EISTI
Ecole Internationale des Sciences du Traitement de l'Information

Architecture réseau

Didier Rousseau et Bruno Péan

TP : Eric Daguet

Allied Telesis

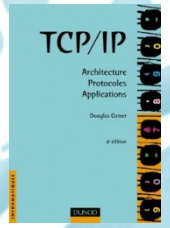
Planning

- 7 Février
- 21 Février
- 28 Février
- 21 Mars
- 28 Mars
- 4 Avril

Evaluation

- TP noté du 28 Février : 20%
- TP noté du 04 Avril : 20%
- Examen PAPIER : 60%
  - Choses autorisées sur la table ou a proximité:
    - documents personnels papier y compris brouillon,
    - Montres ou réveil
    - Crayons, gommes
  - Choses interdites sur la table ou a proximité:
    - Le reste (téléphone, ordinateur, tablette,…)

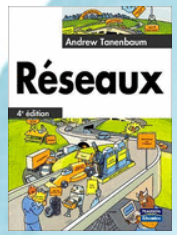
Bibliographie



- TCP/IP : Architecture, protocoles et applications

  Auteur : Douglas Comer

  Edition : Dunod



- Réseaux

  Auteur : Andrew S. Tanenbaum

  Edition : Pearson

- Support de cours orienté TCP/IP

  http://bp.perso.eisti.fr/doc/reseaux/

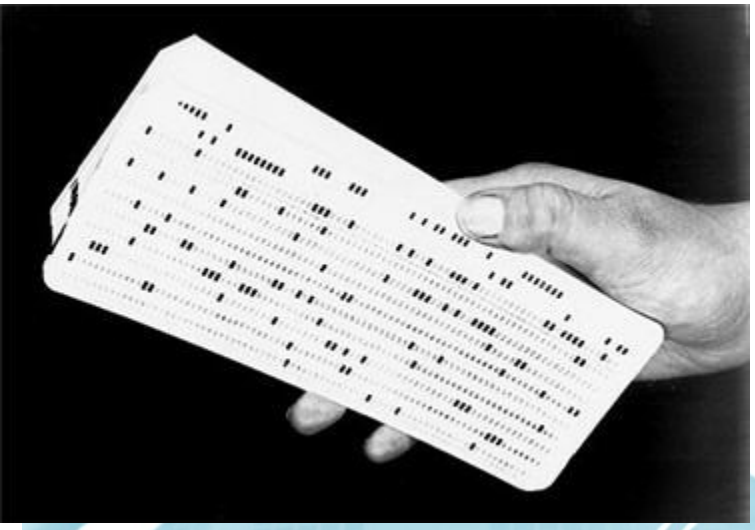
- Des explications par FrameIP (http://www.frameip.fr)

  http://www.frameip.com

Définition

- Un **réseau informatique** est un ensemble d'équipements reliés entre eux permettant d'échanger des informations numériques

- On appel **nœud** un élément physique du réseau soit terminal (exemple un PC) soit de transition (exemple commutateur, concentrateur ou Routeur)



Histoire

- La carte perforée
- inventées dès le 18e siècle pour répondre aux besoins industriels
- 1889 : Herman Hollerith (fondateur en 1896 de IBM) invente la première machine de traitement des données utilisant un métier à tisser Jacquard pour mécaniser la lecture des fiches de recensement
- 1928 IBM Lance la carte de 80 colonnes

Histoire

- La bande perforée
  - En 1844 le télégraphe Morse
    - Les codes reçus sont imprimés sous forme de points et lignes
  - En 1870, le télégraphe Wheatstone
    - utilise une bande de papier pré perforée afin d'atteindre la vitesse de transmission de 80 signes à la seconde
  - 1887 la monotype

Histoire

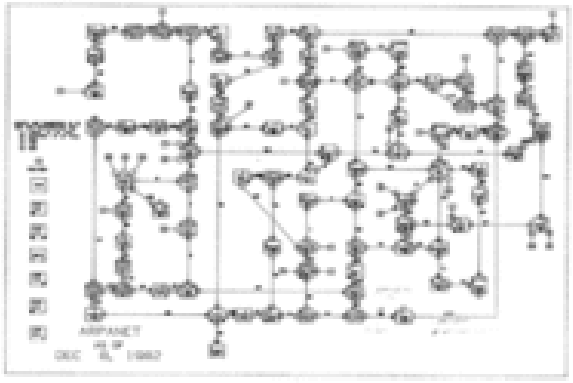
- Les bandes magnétiques
- Une invention peu spectaculaire – la colonne à dépression – allait donner naissance, dans les années cinquante, à une technologie entièrement nouvelle de stockage de l'information reposant sur des bandes magnétiques. Cette technologie a permis d'accélérer le traitement des données et de résoudre le problème des masses de cartes perforées qui encombraient les entreprises et les administrations.

Histoire

- **1955** : Premier réseau informatique à but commercial : **SABRE** (Semi Automated Business Related Environment) réalisé par **IBM**. Il relie 1200 téléscripteurs à travers les Etats-Unis pour la réservation des vols de la compagnie **American Airlines**.

Histoire

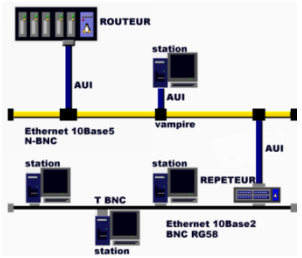
- 1960 La DARPA lance un projet visant à réaliser un réseau de transmission de données à grande distance entre différents centres de recherche sous contrat.



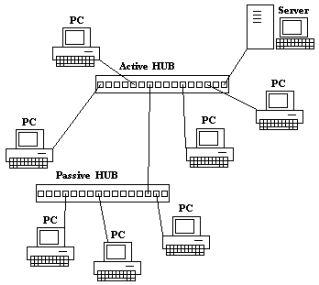
- 1969 l'ARPANET voie le jour. Le premier nœud de raccordement relie alors l'Université de Californie à Los Angeles (UCLA) et l'Institut de recherche de Stanford, suivis de peu par les universités de Californie à Santa Barbara et de l'Utah puis s'étend progressivement jusqu'à connecter une quarantaine de sites en 1972.

Histoire
Les topologies

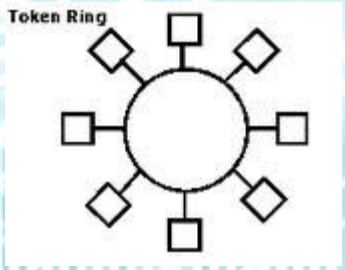
- 1970-1973 Premier Lan ETHERNET à 2.94 Mb/s par XEROX



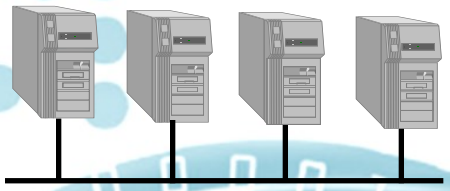
- 1976-1977 ArcNet par Datapoint à 2.5 Mb / s



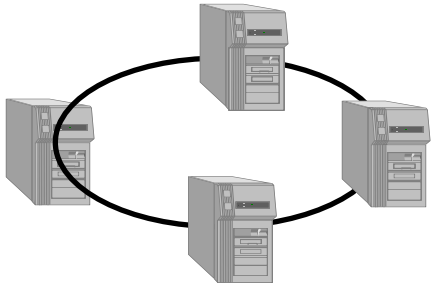
- 1984 Token Ring par IBM à 4 Mb/s



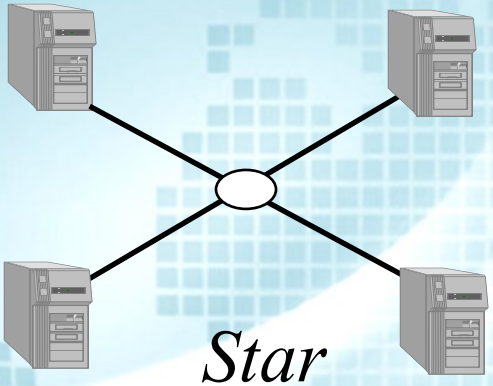
Topologies



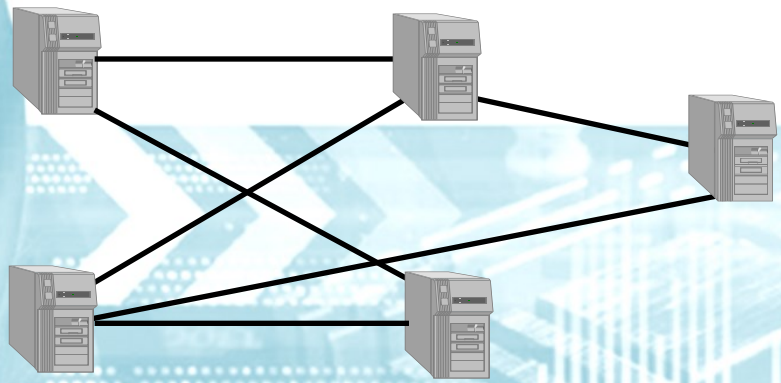
Bus



Ring

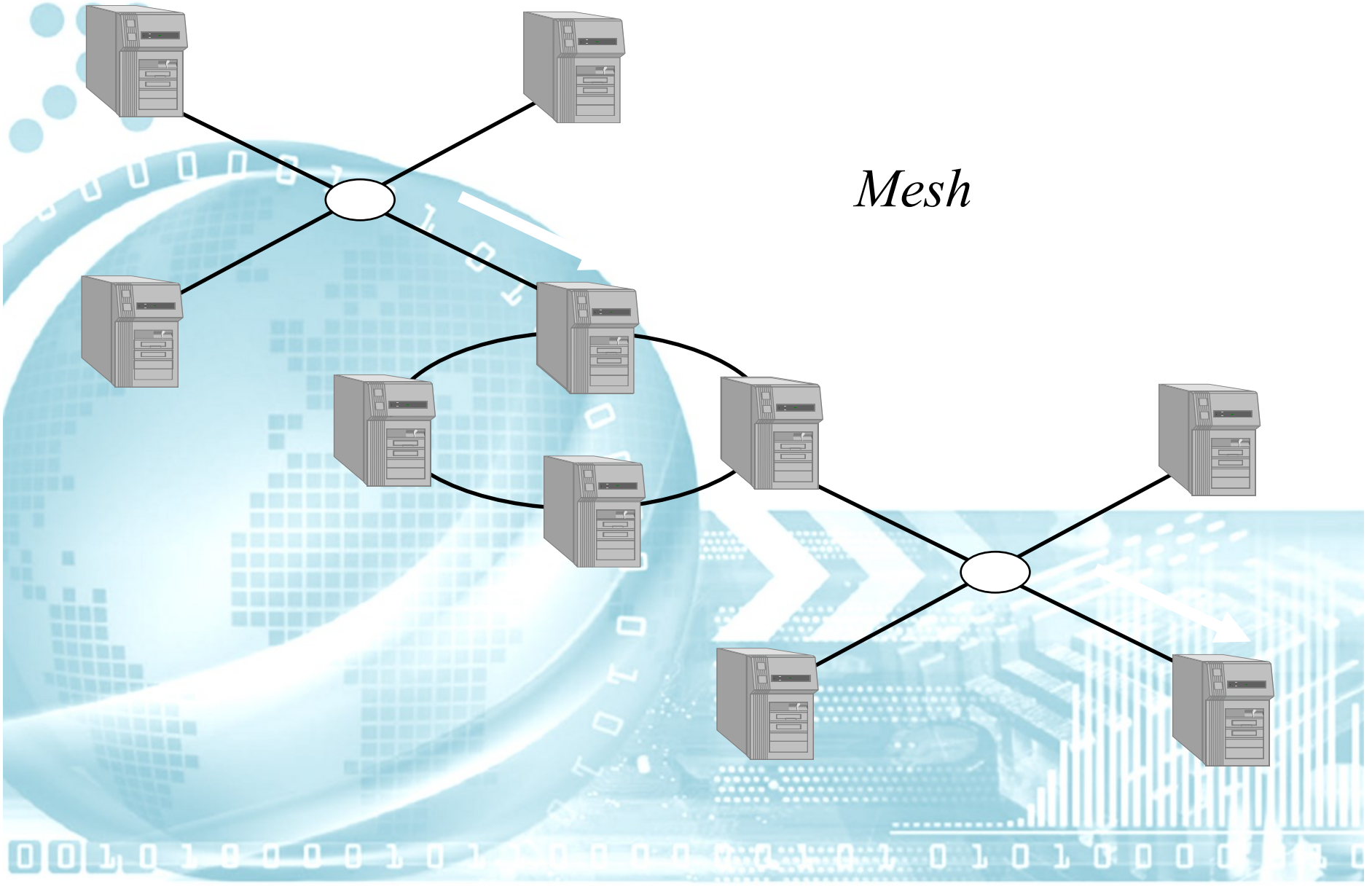


Star

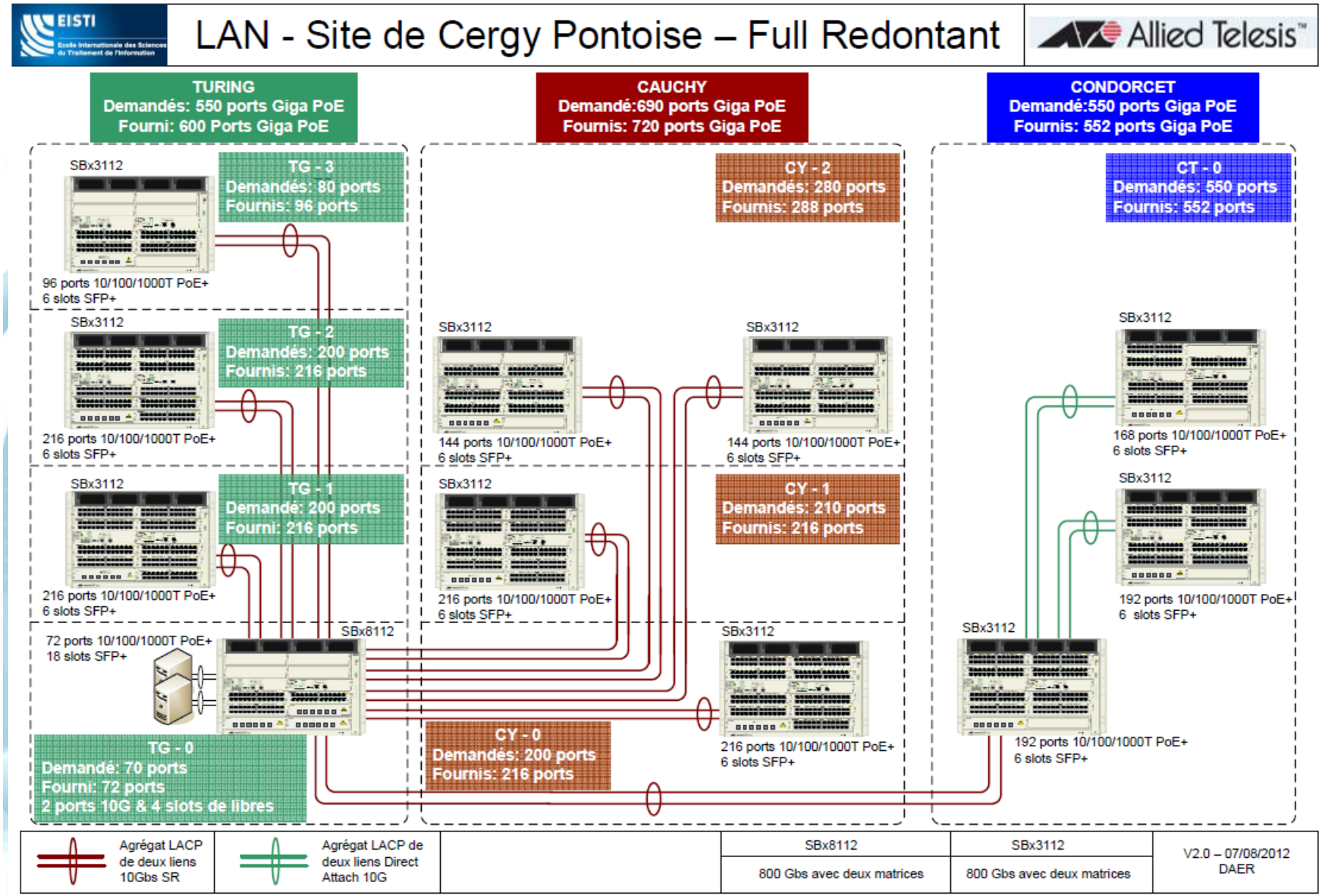


Mesh

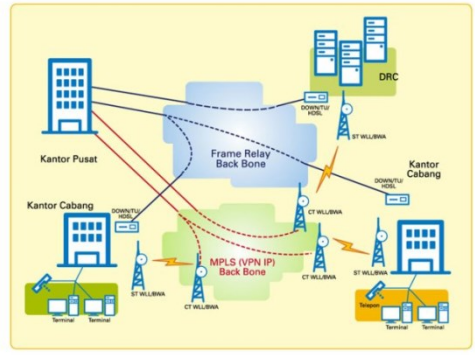
Topologie

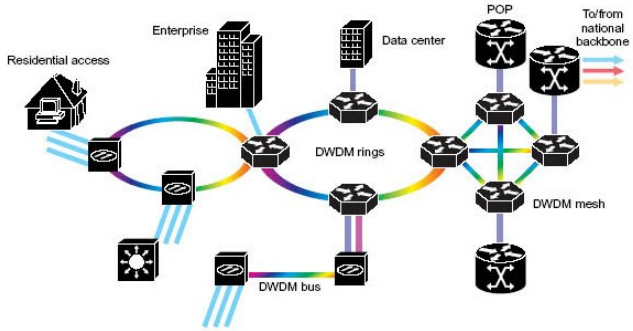


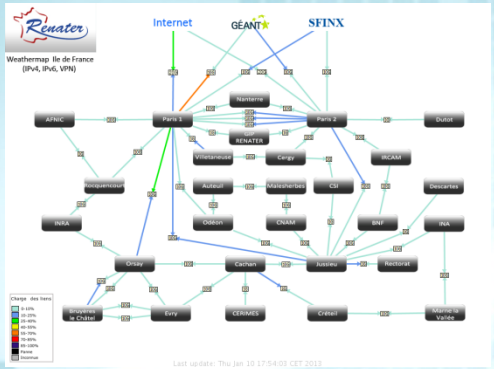
Différents réseaux :LAN

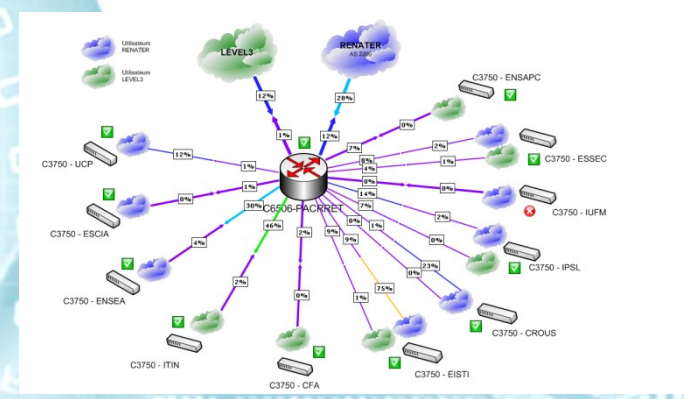


Différents réseaux :MAN

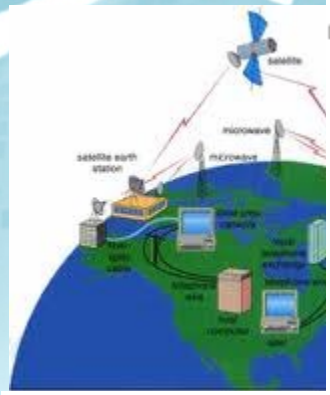


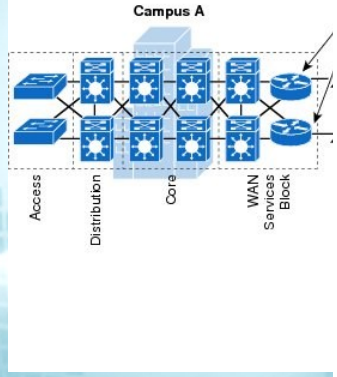


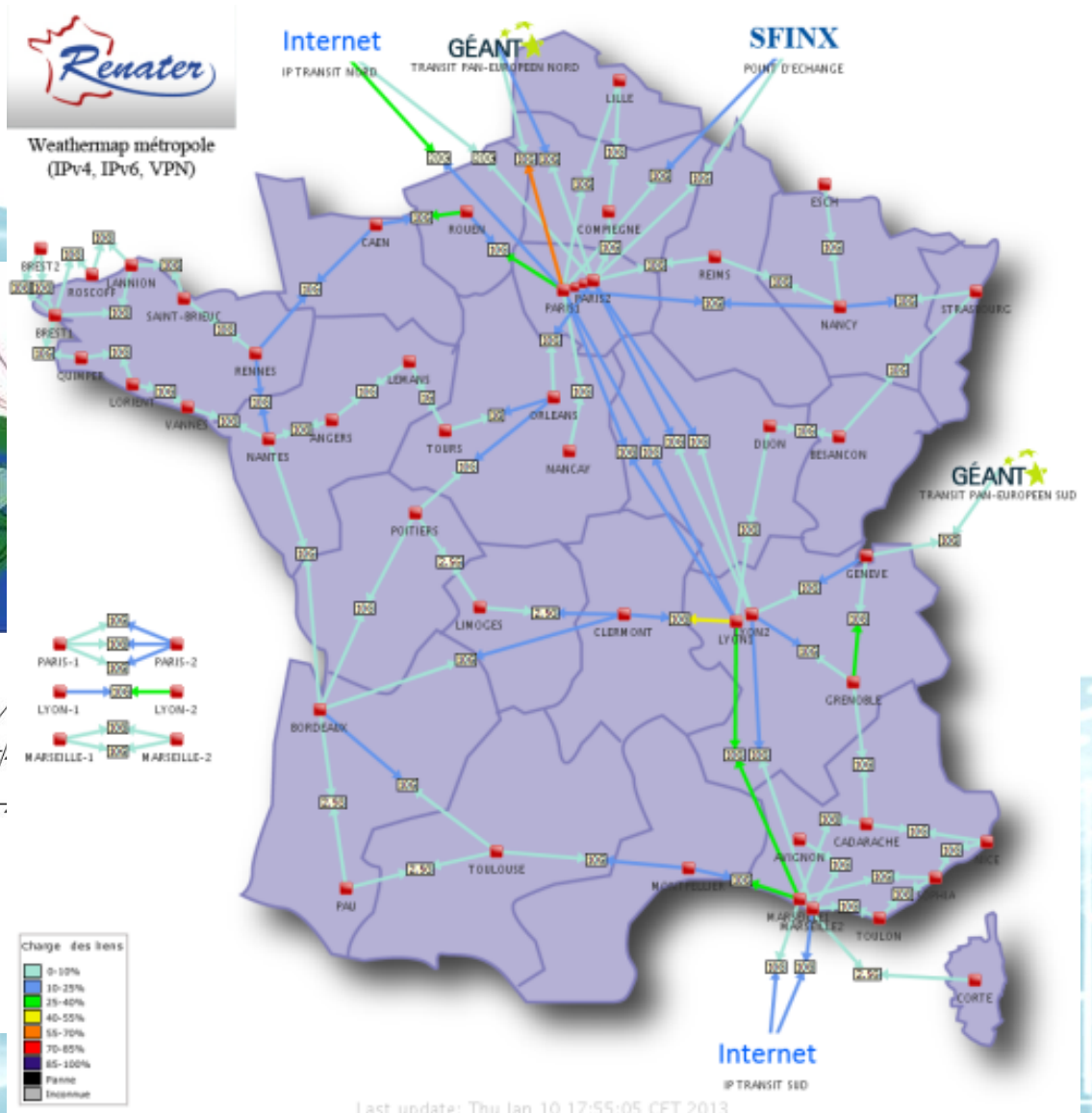




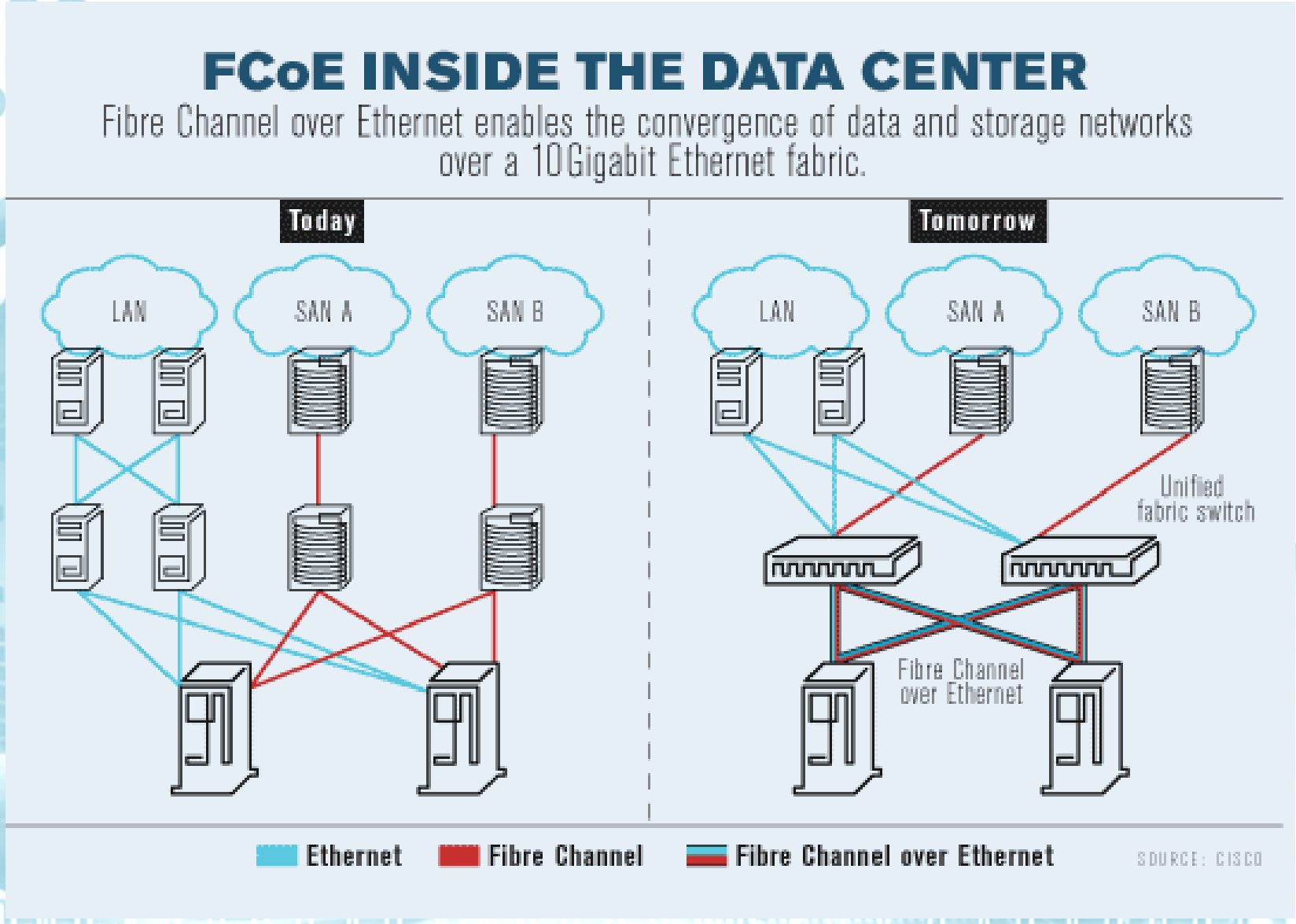
Différents réseaux :WAN







Différents réseaux :SAN



OSI ou ISO?

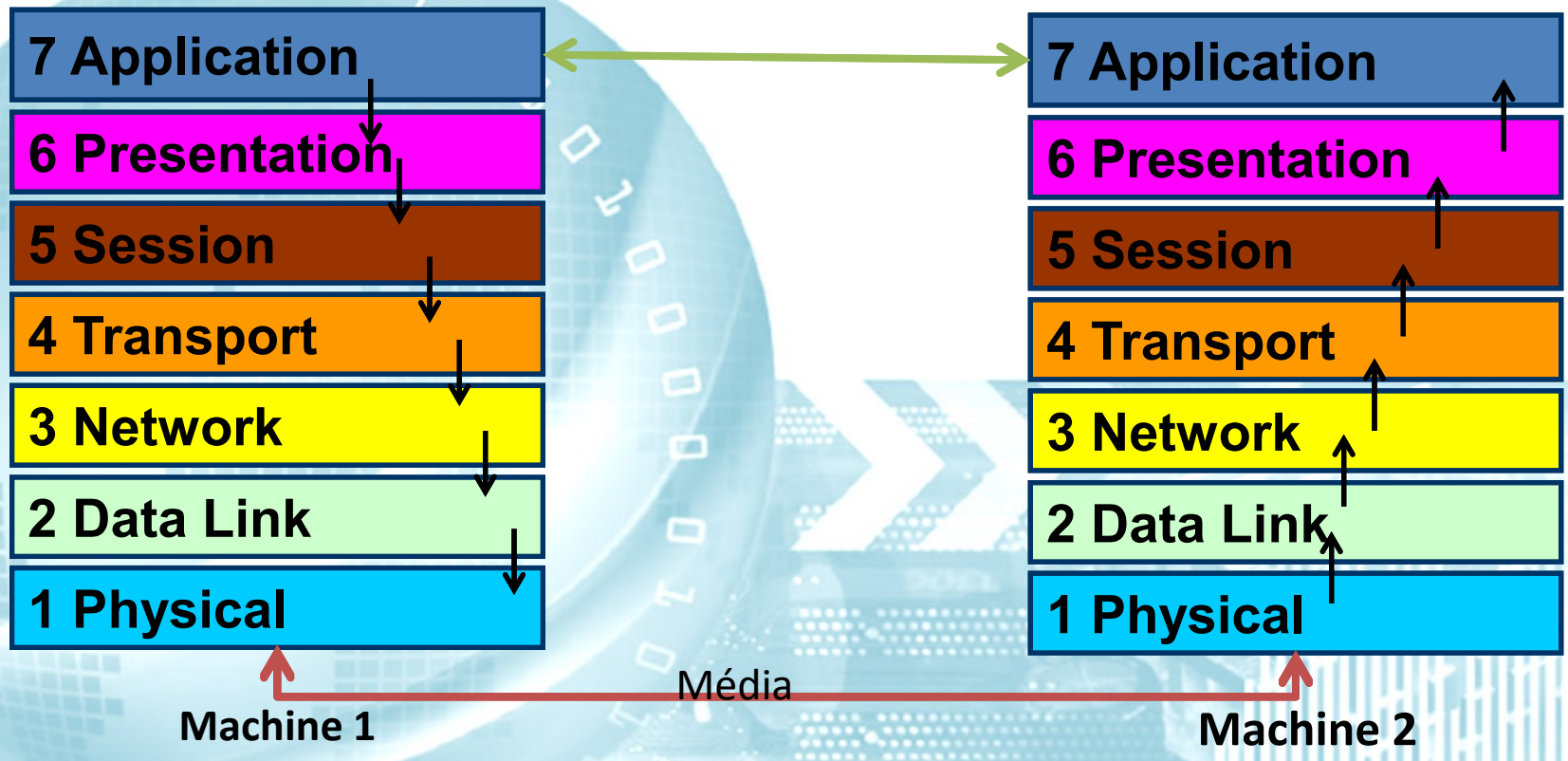
- L'ISO a défini un modèle qui permet de modéliser la communication entre 2 **applications** fonctionnant sur 2 machines connectées sur un même réseau ou sur des réseaux interconnectés.

- Ces machines peuvent être différentes, sur des réseaux disjoints, utilisant des technologies et de protocoles différents,…

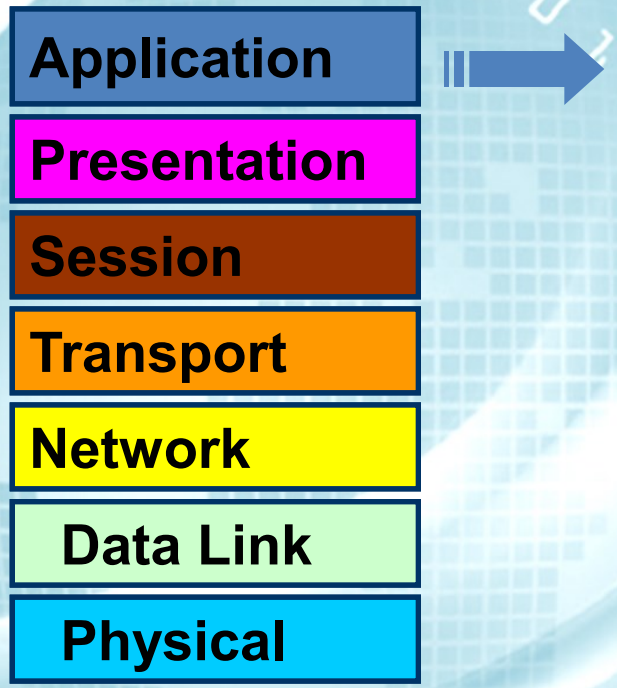
- Pour résoudre ces problèmes le modèle est découpé en 7 couches.

