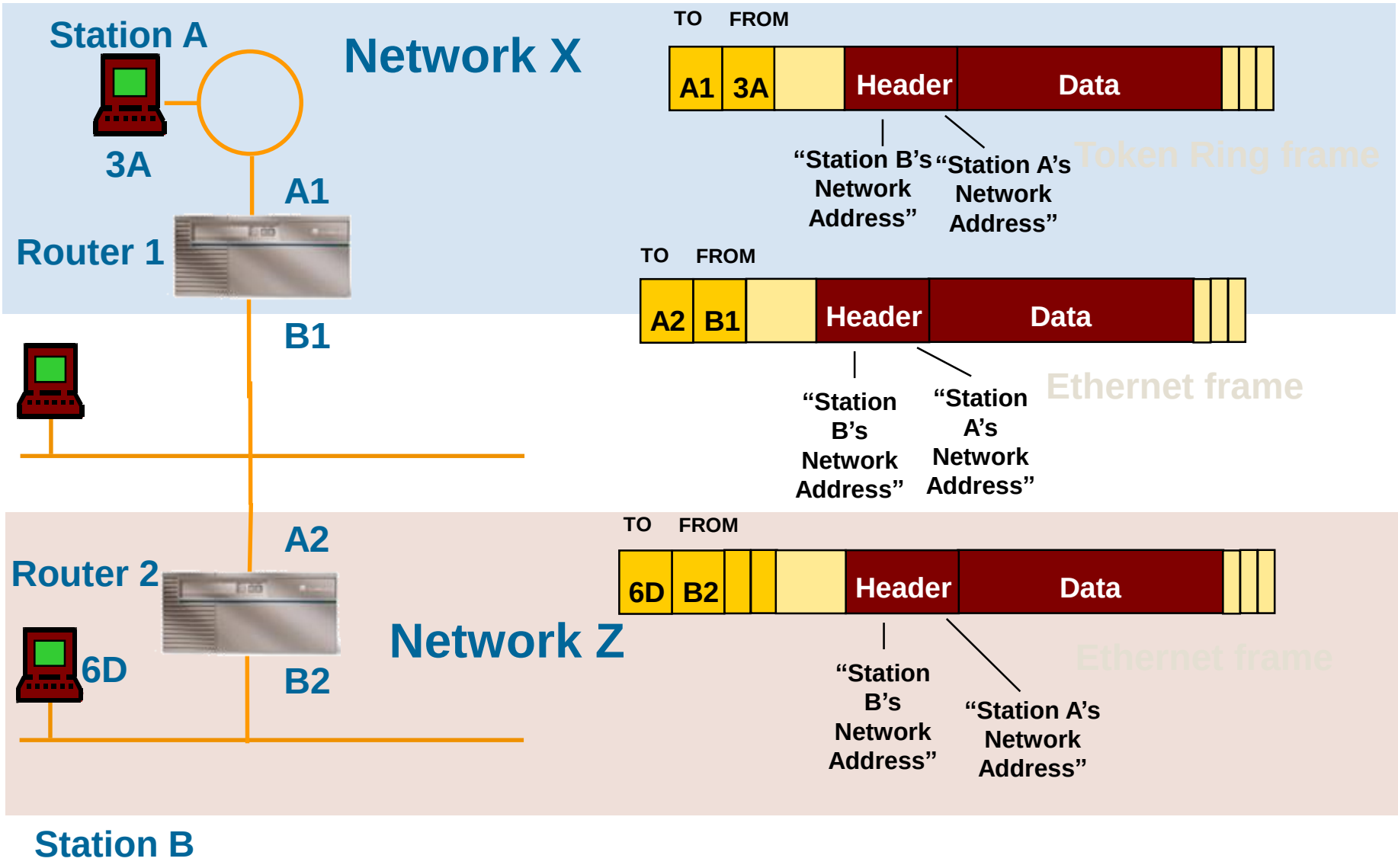
- Internetworking Devices.
- Intelligence of a router with performance of a LAN switch.
- Used as substitutes of routers to handle LAN backbone traffic.
- Usually optimized for IP traffic.
- Used for LAN traffic only (no WAN).



Routing example



How Does a Router Work?



Layer 3: Network

- Network protocols (not IP)
- Routing protocols, e.g. OSPF, RIP, …
- Network protocols, IP protocol:
  - IPv4
  - Address Resolution Protocol (ARP)
  - Internet Control Message Protocol (ICMP)
  - IPv6

