Module U3d
Bases des réseaux WiFi

Licences R&T IRM et ISVD 2010-2011

L. Sassatelli

sassatelli@i3s.unice.fr

Organisation du module *(initiale)*

- 6h de cours magistral
- 6h de TP

Notes:

- 1 DS écrit de 1.5h
- 1 note de TP dont toutes les séances sont notées

Plan général

1. Notions de base sur les réseaux
2. Introduction aux réseaux sans-fil
3. La norme WiFi 802.11
4. Configurer un réseau WiFi
5. Matériel: portée, débits et puissance
6. Sécurité
7. Compléments

Sources bibliographiques

- Cours LP 2009-2010 de S. Frati
- Cours de Pr. Jörg Liebeherr – University of Toronto
- Cours de Patrick Vincent (erasme.org)

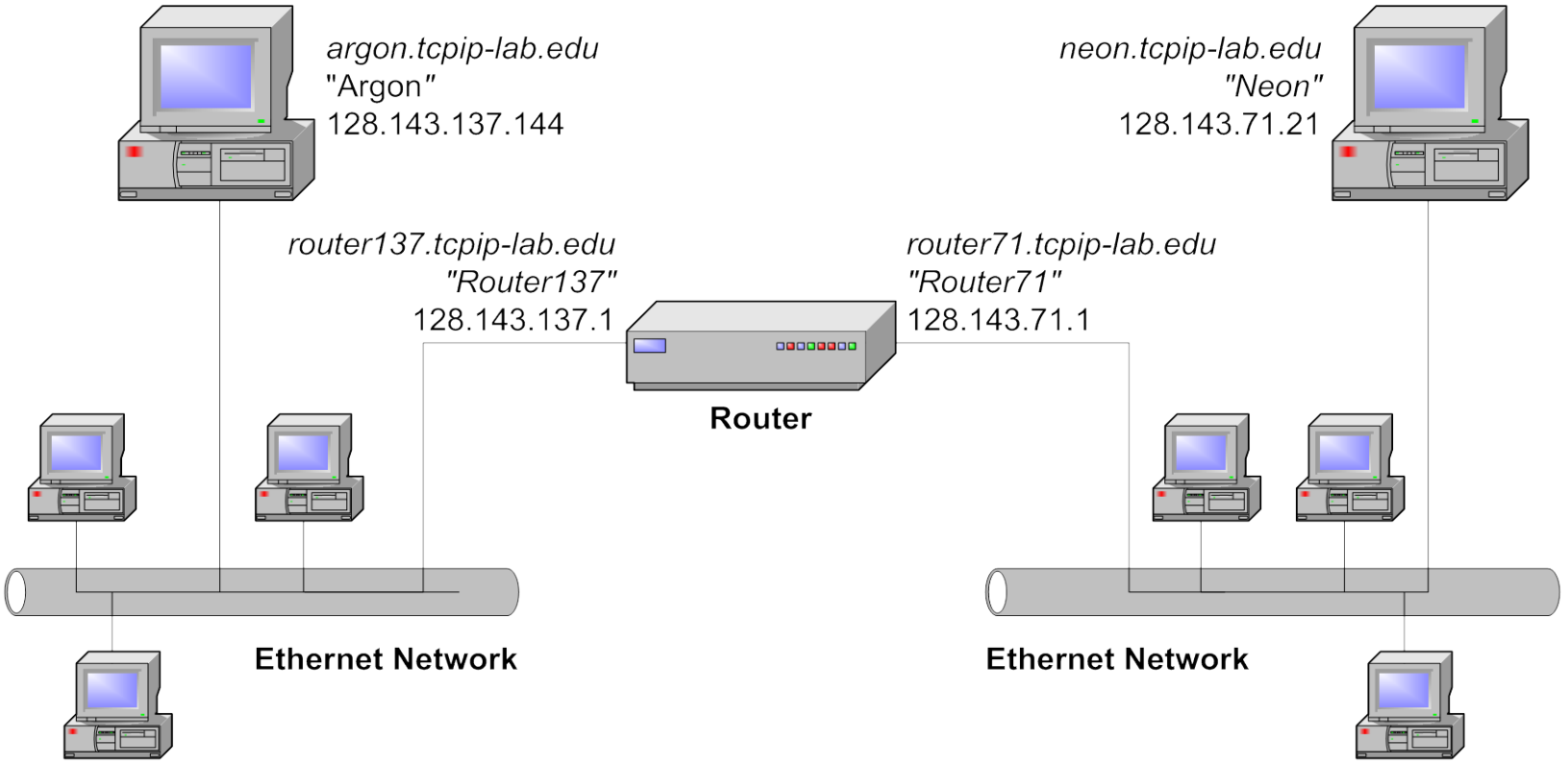
Review of Important Networking Concepts

Lecture of Pr. Jörg Liebeherr – University of Toronto

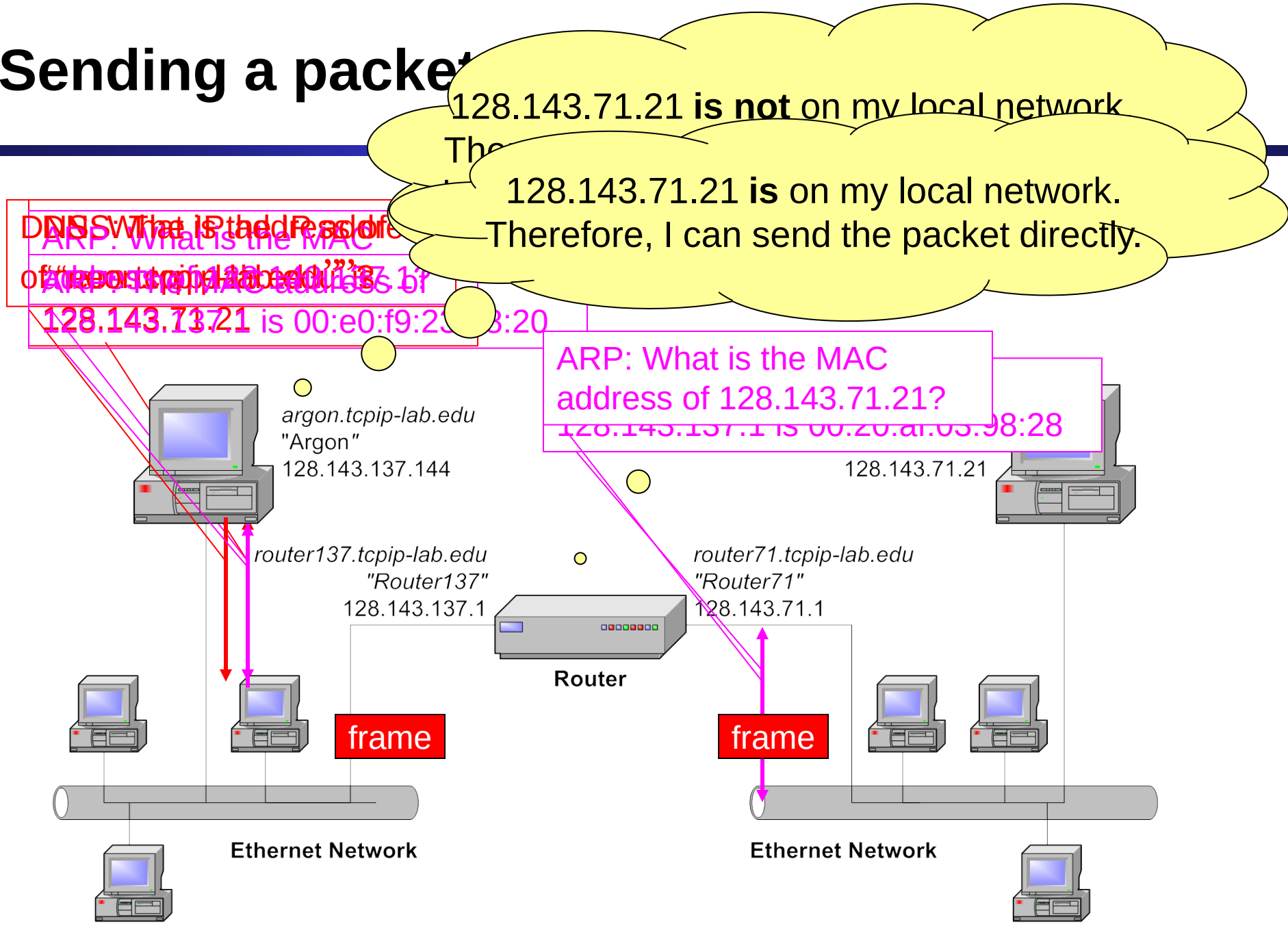
Networking Concepts

- Protocol Architecture
- Protocol Layers
- Encapsulation
- Network Abstractions

Sending a packet from Argon to Neon



Sending a packet

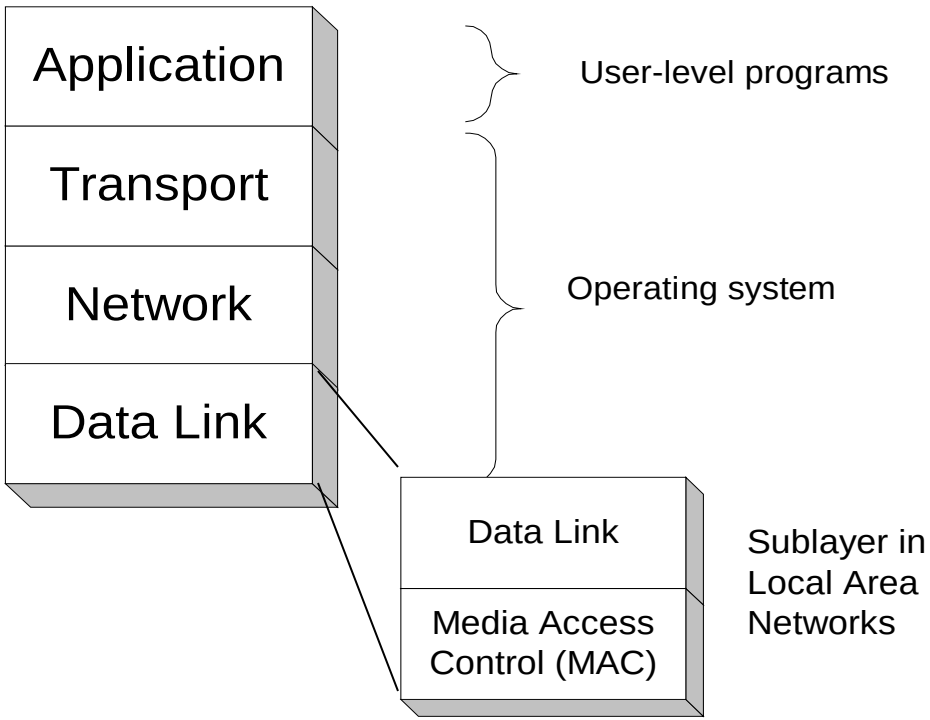


Communications Architecture

- The complexity of the communication task is reduced by using multiple protocol layers:
  - Each protocol is implemented independently
  - Each protocol is responsible for a specific subtask
  - Protocols are grouped in a hierarchy
- A structured set of protocols is called a communications architecture or protocol suite

TCP/IP Protocol Suite

- The TCP/IP protocol suite is the protocol architecture of the Internet
- The TCP/IP suite has 4 layers: Application, Transport, Network, Data Link Layer
- End systems (hosts) implement all 4 layers. Gateways (Routers) only have the bottom 2 layers.

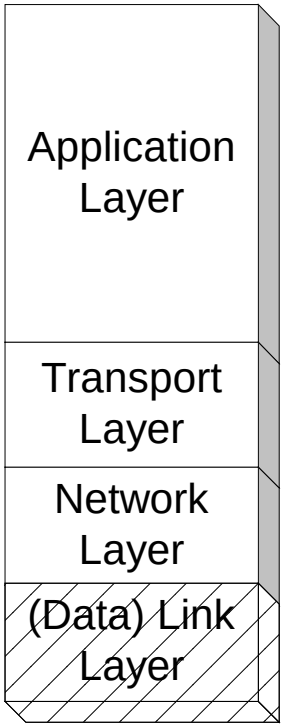


Functions of the Layers

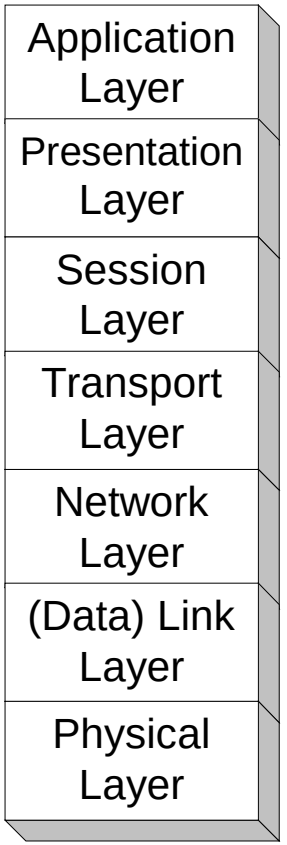
- Data Link Layer:
  - Service: Transfer of frames over a link
Media Access Control on a LAN
  - Functions: Framing, media access control, error checking
- Network Layer:
  - Service: Move packets from source host to destination host
  - Functions: Routing, addressing
- Transport Layer:
  - Service: Reliable transfer of data between hosts
  - Functions: Connection establishment/termination, error control, flow control
- Application Layer:
  - Service: Application specific (delivery of email, retrieval of HTML documents, reliable transfer of file)
  - Functions: Application specific

TCP/IP Suite and OSI Reference Model

The TCP/IP protocol stack does not define the lower layers of a complete protocol stack