Les 7 couches

- Les 7 couches du modèle OSI de L'ISO

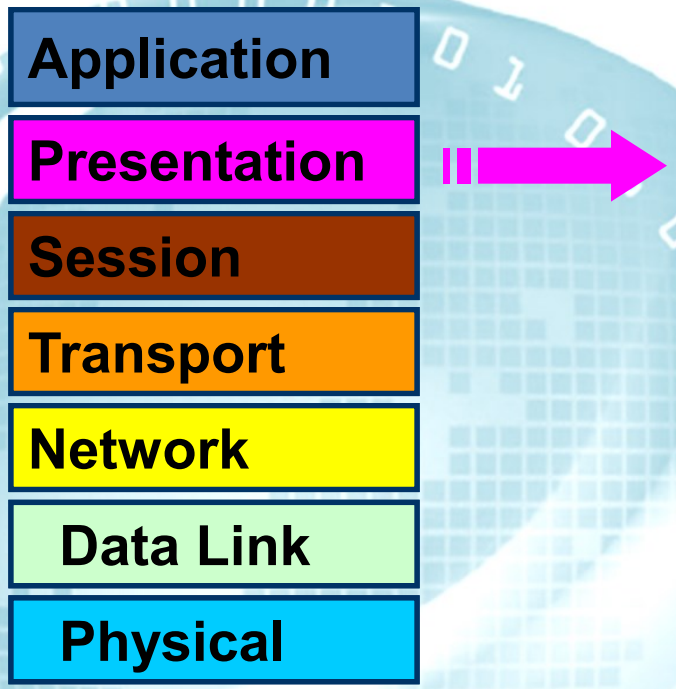


OSI : 7



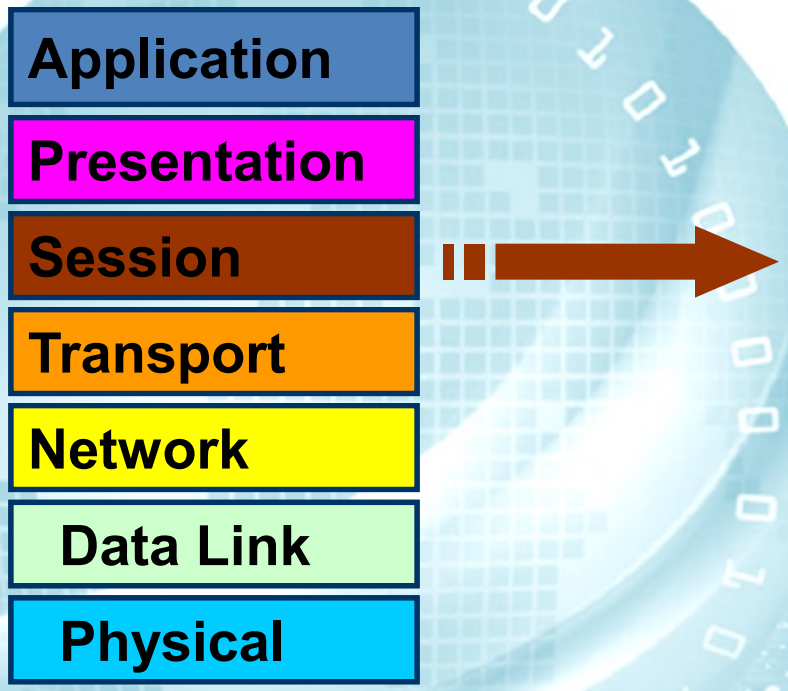
- It's the interface between applications on the system (software that belongs to the operating system or software necessary to use the network)
- Examples:
  - VT: Virtual Terminal, interactive link to a remote machine
  - FTAM: File Transfer and Access Management
  - X.400: Electronic mail
  - X.500: Directory Service

OSI : 6



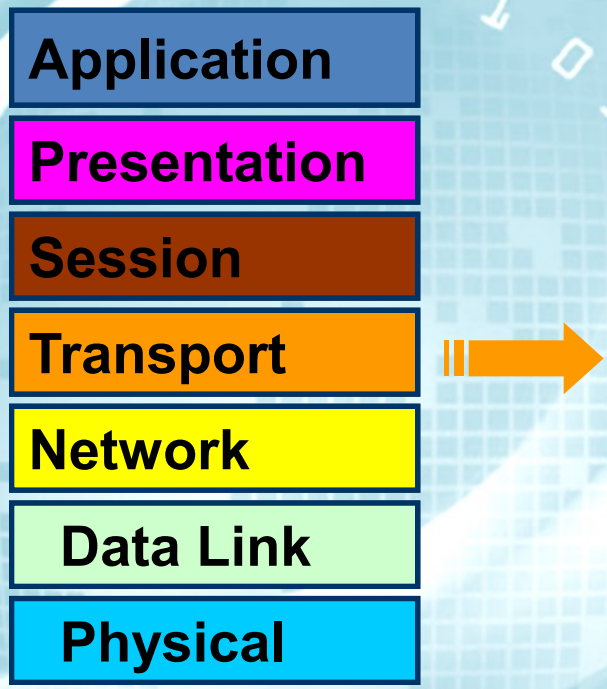
- Defines data conversion
- It manages the syntax of information to be transferred
- It ensures that data is presented to applications in an understandable format, since information is represented in different ways on different machines - ASCII or EBCDIC

OSI : 5



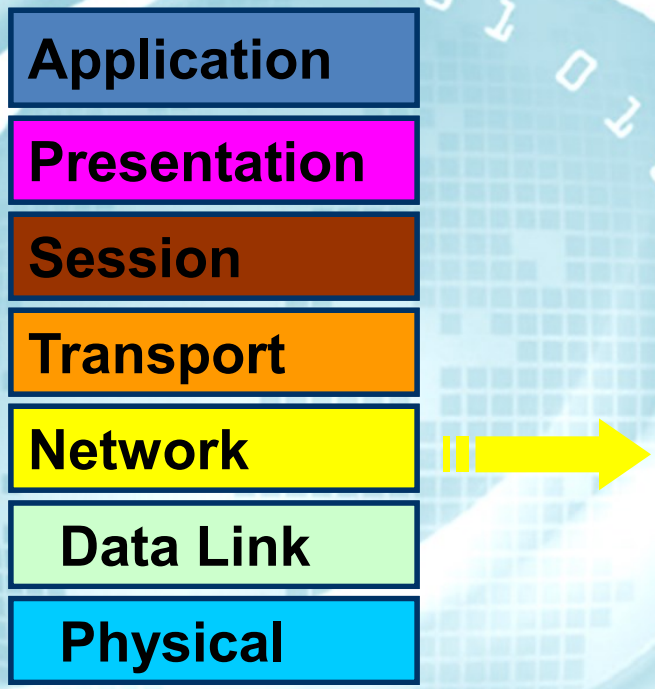
- It is responsible for establishing the dialogue and synchronising systems and data exchange

OSI : 4



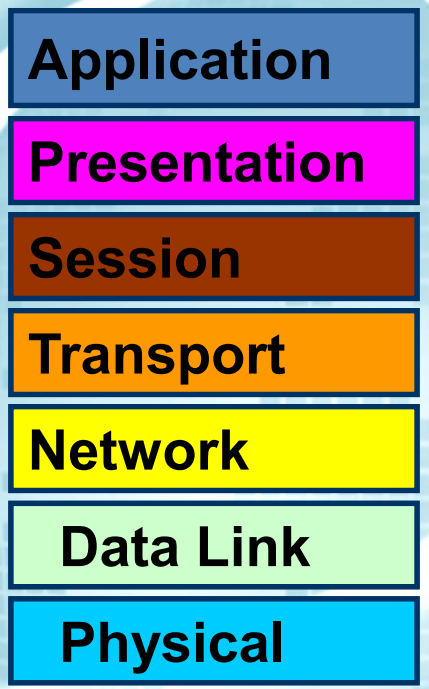
- Provides services to transfer data end-to-end
- Layer 4 can
  - fragment frames to adapt them to Layer 3 dimensions
  - find/correct errors
  - check data flow and congestion
- It is responsible for the reliability of data transmitted over the network

OSI : 3



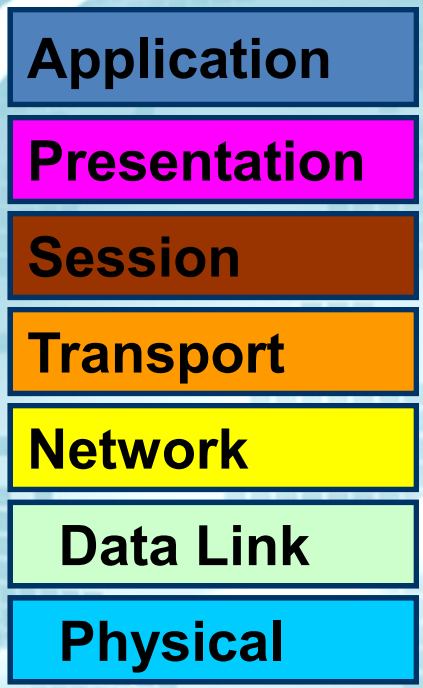
- Manages packet routing:
  - decides through which ISs a packet has to run in order to reach its destination
- Layer 3 uses routing tables to optimise network traffic
  - IS: Intermediate System

OSI : 2



- To transmit frames in a secure way
- It accepts frames as input and transmits their octets in sequence (serial transmission)
- It verifies the presence of errors and adds Frame Check Sequence (FCS)
- It can manage error correction procedures implementing retransmission
- It manages addressing

OSI : 1

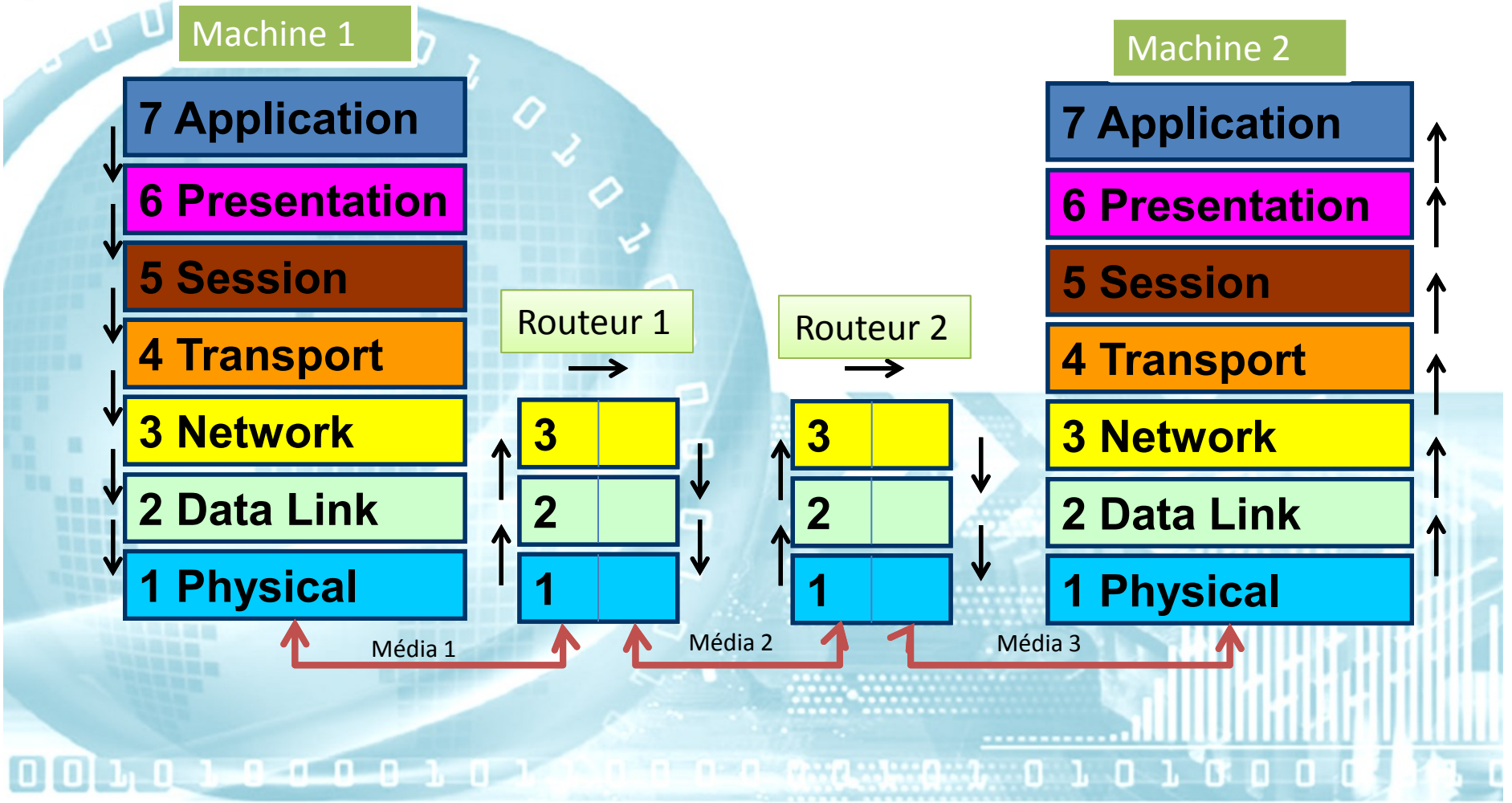


- Transmits binary sequences onto the channel
- This layer specifies
  - mechanical interfaces
  - voltages relative to 0 and 1
  - cable type, dimension, electrical characteristics and properties
  - type of connectors

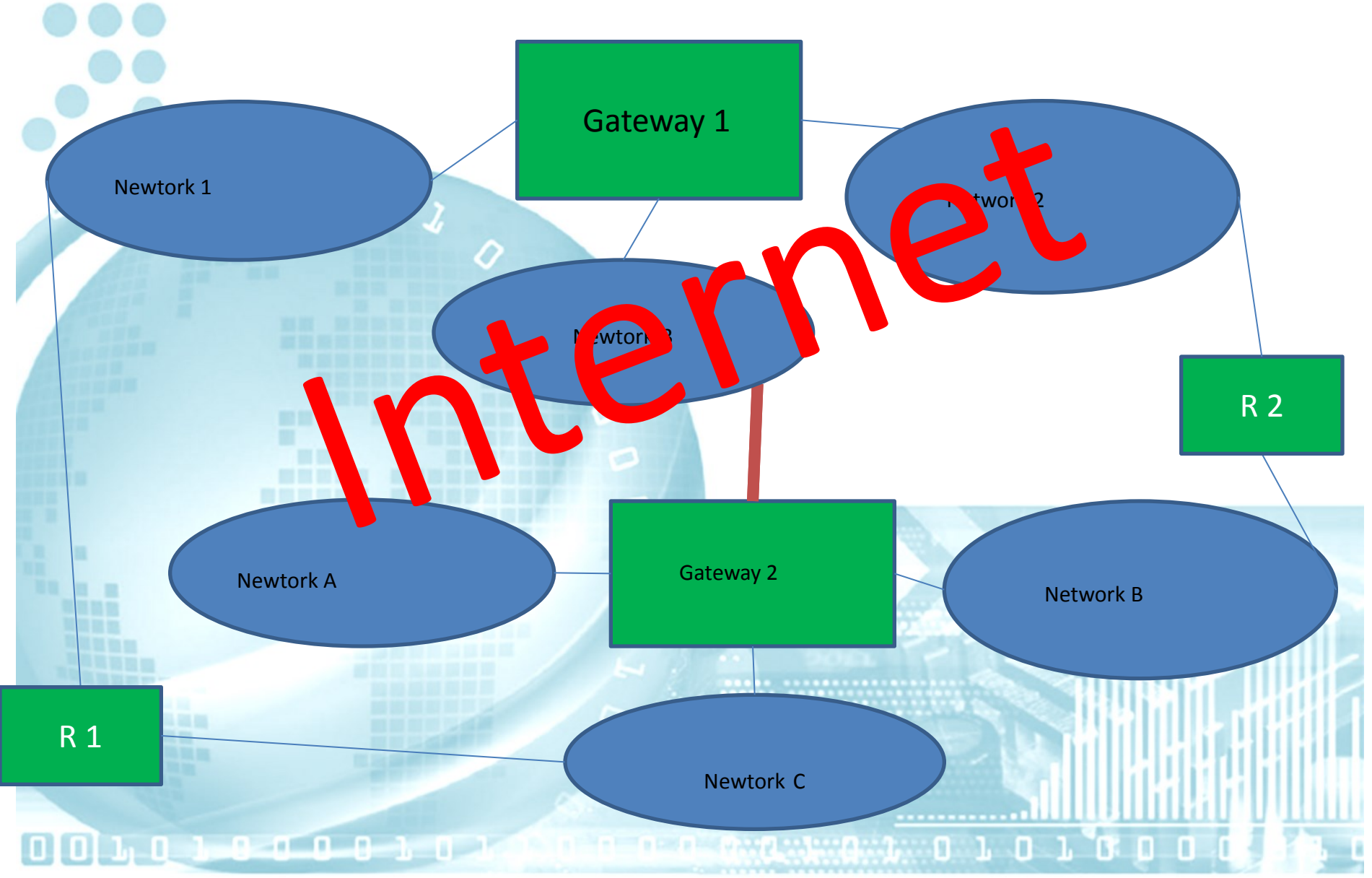
OSI : résumé


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

ISO sur réseaux disjoints



Un réseau maillé particulier



Couche physique

- L'électricité
- La lumière
- Les ondes
  - Les pigeons voyageurs
  - La fumée
  - Le Tam-Tam
  - Le pneumatique
  - Les sémaphores

Couche Liaison

- **L'adresse physique (ou adresse MAC)**
  - L'adresse *Ethernet ou token-ring d'un ordinateur (ou adresse MAC pour Media Access Control) est celle attribuée (par construction normalement unique)* à l'interface réseau. C'est aussi ce qu'on appelle l'adresse physique de l'interface réseau, et est représentée par un nombre hexadécimal de la forme 00:01:02:ab:cd:34. les 6 premiers caractères étant la OUI (Organizationally Unique Identifier) déterminant le constructeur :

    exemple de 00:00:00 à 00:00:09 c'est XEROX

    http://www.wireshark.org/tools/oui-lookup.html

Couche Liaison

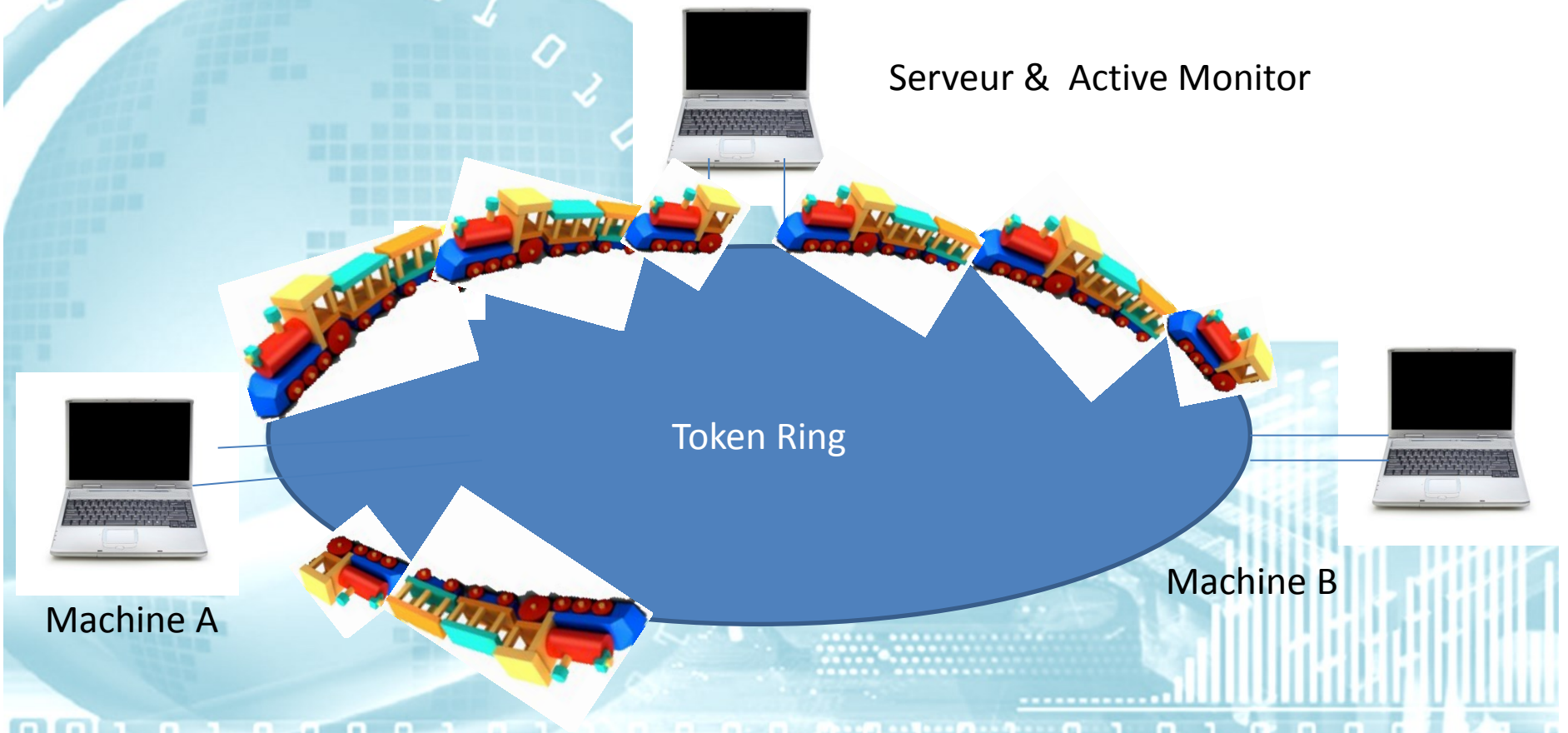
- Token Ring (*norme* IEEE *802.5)*
  - La méthode de communication pour le token Ring est le Simplex (les données ne circulent que dans un sens)
  - Les données sont transmis a la suite d'un Jeton qui circule dans toutes les cartes du réseau. Le signal est lut et régénéré par toutes les cartes ce qui donne une très grande fiabilité à c type de resau
  - 2 Vitesses initialement 4 Mb/s (première version) et 16 Mb/s seconde versions avec libération anticipée du jeton

Couche Liaison

- Token Ring 4 Mb /s

Couche Liaison

- Token Ring 16 Mb /s



Couche Liaison

- Token Ring le format de la trame

Le format d'un Jeton

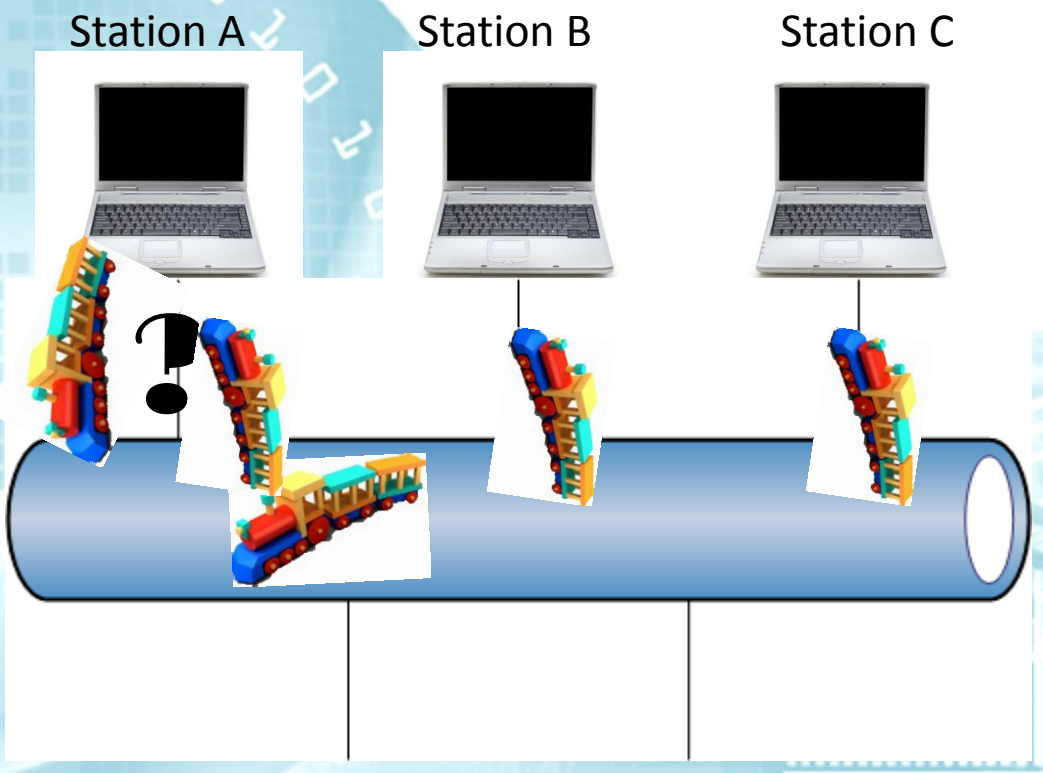
SD : Starting Delimiter (1 octet)
AC : Access Control (1 octet)
FC : Frame Control (1 octet)
DA : Destination Address (2 ou 6 octets)
SA : Source Address (2 ou 6 octets)
Datas : Information (0 à 4027 ou 18 000 octets)
FCS : Frame Check Sequence (4 octets)
ED : Ending Delimiter (1 octet)
FS : Frame Status (1 octet)

Couche Liaison

- Ethernet (*norme* IEEE *802.3)*
  - La méthode générale est le duplex (Half ou full)
  - La méthode CSMA/CD (filaire)
    - CS : C*arrier Sense (détection de porteuse)*
    - *MA : Multiple Access (Accès multiples)*
    - *CD : Collision Detection (détection de collision)*
  - La méthode CSMA/CA (WiFi) (*norme IEEE 802.11)*
    - CS : C*arrier Sense (détection de porteuse)*
    - *MA : Multiple Access (Accès multiples)*
    - *CA : Collision Avoidance (*esquive de collision)
    - *http://www.youtube.com/watch?v=RKkxKG5usaw*

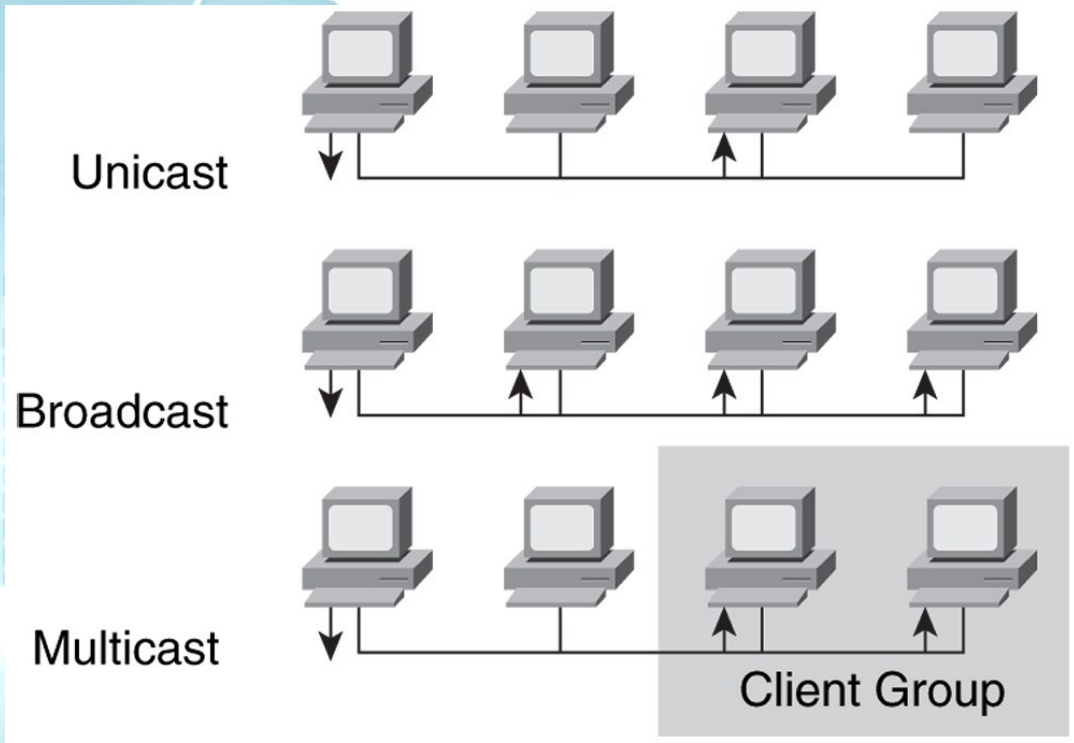
Couche Liaison

- Ethernet (*norme* IEEE *802.3)*



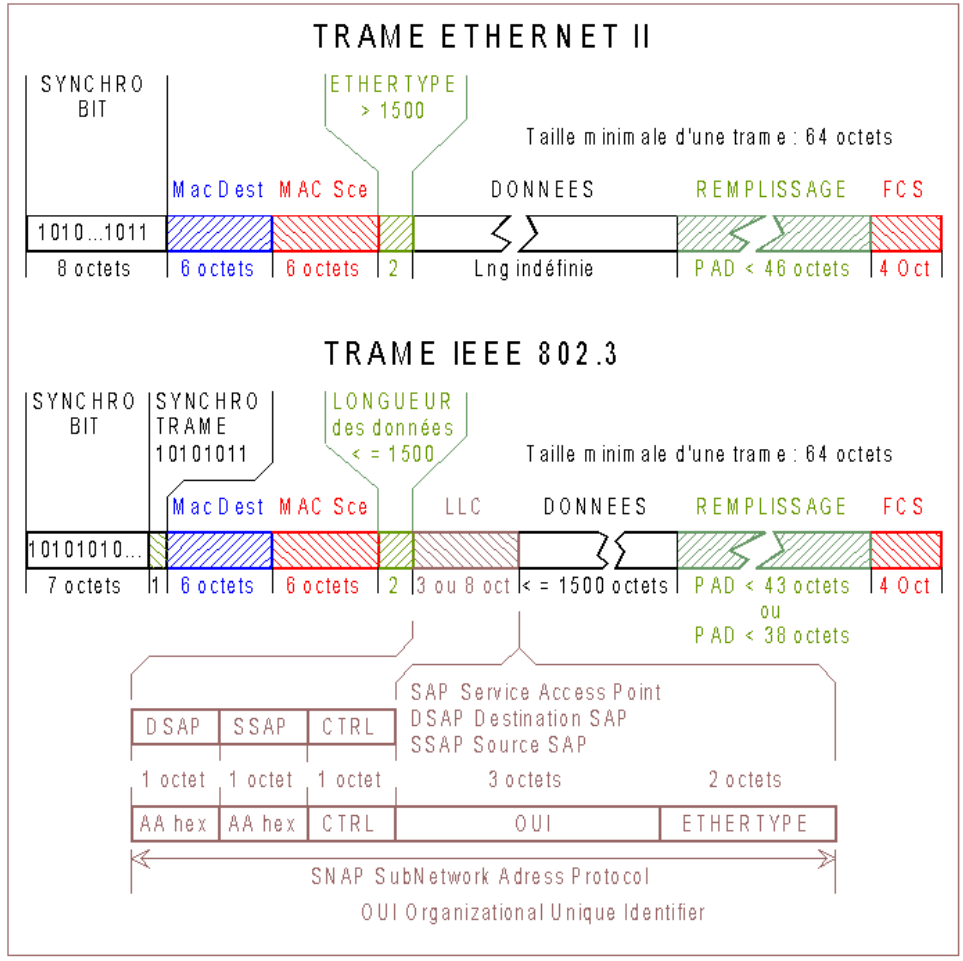
Couche Liaison

La communication dans un réseau Ethernet peu se faire suivant 3 métodes

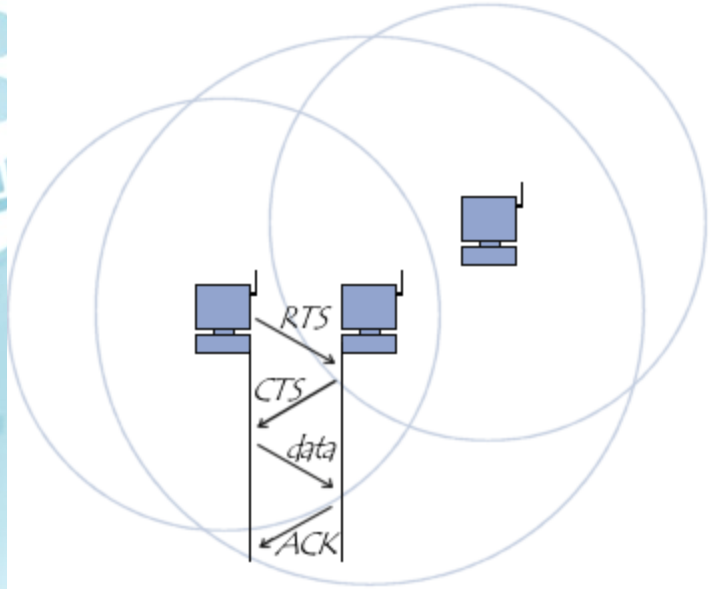


Couche Liaison

- Ethernet

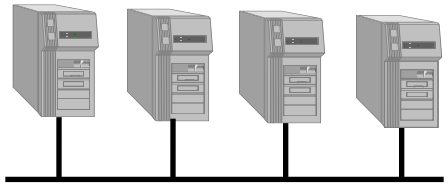


Couche liaison wireless



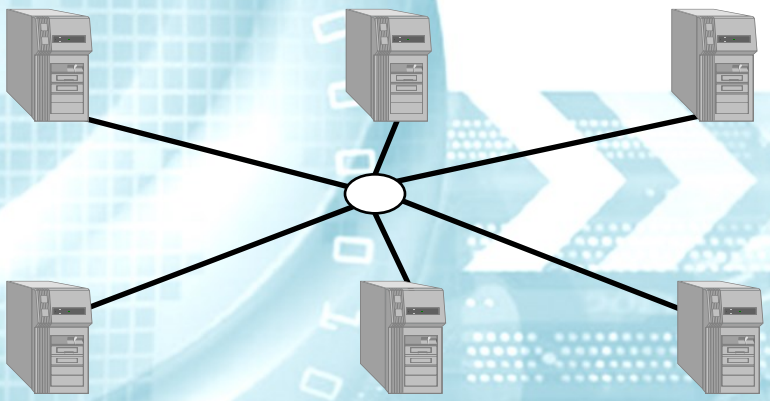
Ethernet : Bus ou étoile?