- Routing:
  - Static
  - Dynamic

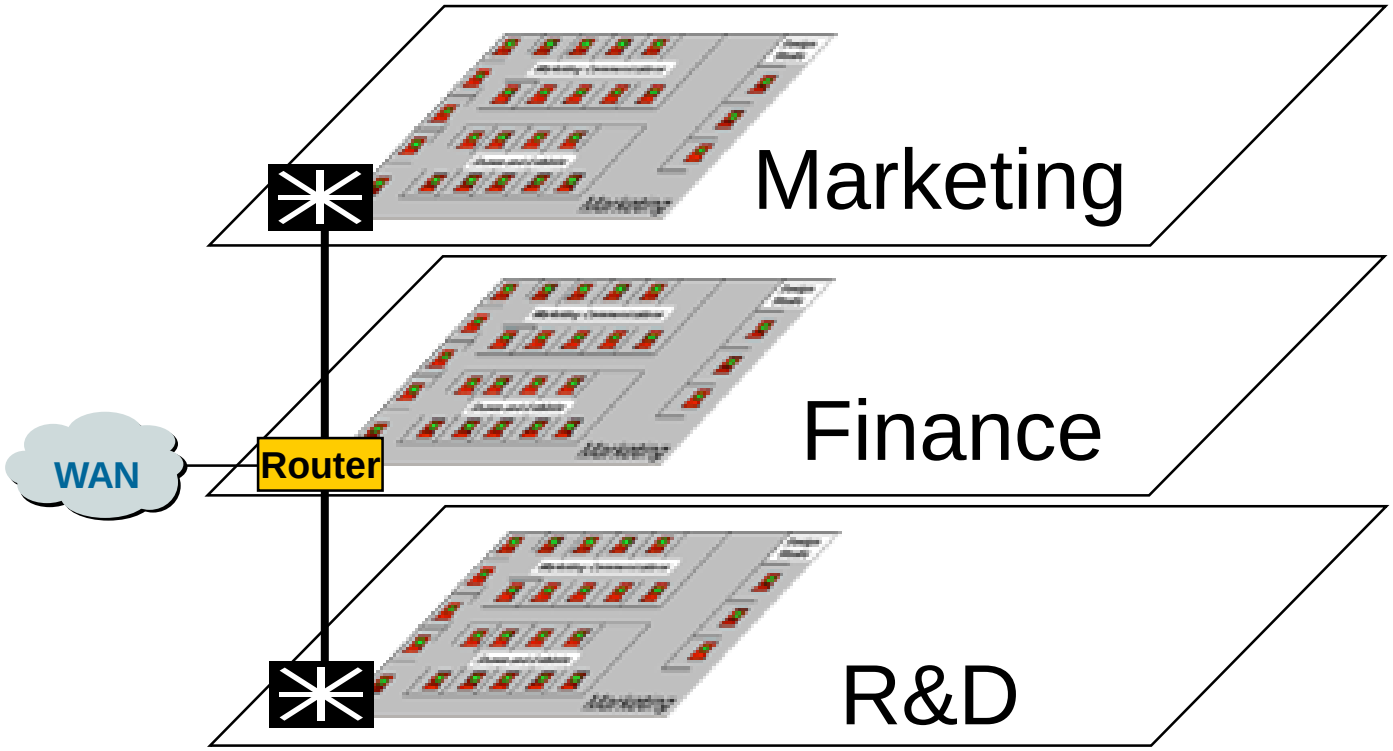
Layer 3 protocols

- IP
- Appletalk
- DECNET
- LAT
- IPX/SPX
- ...

- ~~NetBeui~~

Network Backbones

- **Backbone**
  - Interconnection of different LANs

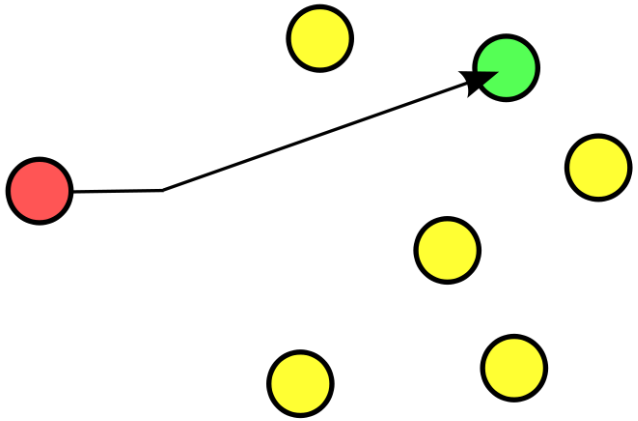


Routing schemes: notions

- Several possibility to send a packet on the network.

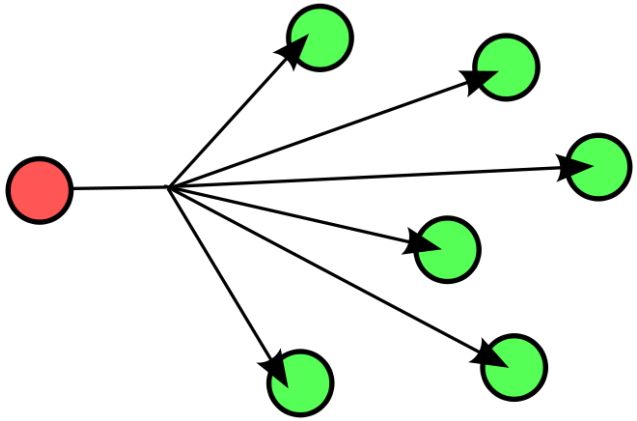
- Routing topology can be divided in the following categories:
  - Unicast
  - Broadcast
  - Multicast
  - Anycast
  - Geocast

Routing schemes: unicast



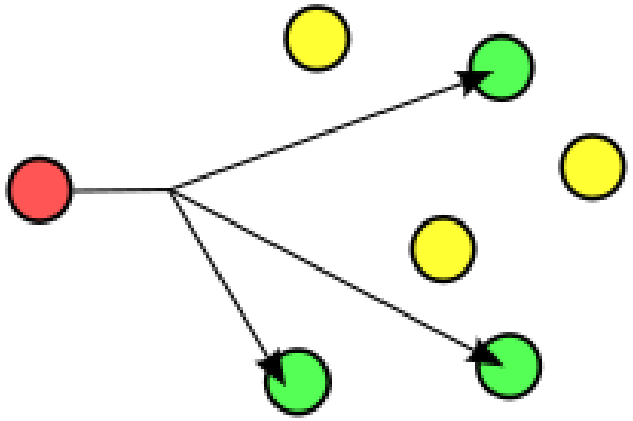
- The message is delivered from a single node to a single node.
- Most used communication scheme on local network and internet.

Routing schemes: broadcast



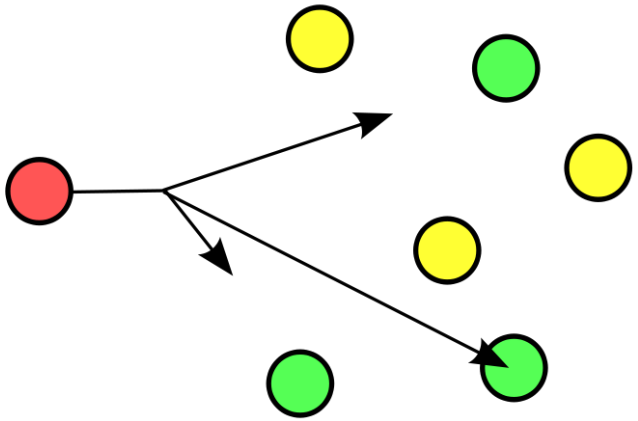
- The packet/frame is sent to all nodes of the network.
- Used in protocols which require this type of communication, e.g. for ARP (OSI Layer 2) and DHCP (OSI Layer 7).