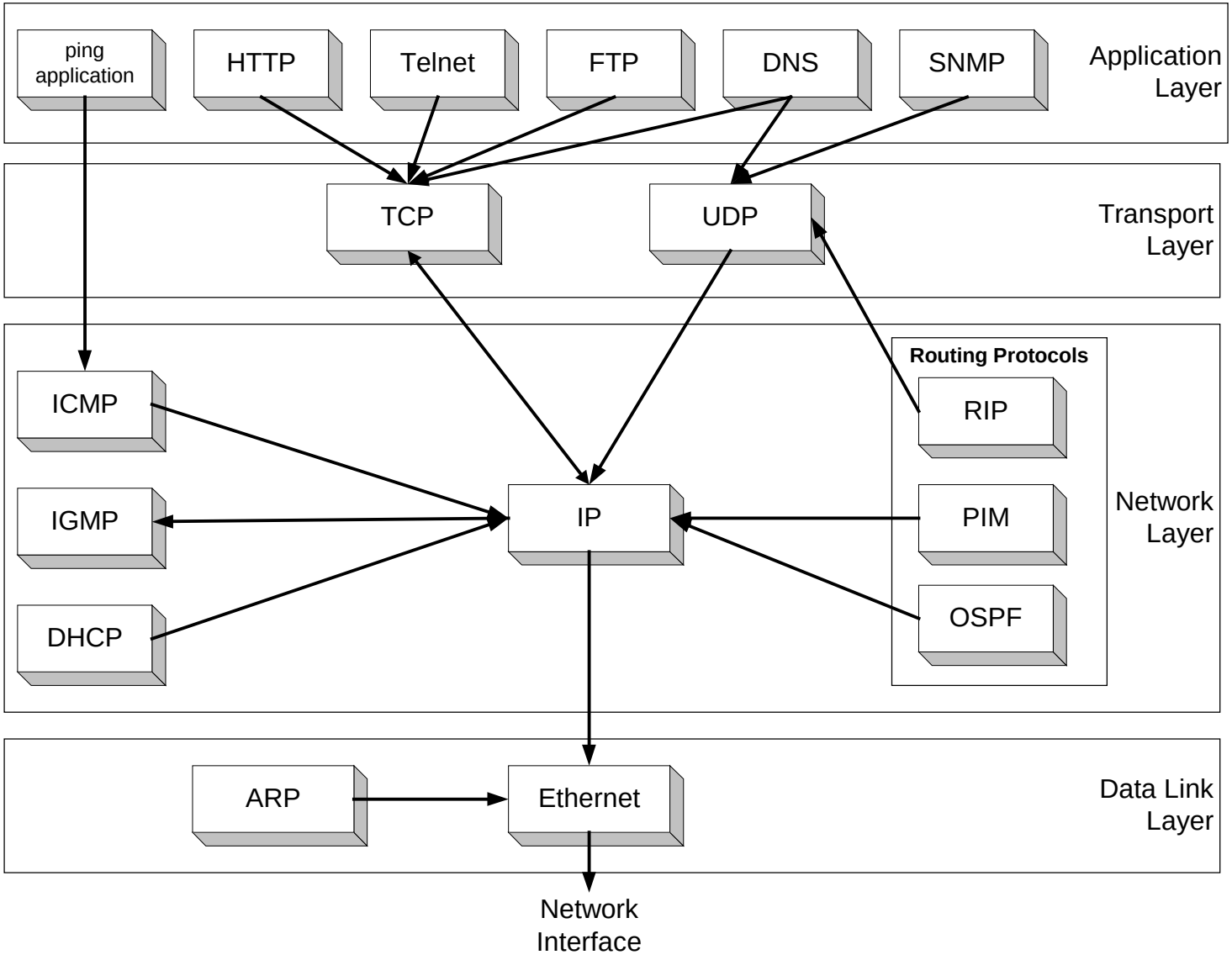


TCP/IP Suite



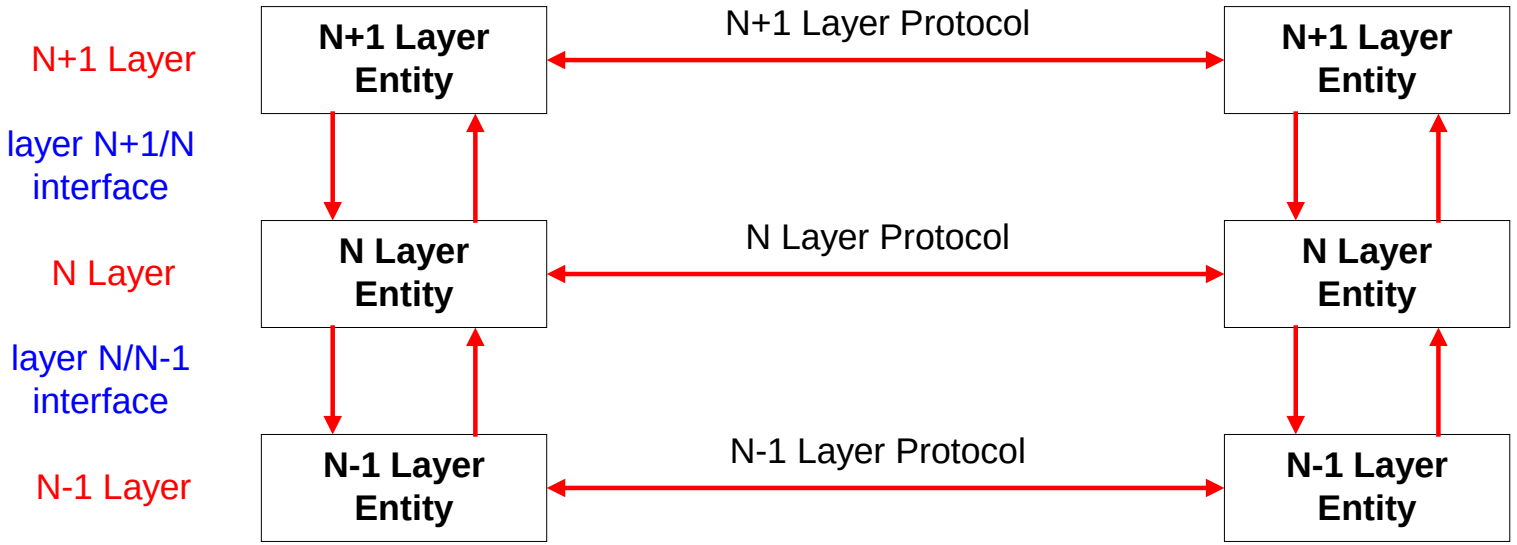
OSI Reference Model

Assignment of Protocols to Layers



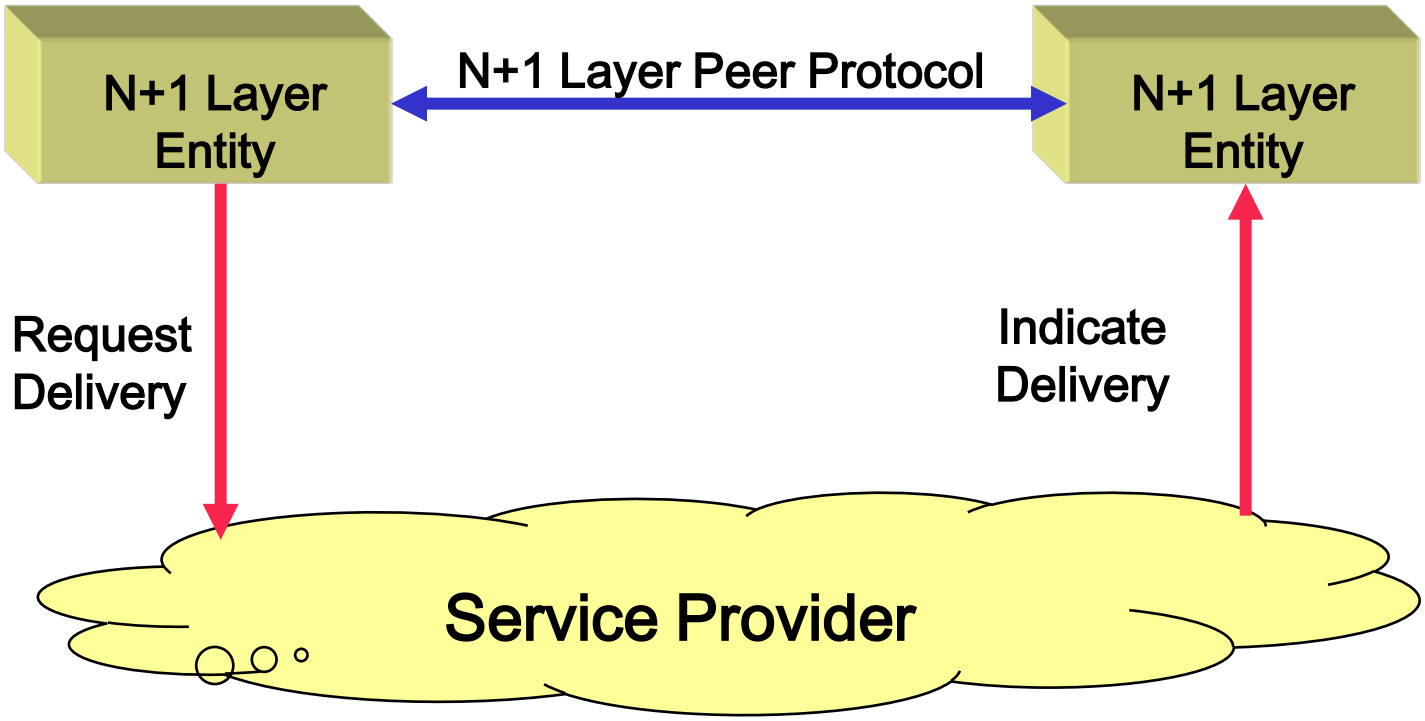
Layered Communications

- An entity of a particular layer can only communicate with:
  1. a peer layer entity using a common protocol (**Peer Protocol**)
  2. adjacent layers to provide services and to receive services



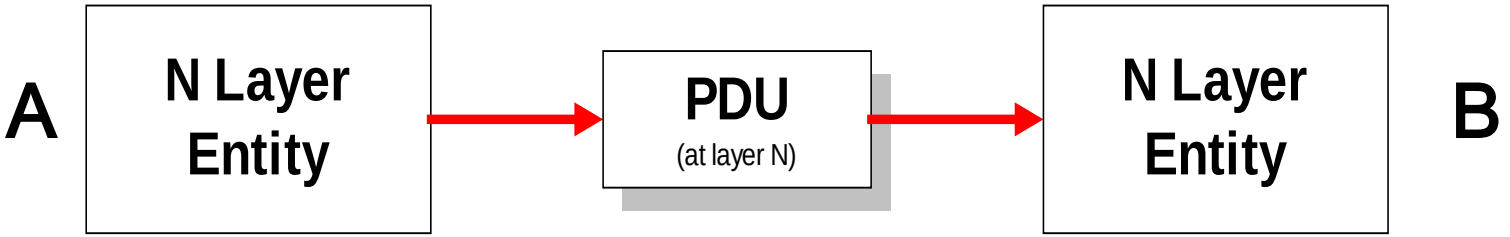
Layered Communications

A layer N+1 entity sees the lower layers only as a service provider



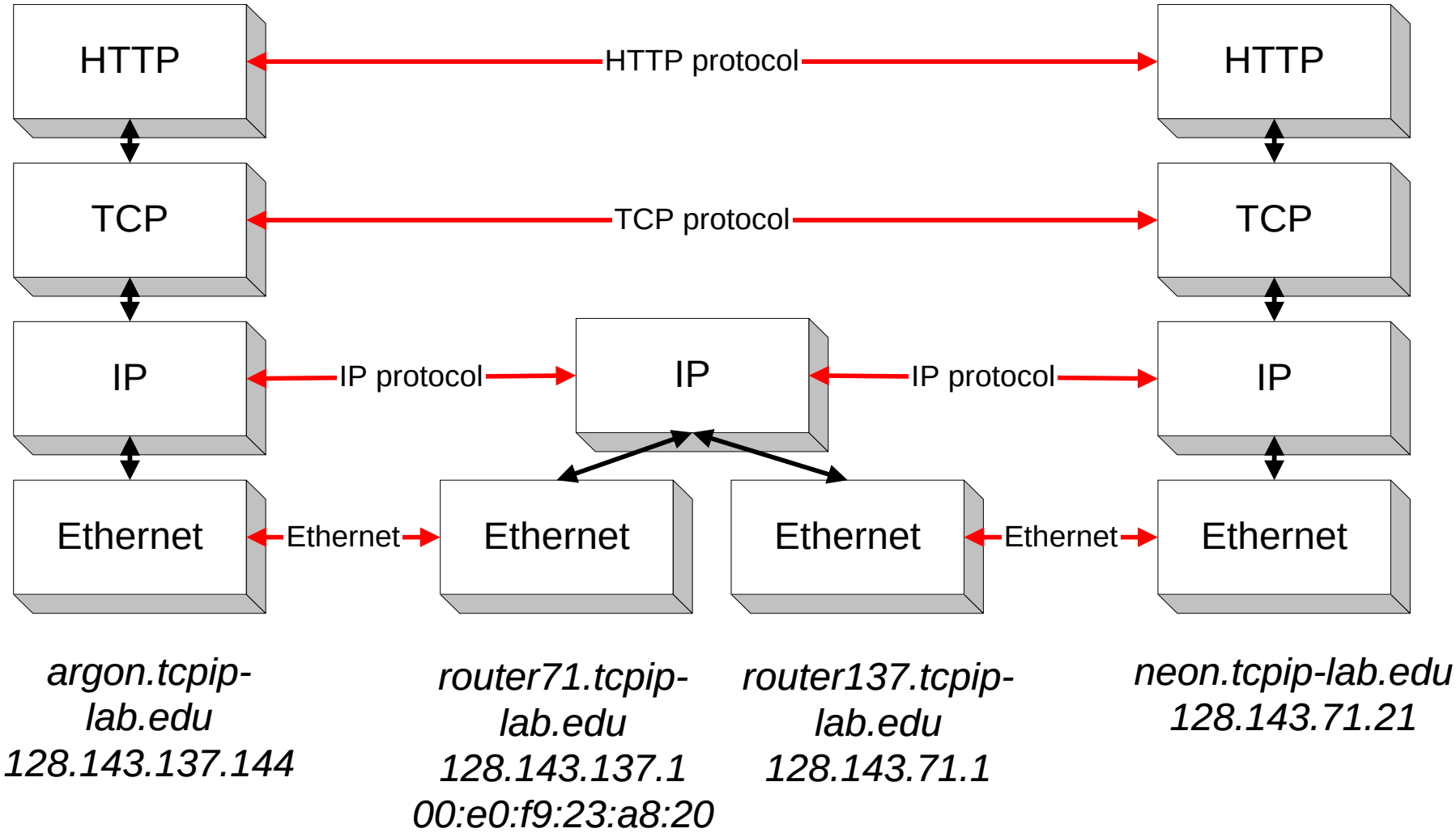
Exchange of Data

- The unit of data send between peer entities is called a **Protocol Data Unit (PDU)**
- For now, let us think of a PDU as a single packet