- Bus :



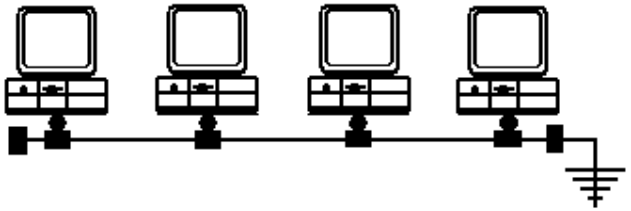
Bus

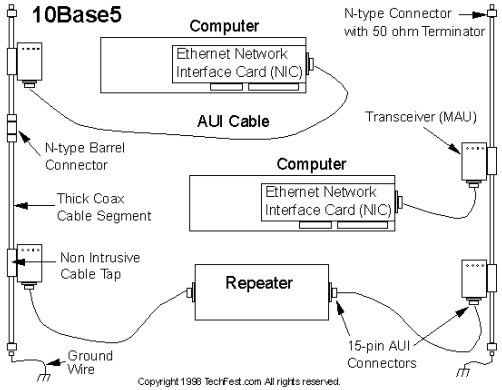
- Etoile



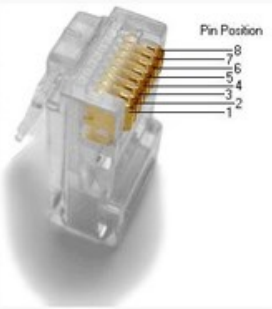
Les 2 mon capitaines …

- Bus
  - 10B5
  - 10B2
- Etoile
  - 10Tx
  - 100Tx
  - 1000Tx
  - ABFx, …





Pin	Connection 1: T568A			Connection 2: T568B			Pins on plug face
	signal	pair	color	signal	pair	color	
1	BI_DA+	3	white/green stripe	BI_DB+	2	white/orange stripe	
2	BI_DA-	3	green solid	BI_DB-	2	orange solid	
3	BI_DB+	2	white/orange stripe	BI_DA+	3	white/green stripe	
4		1	blue solid		1	blue solid	
5		1	white/blue stripe		1	white/blue stripe	
6	BI_DB-	2	orange solid	BI_DA-	3	green solid	
7		4	white/brown stripe		4	white/brown stripe	
8		4	brown solid		4	brown solid	

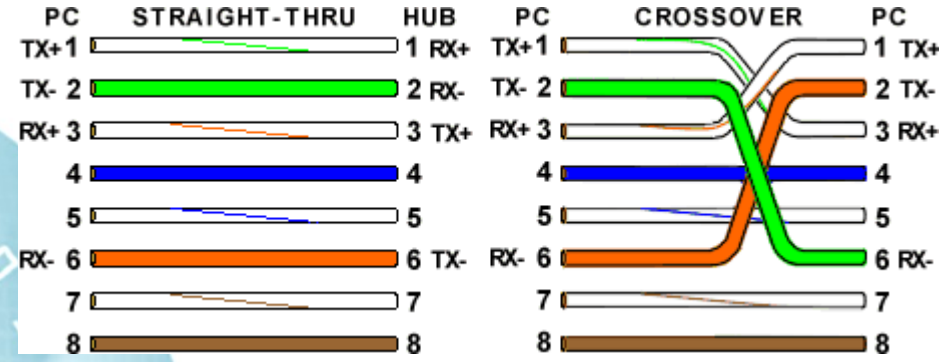


Les câbles 4 paires

10 et 100 TX

(1-2) emission

(3-6) réception



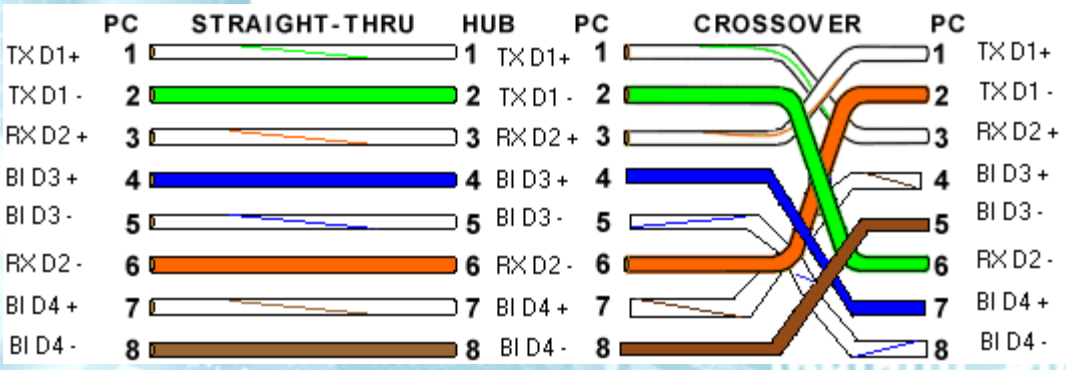
1000TX

(1-2) emission

(3-6) réception

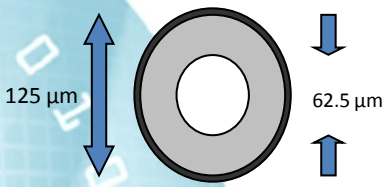
(4-5)

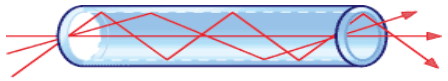
(7-8)



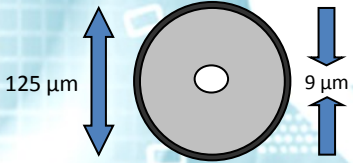
La fibre

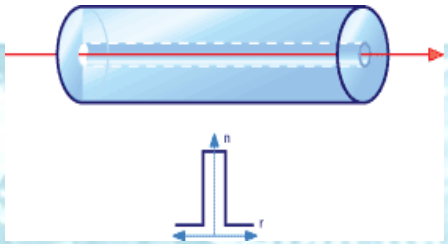
- Multimode
  - « gros diamètre » plusieurs dizaines de micromètres
  - Les rayons lumineux peuvent suivre des trajets différents suivant l'angle de réfraction.





- Multimode
  - Cœur très fin
  - les rayons suivent un seul chemin.
  - Très longue distance jusqu'à 80 Km





- http://fr.wikipedia.org/wiki/Fibre_optique

Les connecteurs fibres

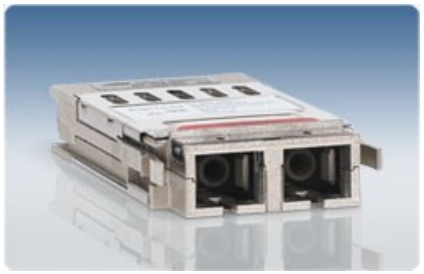
- FC

- SC

- ST

- LC

Gbic



SFP ou SFP+

Fibres et vitesse

	OS1	OM1	OM2	OM3	OM4
Multimode ou monomode	monomode	multimode	multimode	multimode	multimode
Diamètre de la fibre	9/125µ	62,5/125µ	50/125µ	50/125µ	50/125µ
Domaines d'application principal	Déport très longue distance (vidéosurveillance et réseau)	Déport longue distance, vidéosurveillance (inférieur à 4 km) et réseau	Déport longue distance, vidéosurveillance (inférieur à 4 km) et réseau	Déport moyenne distance, réseau gigabit et datacenter	Datacenter, liaison inter-bâtiments (EISTI)
Vitesses	10/100Mb/s 1/10Gb/s	100 Mb/s	100Mb/s et 1Gb/s	10Gb/s	10Gb/s
Bande passante Longueur d'onde	- -	200 MHz.km 850nm	500 MHz.km -	1500MHz.km 850nm	3500MHz.km 850nm

Half ou Full duplex

- Half duplex
  - Seul une communication dans un seul sens est supportée à un instant donné : A émet vers B.
- Full duplex
  - Une communication bidirectionnelle est supportée à tout instant : A émet vers B et B peut émettre vers A.

Négociation entre nœuds

- The priority level (highest to lowest) for Auto-Negotiation are:
  - 1000BASETX Full Duplex
  - 100BASET2 Full Duplex
  - 100BASET2 Half Duplex
  - 100BASETX Full Duplex
  - 100BASET4 Half duplex
  - 100BASETX Half Duplex
  - 10BASET Full Duplex
  - 10BASET Half Duplex

Ethernet Half ou Full duplex ?

- Bus :
  - half !!! (CSMA/CD)
- Wireless
  - Half (CSMA/CA)
- zzzTx ou zzzFX ?
  - les 2 mon capitaines!

Duplex paires torsadées et fibres

- Hub (concentrateur) couche 1 OSI
  - Répète sur tous les ports ce qui arrive sur un.

    => se comporte comme un bus -> CSMA/CD

Seul Half Duplex

Duplex paires torsadées et fibres

- Switch (commutateur)
  - Etablit un canal virtuel entre 2 ports.
  - Possibilité de créer plusieurs canaux simultanés
  - Canal dédié entre 2 nœuds donc bidirectionnel
  - Vitesse de commutation max = vitesse cable * nombre de port.

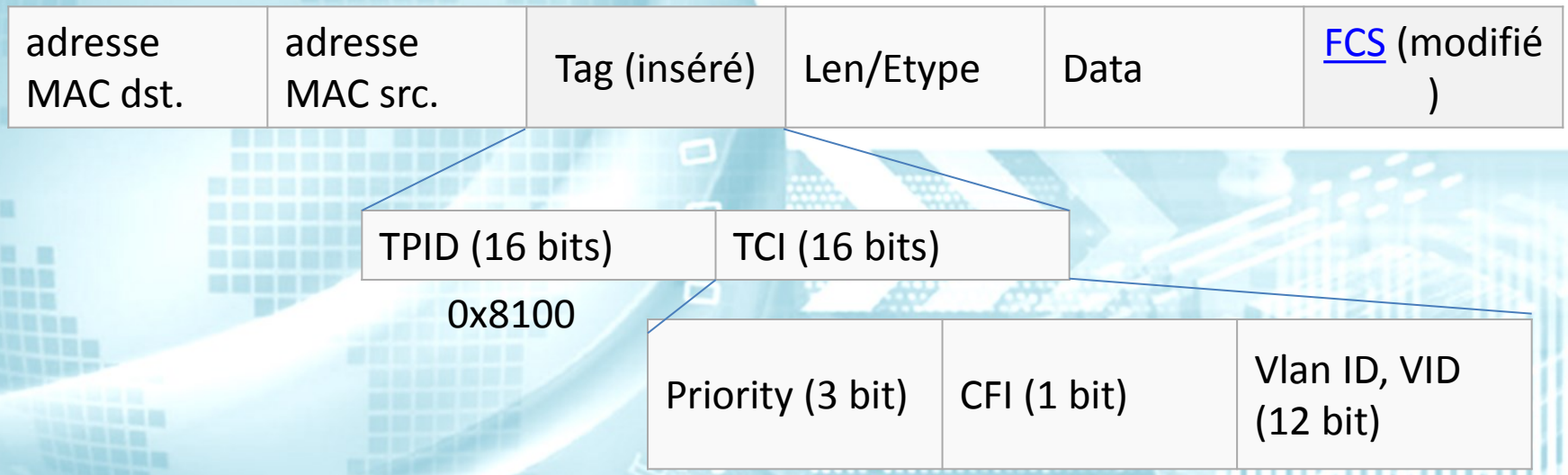
FULL Duplex possible

Switch Fonctionnement

- Table de VLANs (IEEE 802.1Q)
  - On renseigne éventuellement une table des vlans:

  ->On donne la liste des ports qui appartiennent à un vlan.

  -On indique si les trames doivent être tagguées ou inversement dé taguées.



Switch Fonctionnement

- Table des MAC
  - Le switch tient à jour une table lui indiquant quelle MAC est sur quel port pour établir les canaux virtuels
  - Cette tables est mise à jour à chaque fois qu'une trame est envoyée
  - L'information est retenue un certain temps
  - Quand il ne connait pas le port de destination, fonctionnement en hub

Switch décision d'ouverture d'un canal

- Le port recevant la trame contenant l'adresse source et le port devant émettre vers l'adresse de destination sont dans le même vlan ?
  - OUI ->OK établissement du canal entre les 2 ports
  - NON -> drop de la trame.
- Un switch décode une trame avant de la traiter. -> Induit de la latence
- Un switch vérifie la validité de la trame

Un câble entre 2 ports ?

- Sur un hub
  - Réseau aux fraises
- Sur un switch
  - Réseau à genoux
  - Sauf si mise en place d'un protocole spécifique ou Uplink.

Spanning Tree RSTP

Propriétaires Loop Protection

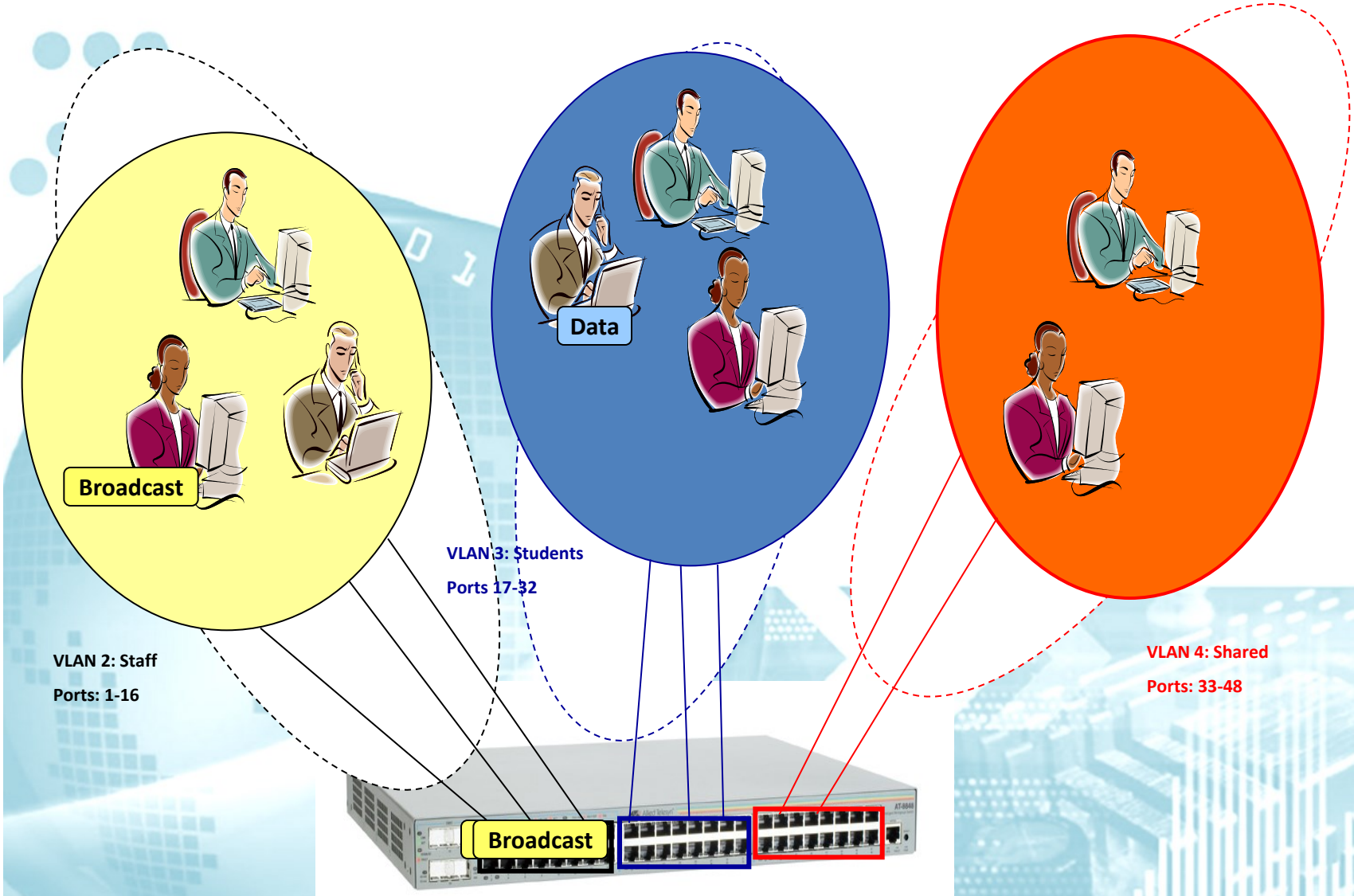
Auto-Negotiation Priorities

- The priority level (highest to lowest) for Auto-Negotiation are:
  - 1000BASETX Full Duplex
  - 100BASET2 Full Duplex
  - 100BASET2 Half Duplex
  - 100BASETX Full Duplex
  - 100BASET4 Half duplex
  - 100BASETX Half Duplex
  - 10BASET Full Duplex
  - 10BASET Half Duplex

Vlan

- Virtual Local Area Networks (VLANs) are a logical grouping of network users and resources connected to defined ports on the switch.
- VLAN features allow the network to be segmented by software management, improving network performance and security
- A Virtual LAN is a software-defined broadcast domain

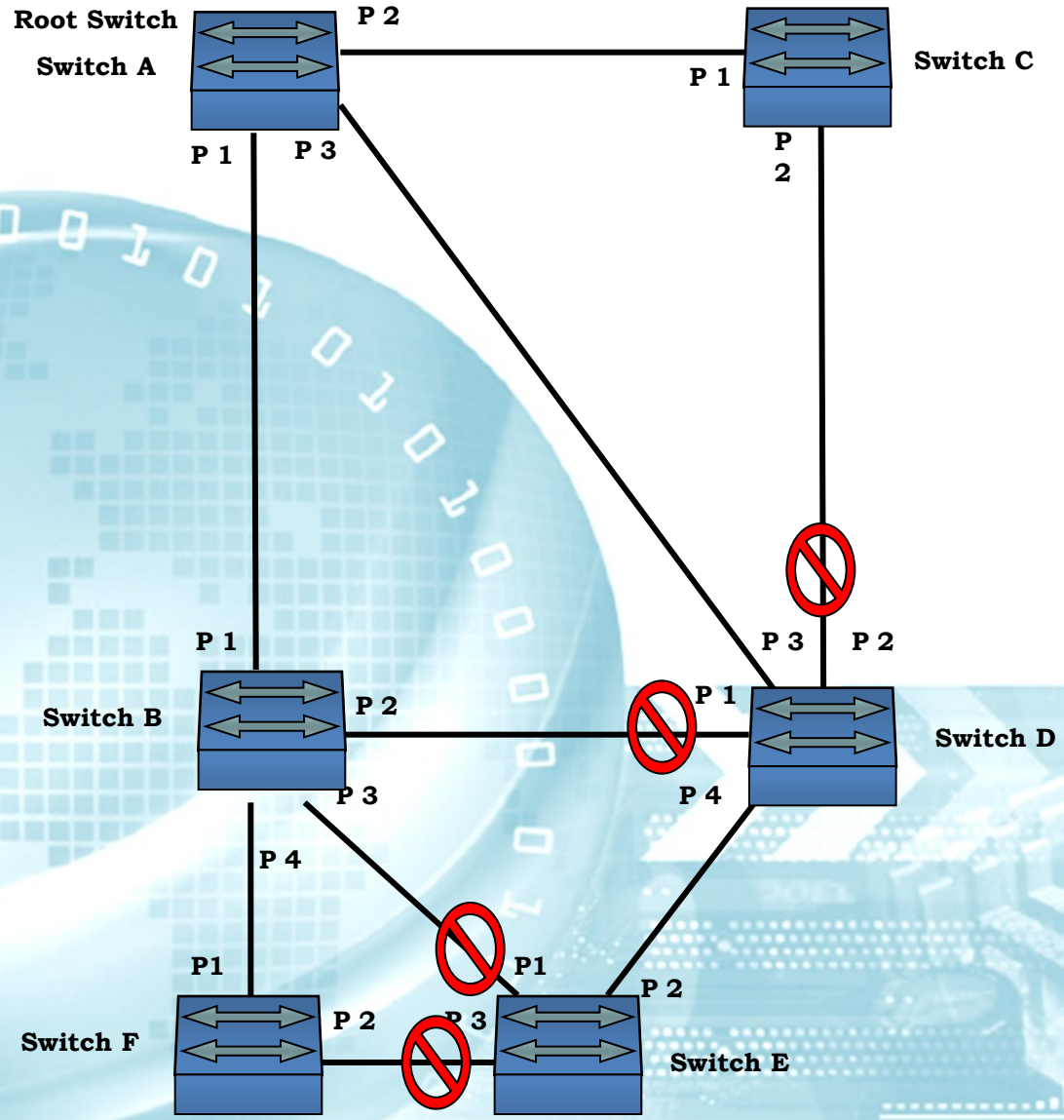
Vlan


Broadcast
Data
VLAN 3: Students
Ports 17-32
VLAN 2: Staff
Ports: 1-16
VLAN 4: Shared
Ports: 33-48
Broadcast

Vlan advantages

- Further improve LAN performance, as broadcast traffic is limited to LAN segments serving members of the VLAN to which the sender belongs
- Provide security, frames are only forwarded to those stations belonging to the sender's VLAN, and not to stations in other VLANs on the same physical LAN.
- Reduce the cost of moving or adding stations to function or security based LANs, as this generally requires only a change in the VLAN configuration

Spanning Tree Protocol



EISTI
Ecole Internationale des Sciences du Traitement de l'Information

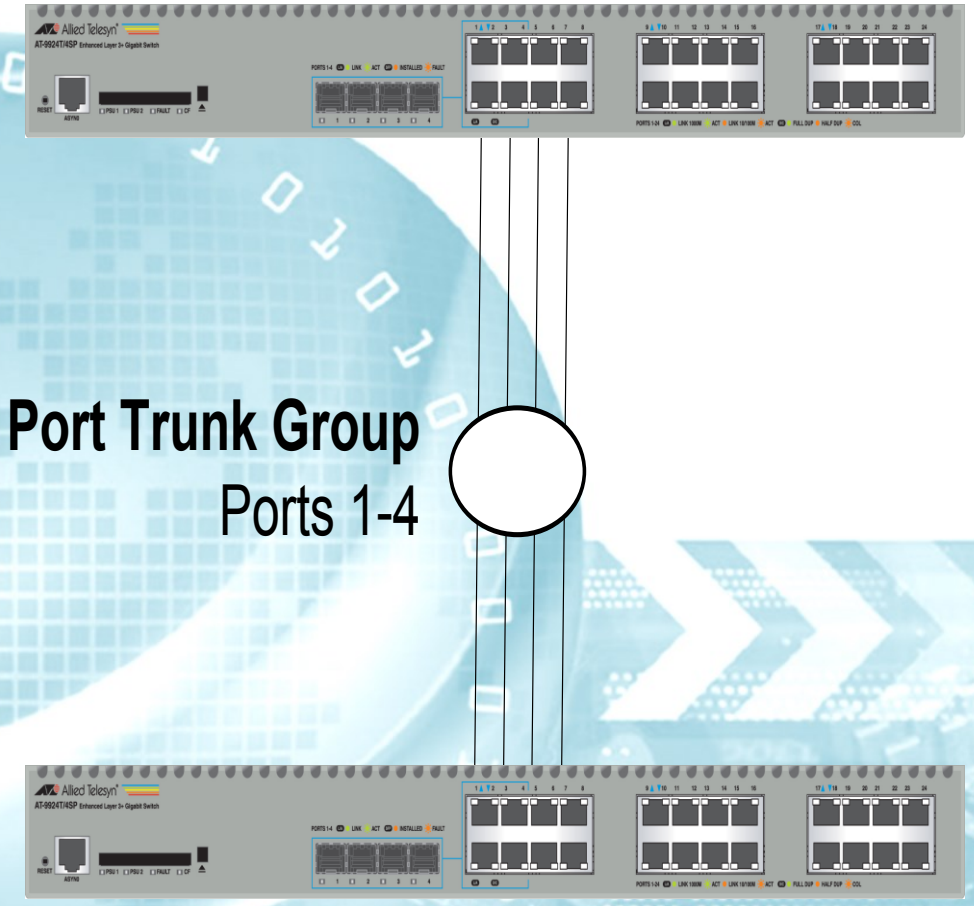
Port Aggregation

Port Trunking or link Aggregation

- Ability to support multiple, point-to-point, parallel active links between switches or between a switch and a server
- Link Aggregation allows a number of ports to be configured to join together to make a single logical connection providing:
  - Higher Bandwidth
  - Redundancy
  - Load Sharing
- A trunk group may not include Ethernet ports and Gigabit ports or Copper and Fiber ports

Port Trunking or link Aggregation

Port Trunking



EISTI
Ecole Internationale des Sciences du Traitement de l'Information

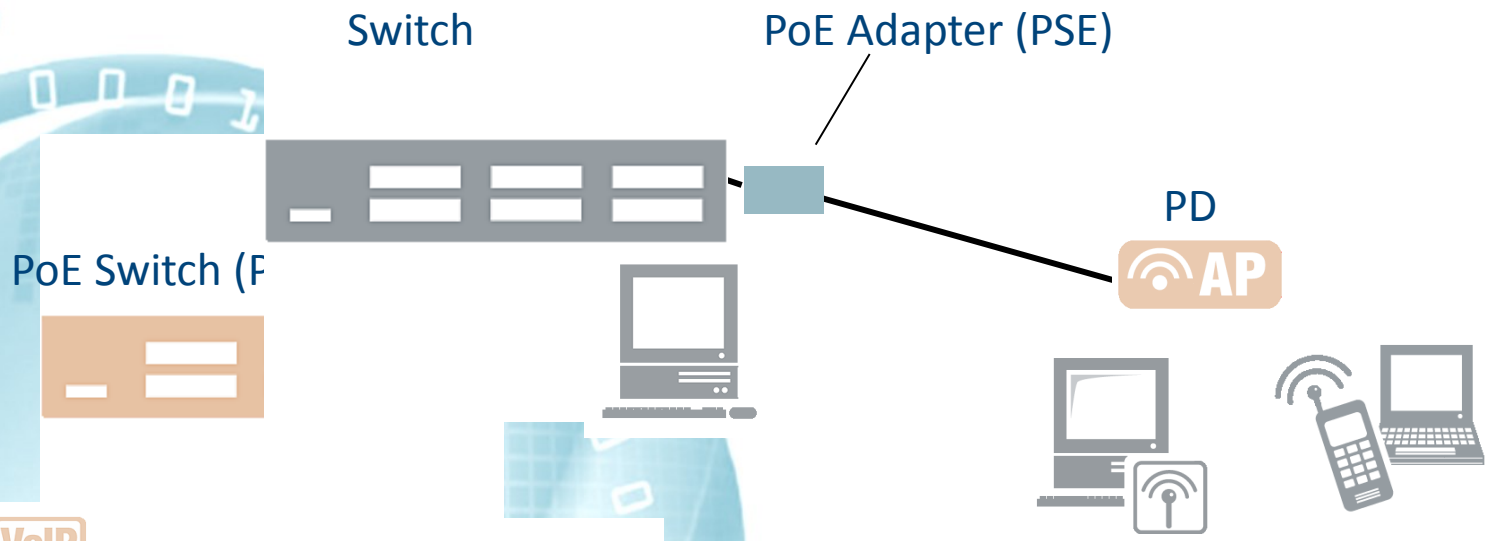
Power Over Ethernet

PoE

Power over Ethernet (PoE)

- Power over Ethernet (PoE) is a technology allowing devices such as IP telephones to receive power over existing LAN cabling
- Power is supplied to network devices over the same cabling used to carry network traffic
- Devices that require power are called Powered Devices (PDs)
- Devices that provide power to PDs are called Power Sourcing Equipment (PSE)

Power over Ethernet (PoE)



PSE: Power Sourcing Equipment
PD: Powered Device

Advantages of PoE

- A single cable between switch and Powered Device (PD)
- No separate power installation/ connection needed for PD’s
- Device placement is not limited to nearby power sources
- PD’s can be easily moved to wherever there is LAN cabling
- Safer - no mains voltages anywhere
- A UPS can guarantee power to devices during mains failure
- Devices can be shut down or reset remotely
- Little configuration or management required

Delivered Power

- The IEEE 802.3af standard supports delivery of up to 15.4 watts per port

- The IEEE 802.3at standard supports delivery of up to 30 watts per port

Power Classes

- The power classes outlined by IEEE 802.3af/at are:

Class	Power usage
0	0.44 W to 30W (default)
1	0.44 W to 3.84 W
2	3.84 W to 6.49 W
3	6.49 W to 12.95 W
4	30w

EISTI
Ecole Internationale des Sciences du Traitement de l'Information

TCP / IP

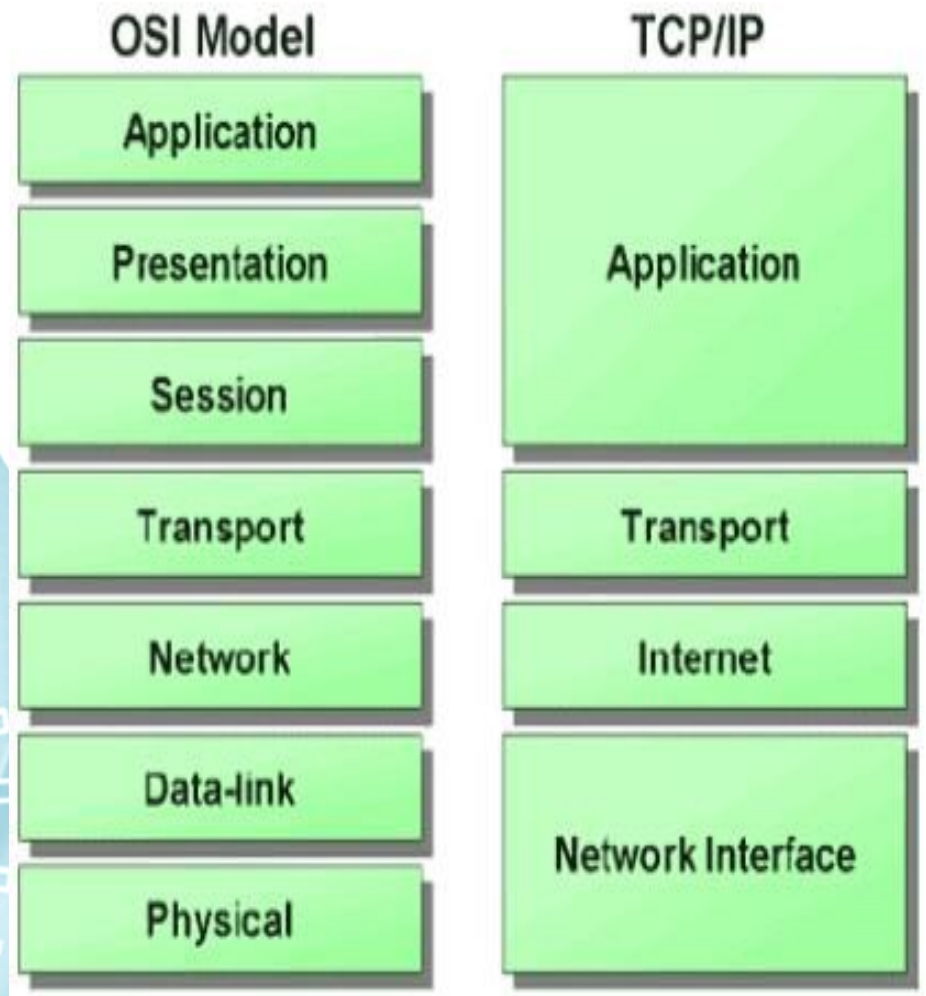
IPv4

Introduction to TCP/IP

- TCP/IP began as a non-commercial project in the 1970s. It was a military project of the U.S. Defence Advanced Research Projects Agency (DARPA)
- The TCP/IP suite is a layered model similar to the OSI reference model.
- Its name is actually a combination of two individual protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP).
  - It is divided into layers, each of which performs specific functions in the data communication process.