Routing schemes: multicast



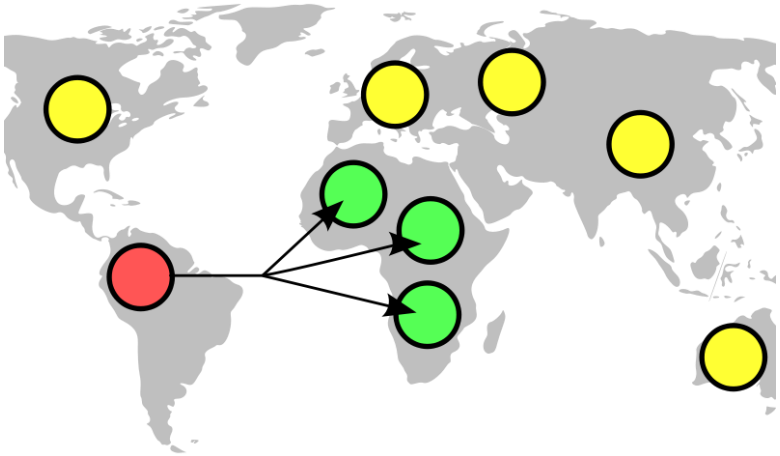
- Similar to broadcast, it is a 1-to-many communication.
- It differs from broadcast because the recipients are not all nodes but the recipient is a well defined group of nodes.
- It uses IGMP protocol, the protocol can manage nodes enrollment to receive a message.
- It is mainly used on *streaming* (IPTV, radio).

Routing schemes: anycast



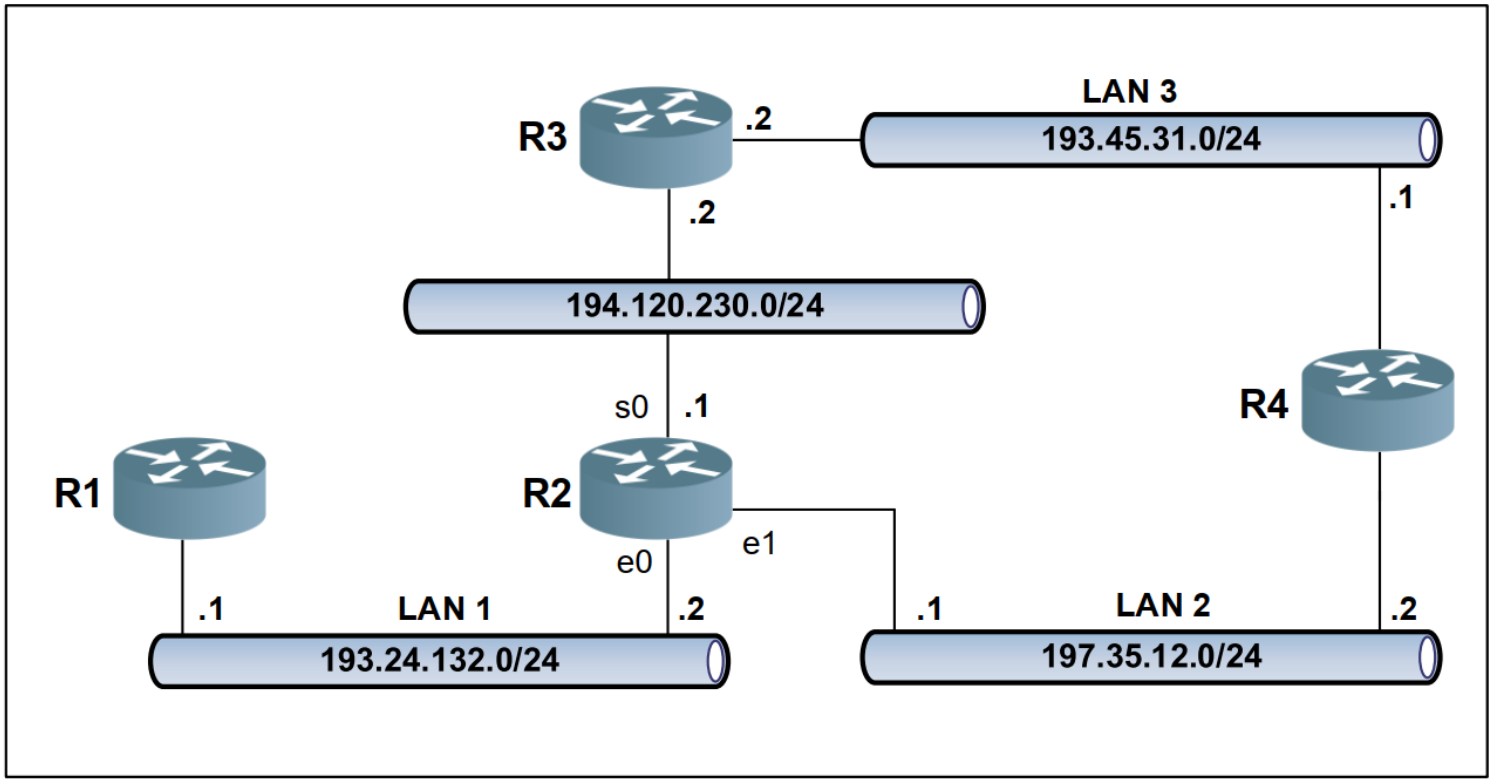
- Similar to multicast, 1-to-(1 out of many) communication.
- The recipients are part of a well defined group of nodes (like multicast).
- The communication requires only 1 out of the target multicast group, selection based on some criteria (e.g. 1st respondent)
- The evaluation criteria may vary for each message.
- BGP protocol.
- Mainly used in peer-to-peer networks.