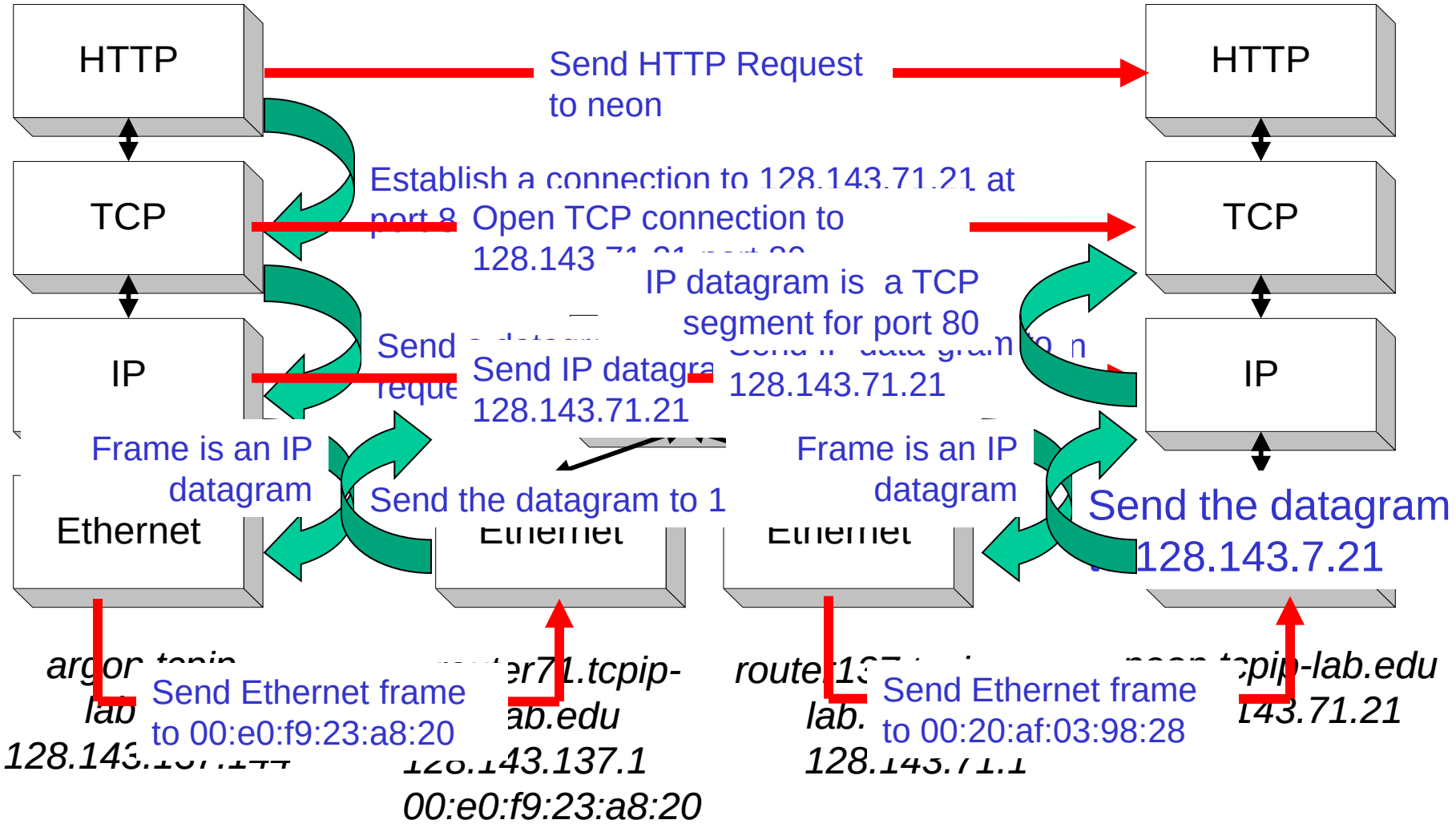


- **Scenario:** Layer-N at A sends a layer-N PDU to layer-N at B
- What actually happens:
  - A's layer-N passes the PDU to layer-N-1
  - Layer-N-1 entity at A constructs its own (layer-N-1) PDU which it sends to the layer-N-1 entity at B
  - PDU at layer-N-1 = layer-N-1 Header + layer –N PDU

Layers in the Example



Layers in the Example



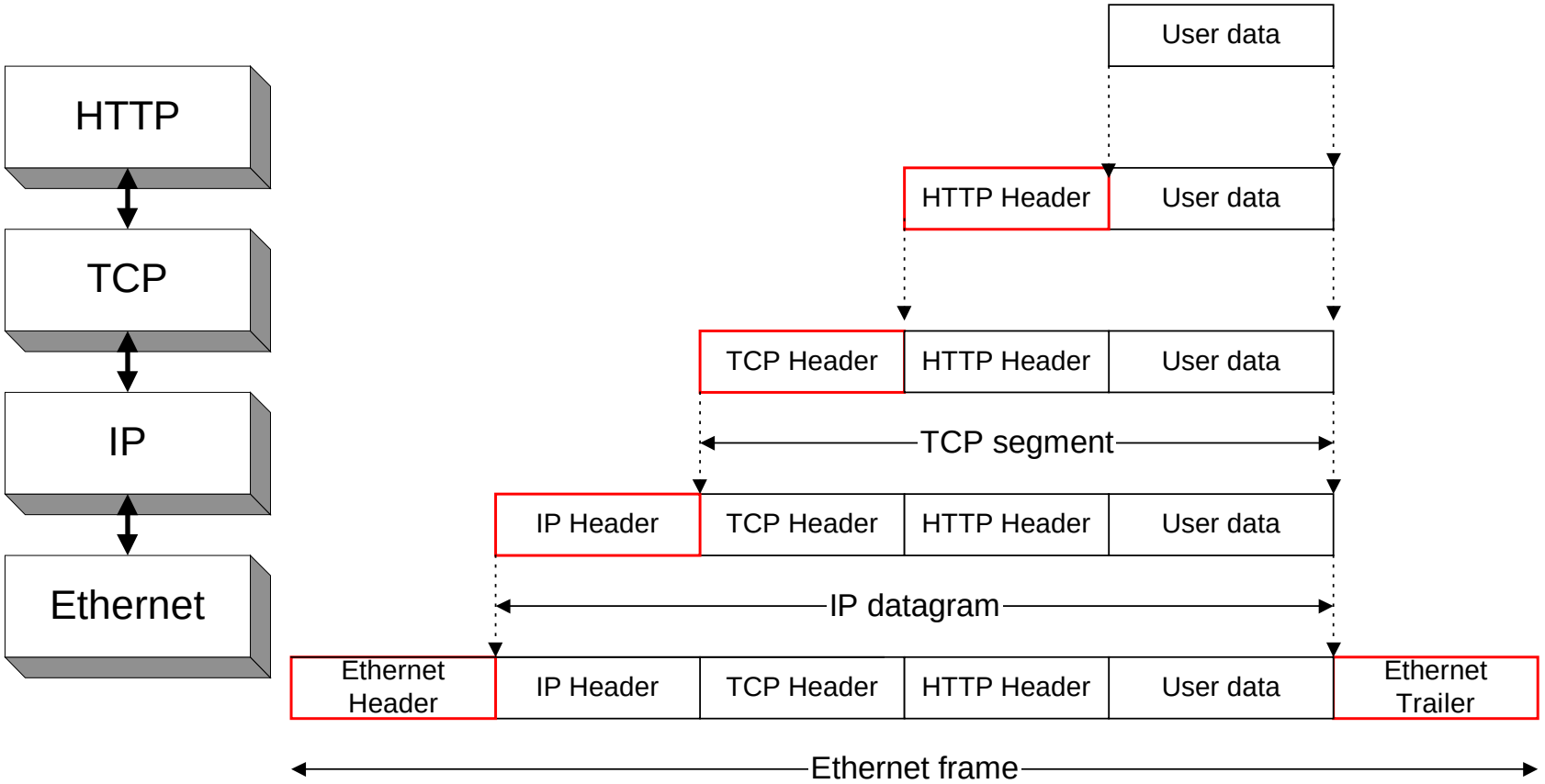
Layers and Services

- Service provided by TCP to HTTP:
  - reliable transmission of data over a logical connection
- Service provided by IP to TCP:
  - unreliable transmission of IP datagrams across an IP network
- Service provided by Ethernet to IP:
  - transmission of a frame across an Ethernet segment

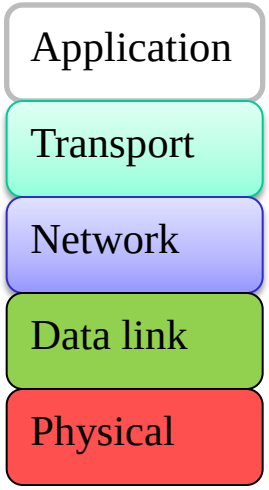
- Other services:
  - DNS: translation between domain names and IP addresses
  - ARP: Translation between IP addresses and MAC addresses

Encapsulation and Demultiplexing

- As data is moving down the protocol stack, each protocol is adding layer-specific control information



The stack



Layers in the
TCP/IP model

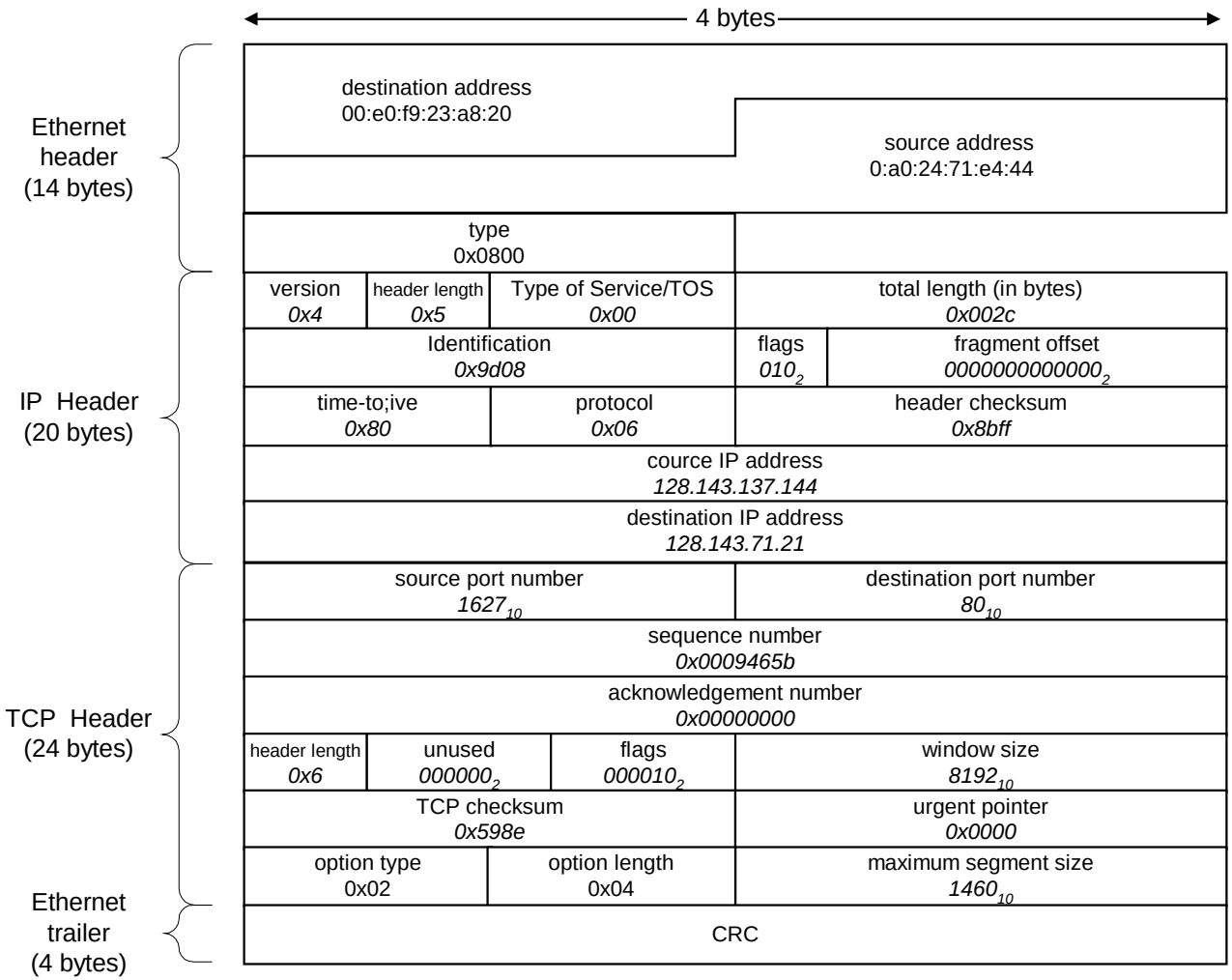
Encapsulation and Demultiplexing in our Example

- Let us look in detail at the Ethernet frame between Argon and the Router, which contains the TCP connection request to Neon.