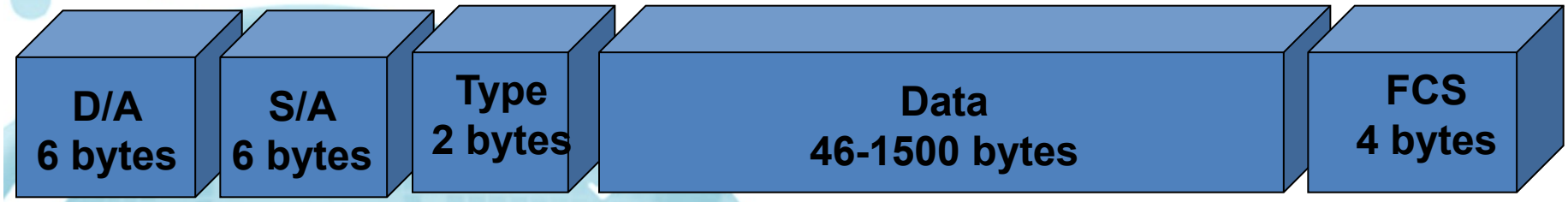
Introduction to TCP/IP

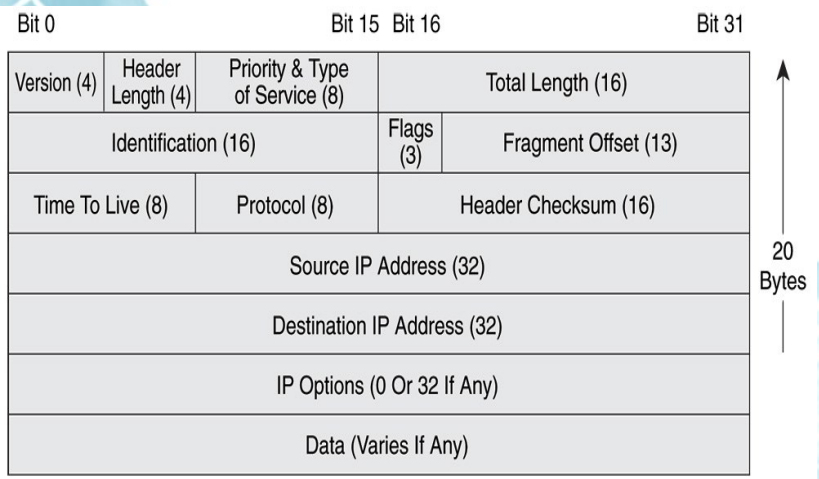
- To understand TCP/IP, it is useful to compare its layers with the OSI Reference Model



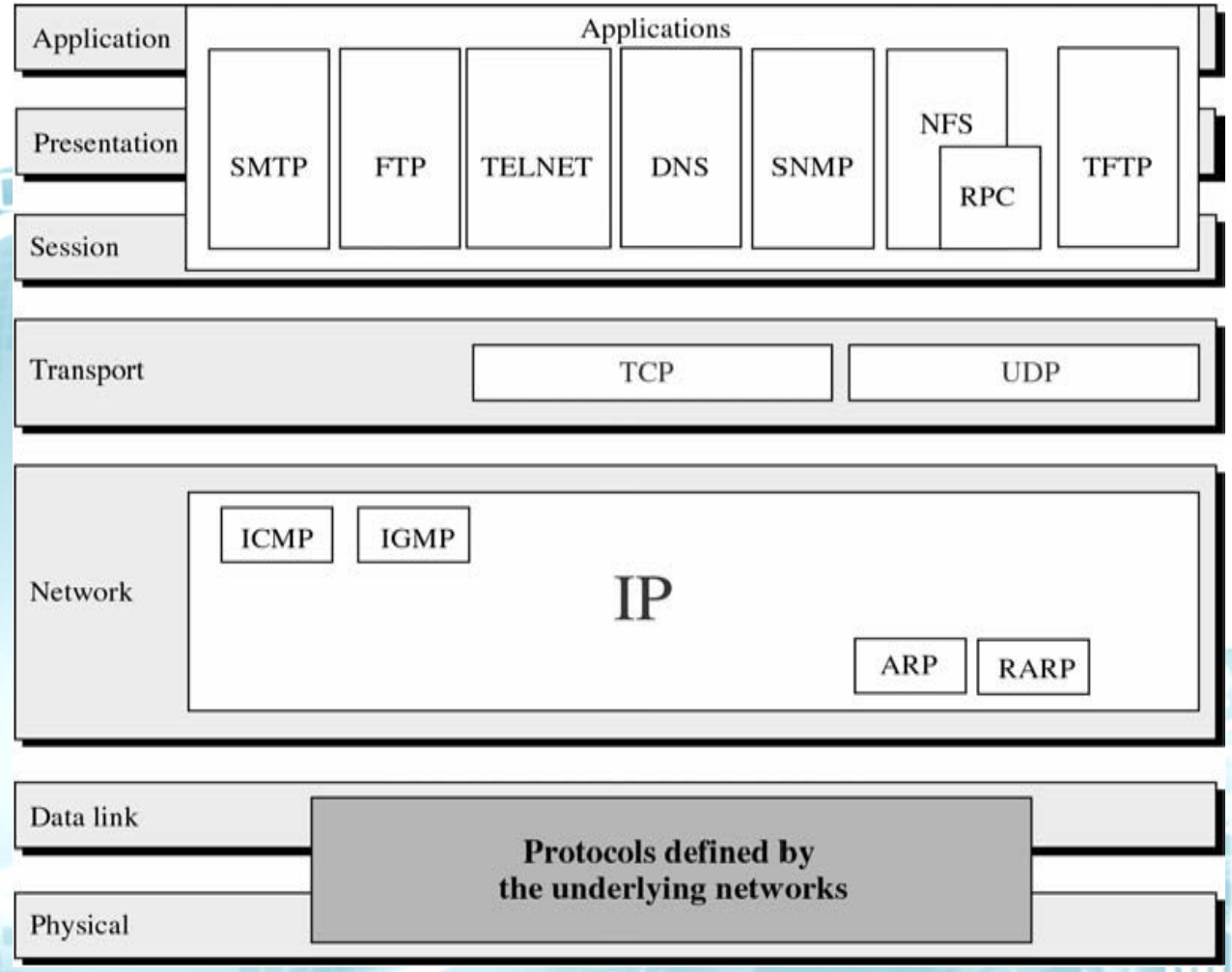
TCP/IP and the OSI model

Ethernet Frame: IP Header

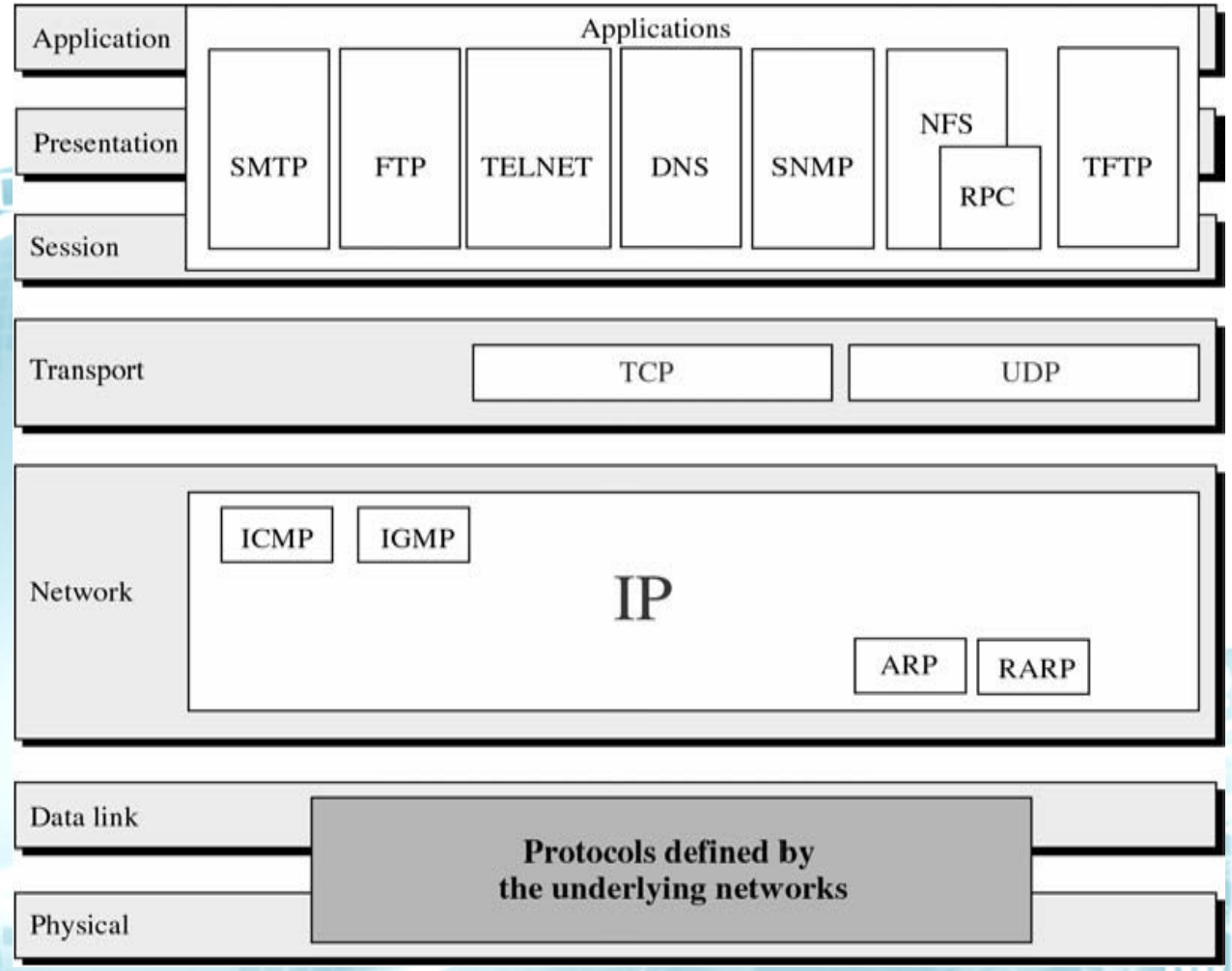




TCP/IP Elements



TCP/IP Elements



Transport Layer - L4

- TCP and UDP are two alternative transport protocols
  - TCP: flow control end-to-end
  - UDP: simple transport, not a reliable protocol
- They can operate simultaneously with many applications using port numbers

TCP/UDP Ports

- In a TCP or UDP packet, the port number defines which application in the upper layer will receive the packet
- Ports are the medium through which client applications address a server application
  - E.g., an FTP client connecting to an FTP server must use
    - the IP address of the remote host
    - the TCP port number associated to the FTP server

Well Known Ports TCP/UDP Ports

Service	Port	TCP	UDP
FTP	21	X	
Telnet	23	X	
SMTP 25	X		
TFTP	69		X
HTTP 80	X		
POP	110	X	
NTP	119	X	
SNMP	161		X
HTTPS	443	X	

Windows: %windir%\System32\drivers\etc\services

Linux : /etc/services

TCP

- Used by applications that need reliable transmission of information (e.g. Telnet, FTP, SMTP, etc.)

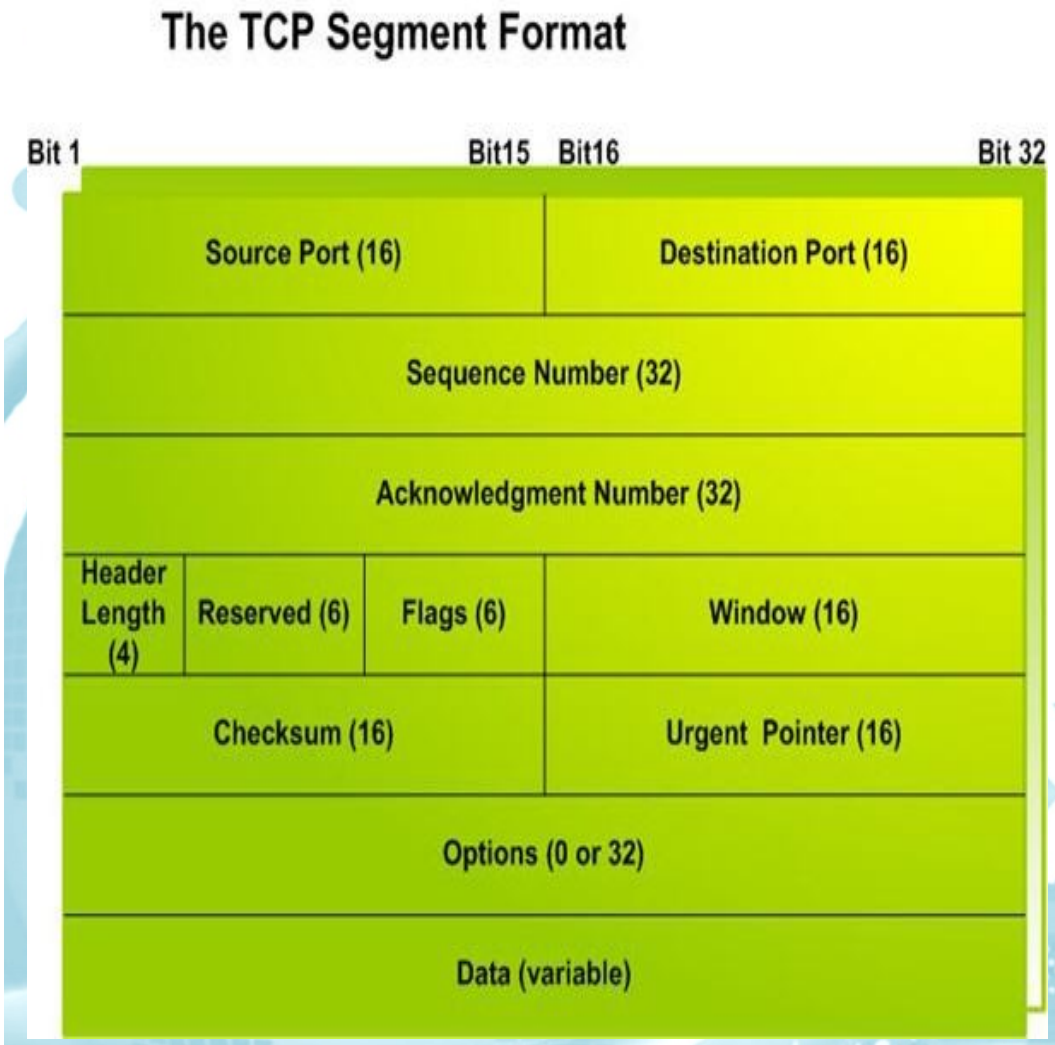
- TCP functions include
  - Error Checking
  - Flow control
  - State check and synchronisation check

- TCP assures packet delivery, UDP does not!

TCP

- A virtual circuit is established between the TCP layers of two communicating nodes
- This virtual circuit is associated to a transport protocol providing for
  - full-duplex communication
  - an acknowledge mechanism
  - flow control
- TCP needs more bandwidth and CPU resources than UDP

TCP Packet



- Source and destination ports identify the end points of the virtual connection
- Sequence number is the serial number of the transmitted packet, used to check if any packet has been lost
- Acknowledgement number indicates the next frame number that the receiver is waiting to receive

UDP

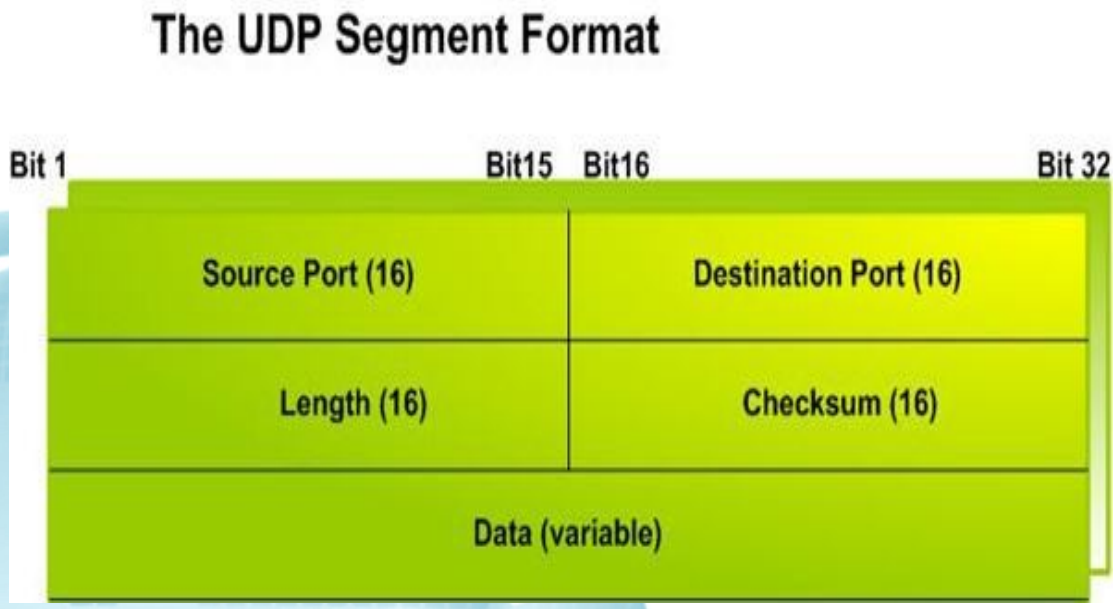
- UDP adds two functions to IP
  - information multiplexing between applications
  - checksums to verify data integrity
- UDP doesn't provide flow control mechanisms
  - it cannot adapt dynamically to traffic flow changes
  - it doesn't provide retransmission after errors; retransmission must be managed by the application
  - it is suitable for multimedia applications
- Error checking
  - it checks the packet integrity, but cannot correct errors

UDP

- The main applications that use UDP are
  - NFS (Network File System)
  - SNMP (Simple Network Management Protocol)
  - Multimedia streaming (multicast traffic)

- Useful when
  - the application encapsulates all data in a single packet
  - it is not important that all packets arrive to destination
  - the application itself manages retransmission

UDP Packet

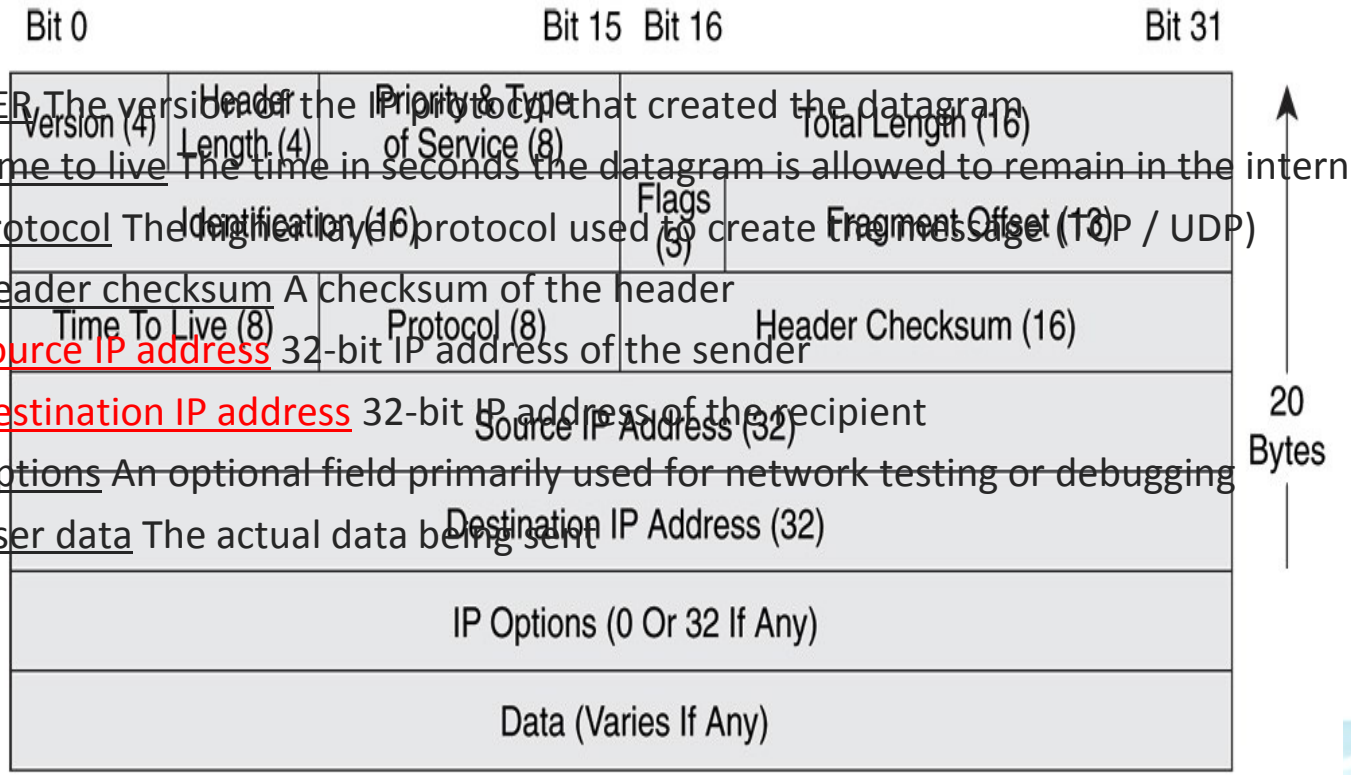


- Source and destination ports identify the end points of the virtual connection
- Checksum and UDP source are optional and can be set to 0

Network Layer - IP

- It receives data from transport layer and encapsulates them in packets
- It routes these packets on the subnet, possibly breaking them into fragments
- At the destination
  - pastes (if necessary) the fragments in packets
  - takes out the transport layer data from these packets
  - sends the data to the transport layer in the order in which they arrived (which could be different from the order in which they were sent)

IP Datagram



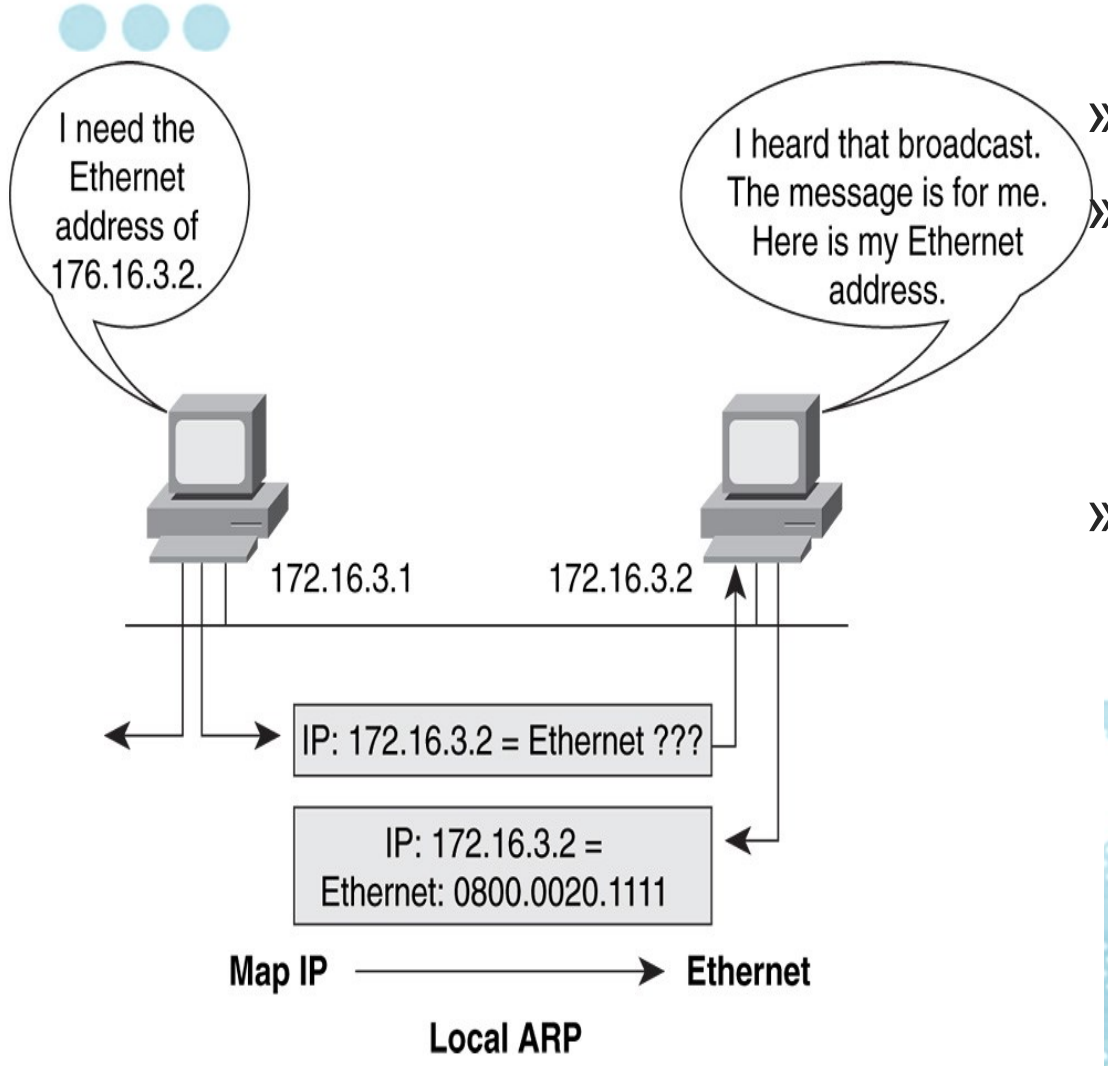
- VER The version of the IP protocol that created the datagram
- Time to live The time in seconds the datagram is allowed to remain in the internet system
- Protocol The higher layer protocol used to create the message (TCP / UDP)
- Header checksum A checksum of the header
- Source IP address 32-bit IP address of the sender
- Destination IP address 32-bit IP address of the recipient
- Options An optional field primarily used for network testing or debugging
- User data The actual data being sent

- IP is the network layer for TCP/IP and it is a simple datagram protocol

Control Protocols

- Some protocols are designed to provide control on IP subnets
  - ARP
  - RARP
  - ICMP (ping)

ARP - Address Resolution Protocol



- ARP works at Layer 2
- For IP on Ethernet, the logical (IP) address needs to be bound to MAC address of its destination.
- Each IP device on a network segment maintains an ARP table in its memory.

ARP - Address Resolution Protocol

- The ARP table maintains a correlation between each IP address and its corresponding MAC address.
- The ARP table, or ARP cache, keeps a record of recent bindings of IP addresses to MAC addresses.
- The ARP table is created and maintained dynamically, adding and changing address relationships as they are used on the local host. The entries in an ARP table usually expire after a period of time, by default 300 seconds; however, when the local host wants to transmit data again, the entry in the ARP table is regenerated through the ARP process.

RARP - Reverse ARP

- It is used to discover the IP address of a host starting from its physical address (data link address)

- Useful when it is necessary to connect stations without a hard disk; during the boot operation they load from a server the image of the binary code of the operating system

Internet Control Message Protocol

- ICMP is used to verify the state of the network
  - Echo request and echo reply
- Used to report wrong behaviours
  - Ping
  - Destination Unreachable
  - Time Exceeded for a datagram
  - Parameter Problem on a datagram

EISTI
Ecole Internationale des Sciences du Traitement de l'Information

TCP / IP

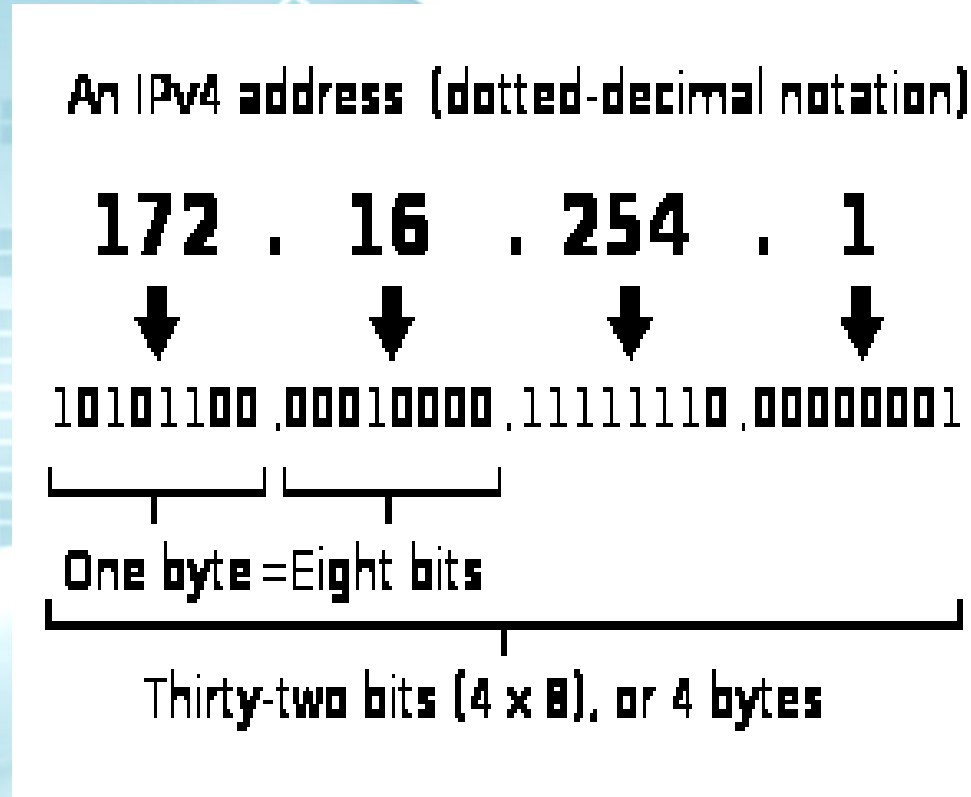
IPv4 Addressing

IPv4 Addressing

- IP addresses are 4 octet (32 bit) numbers that identify both
  - network address, i.e. the number assigned to the IP network; a network is made of a single communication channel connected to the hosts (for example a LAN or a point to point line between two routers)
  - host address, i.e. the number that identifies a specific host

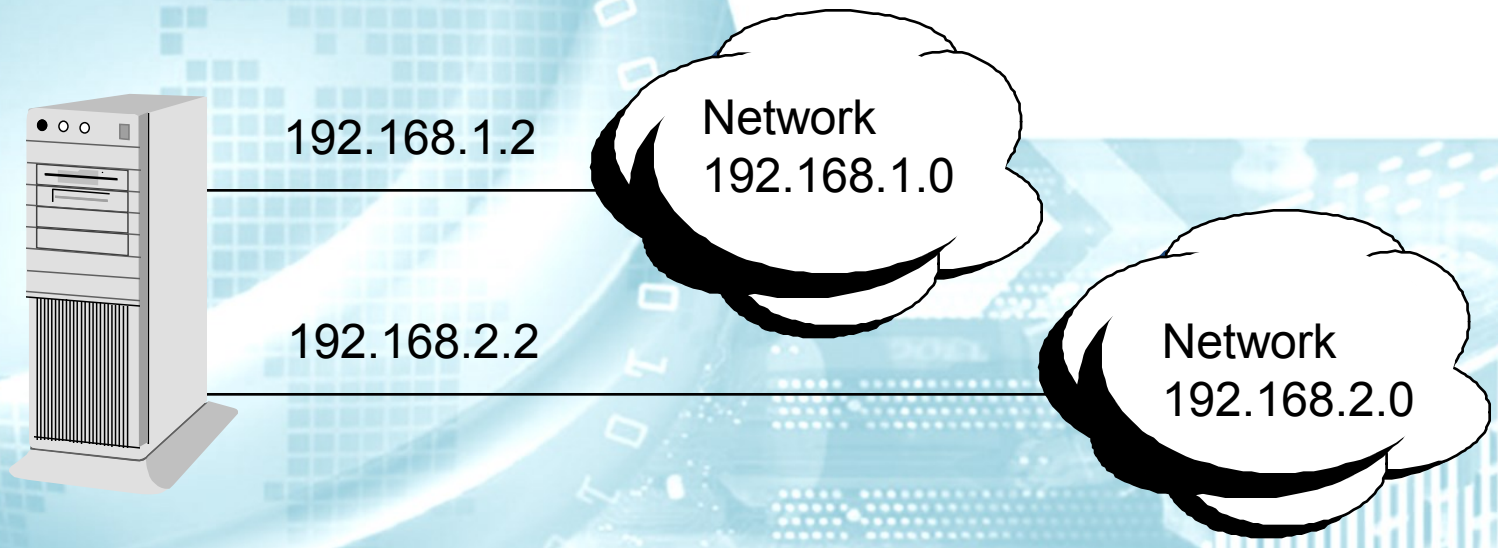
IP Addressing

- IP addresses are represented in dotted decimal notation: each byte is expressed in decimal notation and they are separated by a dot



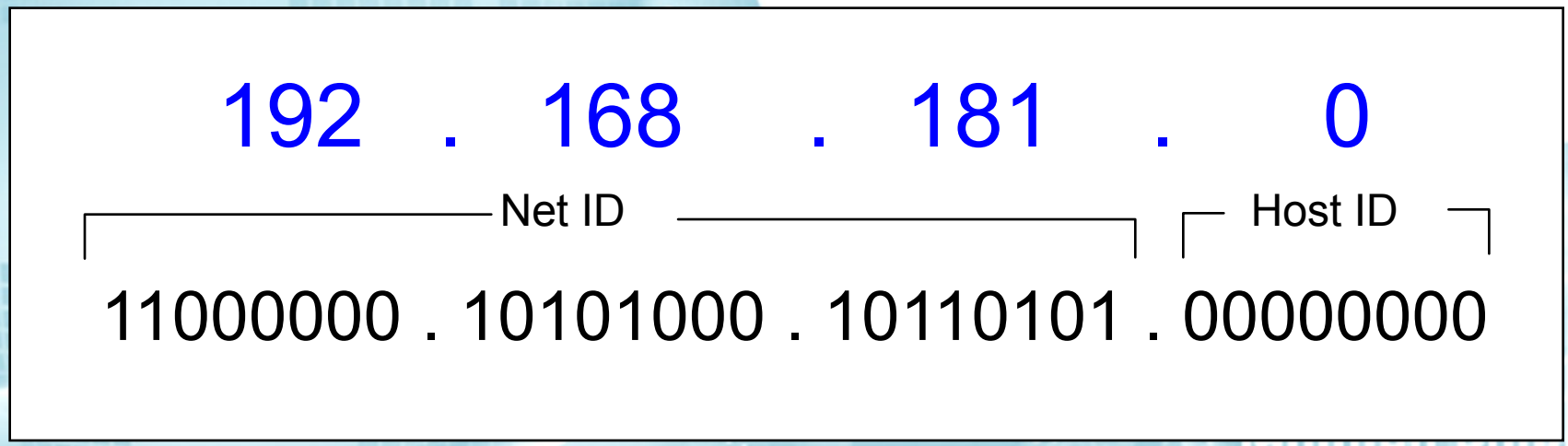
IPv4 Addressing

- Since IP numbers encode both a network and a host address, they do not specify an individual machine, but a connection to a network