Routing schemes: geocast



- Similar to multicast, the recipient's target group consists of nodes having the same geographical location.

Routing table



Router 2: routing table

Network	Interface	Next Hop	Metric
193.24.132.9	e0	-	0
197.35.12.0	e1	-	0
193.45.31.0	e1	197.35.12.2	1
193.45.31.0	s0	194.120.230.2	1

Routing topology

- Directly connected routing network:
  - Every router interface is connected to *at least* un network.
  - Traffic form nodes connected to an interface is routed to the interface assigned to the target network.
- Static routing
  - Routes are manually configured, programmed, communicated and maintained.
  - Does not change, even in case of network failure or degradation.
- Dynamic routing
  - Based on routing tables
  - Tables are populated and automatically updated according to routing protocols.
  - Each router updates its tables based on network status changes.
  - Each router communicates routing information updates to neighbor routers.

Routing protocols

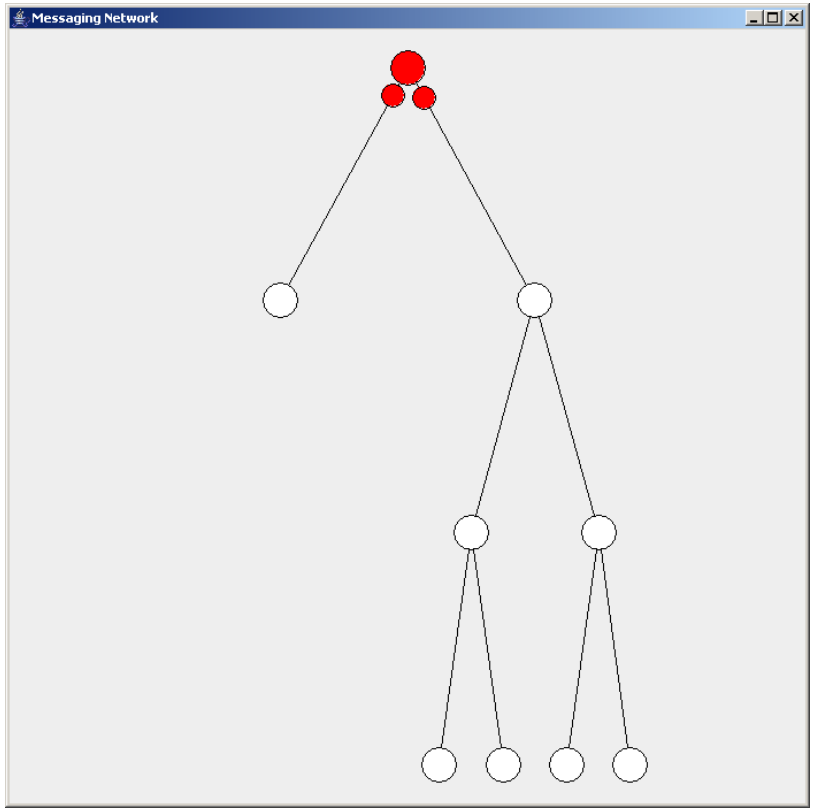
- Routing protocols are used to determine routes and form the routing table.
- They are divided in 2 topologies, according to algorithms and protocols used.

- **Non adaptive routing**
  - The algorithm does **not** use the current state of the network as criteria.
  - Also called *static routing protocols.*

- **Adaptive-routing**
  - Routing algorithms allow decision making based on parameters continuously updated based on network status.
  - Routers exchange information on their neighbors, this allows building up-to-date routing tables, to do this routers exchange multicast packets called “hello packet” .
  - Examples: RIP, IGRP, IS-IS, OSPF, EIGRP.

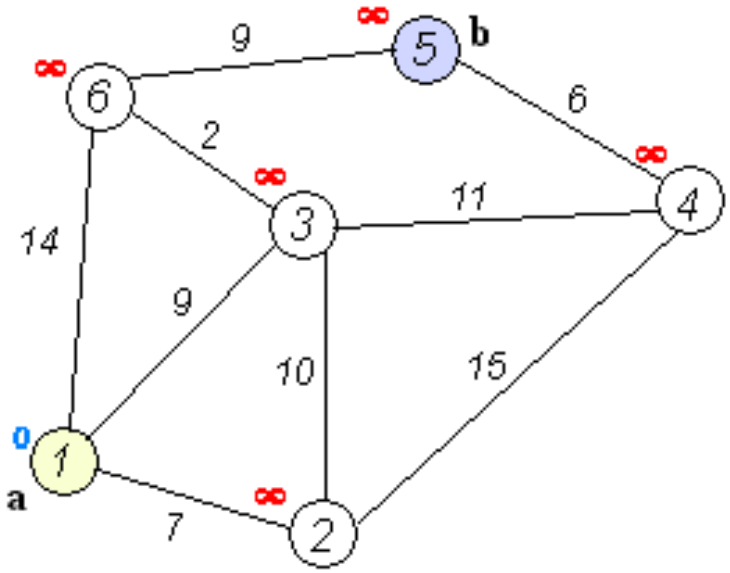
Non-adaptive routing: Flooding

- The router propagates/forwards incoming routing information to all neighbor, except the one which generated it.