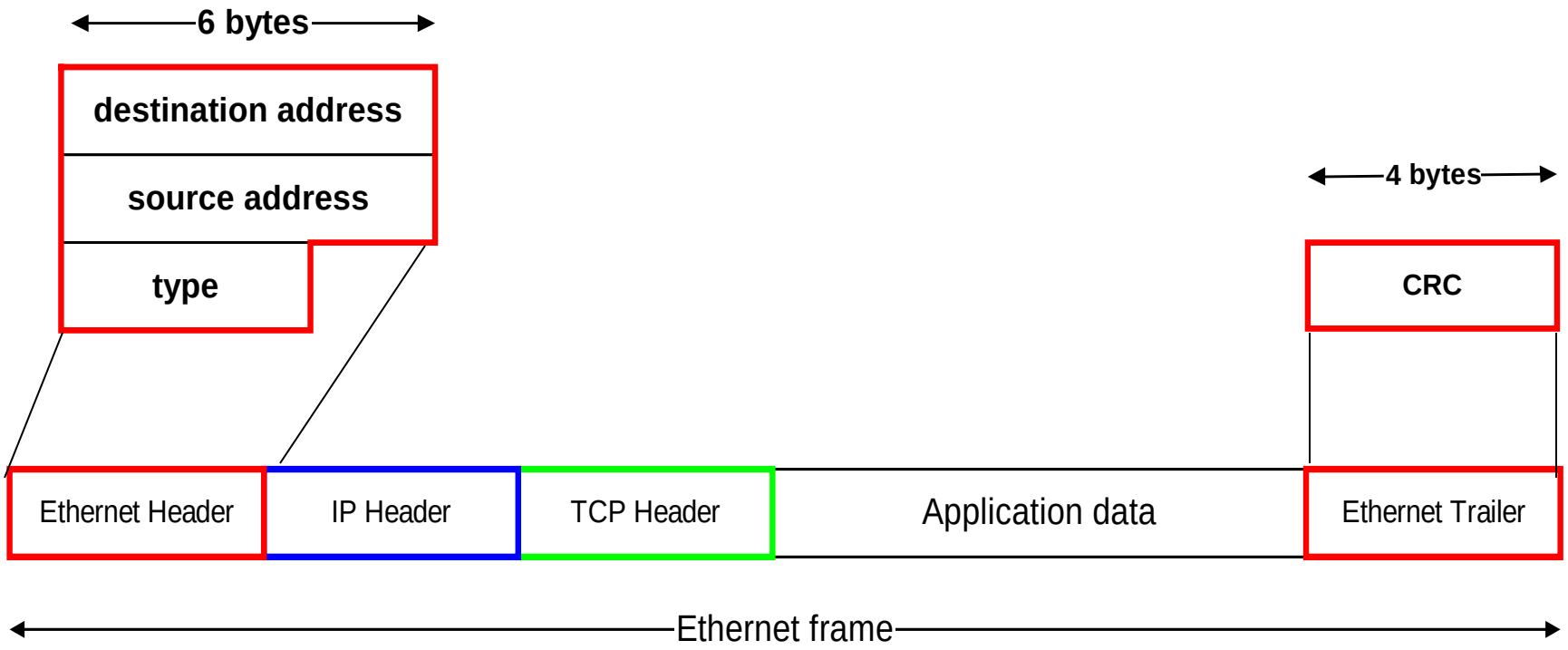
- This is the frame in hexadecimal notation.

```
00e0 f923 a820 00a0 2471 e444 0800 4500 002c
9d08 4000 8006 8bff 808f 8990 808f 4715 065b
0050 0009 465b 0000 0000 6002 2000 598e 0000
0204 05b4
```

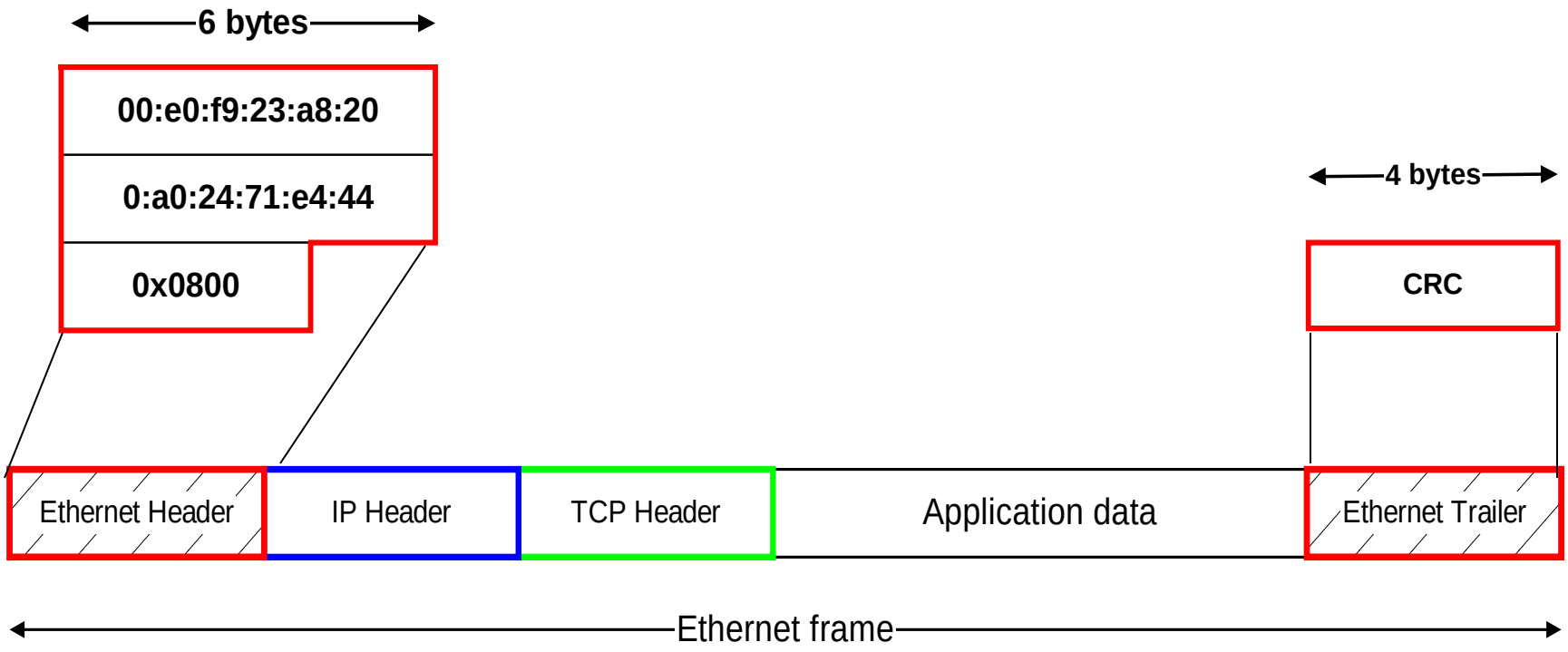
Parsing the information in the frame



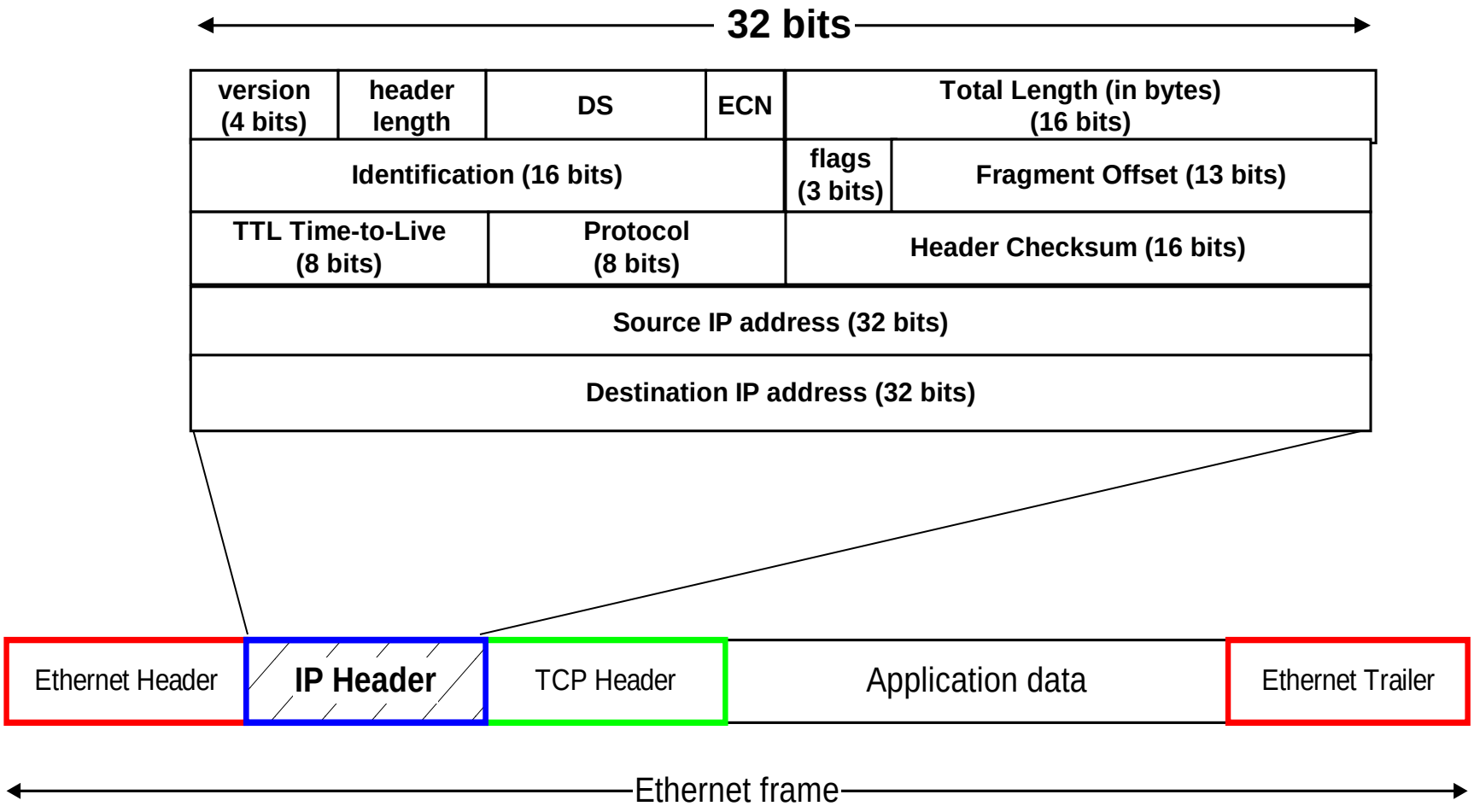
Encapsulation and Demultiplexing



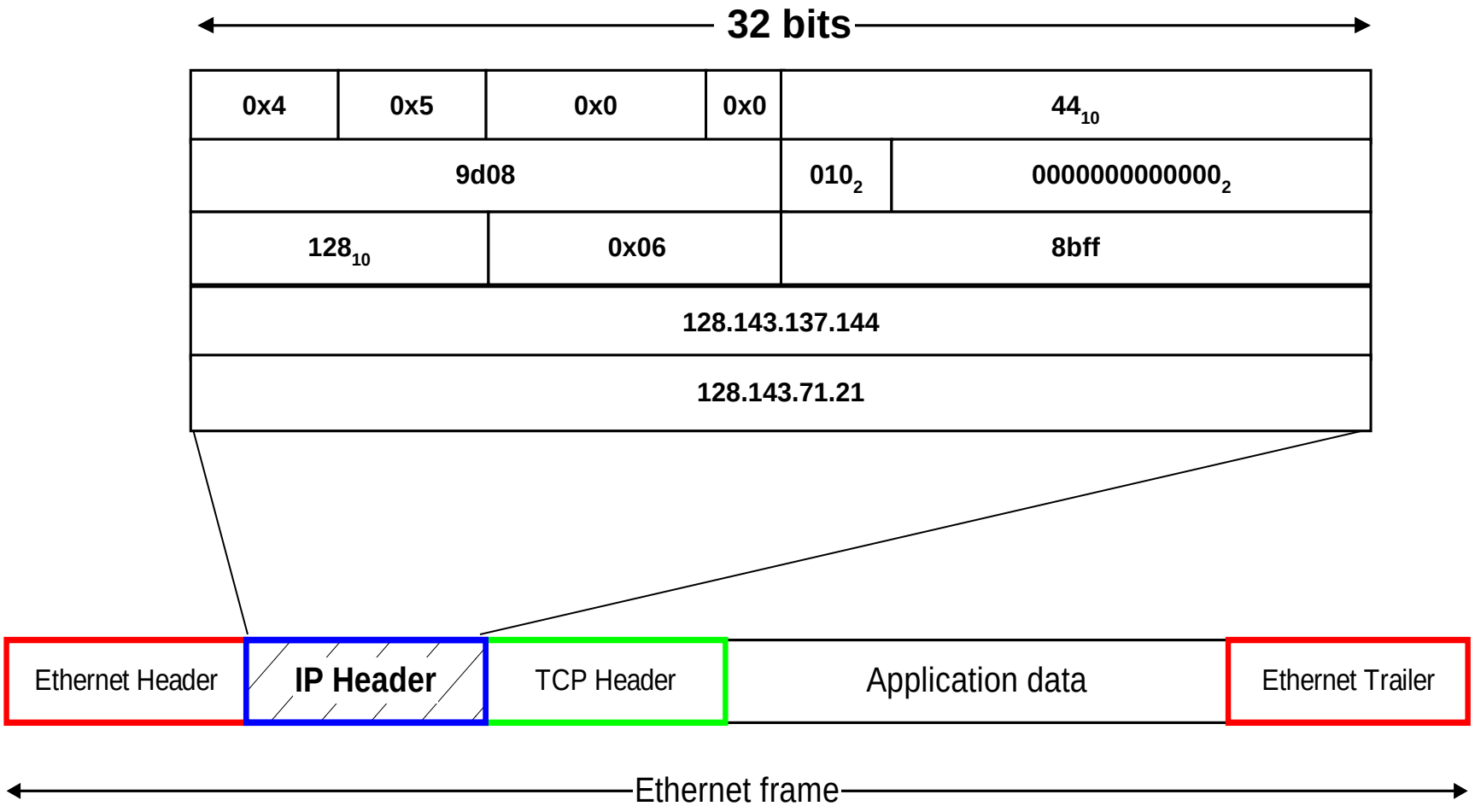
Encapsulation and Demultiplexing: Ethernet Header