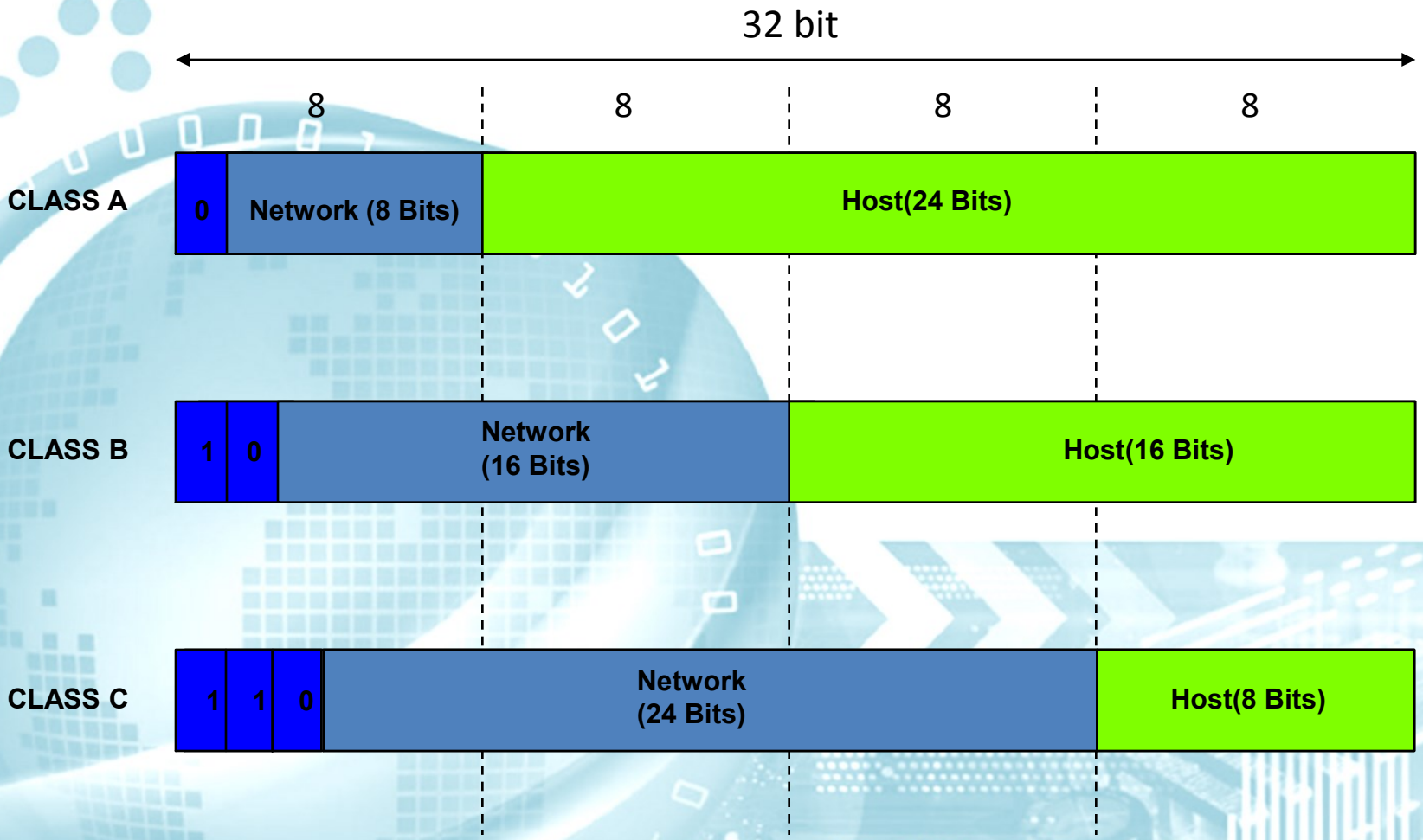


Network Addresses

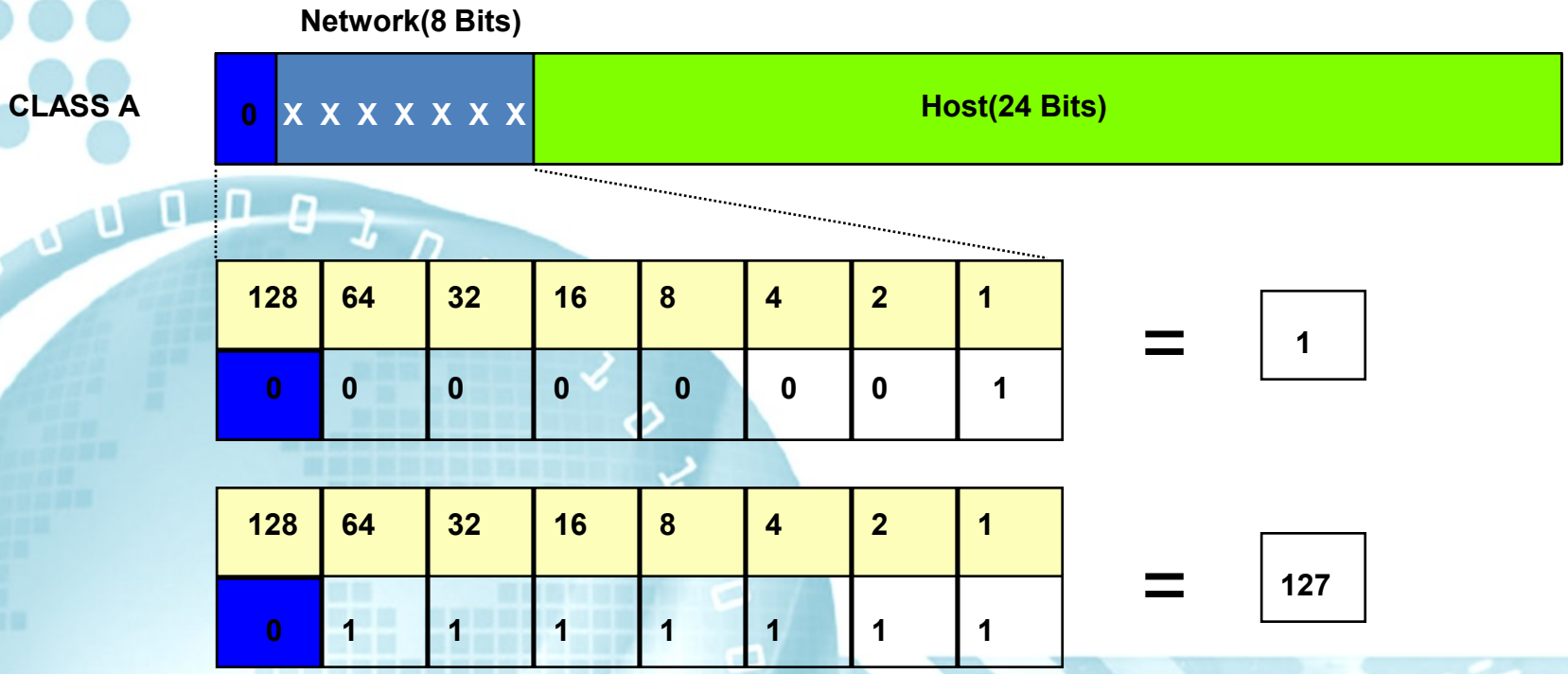
- Internet addresses can be used to refer to networks as well as to individual hosts
- By convention, a network address has a host ID with all bits set to zero



IANA Primary IP Address Classes



CLASS A



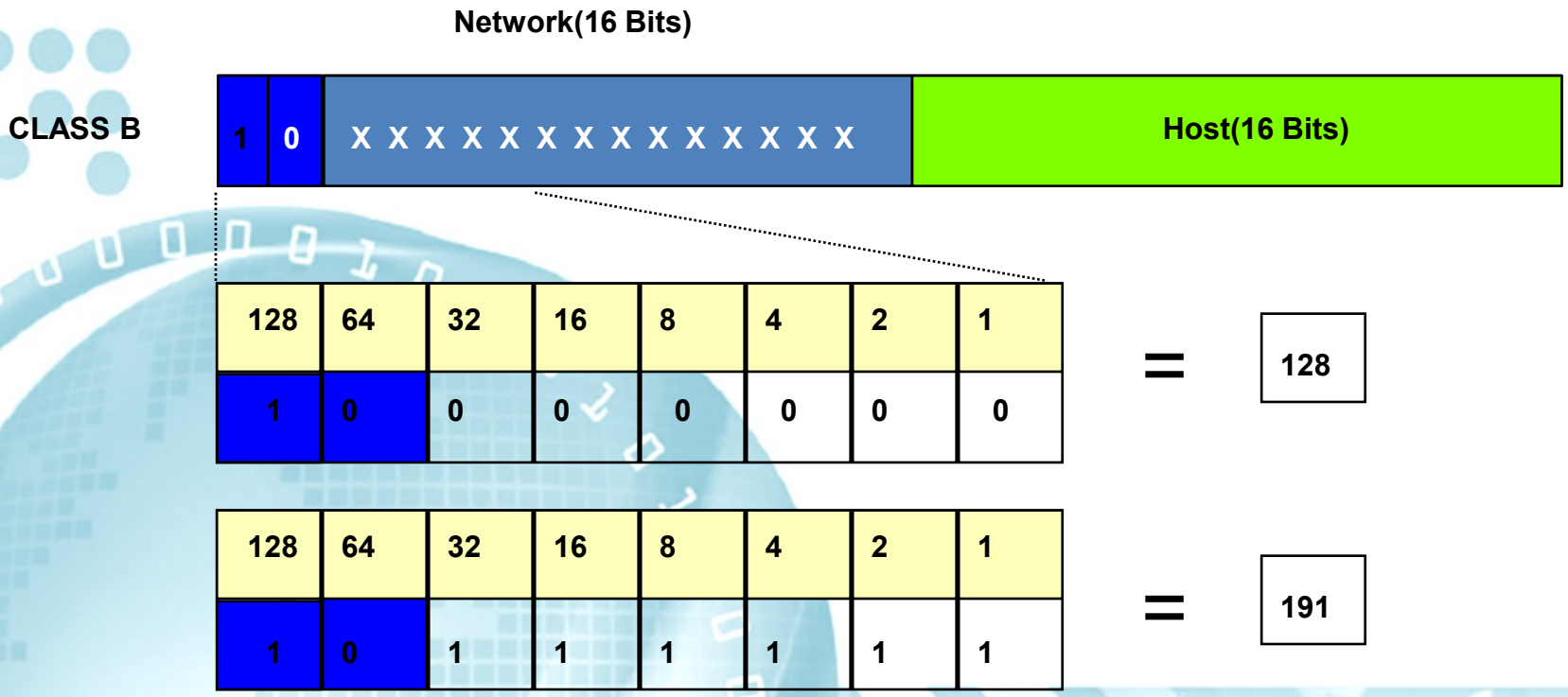
- Class A first byte range: 1-127
- First bit of network field fixed to 0

Class A Addresses

- With class A addresses, the Most Significant Bit (MSB) is reserved and must be zero, this results in the following range of network addresses
  - networks 1 – 126
  - network 127 is reserved for Loopbacks

- There are 126 usable networks
- Each with 16,777,216 (2^{24}) hosts

CLASS B



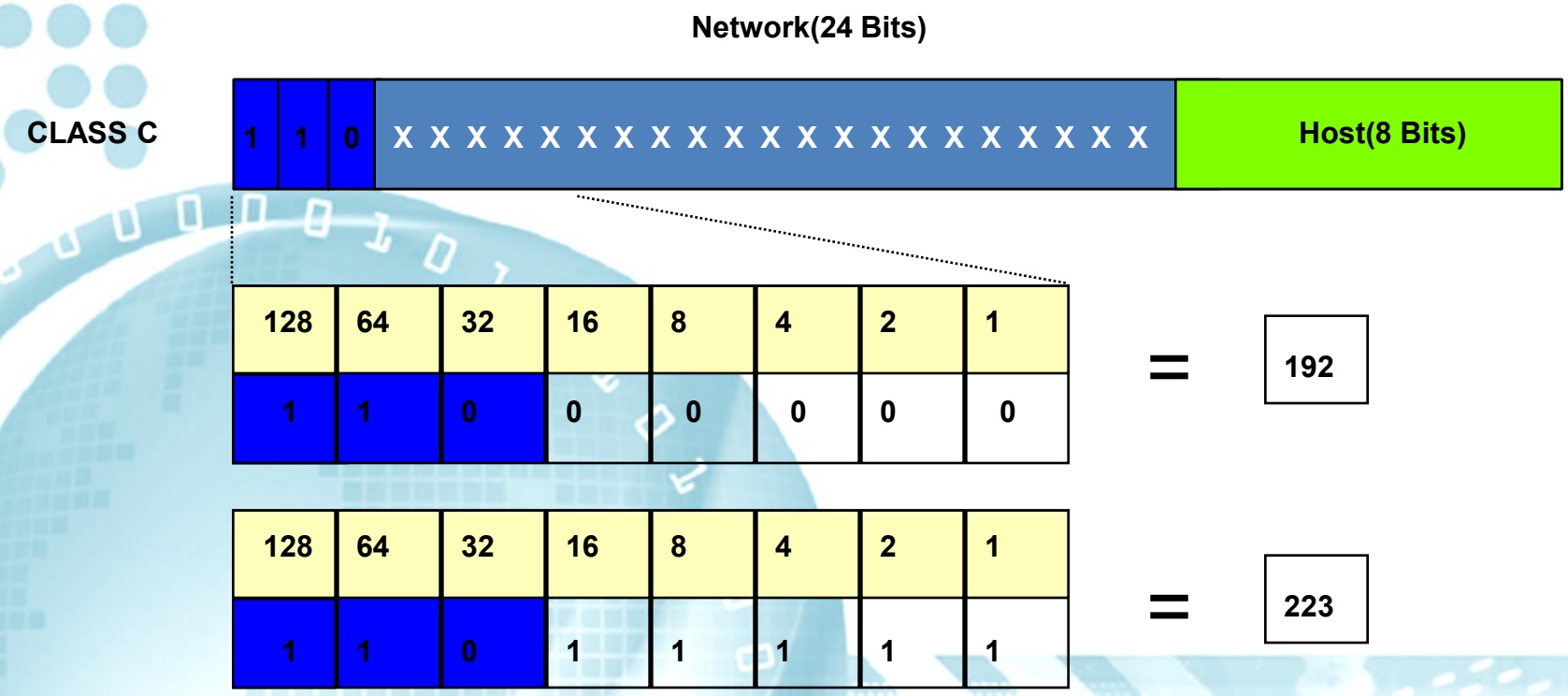
- Class B first byte range: 128-191
- First two bits of network field fixed to 1|0

Class B Addresses

- With class B addresses the two Most Significant Bits (MSB) are reserved (1 0), this results in the following range of network addresses
  - networks 128 – 191

- There are 16,384 (2^6 x 2^8) usable networks
- Each with 65,536 (2^{16}) hosts

CLASS C



- Class C address range: 192-223
- First three bits of network field fixed to 1|1|0

Class C Addresses

- With class C addresses the 3 Most Significant Bits (MSB) are reserved (1 1 0), this results in the following range of network addresses
  - networks 192 – 223

- There are 2,097,152 (2^5 x 2^8 x 2^8) usable networks
- Each with 256 (2^8) hosts

IANA IPv4 Classes

	8 bits	8 bits	8 bits	8 bits
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host
Class D	Multicast			
Class E	Reserved			

Class	**Address range (High octet)**	**Mask**
Class A	0 - 127	255.0.0.0
Class B	128 – 191	255.255.0.0
Class C	192 - 223	255.255.255.0

Special IPv4 Addresses: Loopback and

- Local loopback subnet within each host: address 127.0.0.1 / 8

- Private addresses are needed due to shortage of public addresses
- Private addresses, which should never be declared in a public network
- Access to private addresses from the public network is typically via NAT (Network address translation)

Address Class	Reserved address space
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

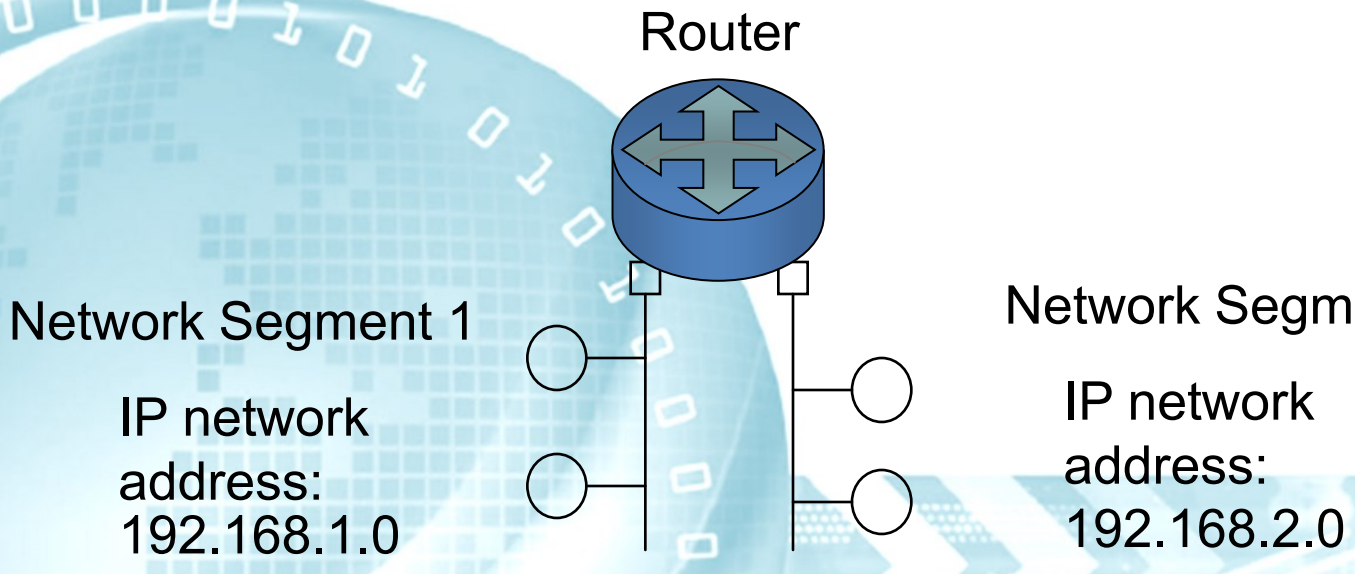
Network Addresses

- In order to establish simple communication, hosts must have the same network addresses

- If hosts have different network addresses, then we must use a router to connect two network segments

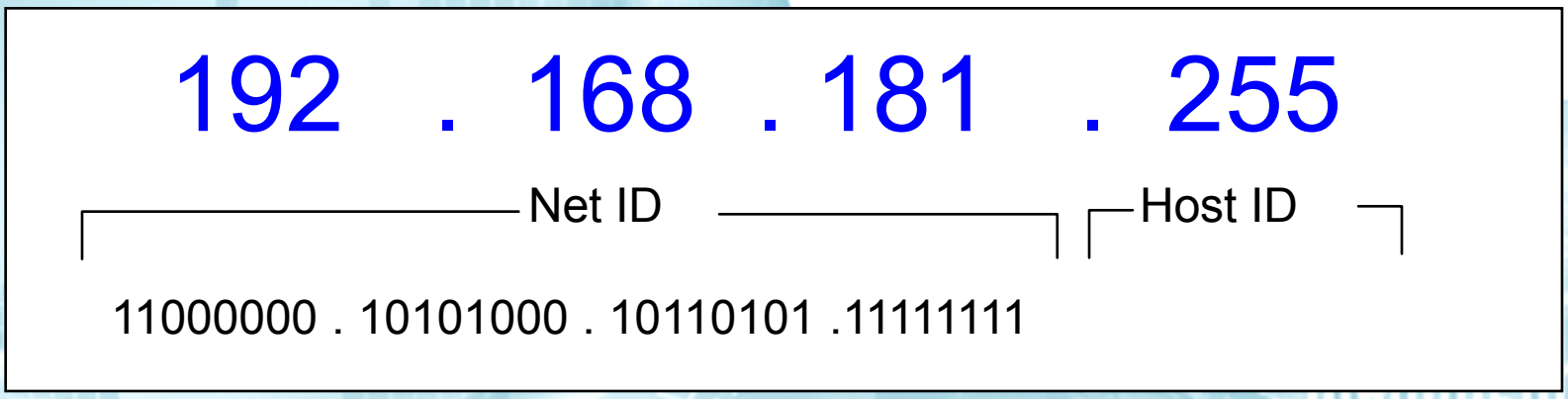
Network Addresses

- A router can connect only IP network segments that have different network addresses



Broadcast Addresses

- The broadcast address is used to send a message to all users on the network
- By convention, a broadcast address has a host ID with all bits set to one



IP Subnet Masks

- Routing is based on the Net ID portion of IP addresses and routers need to extract this portion quickly for efficient routing

- To do this, a subnet mask is used

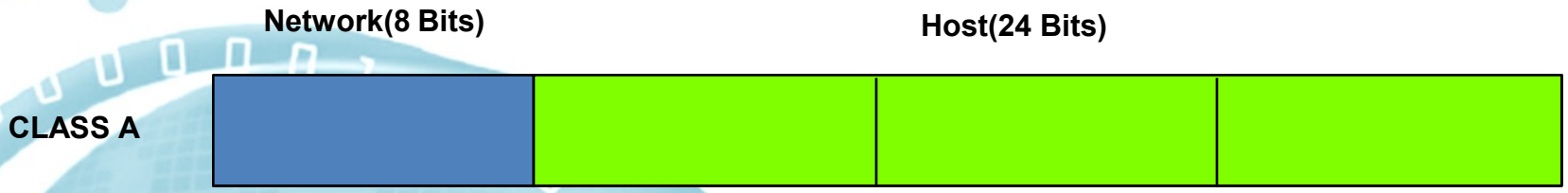
- The subnet mask acts as an indicator of the network portion of an IP address

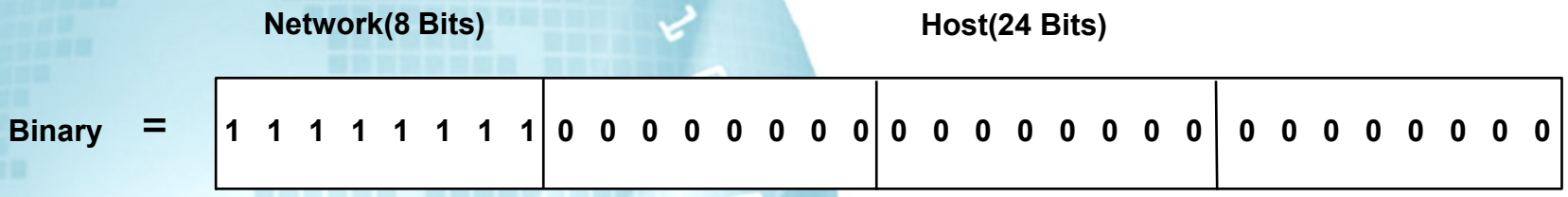
IP Subnet Masks

- The subnet mask uses bits set to 1 to indicate the network portion of the address and bits set to 0 to indicate the host portion

- The mask is written in dotted decimal notation

Class A Default Subnet Mask

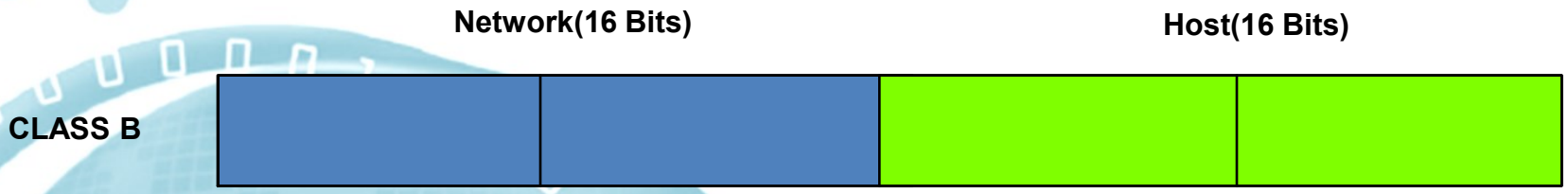


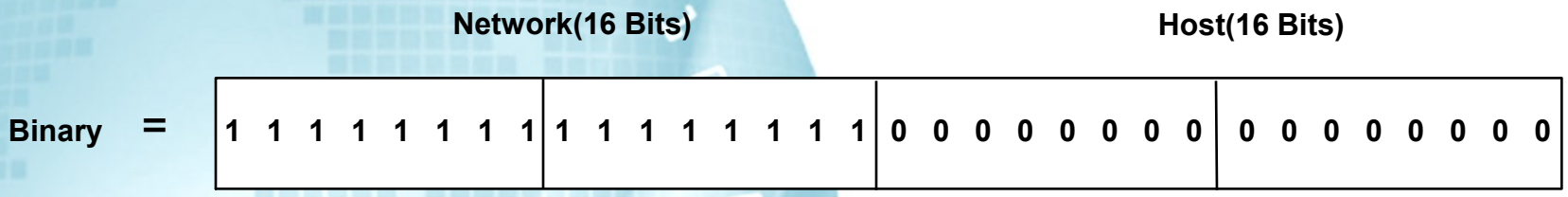


Decimal = 255 0 0 0

In a Class A, the first 8 bits are reserved by default as networking bits and the remaining 24 bits are host bits

Class B Default Subnet Mask

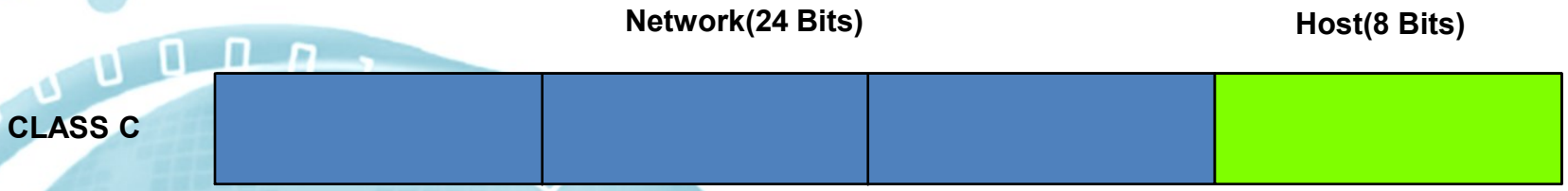


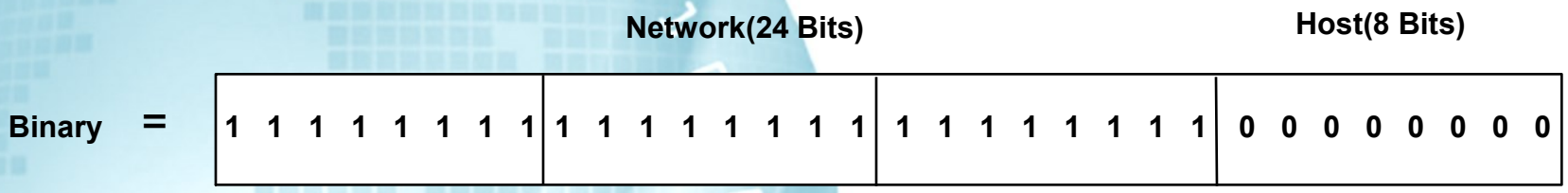


Decimal = 255 255 0 0

In a Class B, the first 16 bits are reserved by default as networking bits and the remaining 16 bits are host bits

Class C Default Subnet Mask





Decimal = 255 255 255 0

In a Class C, the first 24 bits are reserved by default as networking bits and the remaining 8 bits are host bits

Nouvelle table adresses réservées

Bloc	Usage	Référence
0.0.0.0/8	*Adresse réseau par défaut*	RFC 1700
10.0.0.0/8	Adresses privées	RFC 1918
100.64.0.0/10	Espace partagé pour Carrier Grade NAT	RFC 6598
127.0.0.0/8	adresse de bouclage (localhost)	RFC 1122
169.254.0.0/16	adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	Adresses privées	RFC 1918
192.0.0.0/24	Réservé par l'IETF	RFC 5736
192.0.2.0/24	Réseau de test TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 anycast	RFC 3068
192.168.0.0/16	Adresses privées	RFC 1918
198.18.0.0/15	Tests de performance	RFC 2544
198.51.100.0/24	Réseau de test TEST-NET-2	RFC 5737
203.0.113.0/24	Réseau de test TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 5771
240.0.0.0/4	Réservé à un usage ultérieur non précisé	RFC 1112
255.255.255.255/32	broadcast limité	RFC 919

https://fr.wikipedia.org/wiki/CIDR#Plages_d.27adresses_IP_sp.C3.A9ciales

EISTI
Ecole Internationale des Sciences du Traitement de l'Information

The most important !

TCP / IP

IP Addressing: Subneting

Subnetting

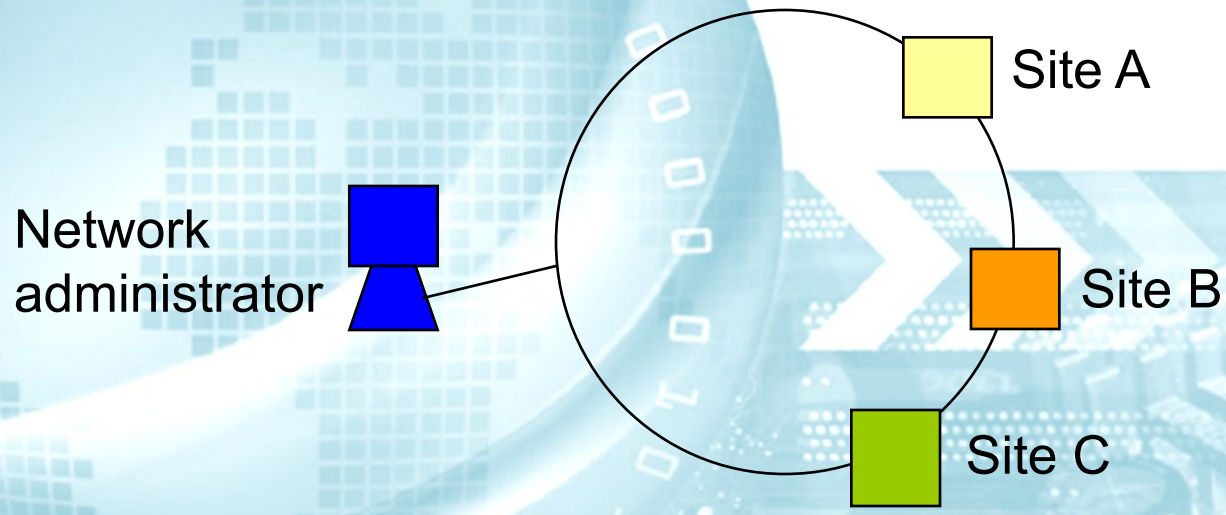
- In order to reduce the number of used networks on the public Internet, every network can be divided into subnets, each one containing its own hosts
- There is no need to communicate this outside a private network
- The original network address can be seen as a couple of numbers: subnet number and host number

Subnetting

- It is possible to obtain many subnets containing few hosts or few subnets with many hosts
- Subnet masks are used to determine which bits in the IP address are networking bits and which are host bits
- The convention is that networking bits are represented by 1 and host bits are represented by 0

Subnetting Example

- Consider a company with many production sites
- There is a LAN in every site with a different network address
- The central site must administrate the whole private network



Subnetting Example

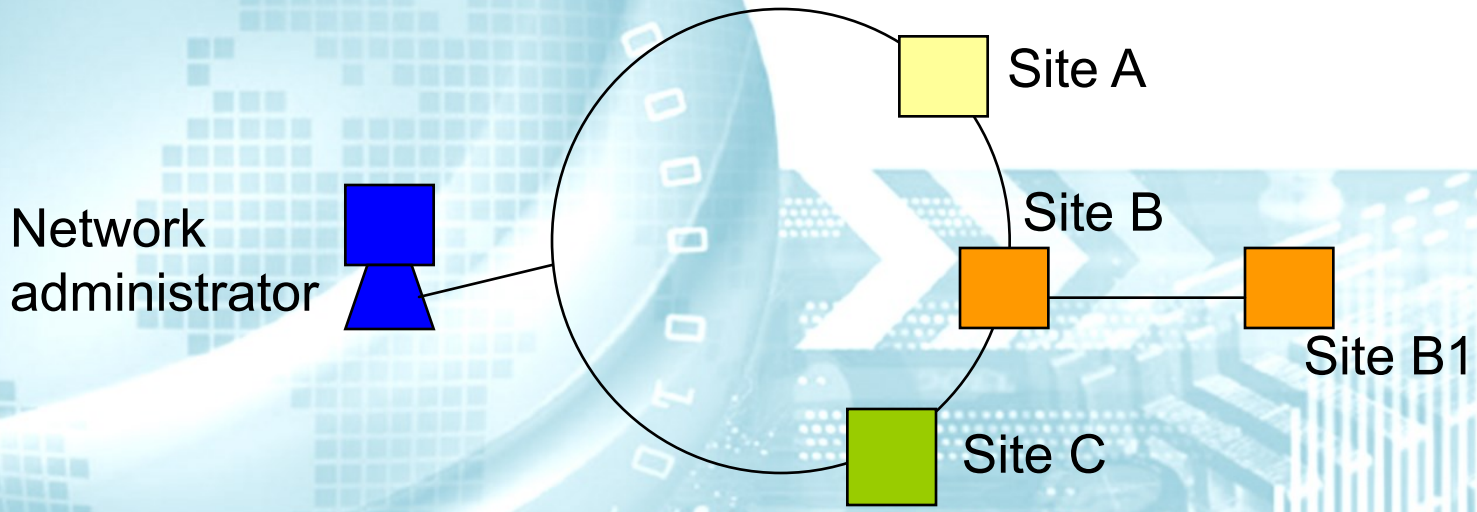
- If site B decides to open a new site (site B1), then the network administrator must give it a new network IP address
- If there are many new sites being opened, the work for the network administrator will become too big
- It is useful to connect the new site to the network in site B instead of the main network

Subnetting Example

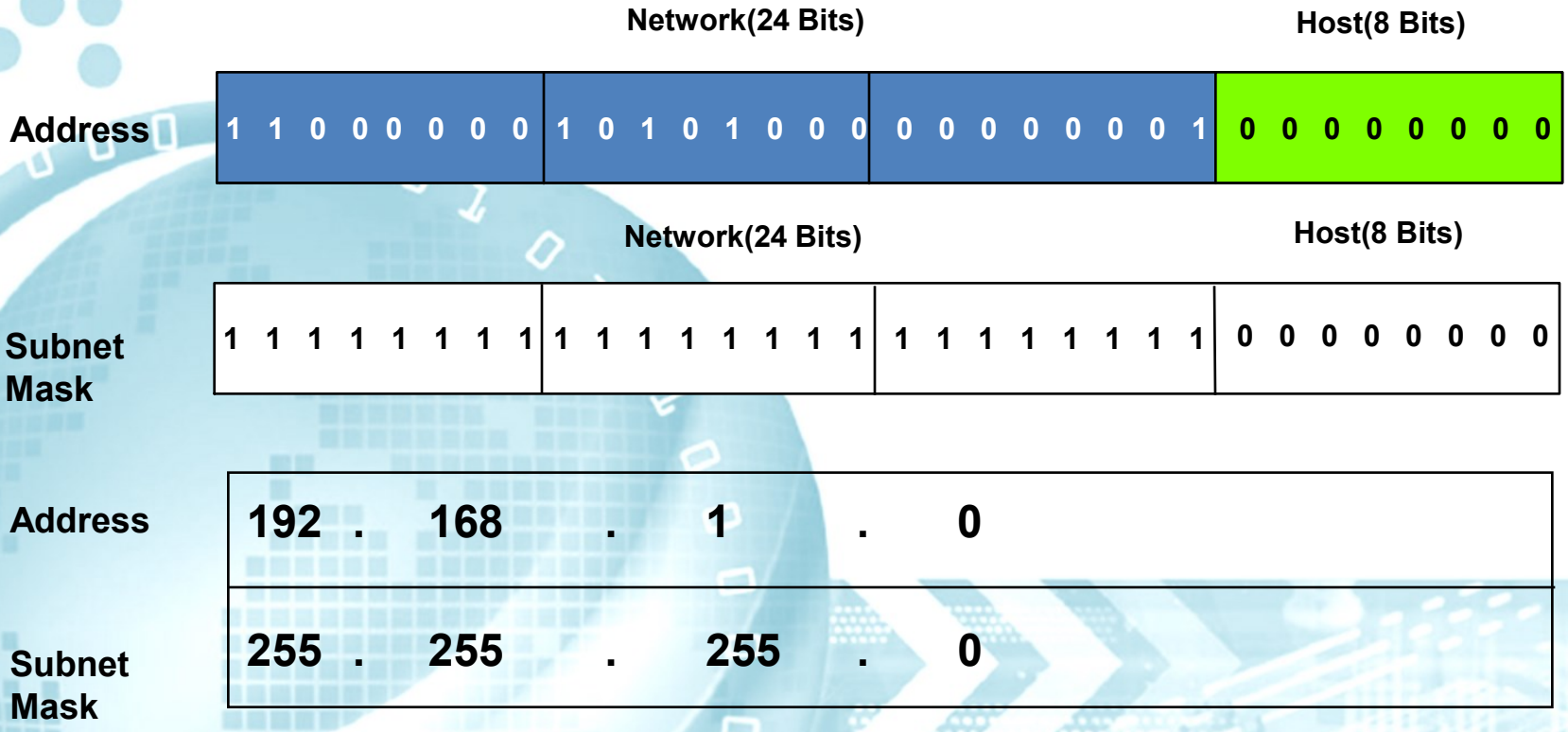
- To do this, site B will use subnetting
- All other stations will not know anything about this change; it is a private operation
- There is no need to add a new IP network address