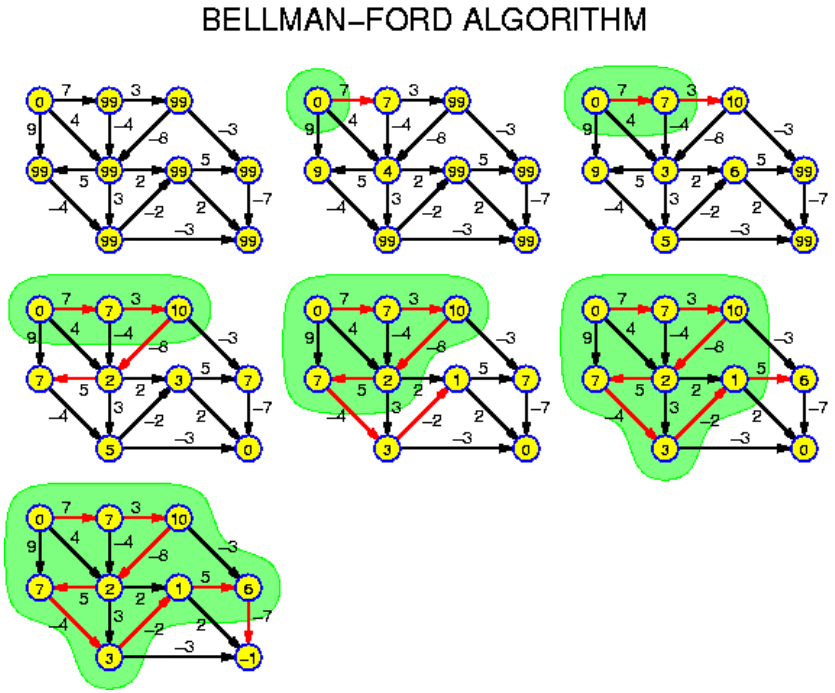
Adaptive routing: shortest path

- The shortest path algorithm is used to find, as suggested by the name, the shortest path; also called: **Dijkstra algorithm**.
- The measurement (cost) is also called *metrics* and is expressed in *hops*, geographical distance, ...



Adaptive routing: RIP

- **Routing Information Protocol**: it is based on the distance vector, and uses the Bellmann-Ford algorithm. Convergence concept.
- The only metric used for routing only optimizes the number of hop (hop count, number of network to reach the target node).



Adaptive routing: IGRP

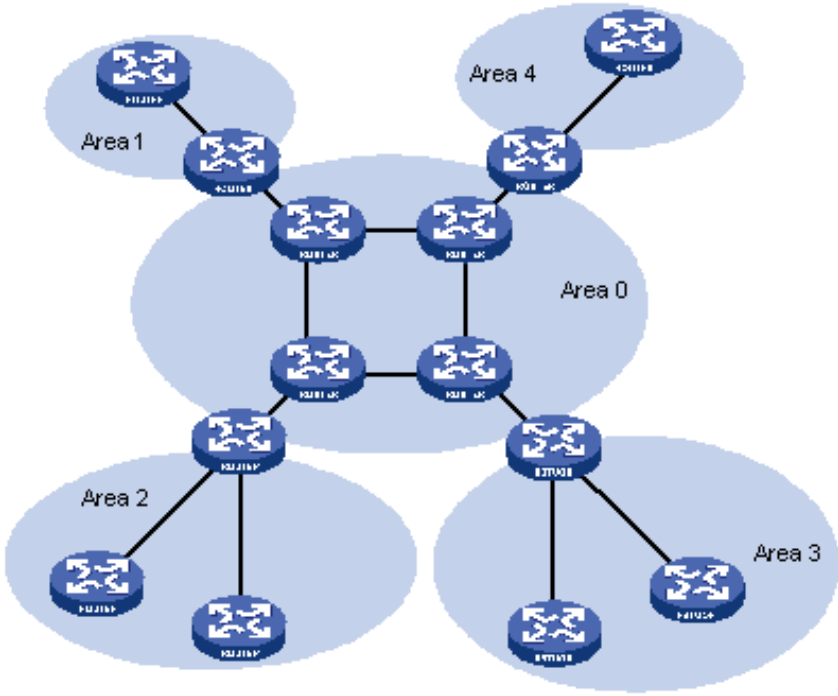
- **Interior Gateway Routing Protocol**: based on distance vector, with additional metrics on network status.
- IGRP supports multiple metrics for each path: bandwidth, line-load, delays and reliability; to compare two path it combines the previous listed metrics with single metrics with constant value.
- Maximum number of hops: 255,
- It was created to overcome the limitation of the RIP protocol (maximum hops: 15).

- Proprietary protocol (CISCO).

- Metric = [K1 * Bandwidth + (K2 * Bandwidth)/(256-load) + K3*Delay] * [K5/(reliability) + K4]
- The default constant values are K1 = K3 = 1 and K2 = K4 = K5 = 0.

Adaptive routing: OSPF

- **Open Shortest Path First**: this protocol is based on the link state.
- The protocols based on the link state have a complete vision of the network topology and its status (unlike distance vector that is limited to hop count).
- The protocol acquires information on the near link states and forwards it information to the other nodes using the algorithm *link state broadcast*.
- Open algorithm (not proprietary).



Adaptive routing: EIGRP

- **Enhanced Interior Gateway Routing Protocol**: protocol based on combination of distance vector and link state information.
- Evolution of IGRP.
- Maximum no. hop: 224.
- IGRP uses a combination of 5 metrics: delay, bandwidth, reliability, Maximum Transmission Unit (MTU), load.