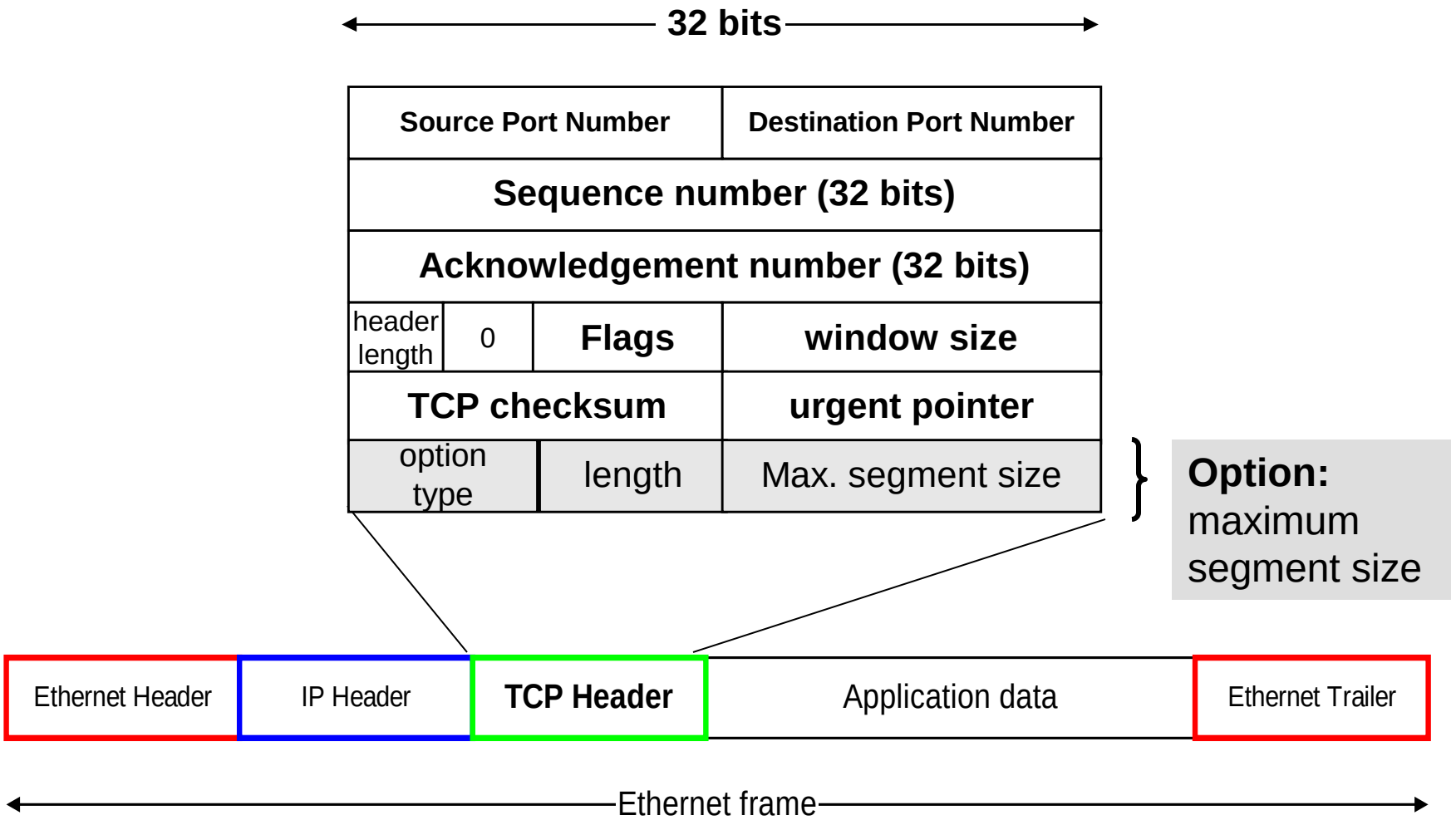
Encapsulation and Demultiplexing: IP Header



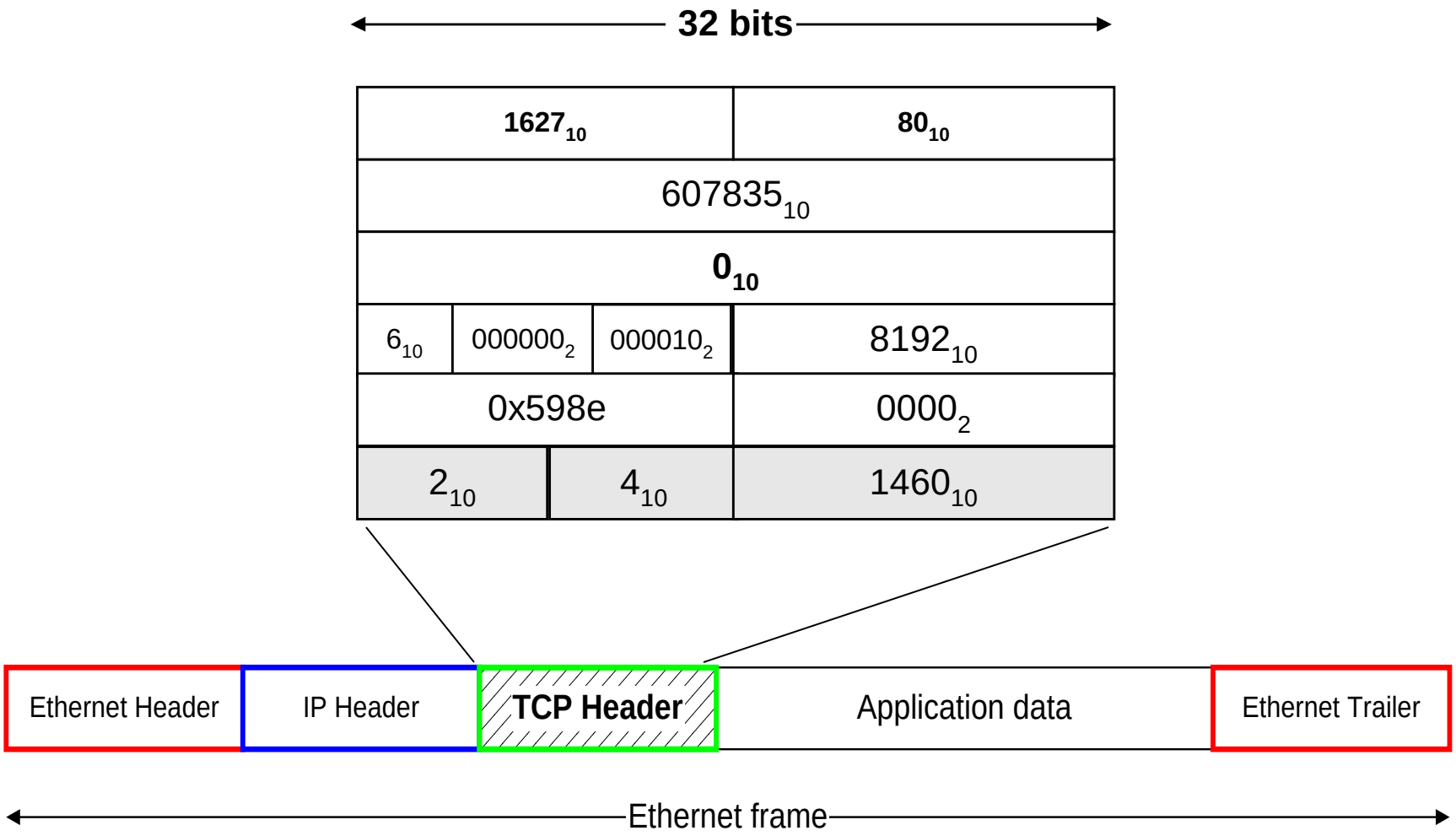
Encapsulation and Demultiplexing: IP Header



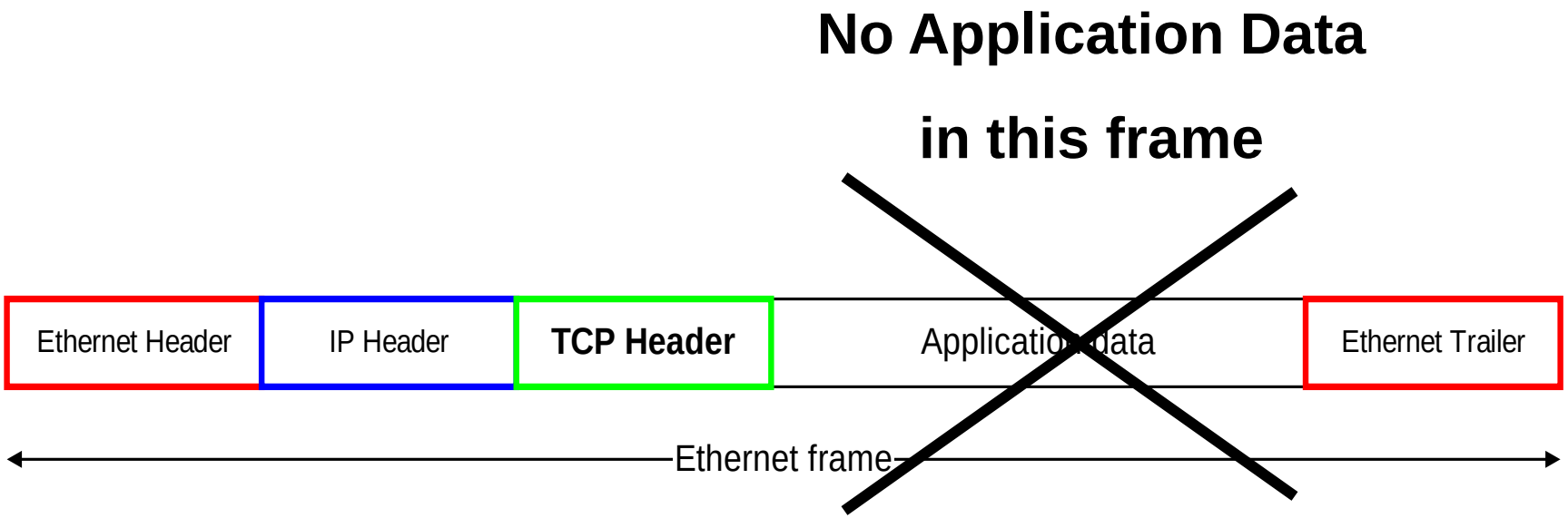
Encapsulation and Demultiplexing: TCP Header