Subnetting Example

- To create the subnet for site B1, both B and B1 must change their subnet mask number in order to obtain at least two subnets from the original network



Class C Address

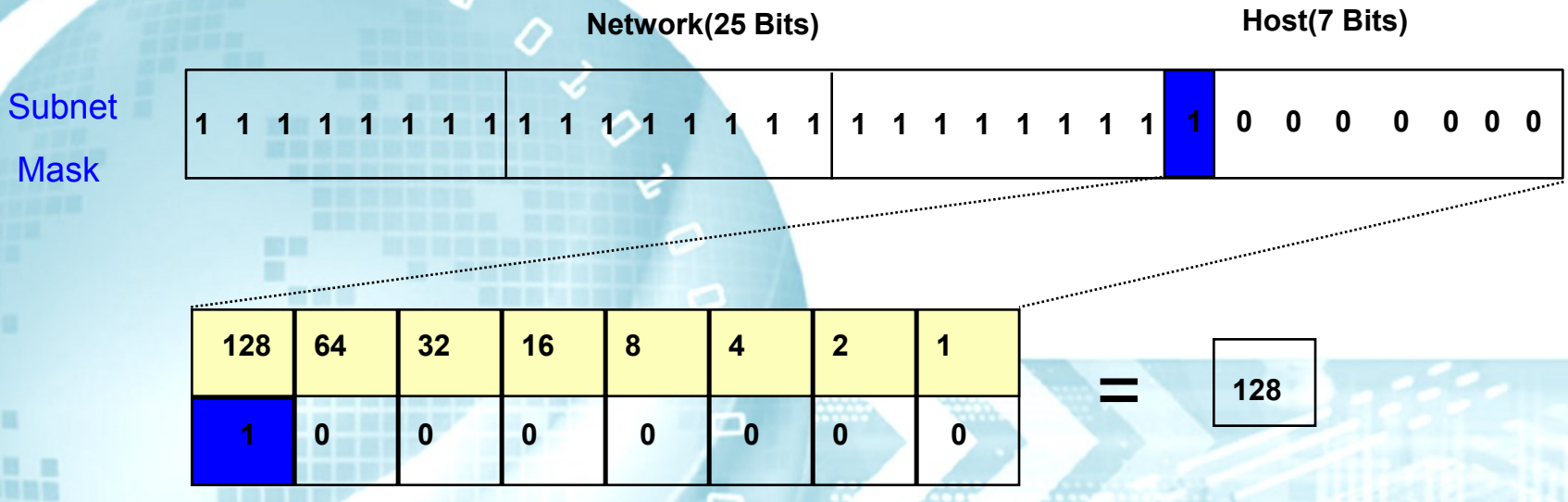


Address	192 .	168 .	1 .	0
Subnet Mask	255 .	255 .	255 .	0

Here you can see a class C address with its default mask

Two Logical Networks

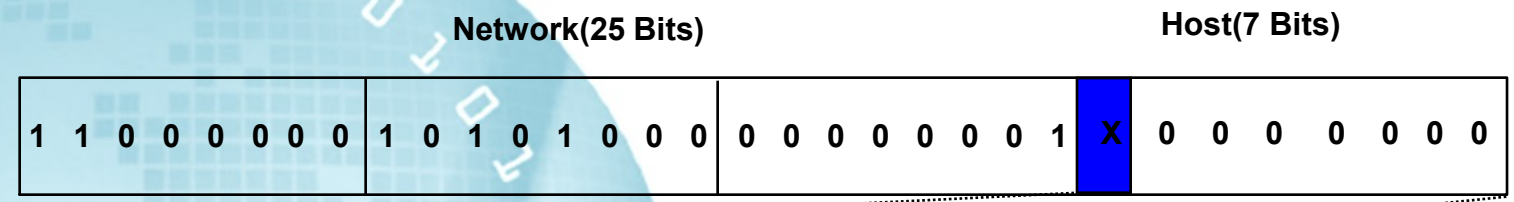
Address	192	.	168	.	1	.	0
Subnet Mask	255	.	255	.	255	.	128



If you want to obtain two logical networks from a class C address, you must modify the subnet mask to 255.255.255.128

Two Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 128



	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
Logical Network 1	1	0	0	0	0	0	0	0	=	128

Subnet 0 address: 192.168.1.0

Subnet 1 address: 192.168.1.128

Two Logical Networks

- In the previous example, the most significant bit of the last octet has been designated as a networking bit, which will effectively subdivide the Class C network into two logical networks, each being able to support 126 hosts and a broadcast address

Two Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.128

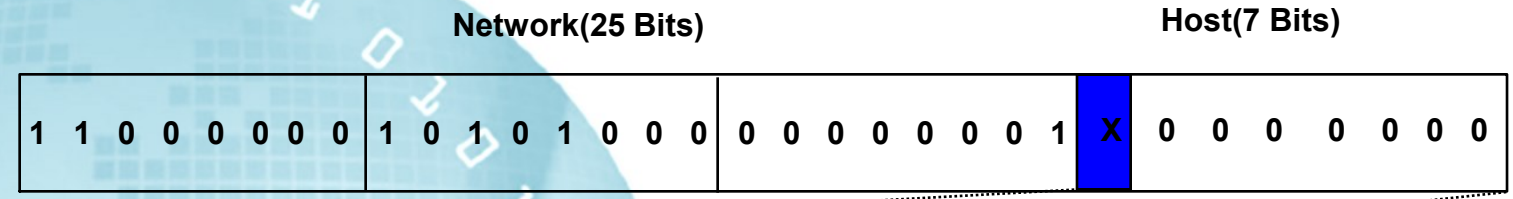
Network address 192.168.1.0
First Host address 192.168.1.1
Last Host address 192.168.1.126
Broadcast address 92.168.1.127

Logical network 1 - 255.255.255.128

Network address 192.168.1.128
First Host address 192.168.1.129
Last Host address 192.168.1.254
Broadcast address 92.168.1.255

Two Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 128

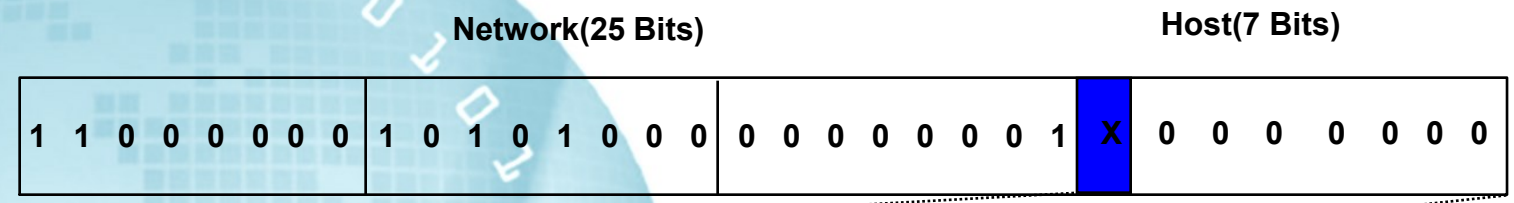


	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
First Host	0	0	0	0	0	0	0	1	=	1
Last Host	0	1	1	1	1	1	1	0	=	126

For the hosts on subnet 0 you can use the range of addresses from .1 to .126

Two Logical Networks

Address	192 . 168 . 1 . 128
Subnet Mask	255 . 255 . 255 . 128



	128	64	32	16	8	4	2	1		
Logical Network 1	1	0	0	0	0	0	0	0	=	128
First Host	1	0	0	0	0	0	0	1	=	129
Last Host	1	1	1	1	1	1	1	0	=	254

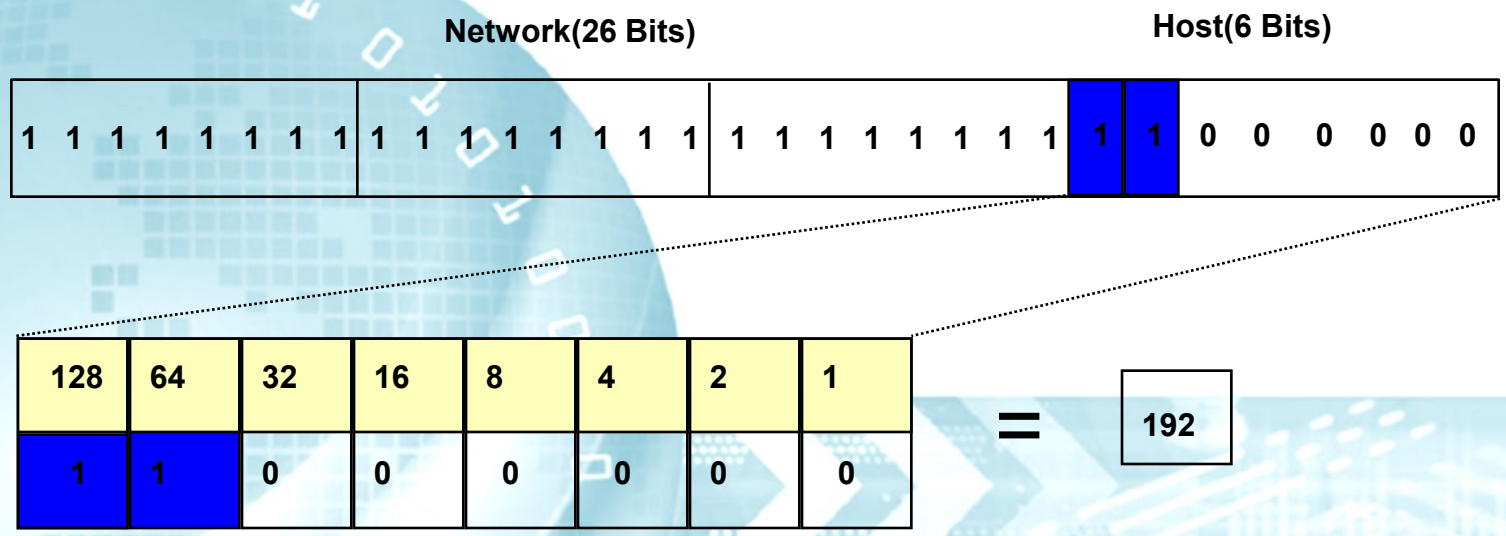
For the hosts on subnet 1 you can use the range of addresses from .129 to .254

Summary: Two Logical Networks

- If you must divide a Class C address into two networks, set the subnet mask to 255.255.255.128
- Logical network addresses
  - subnet 0 address is 192.168.1.0
  - subnet 1 address is 192.168.1.128
- Address Ranges
  - subnet 0 range is from .1 to .126
    - broadcast is .127
  - subnet 1 range is from .129 to .254
    - broadcast is .255

Four Logical Networks

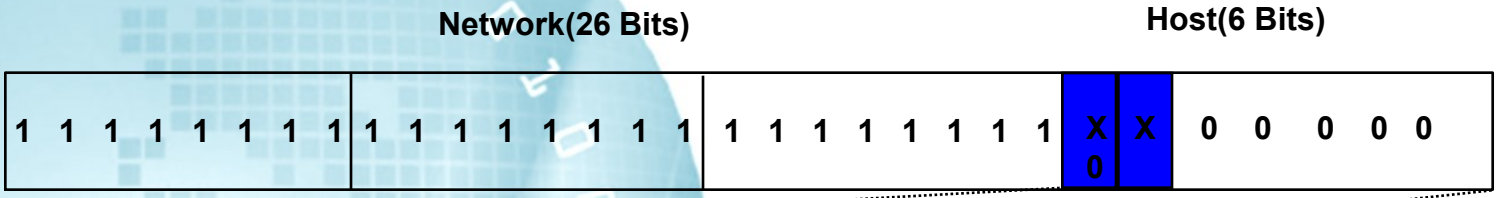
Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192



If you want to obtain four logical networks from a class C address, you must modify the subnet mask to 255.255.255.192

Four Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192



	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
Logical Network 1	0	1	0	0	0	0	0	0	=	64
Logical Network 2	1	0	0	0	0	0	0	0	=	128
Logical Network 3	1	1	0	0	0	0	0	0	=	192

Four Logical Networks

- In the previous example, the two most significant bits of the last octet have been designated as a networking bits which, will effectively subdivide the Class C network into four logical networks, each supporting 62 hosts and a broadcast address

Four Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.192

Network address 192.168.1.0
First Host address 192.168.1.1
Last Host address 192.168.1.62
Broadcast address 192.168.1.63

Logical network 1 - 255.255.255.192

Network address 192.168.1.64
First Host address 192.168.1.65
Last Host address 192.168.1.126
Broadcast address 192.168.1.127

Logical network 2 - 255.255.255.192

Network address 192.168.1.128
First Host address 192.168.1.129
Last Host address 192.168.1.190
Broadcast address 192.168.1.191

Logical network 3 - 255.255.255.192

Network address 192.168.1.192
First Host address 192.168.1.193
Last Host address 192.168.1.254
Broadcast address 192.168.1.255

Four Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.192

Network address 192.168.1.0
First Host address 192.168.1.1
Last Host address 192.168.1.62
Broadcast address 192.168.1.63

Logical network 1 - 255.255.255.192

Network address 192.168.1.64
First Host address 192.168.1.65
Last Host address 192.168.1.126
Broadcast address 192.168.1.127

Logical network 2 - 255.255.255.192

Network address 192.168.1.128
First Host address 192.168.1.129
Last Host address 192.168.1.190
Broadcast address 192.168.1.191

Logical network 3 - 255.255.255.192

Network address 192.168.1.192
First Host address 192.168.1.193
Last Host address 192.168.1.254
Broadcast address 192.168.1.255

Four Logical Networks

Original Addressing

192.168.1.0

255.255.255.0

Logical network 0 - 255.255.255.192

Network address 192.168.1.0
First Host address 192.168.1.1
Last Host address 192.168.1.62
Broadcast address 192.168.1.63

Logical network 1 - 255.255.255.192

Network address 192.168.1.64
First Host address 192.168.1.65
Last Host address 192.168.1.126
Broadcast address 192.168.1.127

Logical network 2 - 255.255.255.192

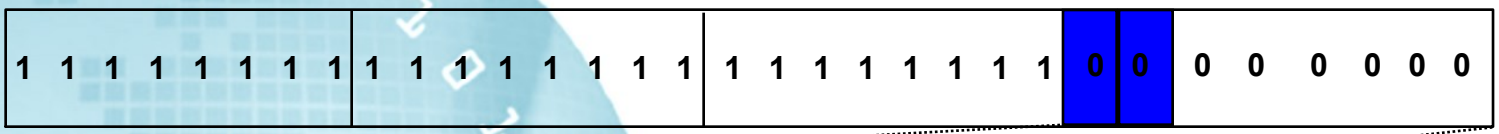
Network address 192.168.1.128
First Host address 192.168.1.129
Last Host address 192.168.1.190
Broadcast address 192.168.1.191

Logical network 3 - 255.255.255.192

Network address 192.168.1.192
First Host address 192.168.1.193
Last Host address 192.168.1.254
Broadcast address 192.168.1.255

Four Logical Networks

Address	192 . 168 . 1 . 0
Subnet Mask	255 . 255 . 255 . 192

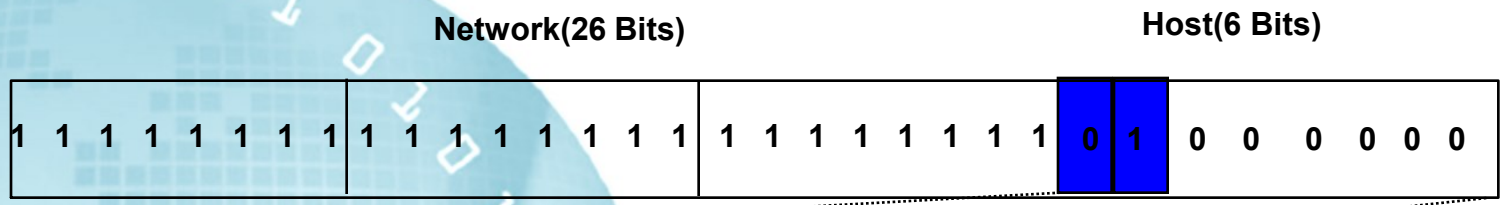


	128	64	32	16	8	4	2	1		
Logical Network 0	0	0	0	0	0	0	0	0	=	0
First Host	0	0	0	0	0	0	0	1	=	1
Last Host	0	0	1	1	1	1	1	0	=	62

For the hosts on subnet 0 you can use the range of addresses from .0 to .62; broadcast address 192.168.1.63

Four Logical Networks

Address	192 . 168 . 1 . 64
Subnet Mask	255 . 255 . 255 . 192

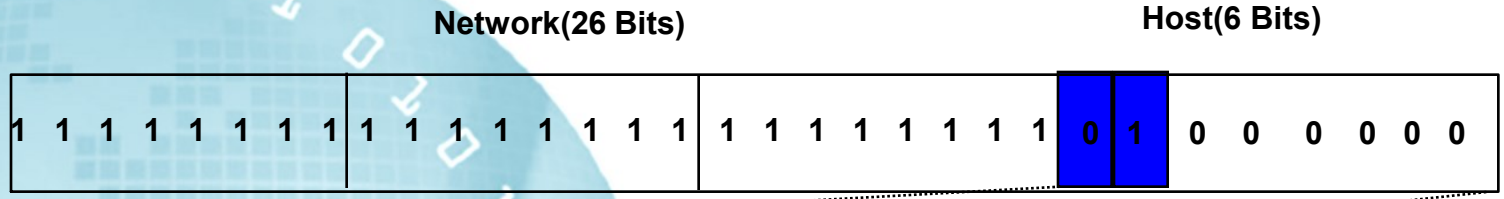


	128	64	32	16	8	4	2	1		
Logical Network 1	0	1	0	0	0	0	0	0	=	64
First Host	0	1	0	0	0	0	0	1	=	65
Last Host	0	1	1	1	1	1	1	0	=	126

For the hosts on subnet 1 you can use the range of addresses from .65 to .126; broadcast address 192.168.1.127

Four Logical Networks

Address	192 . 168 . 1 . 64
Subnet Mask	255 . 255 . 255 . 192

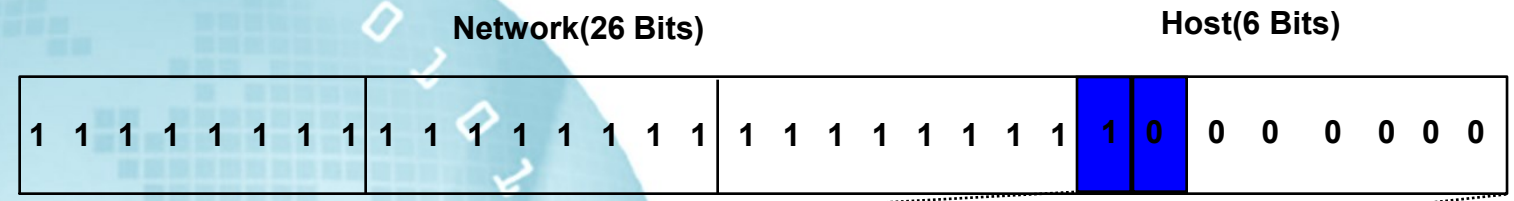


	128	64	32	16	8	4	2	1		
Logical Network 1	0	1	0	0	0	0	0	0	=	64
First Host	0	1	0	0	0	0	0	1	=	65
Last Host	0	1	1	1	1	1	1	0	=	126

For the hosts on subnet 1 you can use the range of addresses from .65 to .126; broadcast address 192.168.1.127

Four Logical Networks

Address	192 . 168 . 1 . 128
Subnet Mask	255 . 255 . 255 . 192



	128	64	32	16	8	4	2	1		
Logical Network 2	1	0	0	0	0	0	0	0	=	128
First Host	1	0	0	0	0	0	0	1	=	129
Last Host	1	0	1	1	1	1	1	0	=	190

For the hosts on subnet 2 you can use the range of addresses from .129 to .190; broadcast address 192.168.1.191

Four Logical Networks

Address	192 . 168 . 1 . 192
Subnet Mask	255 . 255 . 255 . 192

	Network(26 Bits)																Host(6 Bits)						
Address	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

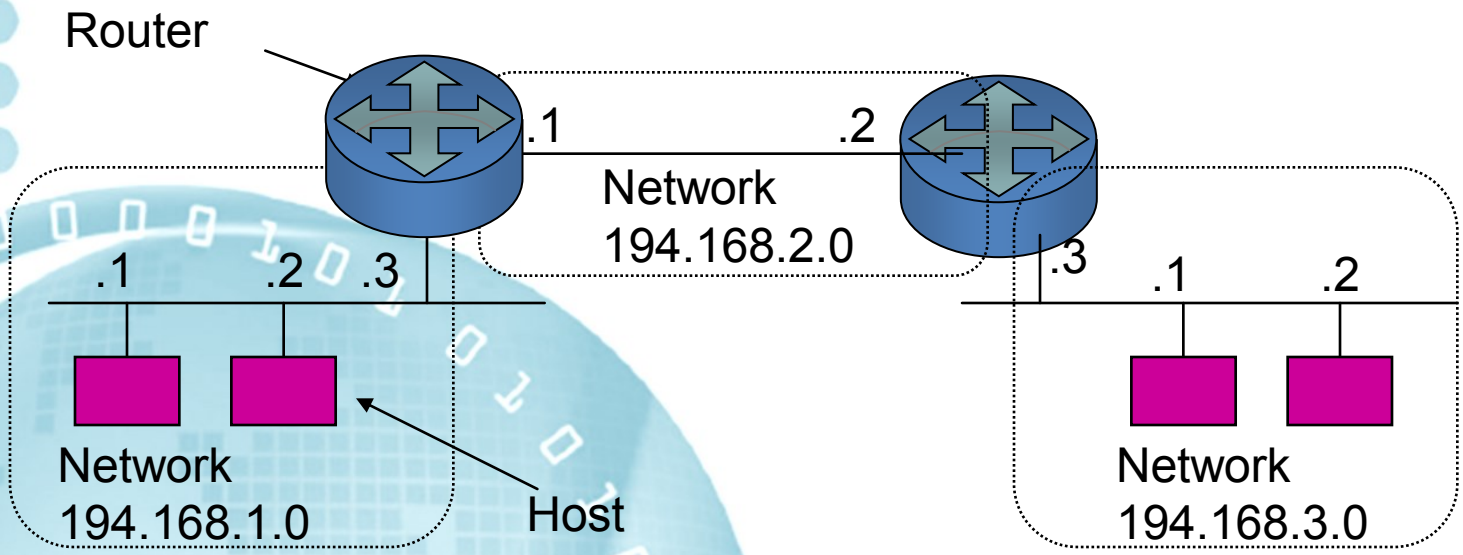
	128	64	32	16	8	4	2	1		
Logical Network 3	1	1	0	0	0	0	0	0	=	192
First Host	1	1	0	0	0	0	0	1	=	193
Last Host	1	1	1	1	1	1	1	0	=	254

For the hosts on subnet 3 you can use the range of addresses from .193 to .254; broadcast address 192.168.1.255

Subnet Masks - Binary Representation

Decimal	Hex	Binary
.128	80	10000000
.192	C0	11000000
.224	D0	11100000
.240	F0	11110000
.248	F8	11111000
.252	FC	11111100
.254	FE	11111110
.255	FF	11111111

Subnetting Example



- Consider three networks with class C addresses and default subnet mask (255.255.255.0)
- How can we use only one class C network to obtain at least three subnets?

Exercises on IP Addressing

1. Choose one class B IP address from the following network IP addresses
   192.168.1.0 - 198.124.144.0 - 146.44.63.0 - 10.10.1.0
2. Which is the default subnet mask for class B IP addresses?
3. Now modify the subnet mask number to obtain subnets with at most 6 hosts for each subnet; find the right one among the following subnet numbers
   255.255.128.0 - 255.255.248.0 - 255.255.255.248

- Remember that in the range of IP addresses there must always be a network address and a broadcast address

Exercises on IP Addressing

1. Choose one class B IP address from the following network IP addresses
   192.168.1.0 - 198.124.144.0 - 146.44.63.0 - 10.10.1.0
2. Which is the default subnet mask for class B IP addresses?
3. Now modify the subnet mask number to obtain subnets with at most 6 hosts for each subnet; find the right one among the following subnet numbers
   255.255.128.0 - 255.255.248.0 - 255.255.255.248

- Remember that in the range of IP addresses there must always be a network address and a broadcast address

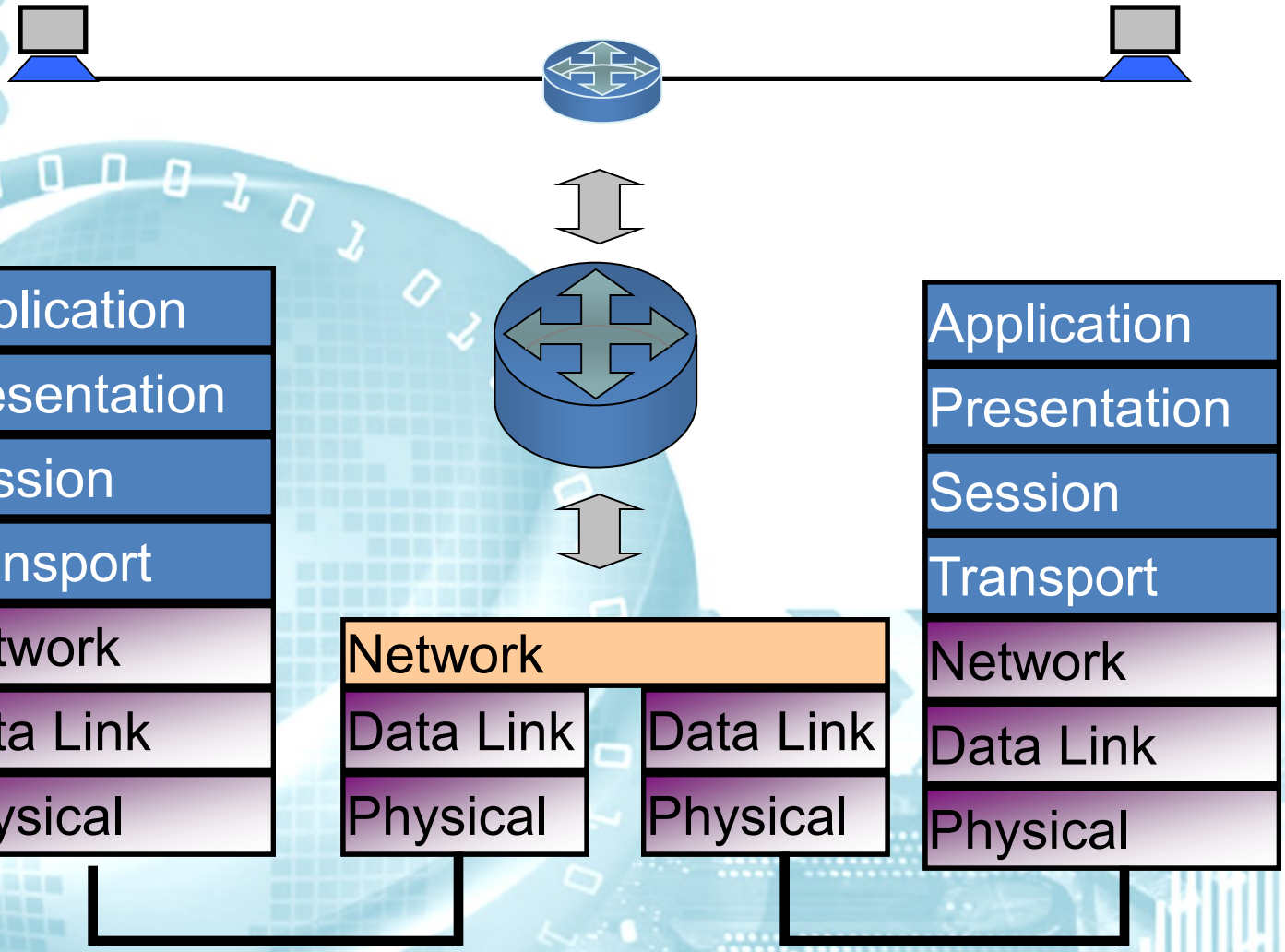
EISTI
Ecole Internationale des Sciences du Traitement de l'Information

How Routers Work

How Routers Work

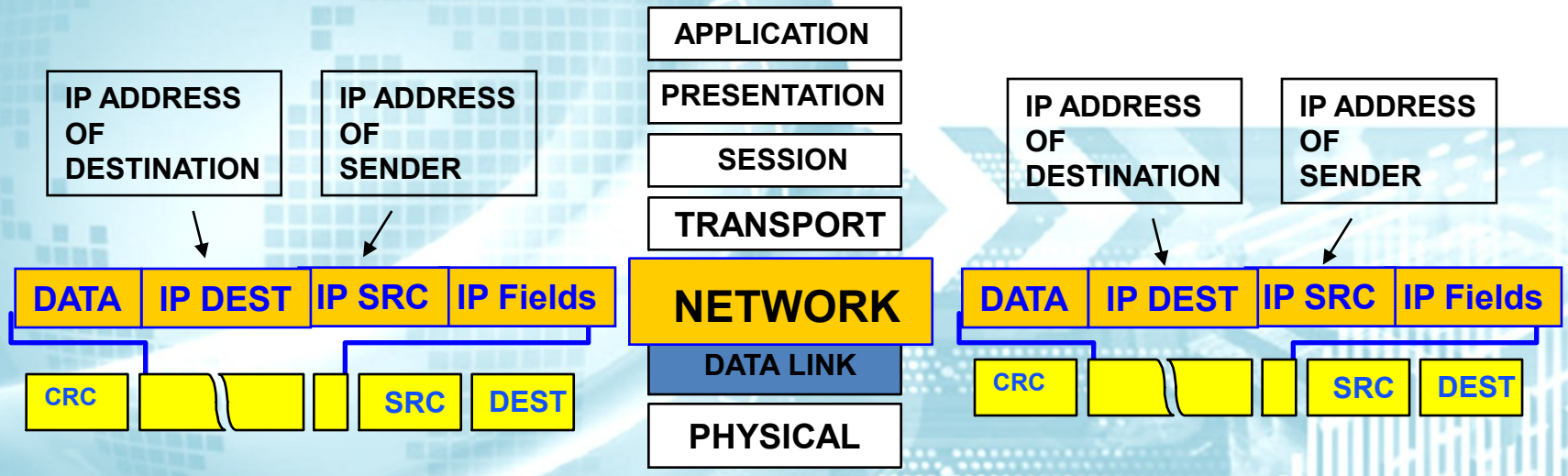
- A router works at the Network Layer
- Routers understand Network Layer Protocols and transfer data based on logical network addresses
- A router is able to take more intelligent routing decisions than bridges, based on higher layer protocols

Intermediate System



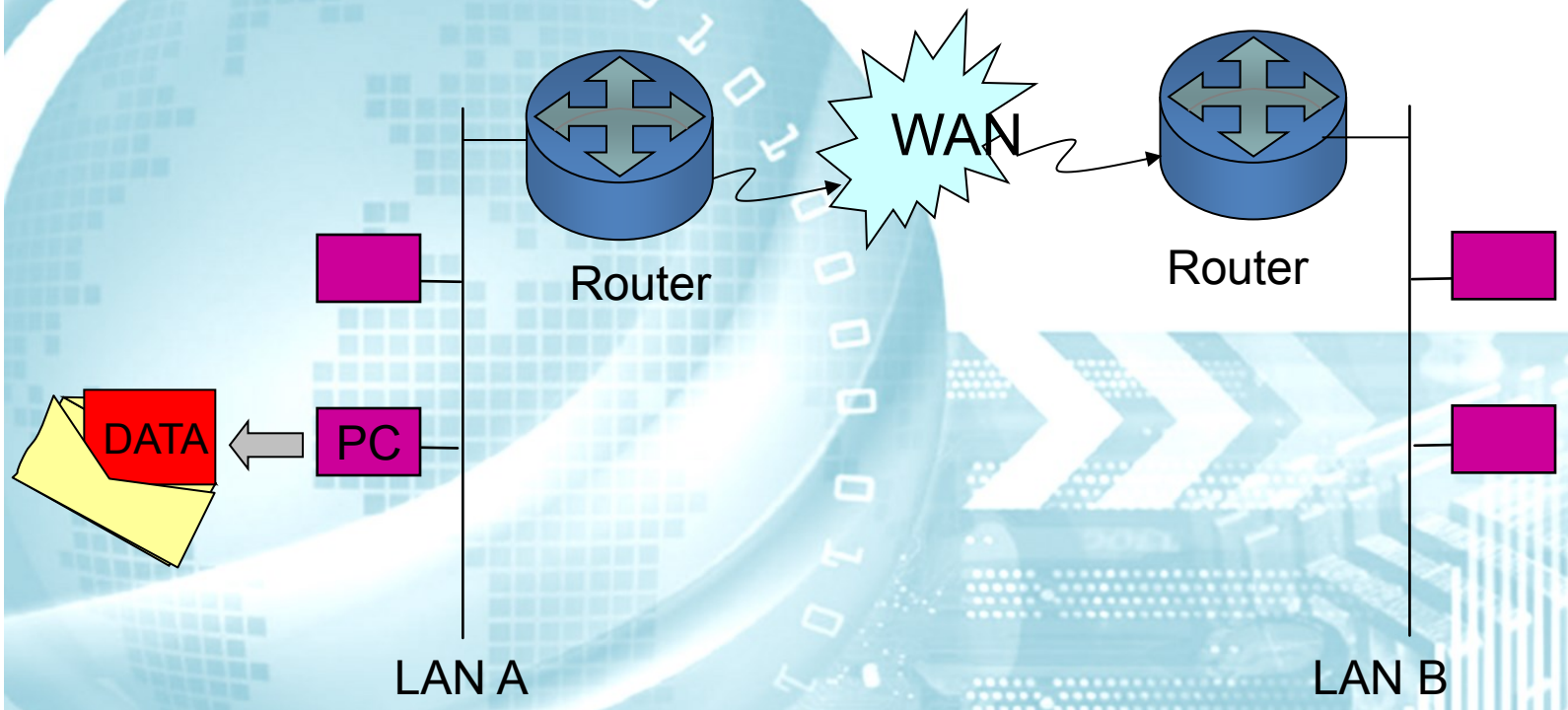
Routing by Network Address

- Routers are Intermediate Systems that read Network Layer Information to forward packets
- Routers use the destination address as access key to the routing table
- This technique used in IP, Decnet and OSI