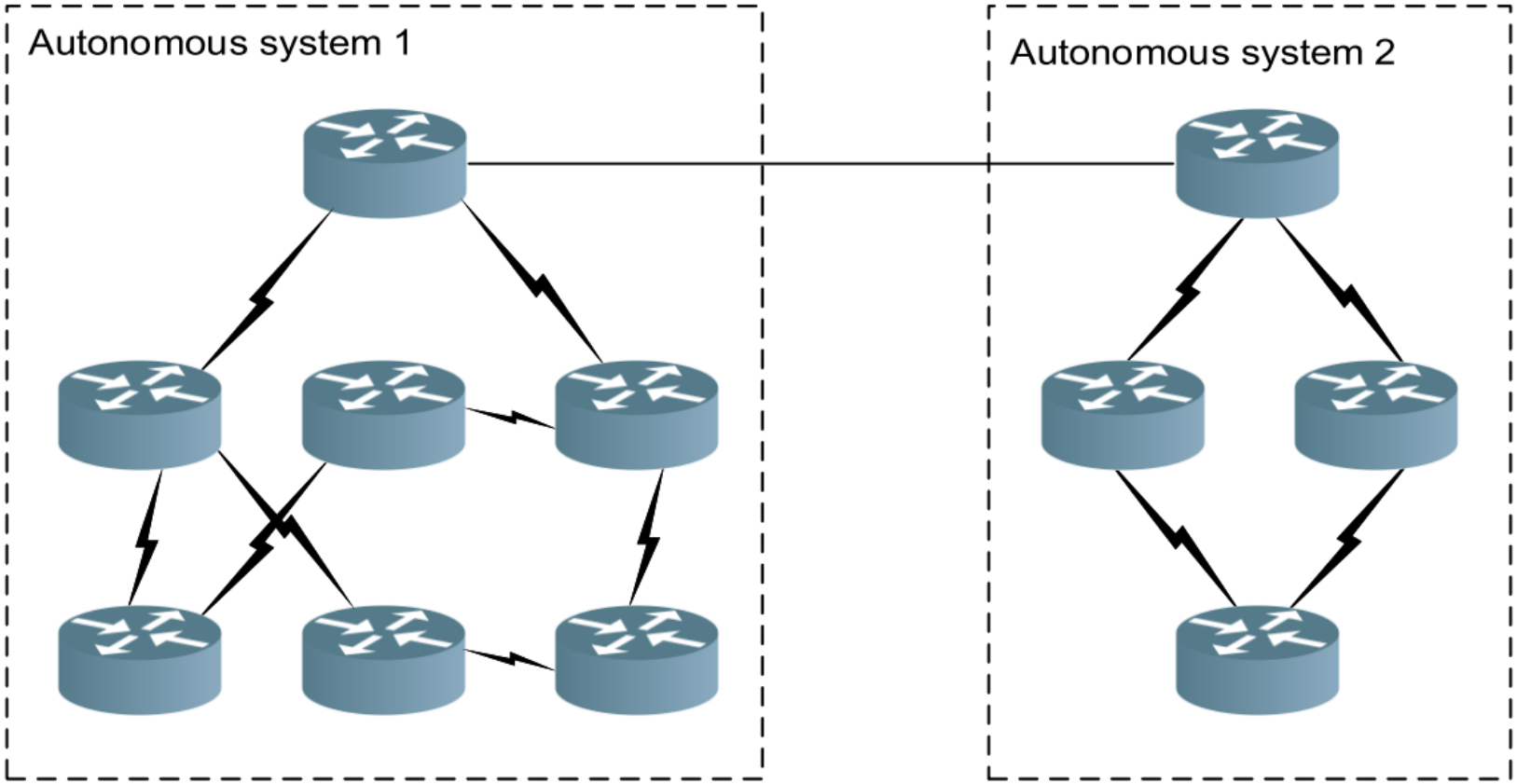
- Proprietary protocol (CISCO).

Algorithm comparison

Feature	RIP	IGRP	OSPF	EIGRP
Algorithm	Distance vector	Link state	Link state	Both distance vector & link state
Metric	Hop count	Based on delay, bandwidth, channel occupancy and reliability of the path.	Routing based on on bandwidth delays, throughput and RTT	Bandwidth, load, delay, hop count and reliability
Maximum no. of hops	15/16 hops is considered to be infinity	Maximum 255 (default 100)	Depends on the size of routing tables	Maximum 255
Subsystem segmentation	Autonomous system is treated as single subsystem	No segmentation of the autonomous system (AS)	Breaks the autonomous system in areas	System is not divide in areas
Proprietary/Open	Open	Proprietary	Open	Proprietary