Encapsulation and Demultiplexing: TCP Header

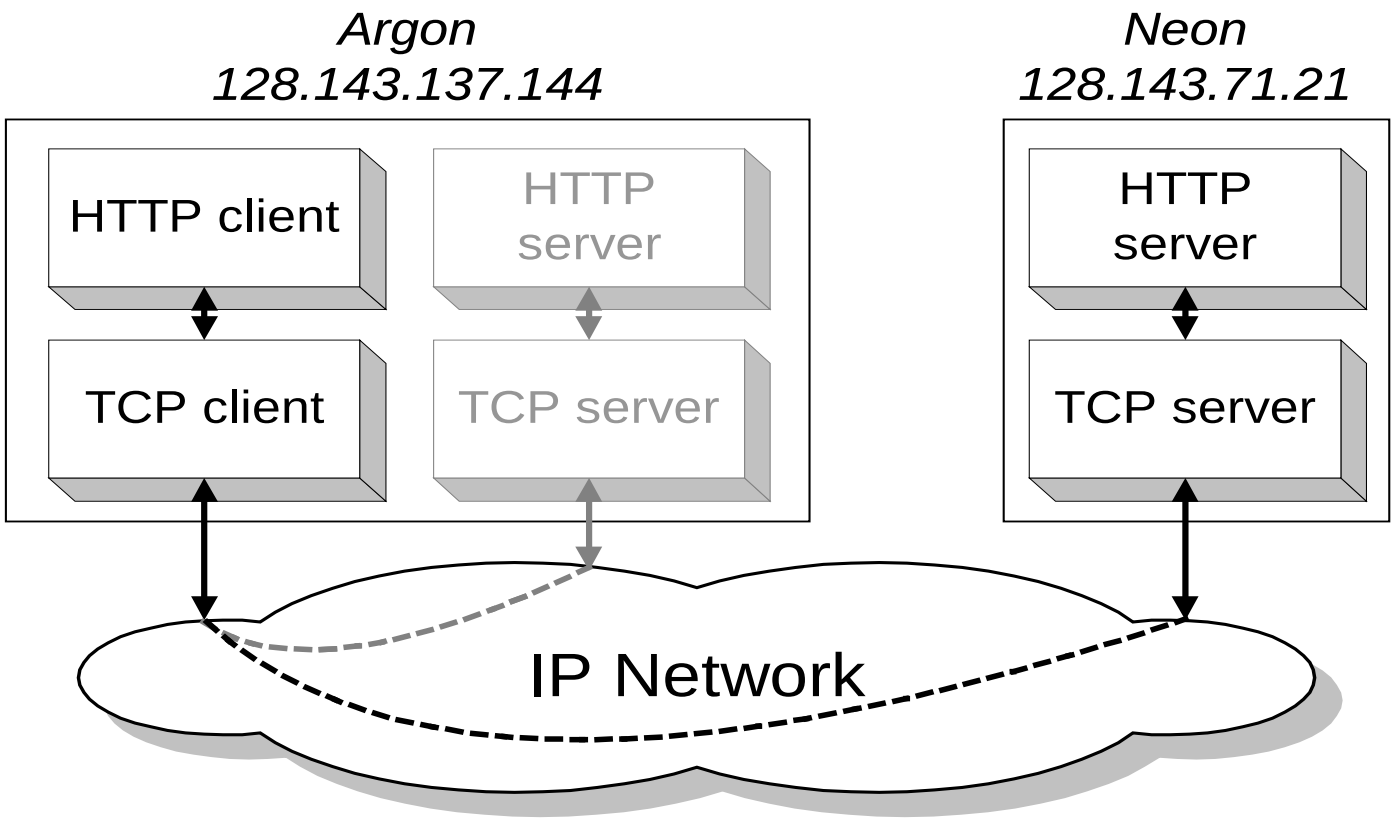


Encapsulation and Demultiplexing: Application data

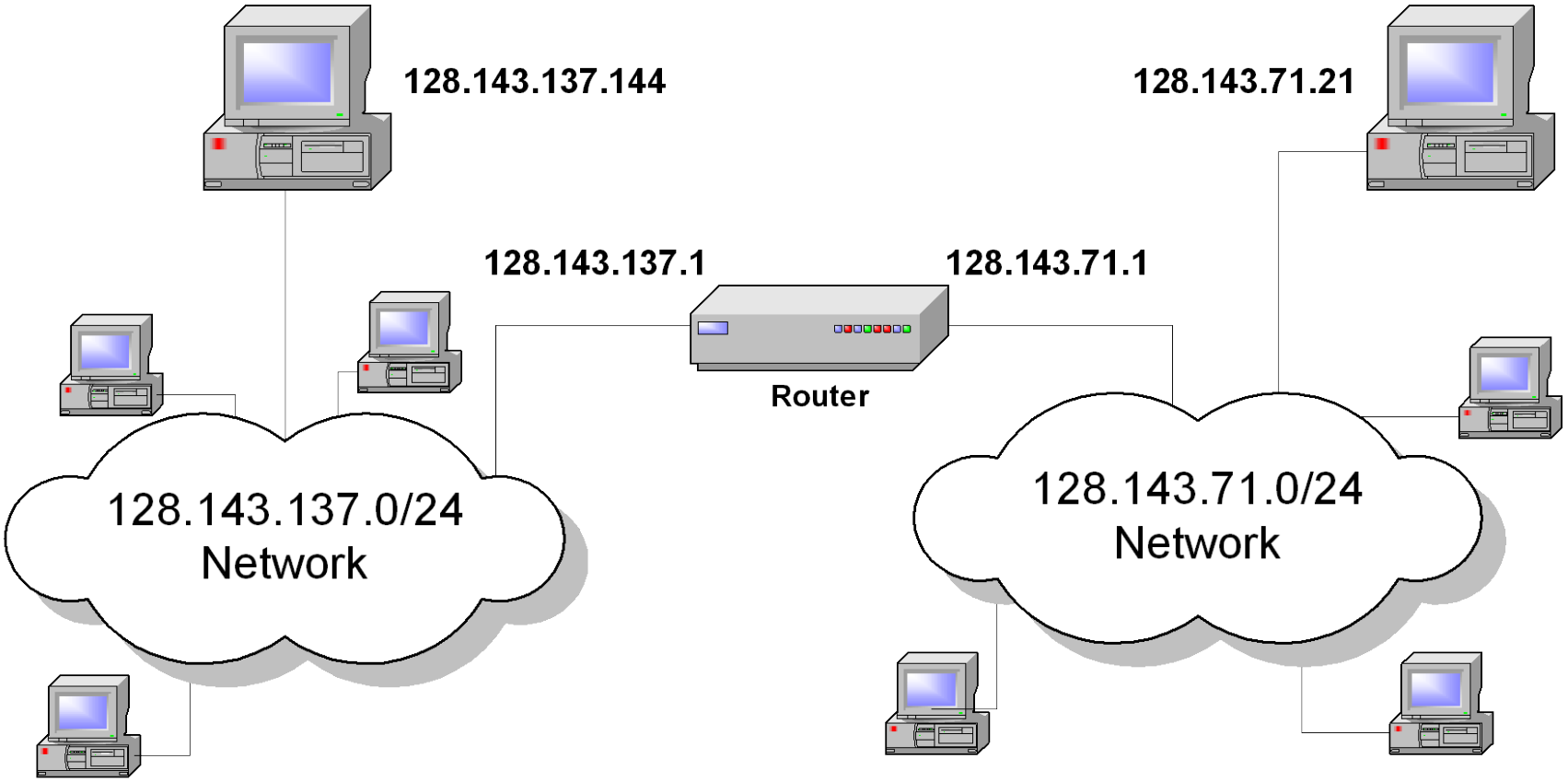


Different Views of Networking

- Different Layers of the protocol stack have a different view of the network. This is HTTP's and TCP's view of the network.

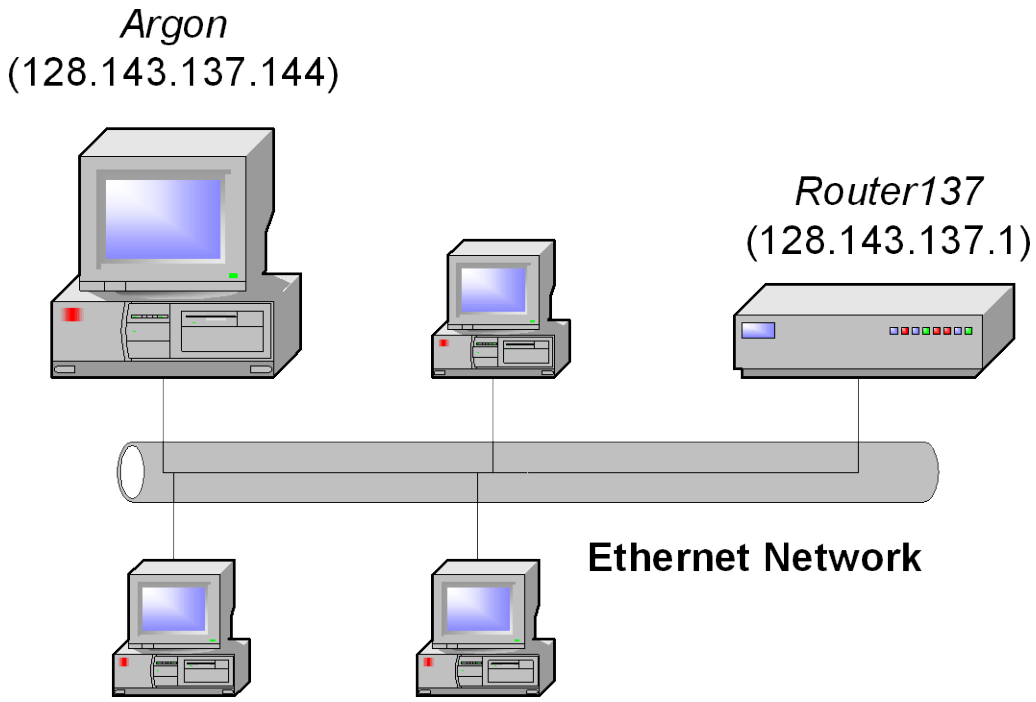


Network View of IP Protocol



Network View of Ethernet

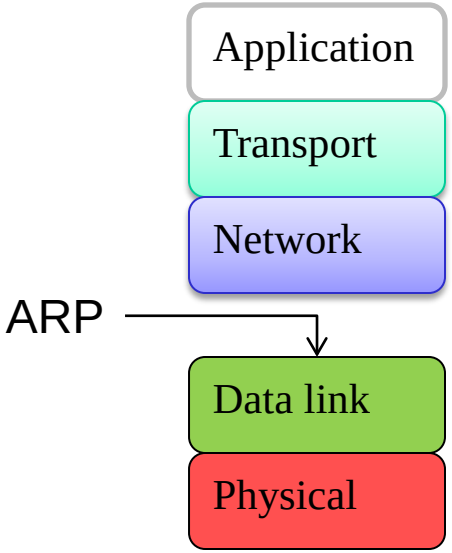
- Ethernet's view of the network



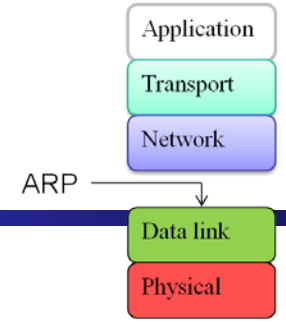
Rappel: Address Resolution Protocol

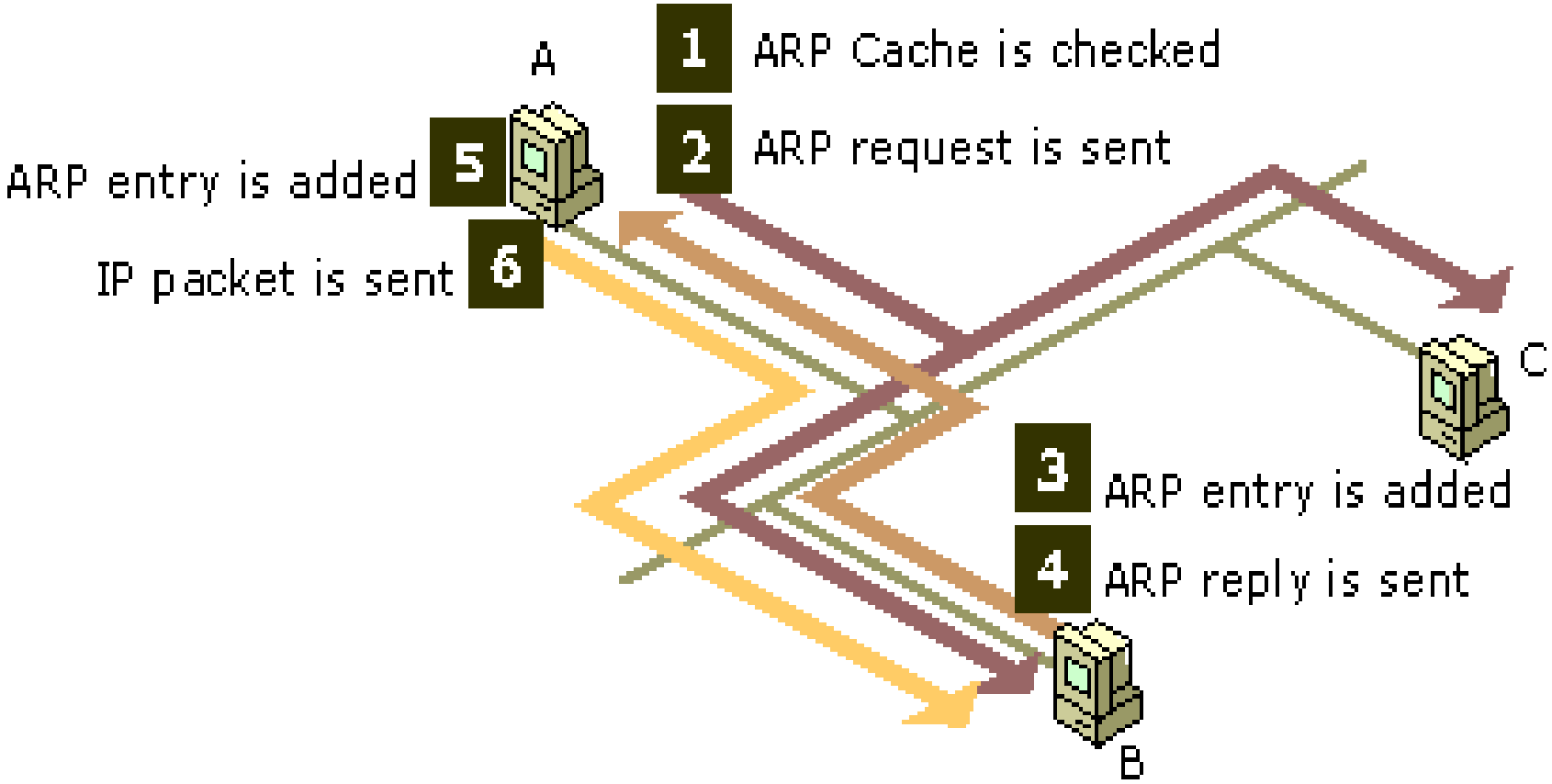
- ARP permet une association (mapping) entre une adresse de 3ème niveau (IP) et une adresse de 2ème niveau (Ethernet)