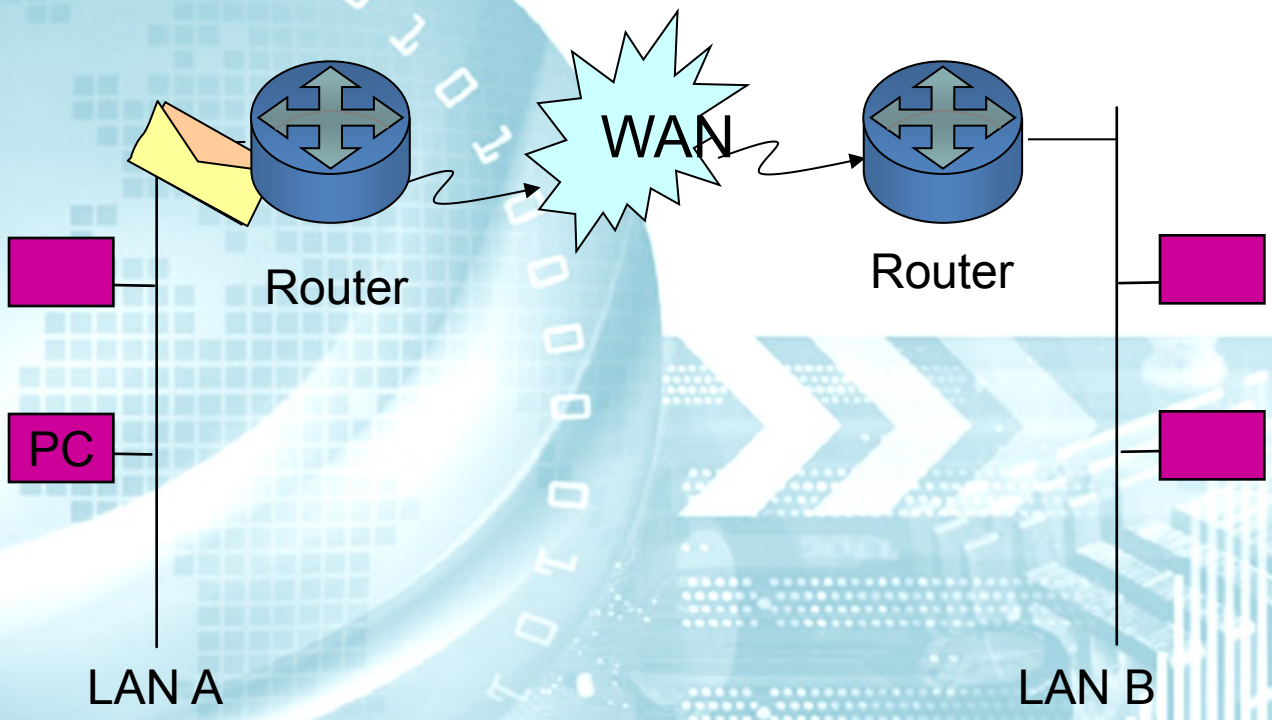
How Routers Work

- Data is encapsulated in a Layer 3 protocol by the PC



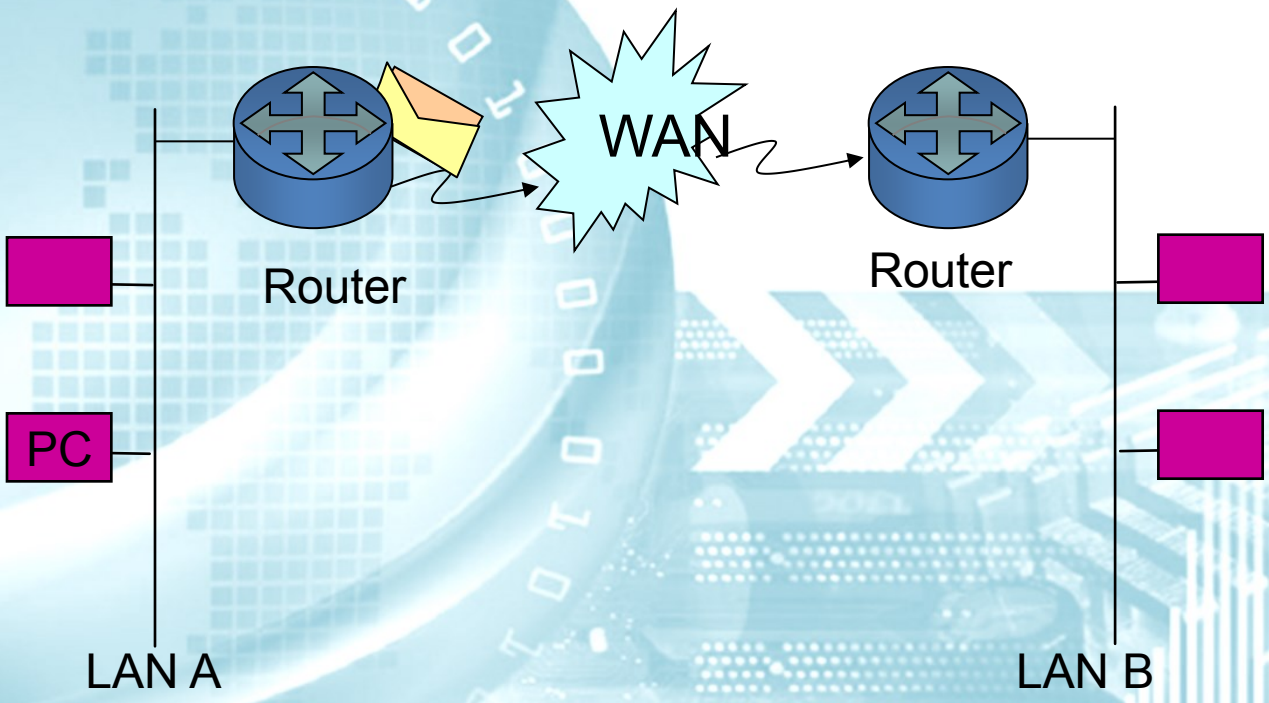
How Routers Work

- This is transmitted across the LAN to the router



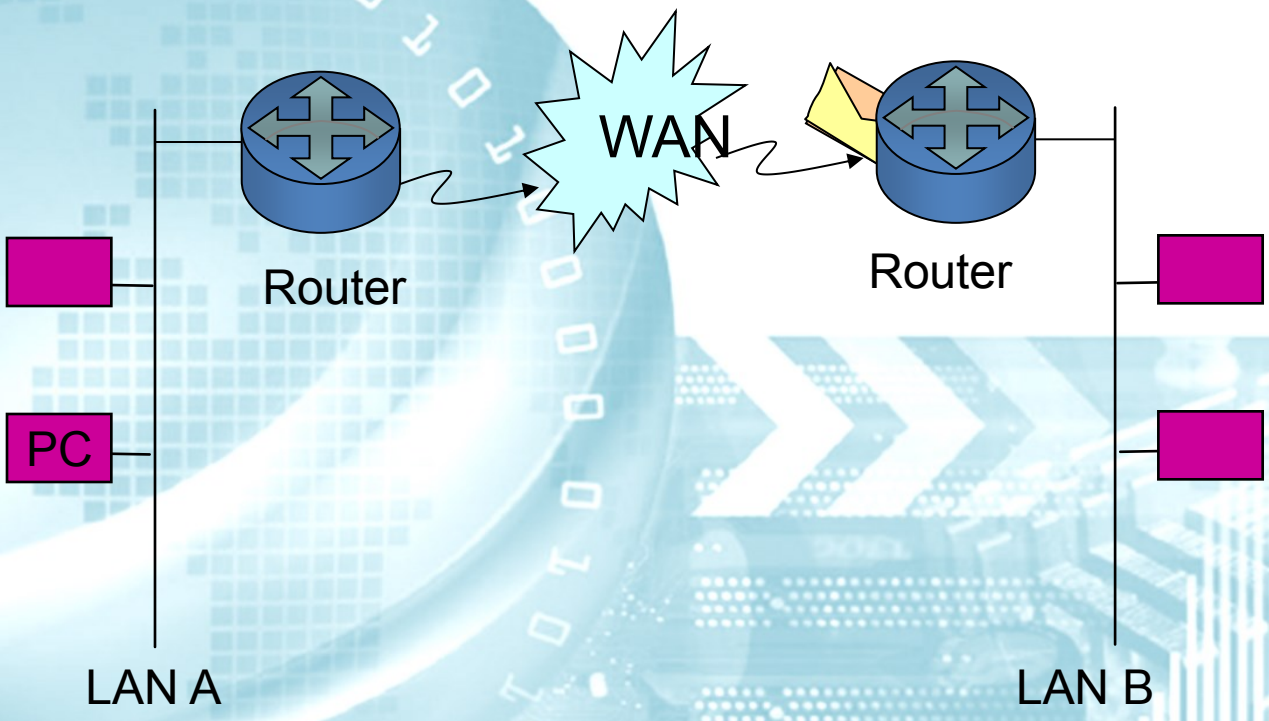
How Routers Work

- The router reads the Layer 3 address, reads the routing table and forwards this packet containing the data to a queue awaiting transmission across the WAN



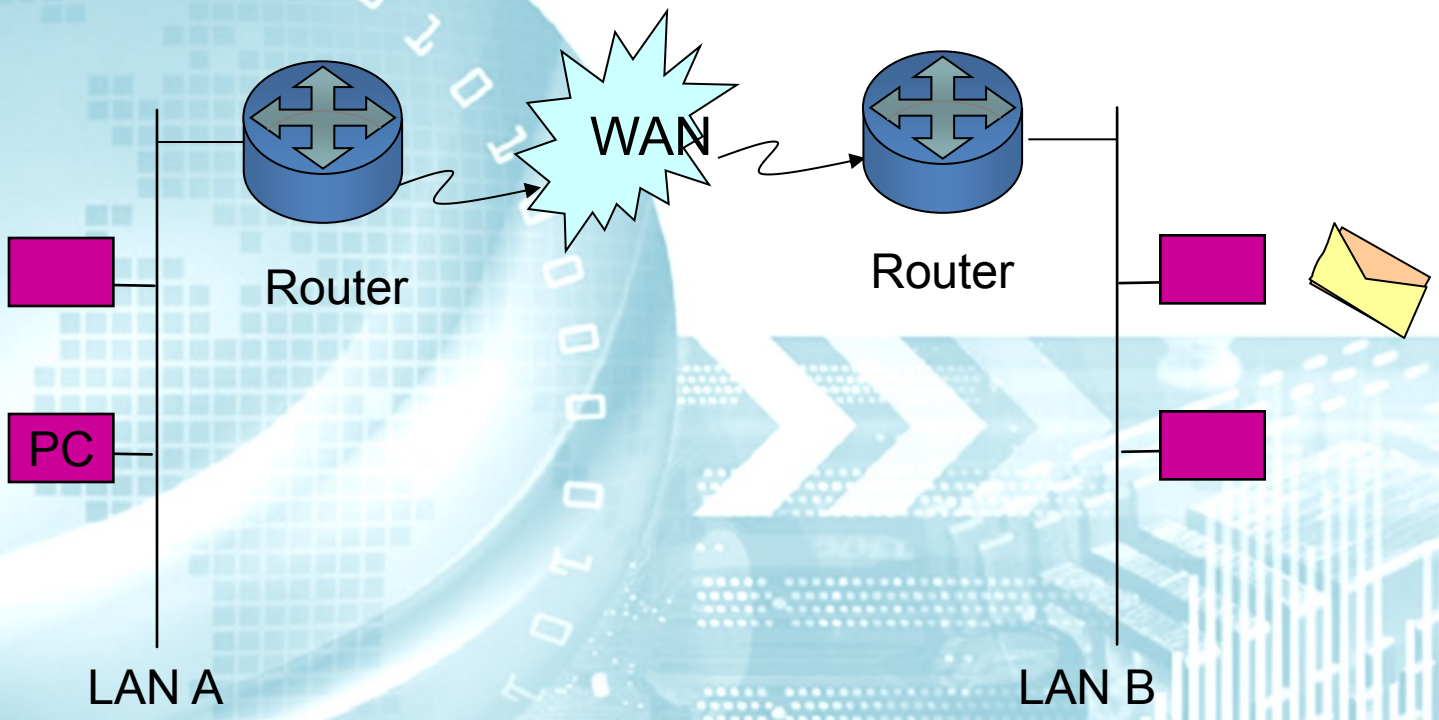
How Routers Work

- The Layer 3 packet containing the data is transported across the WAN to the router connected to the destination network



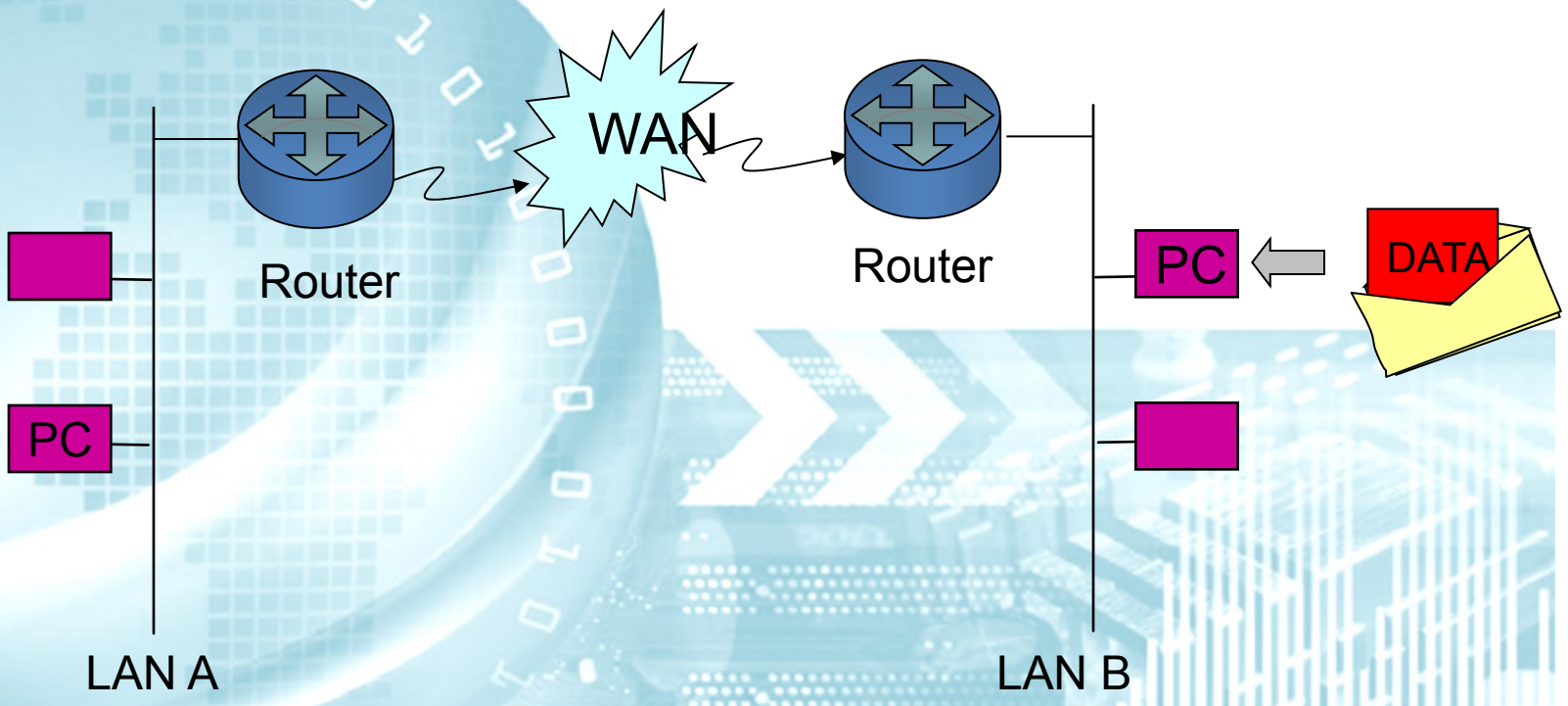
How Routers Work

- The router on the destination network reads the Layer 3 address and forwards the packet via a queue across the LAN to the destination host



How Routers Work

- The destination host reads data from the Layer 3 packet and the data contained can be used by upper layer protocols

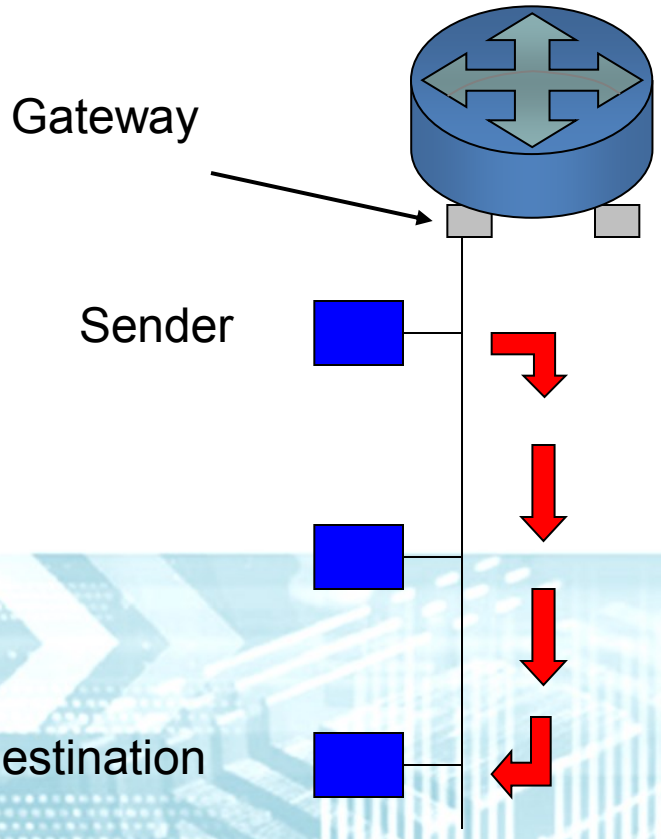


Routing operations

- It is possible to identify three different processes
  - Datagram delivery
  - Direct routing
  - Indirect routing

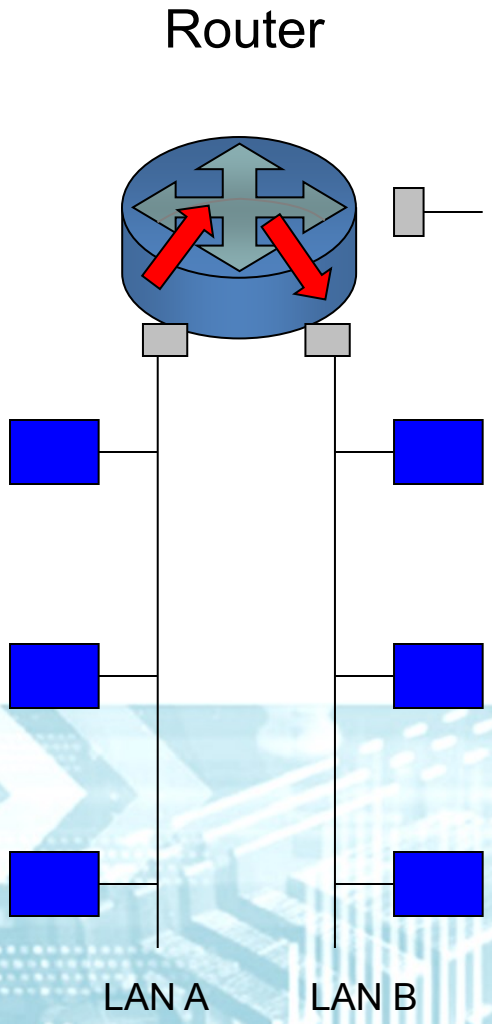
Datagram Delivery

- Transmission of an IP datagram between two machines on a single network does not involve gateways (routers)
- The sender encapsulates the datagram in a physical network frame, binds the destination IP address to a physical hardware address and sends the resulting frame directly to the destination
- Each PC can reach all the other ones without routing



Direct Routing

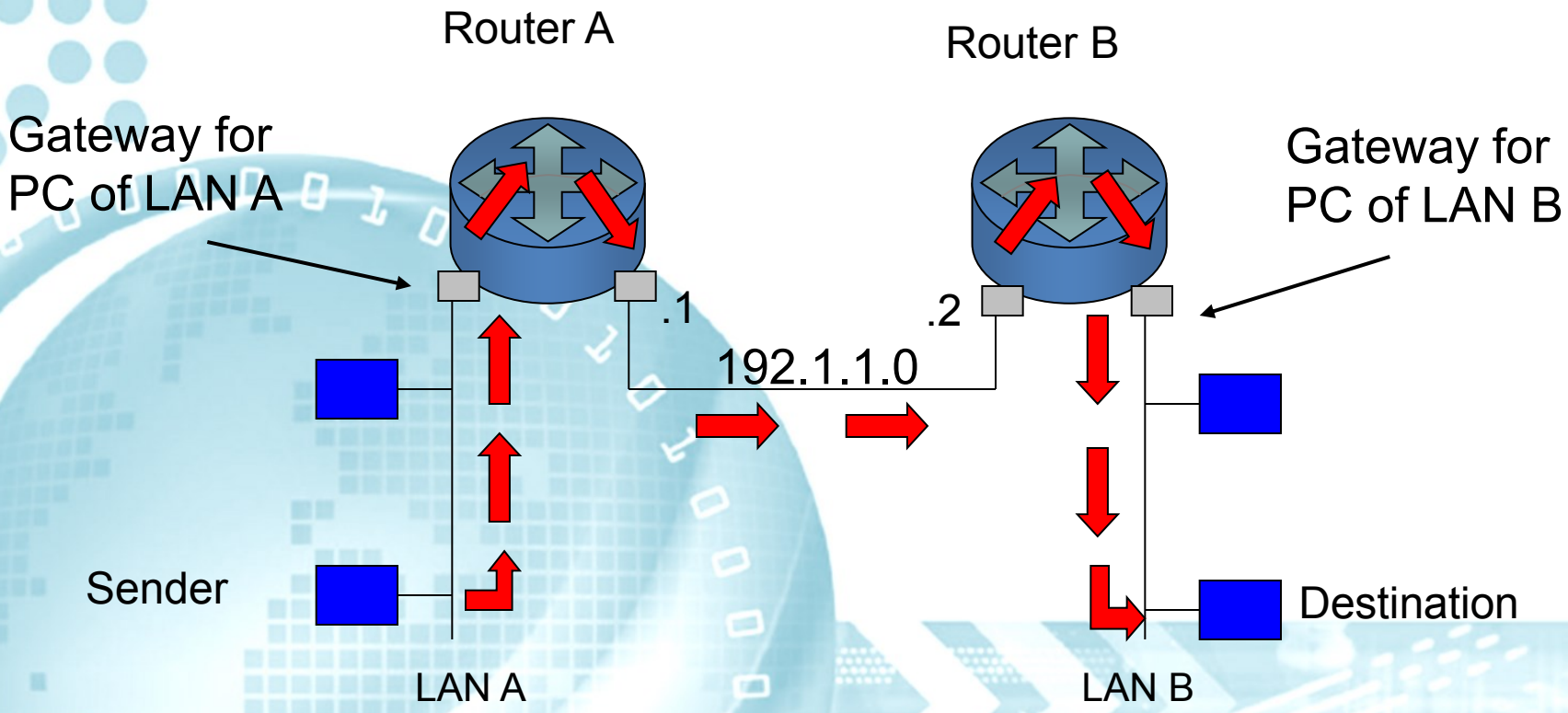
- All PCs on LAN A are able to communicate with all PCs on LAN B without routing instructions on the router
  - configure LAN interfaces Eth0 (LAN A) and Eth1 (LAN B) on the router
  - configure every PC with the right IP address and gateway number (IP address of the Eth interface)



Indirect Routing

- Transmission of an IP datagram between two machines on different networks is achieved via gateways (routers)
- With indirect routing, the sender must identify a router to which the datagram can be sent (gateway address)
- Routers in a TCP/IP internet form a cooperative, interconnected structure: datagrams pass from router to router until they reach a router that can deliver the datagram directly

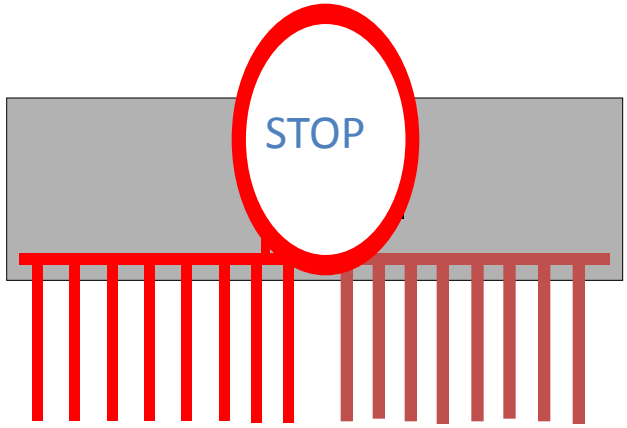
Indirect Routing



- To allow packets to be forwarded from the sender to the destination, it is necessary to add a routing instruction to the routers, so that they know the path that traffic must follow

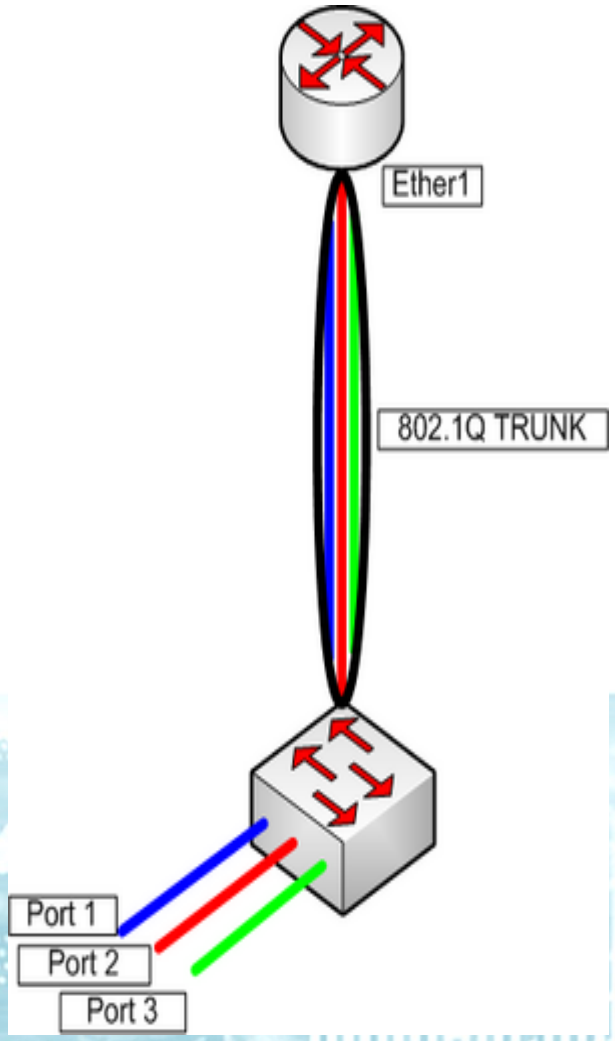
What's a L3 Switch?

- VLANs - security features
- Layer 2 switch no traffic can pass from one VLAN to another
- In the majority of real world applications, some traffic needs to pass from one VLAN to another, typically these include:
  - printers
  - file servers
  - backup servers
  - IT administrators



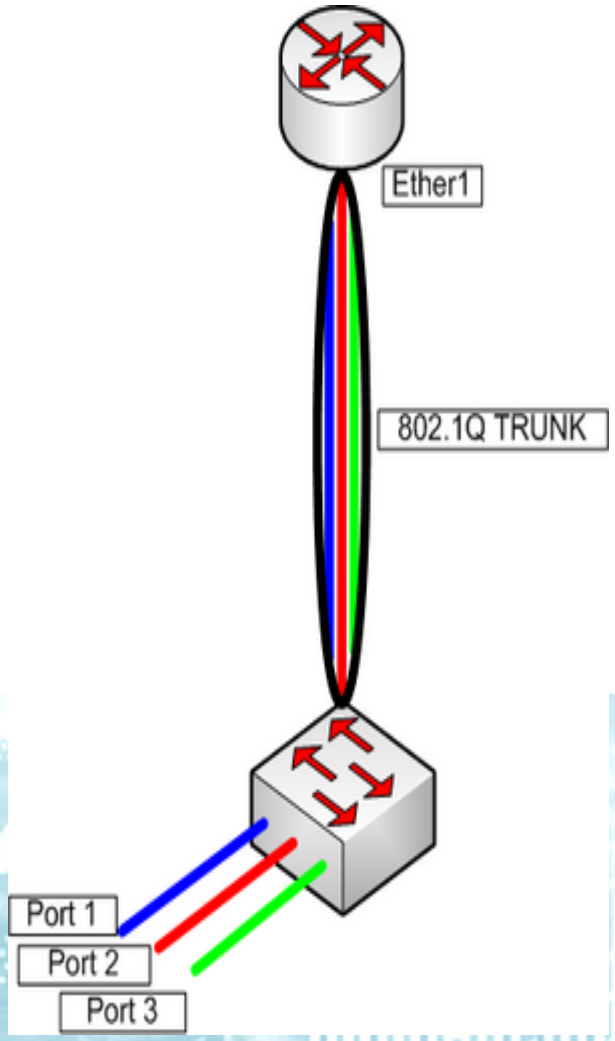
Communicating between VLANs

- External router could route between VLANs…
  - Require a physical interface per VLAN or 802.1q
  - Router are not optimize for routing high traffic between vlans



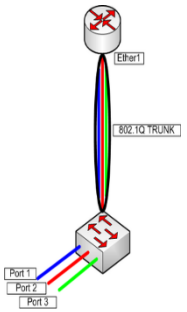
Communicating between VLANs

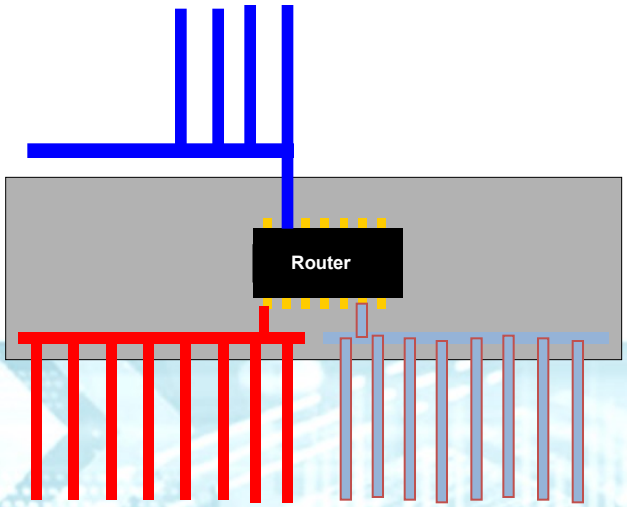
- External router could route between VLANs…
  - Require a physical interface per VLAN or 802.1q
  - Router are not optimize for routing high traffic between vlans



Layer 3 Switches

- Layer 3 switches forward traffic between VLANs without the problems associated with external routers
  - Scalable without need for dedicated port per interface
  - Uses hardware routing ASIC chips forwarding at Gigabit wire speeds.