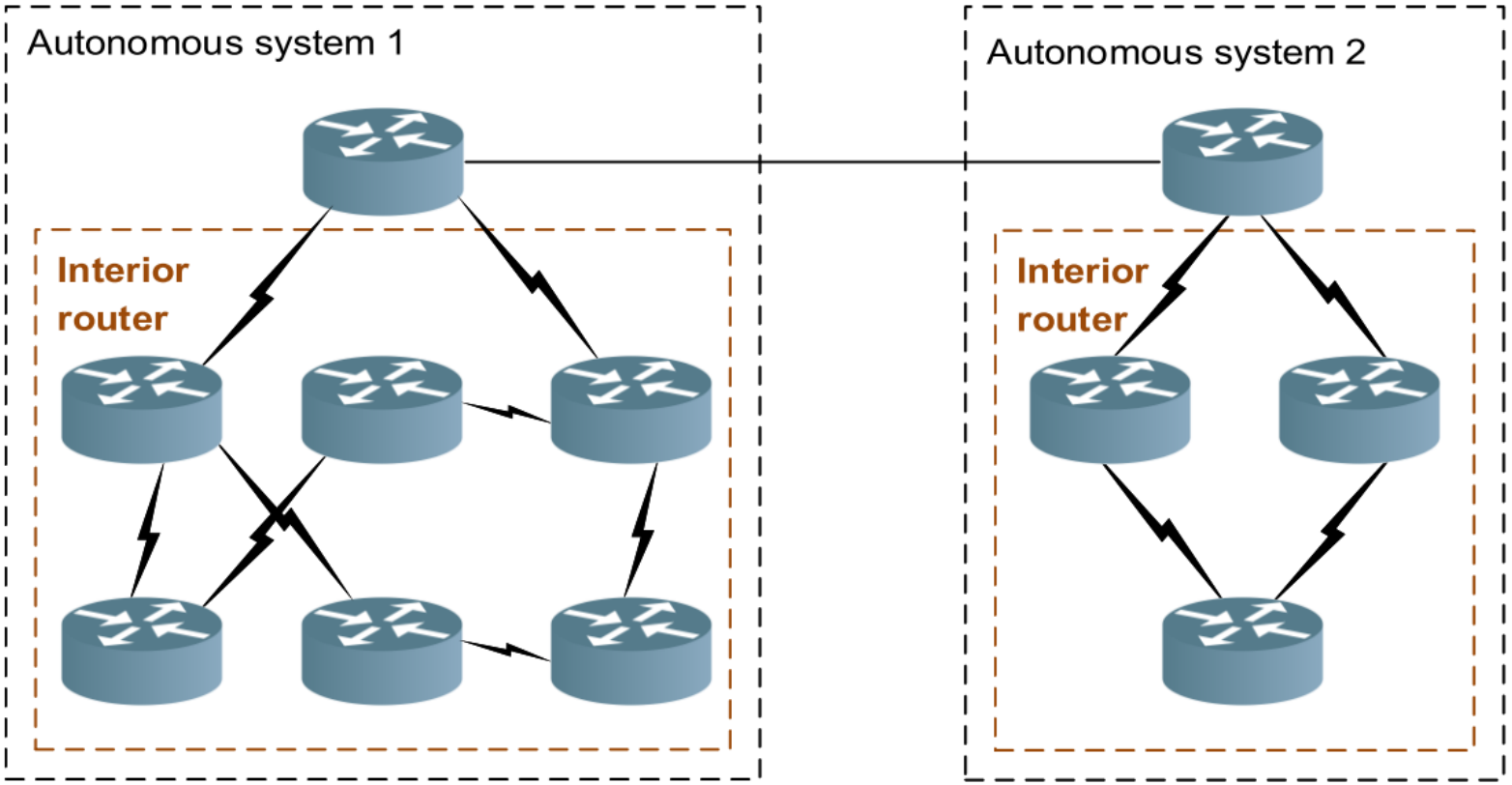
Interconnecting Autonomous Systems

- Defintion of autonomous system.



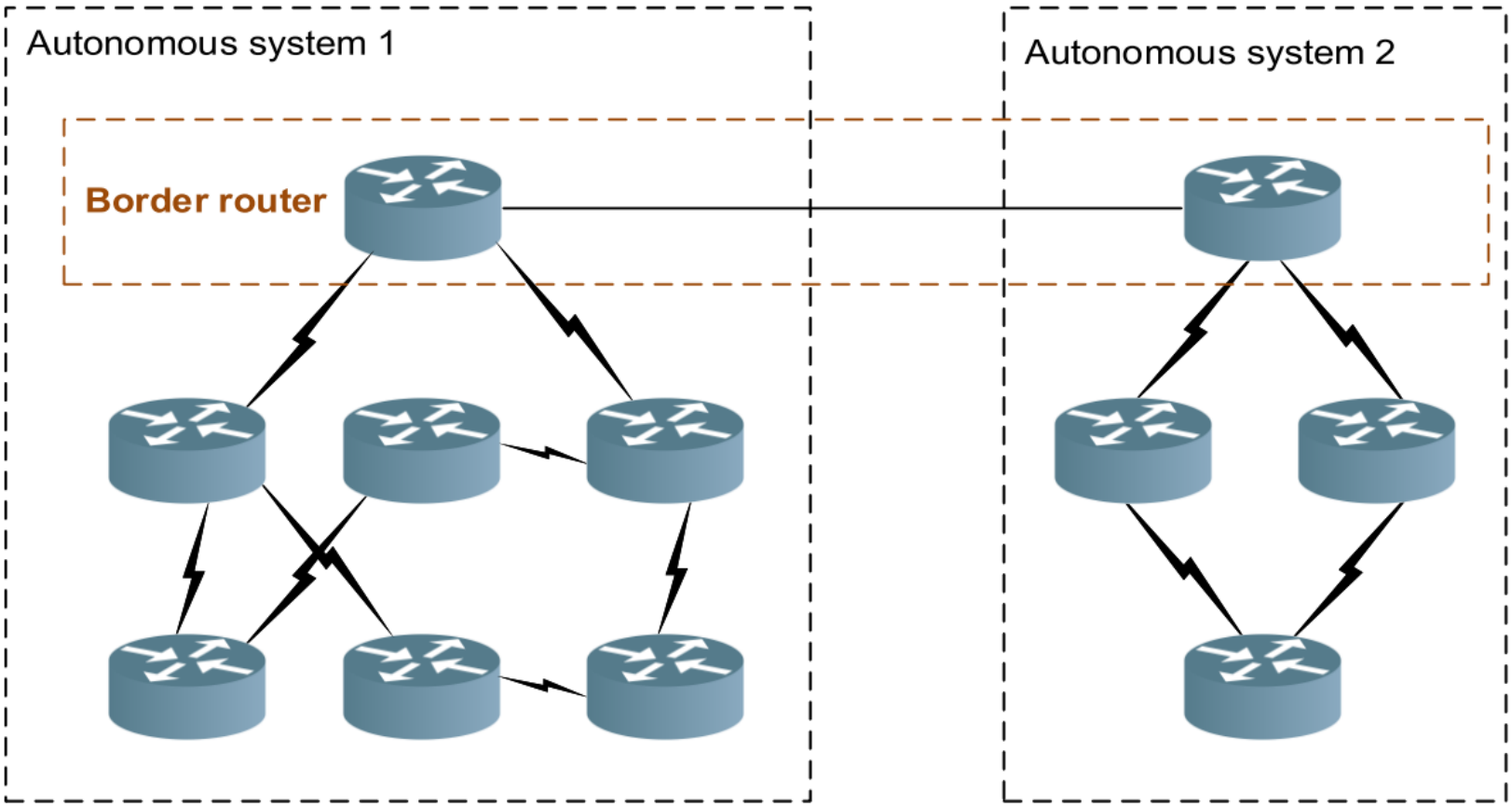
Interconnecting Autonomous Systems (II)

- Interior router definition.