- ARP ”requests” et ”replies”

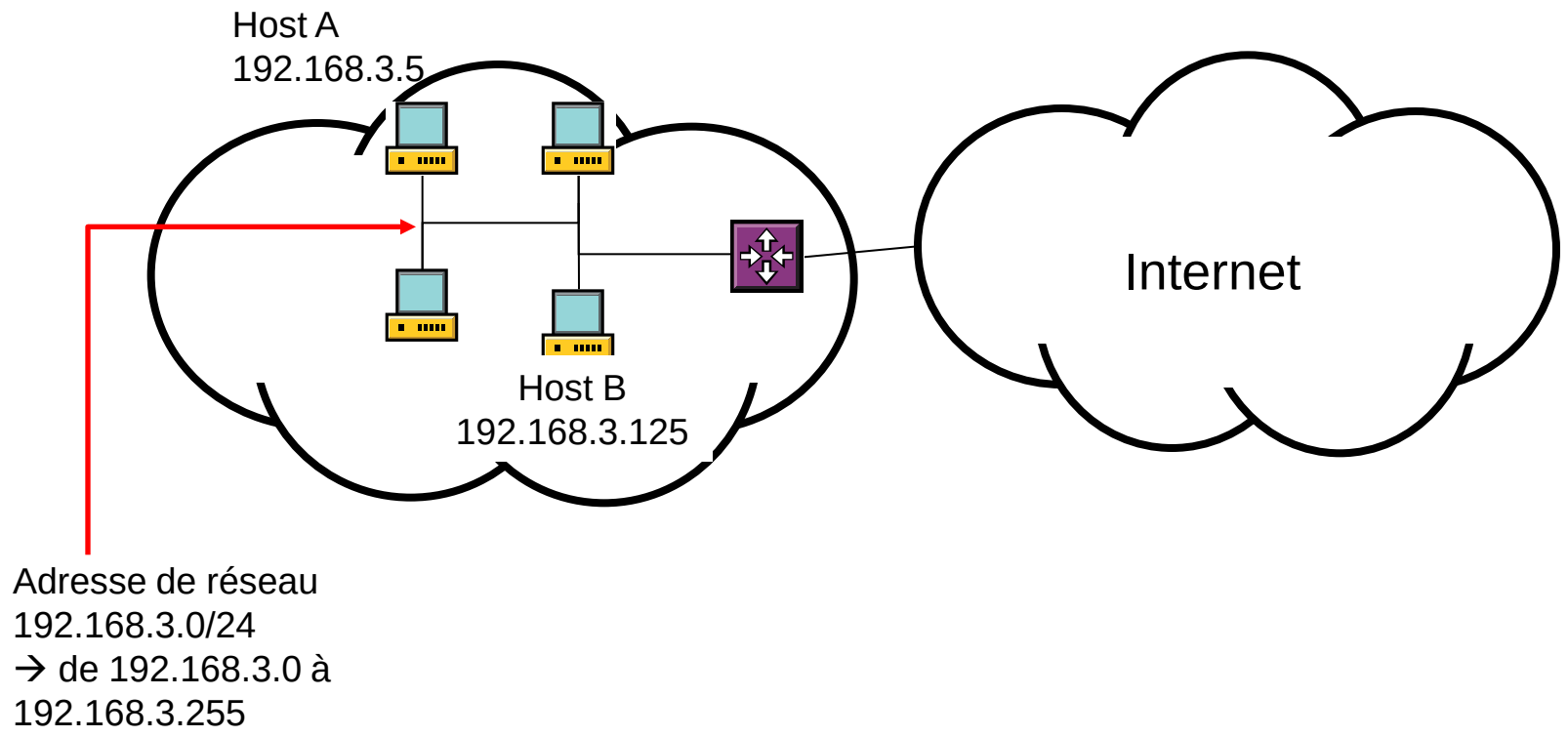


ARP

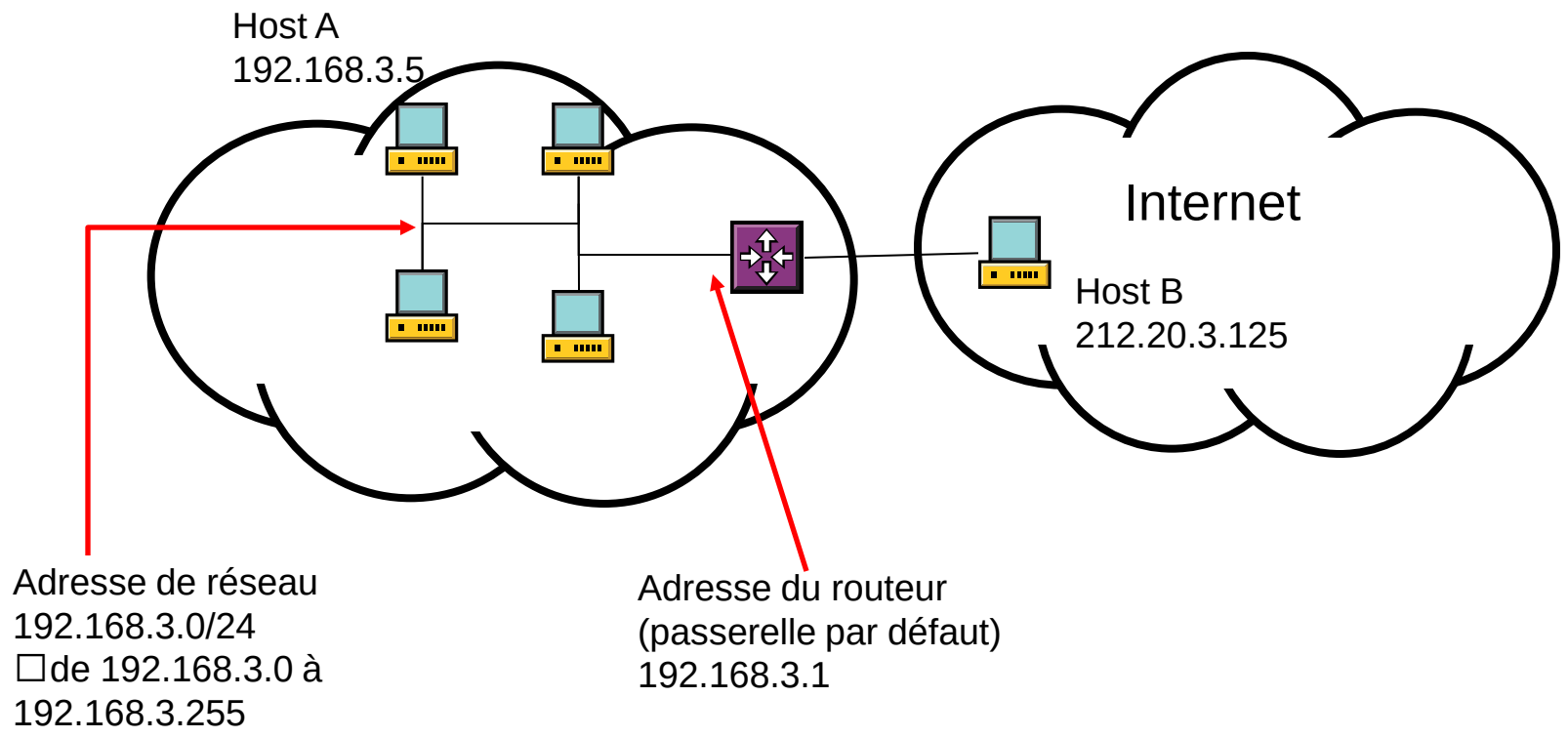

Application
Transport
Network
ARP
Data link
Physical


A
1 ARP Cache is checked
2 ARP request is sent
ARP entry is added
5
IP packet is sent
6
C
3 ARP entry is added
4 ARP reply is sent
B

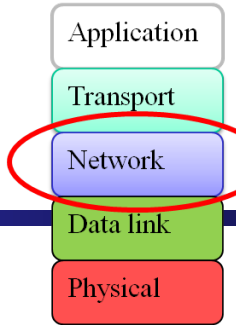
Scénario 1: A veut dialoguer avec B situé sur le même réseau



Scénario 2: A veut dialoguer avec B mais non situé sur le même segment

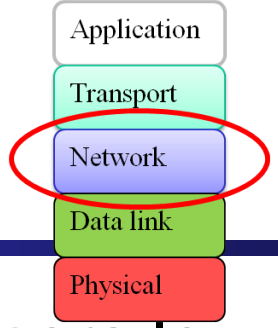


Commandes de configuration du routage

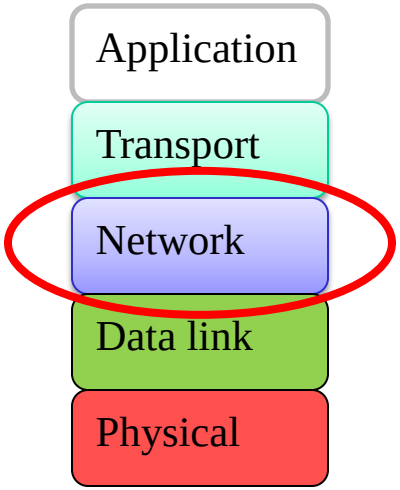


	Windows	Standard UNIX	New UNIX
Configuration de l'adresse IP	>ipconfig (NT, 2K, XP) or >winipcfg (Win9x,Me)	>ifconfig	>ip address show
Configuration du routage	>route print >route add ... >route add -p ... >netstat -rn	>route >route add ... >netstat –rn	>ip route show >ip route add ... >ip mr
Configuration ARP	>arp -a >arp -d	>arp	> ip maddr > ip neighbour

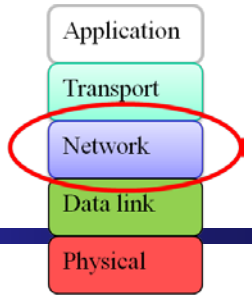
Rappel: Routage IP



- Chaque machine et chaque passerelle sait quel sera le prochain saut (hop) pour router les paquets IP
- Le routage est toujours unidirectionnel
  - Des informations de routage pour chaque direction doivent être définies séparemment
- Le routage peut être:
  - Statique
  - Dynamique
  - Combinaison des deux



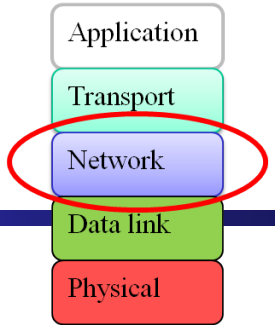
Routage statique

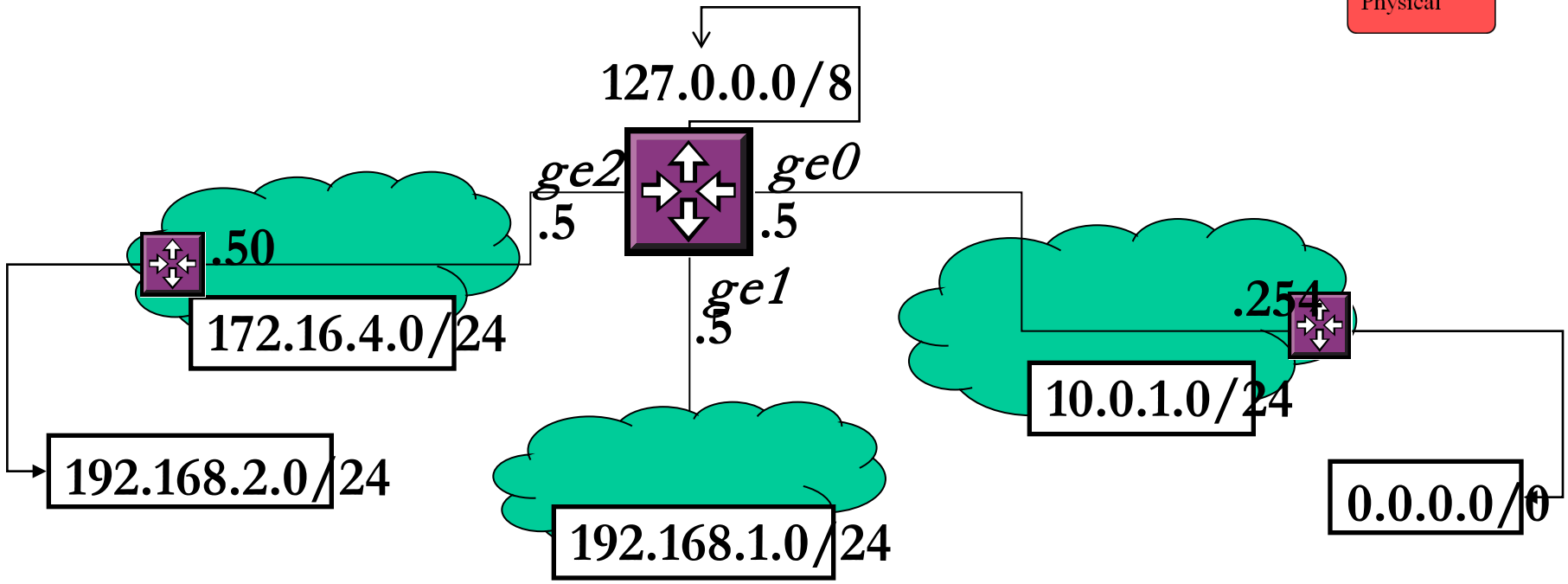


Destination	Gateway	Netmask	Flags	Metric	Ref	Interface
0.0.0.0	10.0.1.254	0.0.0.0	UG	0	0	ge0
10.0.1.0	10.0.1.5	255.255.255.0	U	0	0	ge0
192.168.1.0	192.168.1.5	255.255.255.0	U	0	0	ge1
172.16.4.0	172.16.4.5	255.255.255.0	U	0	0	ge2
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	lo
192.168.2.0	172.16.4.50	255.255.255.0	U	1	0	ge2

- La passerelle par défaut est 10.0.1.254
- La deuxième route indique que pour atteindre ce routeur et ce réseau il faudra utiliser l'interface ge0.
- La route pour le réseau 192.168.1.0/24 passe par l'interface ge1.
- La route pour le réseau 192.168.2.0/24 passe par l'interface ge2.
- La route pour le réseau 172.16.4.0/24 passe par l'interface ge2.
- Le réseau 127.0.0.0 représente l'*interface de loopback*.
- Pour un réseau spécifique de R&D (192.168.2.0/24), le routeur/firewall devra utiliser 172.16.4.50.