EISTI
Ecole Internationale des Sciences du Traitement de l'Information

NAT

Network Address Translation

NAT

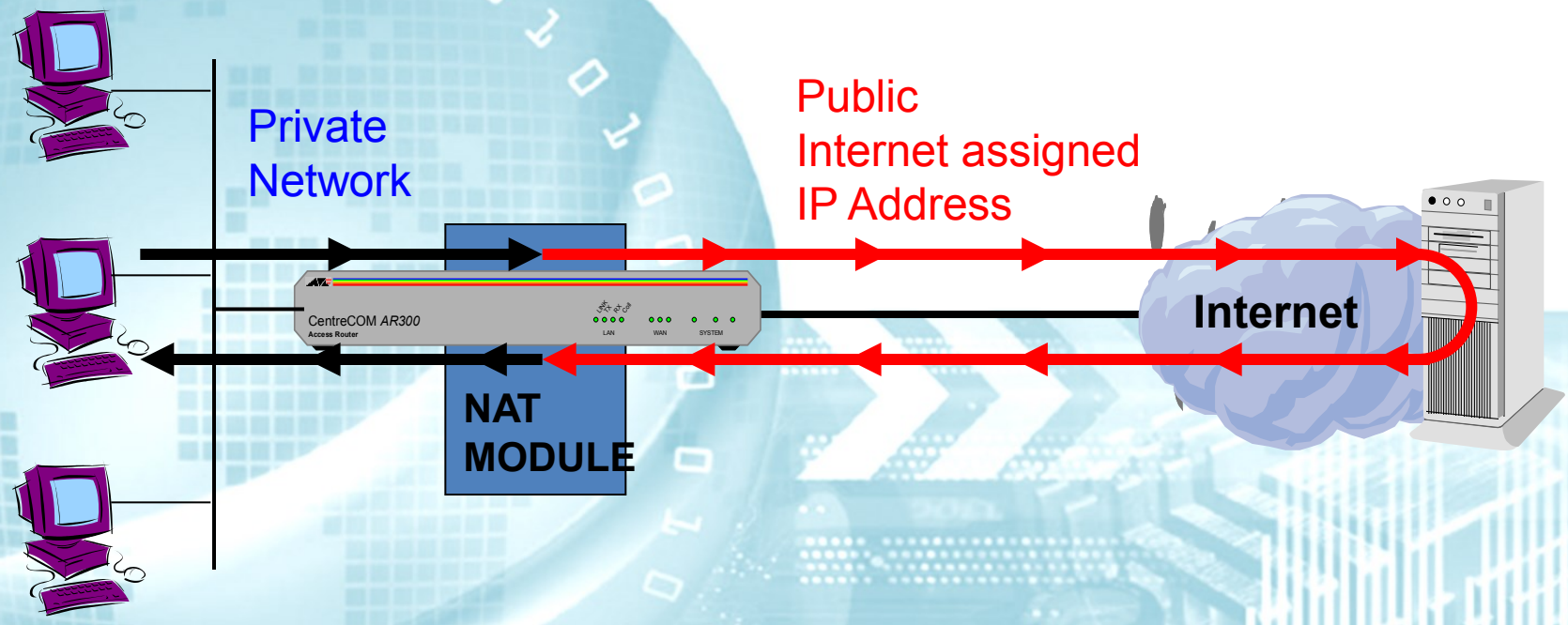
- With NAT, multiple users can connect to Internet using a single IP address
- All IP addresses of the users are translated into one IP global address
- In this way, we can reduce connection costs

NAT

- With NAT, multiple users can connect to Internet using a single IP address
- All IP addresses of the users are translated into one IP global address
- In this way, we can reduce connection costs

NAT

- Addresses are translated automatically between the private and the public network



EISTI
Ecole Internationale des Sciences du Traitement de l'Information

DHCP

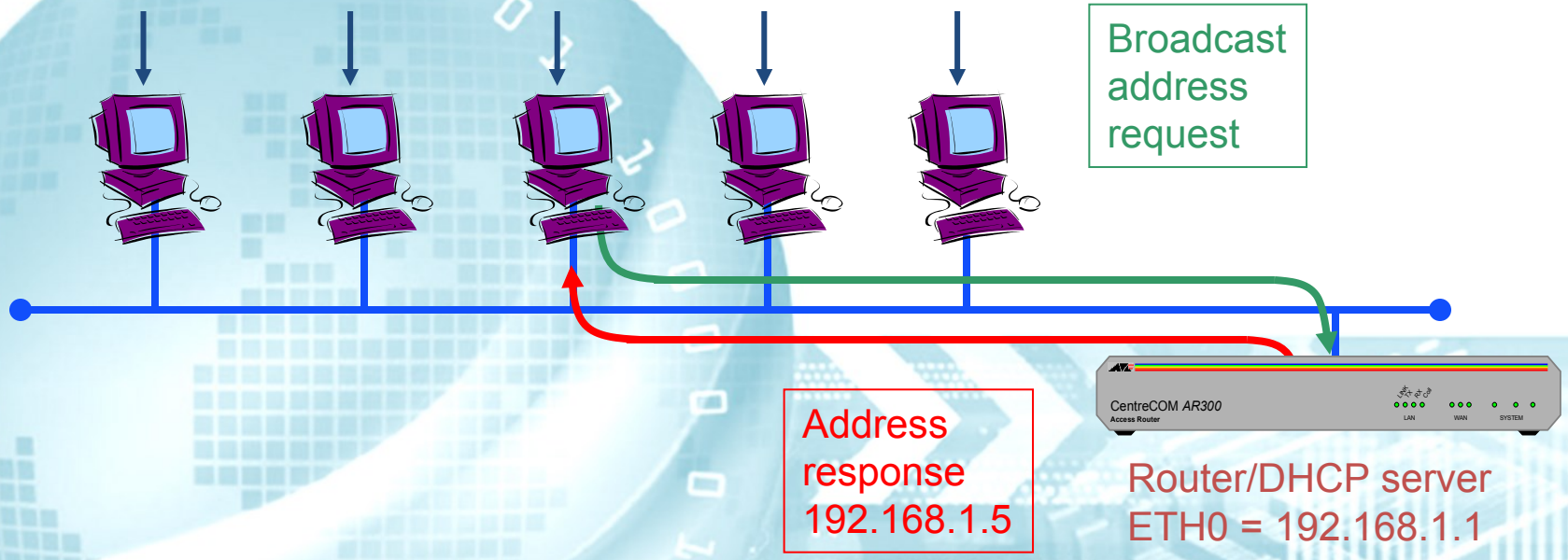
Dynamic Host Configuration Protocol

DHCP

- The Dynamic Host Configuration Protocol provides a method for assigning configuration information to hosts on a TCP/IP network
- The IP configuration is stored on the router (DHCP server), and sent to hosts when they are switched on (DHCP clients)
- With the DHCP function, network management becomes easier, because you need to configure only the router and not every PC

DHCP Server

IP addresses dynamically allocated from address pool in DHCP server 192.168.1.5 to 192.168.1.15



```
option netbios-name-servers 192.168.3.25;
option ntp-servers 193.48.70.2;
option netbios-node-type 2;
ddns-update-style none;
authoritative;

###############################################
# Manifestations Privés
# gateway pour les machines : 192.168.122.1 ( gate 2 )
# Reseau naté
###############################################
subnet 192.168.122.0 netmask 255.255.255.0
    {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.122.255;
    option routers 192.168.122.1;
    option domain-name-servers 193.48.70.2,194.57.186.254;
    option domain-name "evenement.cergy.eisti.fr";
    max-lease-time 1200;
    default-lease-time 600;
    range 192.168.122.10 192.168.122.254;

    # FCA : Netboot
    ## Netboot Linux
    filename "pxelinux.0";
    next-server 194.57.186.254;

    group #admin ( adresse reserve pour le materiel et
l'administration
        {
        host router
            {
            hardware ethernet 00:1b:21:24:64:31;
            fixed-address 192.168.122.1;
            }
        host switch-tg0.evenement.cergy
            {
            hardware ethernet 00:00:00:00:00:01;
            fixed-address 192.168.122.2;
            }
        }
    group # clients
        {
        # 10 a 254 range
        }
}
```

```
###############################################
# CCR Privé
# gateway pour les:machines : 192.168.252.1
###############################################
subnet 192.168.252.0 netmask 255.255.255.0
    {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.252.255;
    option routers 192.168.252.1;
    option domain-name-servers 193.48.70.2,194.57.186.254;
    option domain-name "ccr.eisti.fr";
    # FCA : Valeurs initiales
    max-lease-time 1200;
    default-lease-time 600;
    range 192.168.252.160 192.168.252.254;


    # FCA : Netboot
    ## Netboot Linux
    filename "pxelinux.0";
    next-server 194.57.186.254;

    ## Netboot Windows
    #next-server 193.48.70.105;
    #filename "boot\\x64\\wdsnbp.com";
    # FCA : Fin netboot

    group #Admin
        {
        host TestNagiosDHCP-ccr # pour test nagios adresse facti ne
pas toucher
            {
            hardware ethernet 00:FF:AB:CD:DE:EF;
            fixed-address 192.168.252.1;
            }
        host routeurv6_1
            {
            hardware ethernet 01:c0:17:31:bc:09;
            fixed-address 192.168.252.9;
            }
        host onduleur-tg0
            {
            hardware ethernet 00:03:05:18:20:1E;
            fixed-address 192.168.252.10;
            }
        }
   }
```

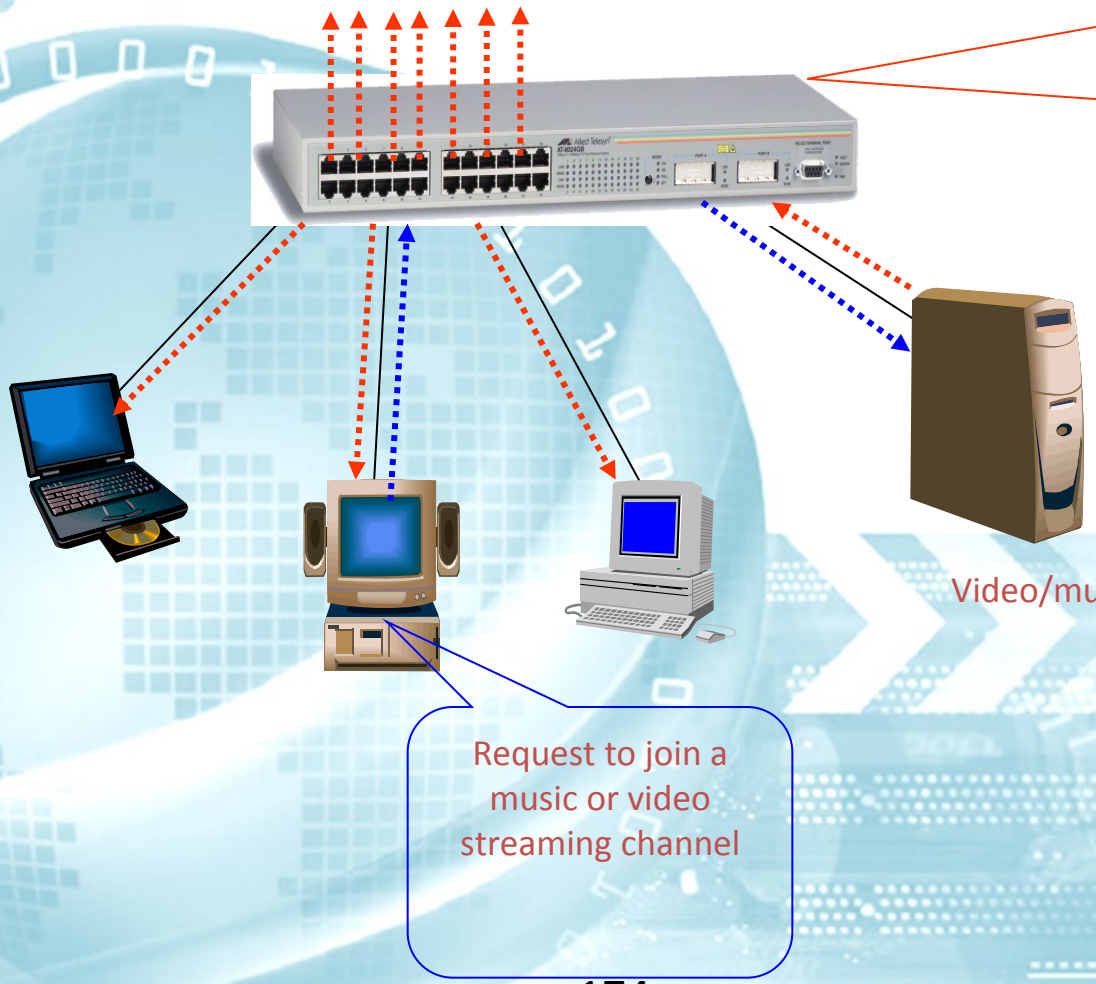
EISTI
Ecole Internationale des Sciences du Traitement de l'Information

Multicast

Multicast

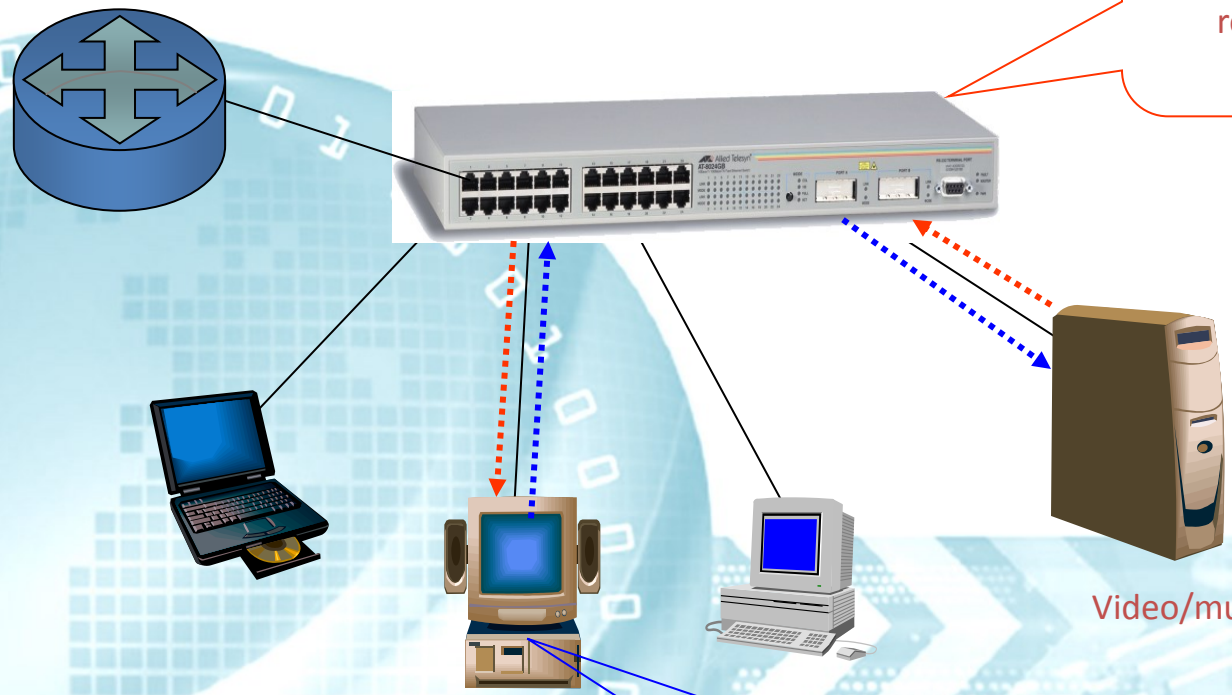
- It is the process of transmitting an IP datagram to a group of hosts
- A host group may contain zero or more hosts
- Packets sent to a group address are only received by members of that group
- A multicast datagram is received by each member of the group as if the datagram had been sent individually to each host as a unicast datagram
- A host group is identified by a single IP address
- Multicast addresses are in the range
  - 224.0.0.0 through 239.255.255.255

Without Multicast



With Multicast

- Router or L3 Switch with multicast support

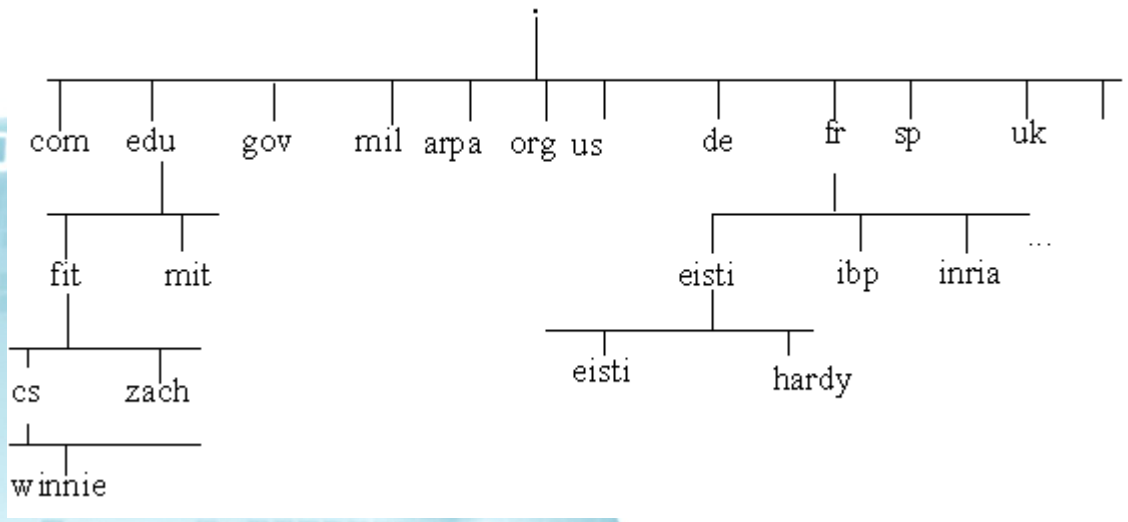


Switch recognizes multicast packet and sends data only to requesting station

Video/music Server

Request to join a music or video streaming channel

Domain Name Services



- Le nom qualifié ou complet (FQDN) d'une machine se lit en partant de la feuille et en remontant dans l'arbre. Chaque niveau est séparé par un "." Ainsi la machine sur laquelle vous avez programmé s'appelle hardy.eisti.fr.
- Le domaine racine n'a pas de nom et par convention est appelé "."

Résolution DNS

- Le fonctionnement du résolveur est très simple. Il est basé sur le modèle client serveur.
- Dans chaque domaine, il y a une (ou plusieurs) machine(s) appelé(s) *SERVEUR DNS* qui connaît l'adresse de toutes les machines de son domaine et les adresses des serveurs de ses sous-domaines.
- Pour trouver l'adresse IP de la machine ayant pour nom A.B.C.D.FR le client :
  - Regarde dans son cache si on ne dispose pas de l'info
  - Sinon demander à ,son résolveur (cf: dhcp, configuration manuelle des résolveurs).
  - Le résolveur Regarde dans son cache s'il ne dispose pas de l'info sinon
    - Interroge le serveur de FR pour soit avoir l'ip de a.b.c.d.fr (peu probable)
    - Interroge le serveur de FR pour soit avoir l'ip du serveur de d.fr
    - Interroge le serveur de d.fr …..
    - ….

Résolution DNS inverse

- BUT:
  - Connaitre le nom connaissant une IP
- Fonctionnement:
  - Inversion de l'IP « a.b.c.d » devient d.c.b.a
  - Interrogation ds serveurs DNS pour obtenir l'enregistrement *PTR* de d.c.b.a.in-addr.arpa.

Application résolution et résolution inverse

- Une machine avec une IP héberge plusieurs serveurs web de non différents …
  - Virtual host sur apache par exemple
    - Arel.eisti.fr -> 193.48.70.4
    - Glpi.eisti.fr ->193.48.70.4
    - …
- Sécurisation des communications
  - double interrogation IP ->Nom puis Nom->IP

WINS

(Windows Internet Naming Service)

- Un serveur de noms et services pour les ordinateurs utilisant NetBIOS. (IE windows)
- *Netbios est un protocole qui ne traverse pas les routeurs.*

  Comment avoir l'IP d'un nom netbios derrière un routeur ?

  -> Chaque poste s'enregistre sur le serveur WINS

  -> Les clients interrogent le serveur WINS

- Depuis windows 2000 les postes sont censé utiliser *l'AD.*

Routage statique

- Un administrateur renseigne sur le(s) routeurs les routes vers des réseaux.
  - Ip route add sous linux …☺

- Bien lorsque peu de routes
- Sources d'erreurs

Routage dynamique

- Les routeurs échangent entre eux (s'ils sont configurés pour le faire) leurs routes connues
  - RIP peu utiliser …
  - BGP (Border Gateway Protocol)
    Echange de routes entre des passerelles en bordures de LAN opéré généralement par des opérateurs différents. On parle dans ce cas de E (exterior) BGP
    http://fr.wikipedia.org/wiki/Border_Gateway_Protocol
  - OSPF (Open Shortest Path First)
    Echange de routes entre serveurs généralement utilisé à l'intérieur d'un même LAN
    http://fr.wikipedia.org/wiki/Open_Shortest_Path_First

Exemple de tables de routage

Gate

```
Hello, this is Quagga (version 0.99.20.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

gate# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
B>* 141.44.38.2/32 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
B>* 153.109.124.23/32 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
C>* 172.16.0.0/16 is directly connected, eth9
B>* 172.17.0.0/16 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
B>* 172.21.0.0/16 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
B>* 172.22.0.0/16 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
O>* 172.23.0.0/18 [110/20] via 192.168.254.1, eth0, 01w4d22h
O>* 172.23.64.0/18 [110/20] via 192.168.254.1, eth0, 02w1d21h
O>* 172.23.128.0/18 [110/20] via 192.168.254.1, eth0, 01w4d22h
O>* 172.23.192.0/18 [110/20] via 192.168.254.1, eth0, 02w1d21h
O>* 172.24.0.0/18 [110/20] via 192.168.254.1, eth0, 01w4d22h
O>* 172.24.64.0/18 [110/20] via 192.168.254.1, eth0, 02w1d21h
O>* 172.24.128.0/18 [110/20] via 192.168.254.1, eth0, 01w4d22h
O>* 172.24.192.0/18 [110/20] via 192.168.254.1, eth0, 02w1d21h
C>* 192.168.1.0/30 is directly connected, to-pau-1
S>* 192.168.1.8/29 [1/0] is directly connected, lo
O>* 192.168.2.0/24 [110/20] via 192.168.254.1, eth0, 11w0d19h
C>* 192.168.3.0/24 is directly connected, eth13
O>* 192.168.6.0/24 [110/20] via 192.168.254.1, eth0, 11w5d02h
S>* 192.168.10.0/24 [1/0] via 193.48.70.5, eth5
C>* 192.168.11.0/24 is directly connected, eth11
O>* 192.168.13.0/26 [110/20] via 192.168.254.1, eth0, 11w5d06h
O>* 192.168.14.0/24 [110/20] via 192.168.254.1, eth0, 12w2d03h
O>* 192.168.15.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
S>* 192.168.16.0/24 [1/0] via 194.57.186.19, eth3
O>* 192.168.17.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
C>* 192.168.20.0/24 is directly connected, eth8
O>* 192.168.21.0/25 [110/20] via 192.168.254.1, eth0, 12w2d07h
O>* 192.168.25.0/24 [110/20] via 192.168.254.1, eth0, 11w1d07h
O>* 192.168.26.0/24 [110/20] via 192.168.254.1, eth0, 11w5d01h
O>* 192.168.32.0/23 [110/20] via 192.168.254.1, eth0, 12w2d07h
S   192.168.32.0/23 [1/0] via 192.168.252.7 inactive
O>* 192.168.42.0/24 [110/20] via 192.168.254.1, eth0, 11w5d01h
O>* 192.168.70.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
S>* 192.168.121.0/28 [1/0] via 194.199.237.84, eth6
S>* 192.168.121.16/28 [1/0] via 194.199.237.84, eth6
O>* 192.168.122.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
S>* 192.168.123.0/24 [1/0] via 194.199.237.115, eth6
B>* 192.168.128.0/18 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
S>* 192.168.201.0/24 [1/0] via 192.168.1.2, to-pau-1
O>* 192.168.250.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
O>* 192.168.251.0/29 [110/20] via 192.168.254.1, eth0, 11w5d05h
O>* 192.168.251.24/29 [110/20] via 192.168.254.1, eth0, 11w5d03h
O>* 192.168.251.32/29 [110/20] via 192.168.254.1, eth0, 11w5d05h
O>* 192.168.251.40/29 [110/20] via 192.168.254.1, eth0, 11w5d05h
O>* 192.168.252.0/24 [110/20] via 192.168.254.1, eth0, 12w2d07h
O>* 192.168.253.0/24 [110/20] via 192.168.254.1, eth0, 11w5d01h
O   192.168.254.0/24 [110/10] is directly connected, eth0, 12w3d20h
C>* 192.168.254.0/24 is directly connected, eth0
O   193.48.70.0/27 [110/10] is directly connected, eth5, 12w2d02h
C>* 193.48.70.0/27 is directly connected, eth5
O>* 193.48.70.32/27 [110/20] via 192.168.254.1, eth0, 12w1d19h
C>* 193.48.70.64/26 is directly connected, eth6
B>* 193.55.155.0/24 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
B>* 194.3.242.73/32 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
C>* 194.57.172.56/29 is directly connected, eth1
C>* 194.57.186.0/24 is directly connected, eth3
K>* 194.57.186.6/32 is directly connected, eth0
O   194.199.237.0/25 [110/10] is directly connected, eth6, 12w3d20h
C>* 194.199.237.0/25 is directly connected, eth6
O>* 194.199.237.128/29 [110/20] via 192.168.254.1, eth0, 12w2d07h
S>* 194.199.237.192/27 [1/0] is directly connected, Null0, bh
O>* 194.199.237.224/27 [110/20] via 192.168.254.1, eth0, 12w2d07h
B>* 194.254.190.0/25 [20/0] via 192.168.1.2, to-pau-1, 02w0d07h
C>* 212.73.216.0/30 is directly connected, eth2
C>* 212.73.216.128/27 is directly connected, eth10
C>* 212.73.216.160/27 is directly connected, eth12
O   212.73.216.192/27 [110/10] is directly connected, eth4, 12w2d02h
C>* 212.73.216.192/27 is directly connected, eth4
O>* 212.73.216.224/27 [110/20] via 212.73.216.194, eth4, 12w2d02h
  *                            via 193.48.70.4, eth5, 12w2d02h
```

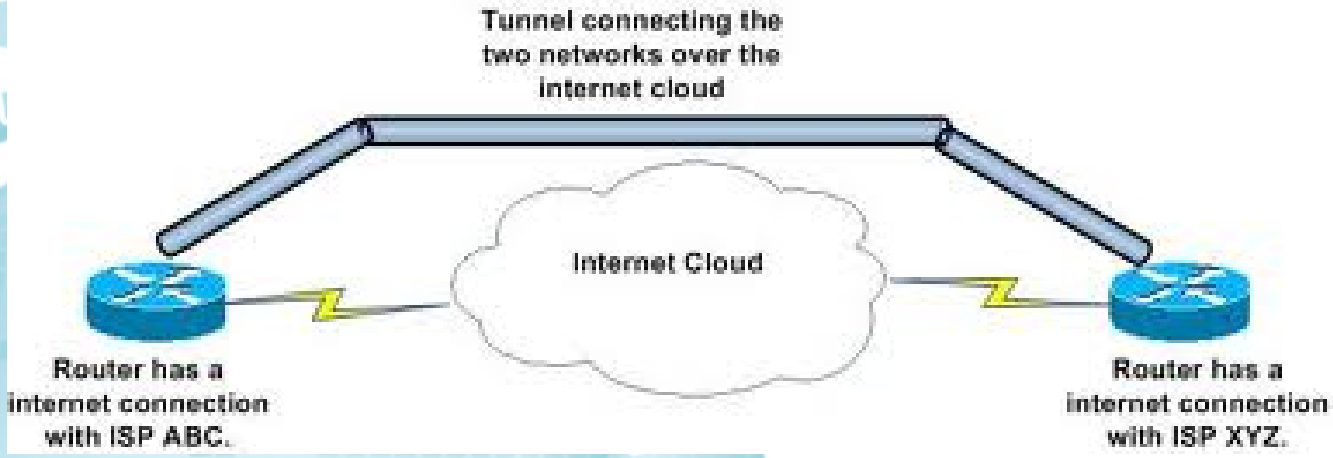
Exemple de tables de routage

EISTI
Ecole Internationale des Sciences du Traitement de l'Information

Gate2

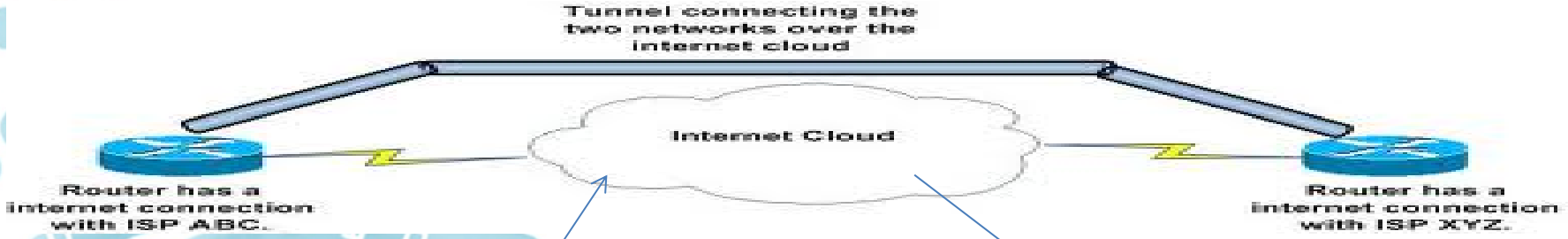
```
Hello, this is Quagga (version 0.99.20.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

K>* 0.0.0.0/0 via 192.168.254.243, eth0
C>* 127.0.0.0/8 is directly connected, lo
O>* 141.44.38.2/32 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 153.109.124.23/32 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 172.16.0.0/16 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 172.17.0.0/16 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 172.21.0.0/16 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 172.22.0.0/16 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 172.23.0.0/18 [110/20] via 192.168.252.49, eth9, 01w4d22h
O>* 172.23.64.0/18 [110/20] via 192.168.252.50, eth9, 02w1d21h
O>* 172.23.128.0/18 [110/20] via 192.168.252.49, eth9, 01w4d22h
O>* 172.23.192.0/18 [110/20] via 192.168.252.50, eth9, 02w1d21h
O>* 172.24.0.0/18 [110/20] via 192.168.252.49, eth9, 01w4d22h
O>* 172.24.64.0/18 [110/20] via 192.168.252.50, eth9, 02w1d21h
O>* 172.24.128.0/18 [110/20] via 192.168.252.49, eth9, 01w4d22h
O>* 172.24.192.0/18 [110/20] via 192.168.252.50, eth9, 02w1d21h
O>* 192.168.1.0/30 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 192.168.1.8/29 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.2.0/24 is directly connected, vlan414
O>* 192.168.3.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.6.0/24 is directly connected, vlan451
O>* 192.168.10.0/24 [110/20] via 192.168.254.243, eth0, 11w0d19h
O>* 192.168.11.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.13.0/26 is directly connected, vlan452
C>* 192.168.14.0/24 is directly connected, eth1
C>* 192.168.15.0/24 is directly connected, vlan410
O>* 192.168.16.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.17.0/24 is directly connected, vlan419
O>* 192.168.20.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.21.0/25 is directly connected, eth2
S>* 192.168.25.0/24 [1/0] via 192.168.251.26, vlan462
S>* 192.168.26.0/24 [1/0] via 192.168.251.34, vlan459
S>* 192.168.32.0/23 [1/0] via 192.168.252.7, eth9
S>* 192.168.42.0/24 [1/0] via 192.168.251.42, vlan461
C>* 192.168.70.0/24 is directly connected, eth4
O>* 192.168.121.0/28 [110/20] via 192.168.254.243, eth0, 06w0d06h
O>* 192.168.121.16/28 [110/20] via 192.168.254.243, eth0, 20:11:45
C>* 192.168.122.0/24 is directly connected, eth12
O>* 192.168.123.0/24 [110/20] via 192.168.254.243, eth0, 05w0d02h
O>* 192.168.128.0/18 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 192.168.201.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 192.168.250.0/24 is directly connected, eth3
C>* 192.168.251.0/29 is directly connected, vlan460
C>* 192.168.251.24/29 is directly connected, vlan462
C>* 192.168.251.32/29 is directly connected, vlan459
C>* 192.168.251.40/29 is directly connected, vlan461
O   192.168.252.0/24 [110/10] is directly connected, eth9, 12w3d19h
C>* 192.168.252.0/24 is directly connected, eth9
S>* 192.168.253.0/24 [1/0] via 192.168.251.6, vlan460
O   192.168.254.0/24 [110/10] is directly connected, eth0, 12w3d19h
C>* 192.168.254.0/24 is directly connected, eth0
O>* 193.48.70.0/27 [110/20] via 192.168.254.243, eth0, 12w2d02h
C>* 193.48.70.32/27 is directly connected, eth10
O>* 193.48.70.64/26 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 193.55.155.0/24 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 194.3.242.73/32 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 194.57.172.56/29 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 194.57.186.0/24 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 194.57.186.6/32 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 194.199.237.0/25 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 194.199.237.128/29 is directly connected, eth8
O>* 194.199.237.192/27 [110/20] via 192.168.254.243, eth0, 12w2d07h
C>* 194.199.237.224/27 is directly connected, eth6
O>* 194.254.190.0/25 [110/20] via 192.168.254.243, eth0, 02w0d07h
O>* 212.73.216.0/30 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 212.73.216.128/27 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 212.73.216.160/27 [110/20] via 192.168.254.243, eth0, 12w2d07h
O>* 212.73.216.192/27 [110/20] via 192.168.254.243, eth0, 12w2d02h
O>* 212.73.216.224/27 [110/20] via 192.168.254.243, eth0, 12w2d02h
```

Tunnel IP: principe



Un tunnel entre 2 routeurs permet de faire circuler du trafic entre 2 réseaux comme s'il existait un lien physique entre les 2 routeurs.

Tunnel IP: fonctionnement



Une station envoie un datagramme vers une machine derrière le tunnel

IP | Data

IP source et destination réelles

IP (tunnel) | Data

IP source et destination des passerelles

IP (tunnel)

IP | Data

Le routeur de fin de tunnel traite le datagramme original

Tunnel: Utilisation

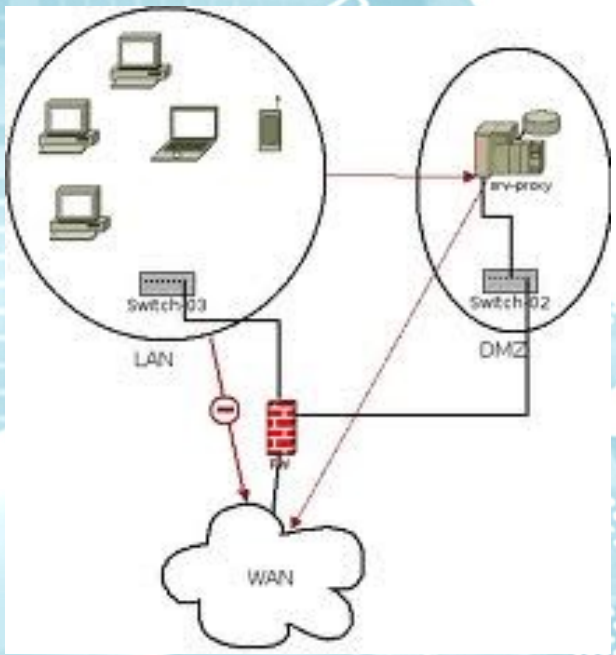
- Echange d'information entre des machines sur des LAN différents ayant des adresses non routées sur internet.
- Sécurisation des données via Chiffrement VPN, IPSEC, …
- Masquage des routes aux utilisateurs entre 2 LAN
- Passage a travers des protocoles différents (IPV6 over IPV4 par exemple)

Firewall

- But:
  Sécuriser l'accès à une machine ou à un lan
- Firewall basic simple à mettre en place sur un routeur :
  Se contente de regarder les enveloppes de trames (IP,TCP, ou UDP) pour prendre des décisions.
- Firewall couche application :
  - Filtrage d'url a partir d'une base de données.
  - Filtrage en fonction du contenu (control parental,…).

Proxy

- Mandataire qui va chercher une information sur internet pour le compte d'une autre machine.
- Possibilité de tracer les communications.



Reverse Proxy

– Permet a des clients externes d'accéder a des ressources internes.