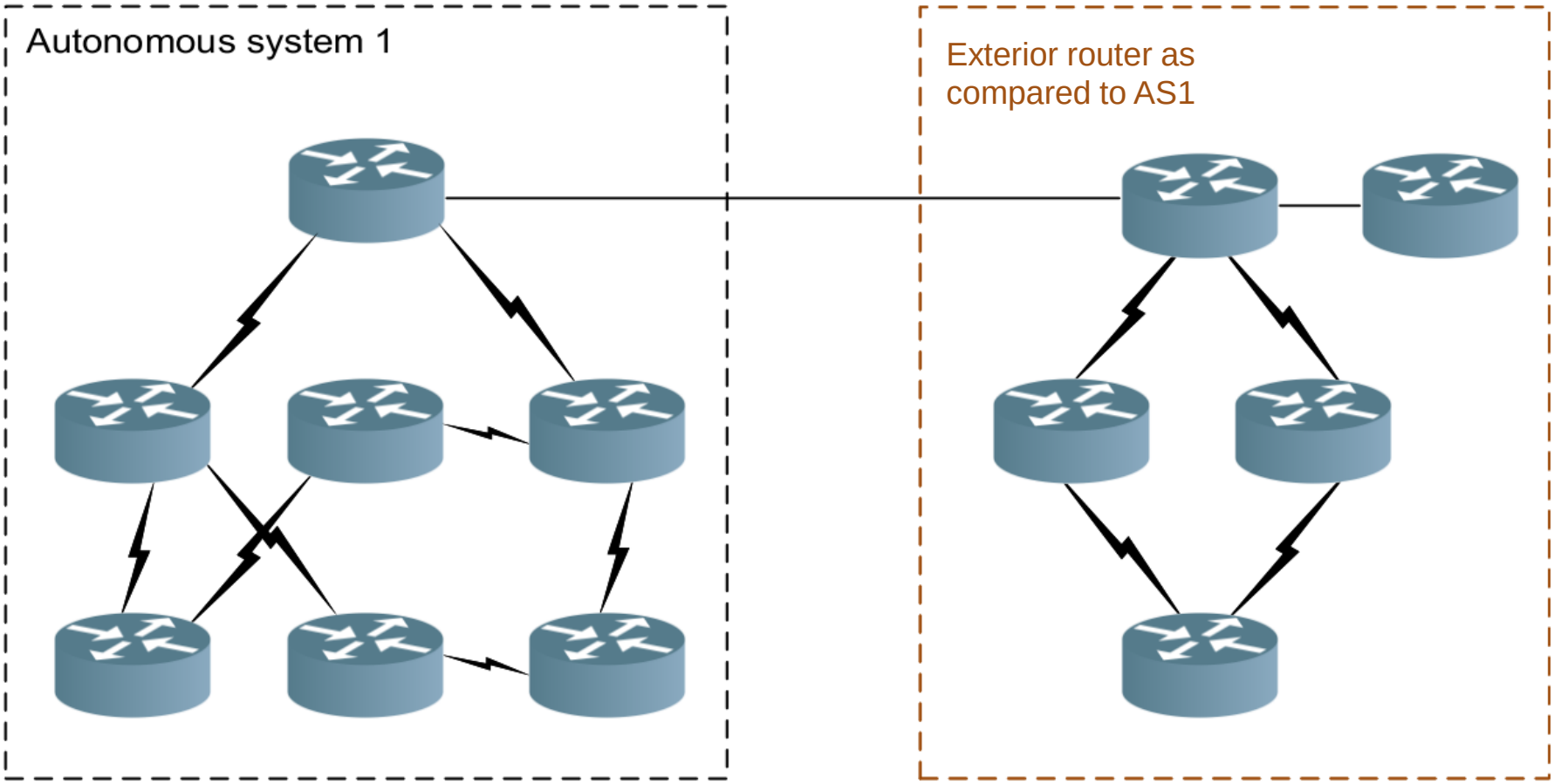
Interconnecting Autonomous Systems (III)

- Border router defintion.



Interconnecting Autonomous Systems (IV)

- Exterior router defintion.



Interior / Exterior gateway protocols

- Autonomous System internal routing: *Intradomain routing*
  - Distance Vector*:* RIP
  - Link state: OSPF
  - Hybrid: IGRP , EIGRP

- Routing between AS (Autonomous System): *Interdomain routing*
  - EGP
  - BGP

Exterior gateway protocols: EGP

- **EGP: Exterior Gateway Protocol:**
- It is the first protocol used to communicate between AS: it dates back in the 80's (RFC 827).
- Characterized by 3 main features:
  - **Neighbor acquisition:**
    - Verifies if there is a agreement to be neighbor.
  - **Neighbor reachability:**
    - Monitor neighbor connection.
  - **Network reachability:**
    - Exchange the information of the network.
- EGP is similar to a *distance vector* protocol:
  - The information sent to the neighbors are pretty much reachability information.
  - There are no rules to define distances.

Exterior gateway protocols: BGP

- **BGP: Border Gateway Protocol**
- BGP was developed to substitute EGP
  - At the moment is at the 4 version. (RFC 1771; RFC 4271)
  - BGP routers exchange informationusing TCP connection on port 179, these are called BGP session.
  - Communication are relabiable.
  - Error detection are delefate at the transport layer → BGP is easier
- There exists 2 types of BGP sessions:
  - External BGP sessions (**eBGP**), these connection are between BGP router belonging to **different AS**.
  - Internal BGP sessions (**iBGP**), these connection are between BGP router belonging to **same AS**.
- The exchanged information is relating to the reachability of IP network according to CIDR classess.

iBGP, eBGP: example