Configuration du Routeur/Firewall

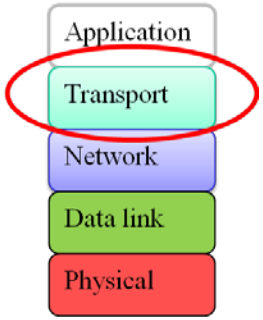




Destination	Gateway	Netmask	Flags	Metric	Ref	Interface
0.0.0.0	10.0.1.254	0.0.0.0	UG	0	0	ge0
10.0.1.0	10.0.1.5	255.255.255.0	U	0	0	ge0
192.168.1.0	192.168.1.5	255.255.255.0	U	0	0	ge1
172.16.4.0	172.16.4.5	255.255.255.0	U	0	0	ge2
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	lo
192.168.2.0	172.16.4.50	255.255.255.0	U	1	0	ge2

4ème niveau - Protocoles de Transport

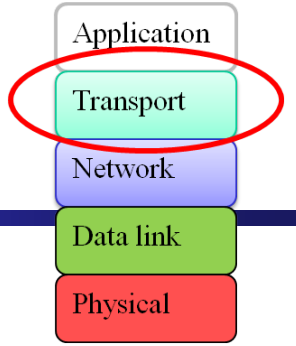
- Les protocoles de transport définissent les points d'arrivée au sein d'une machine (ports)



- Les deux protocoles les plus utilisés
  - transmission control protocol (TCP)
  - user datagram protocol (UDP)

- TCP possède bien plus de fonctionnalités que UDP, mais il est donc plus "complexe" à paramètrer:
  - Gestion de la fiabilité (ACK-based)
  - Maximisation du débit, sous contrainte de
  - Partage équitable de capacité totale (fairness)

UDP

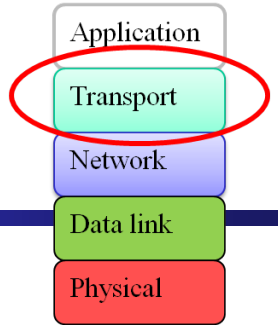


- UDP est un protocole sans connexion
  - connectionless protocol

- Pas de fiabilité rajoutée par dessus le niveau IP
  - Toutes les retransmissions doivent être gérées par le niveau Application

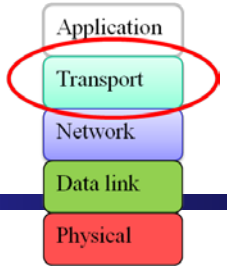
- Simple à implémenter, très suffisant la plupart du temps

UDP header



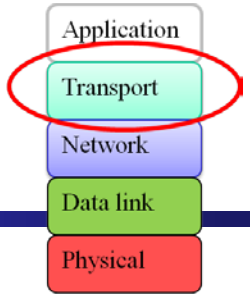

```
 0       7 8      15 16     23 24     31
+--------+--------+--------+--------+
|     Source       |   Destination   |
|      Port        |      Port       |
+--------+--------+--------+--------+
|                  |                 |
|     Length       |    Checksum     |
+--------+--------+--------+--------+
```

TCP



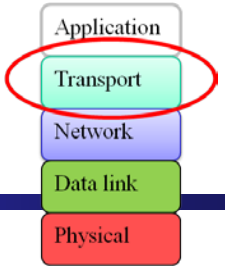
- TCP est un protocole orienté connexion
  - connection-oriented protocol
- Une connexion est établie avant tout envoi de données
- Une connexion TCP se place exactement entre deux points finaux
- Quand la connexion n'est plus utilisée, elle est terminée

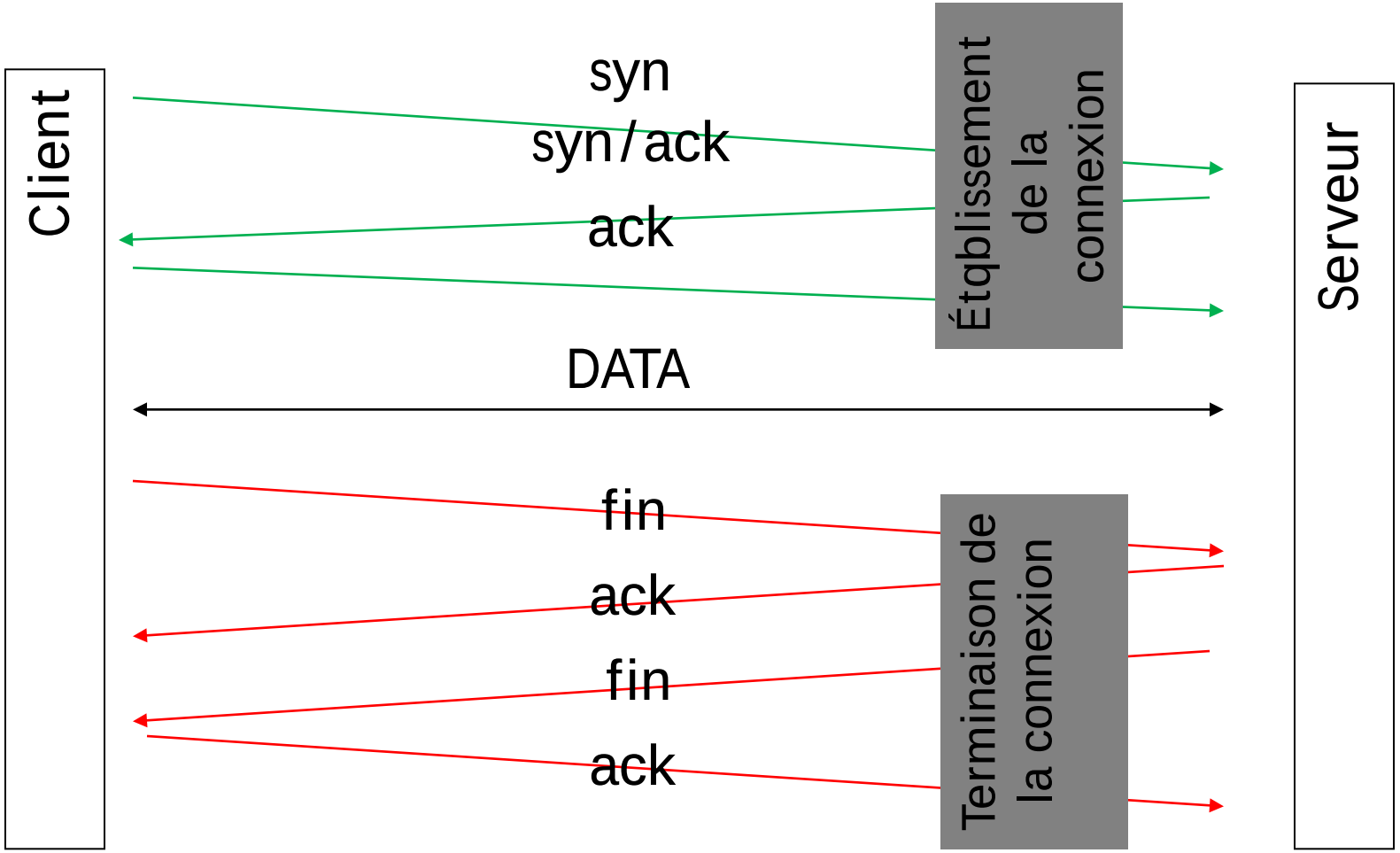
TCP header




```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

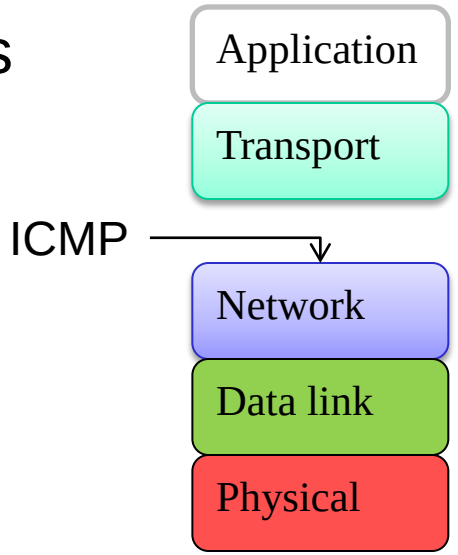
Connexion TCP – “3 way handshake”



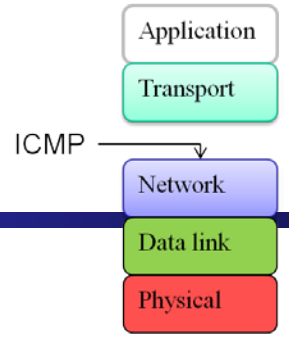


3/4ème niveau – Internet Control Message Protocol

- ICMP permet d'envoyer des messages d'erreur et d'autres indications sur l'état du réseau qui doivent attirer notre attention
- E.g. utilitaires ping, traceroute
- Deux principaux types:
  - Requêtes/réponses - queries/replies
  - Messages d'erreur - error messages

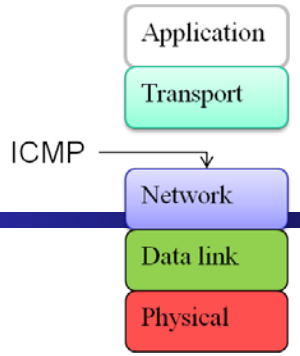


Message ICMP



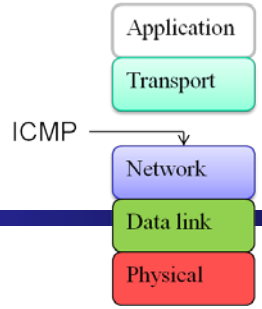

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|              (content depends on type and code)               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Requêtes ICMP



- echo request / reply
  - connu comme ping (certains traceroute)
  - aide à vérifier que la machine distante est “up&running”
- router solicitation / advertisement
  - une machine demande un routeur par défaut par une sollicitation et un routeur présent répond par une publication
- timestamp request / reply
  - une requête pour l’heure depuis minuit (ms)
- address mask request / reply
  - une requête pour un masque de sous-réseau
  - généralement envoyé sur l’adresse de broadcast

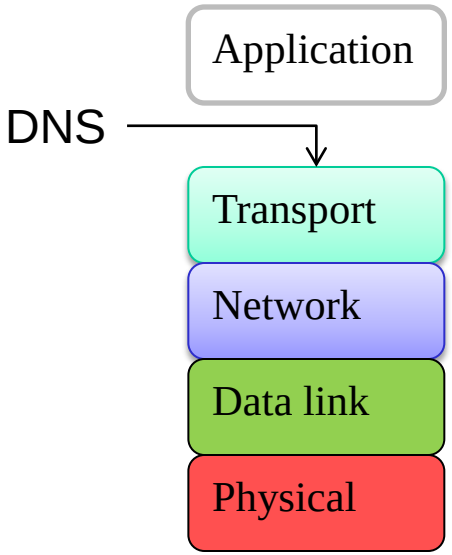
Erreurs ICMP



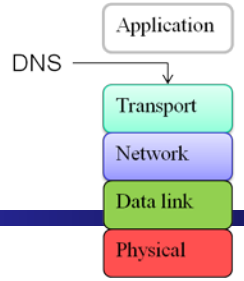
- Le message reprend l'entête IP et les 8 premiers octets du datagramme IP ayant provoqué l'erreur
- destination unreachable
  - network unreachable
  - host unreachable
  - protocol unreachable
  - port unreachable
  - fragmentation needed but don't fragment bit is set
  - source route failed
- redirect
  - Envoyé par un routeur au précédent pour indiquer une route plus rapide
- time exceeded
  - le TTL, décrémenté à chaque saut, est arrivé à 0

Rappel: Domain Name System

- Des noms lisibles par les humains “normaux” sont plus faciles à retenir que des numéros IP
- Le DNS fait la relation entre les adresses IP et les noms de domaines
- Les informations de “mapping” sont distribuées et maintenues par les serveurs DNS à travers la planète entière



Exemple: Navigation Web



Workstation
IP: 10.1.1.220
ws.client.com

DNS local
IP: 10.1.1.1
ns1.client.com

1

4

Internet

6 5

3 2

Serveur Web
IP: 192.168.200.200
www.cible.com

DNS distant
IP: 192.168.168.1
dns.cible.com

Rappel: [uni|multi|broad]cast

- Unicast
  - un destinataire
- Multicast
  - un groupe de destinataires
- Broadcast
  - destiné à "tout le monde"

Adresse Ethernet et *cast

- un octet pair pour l’octet de poids fort (even byte as the most significant byte) de l’adresse MAC indique une adresse de type unicast
- un octet impair indique une adresse de type multicast
- FF:FF:FF:FF:FF:FF est l’addresse de broadcast (un cas particulier de multicast)

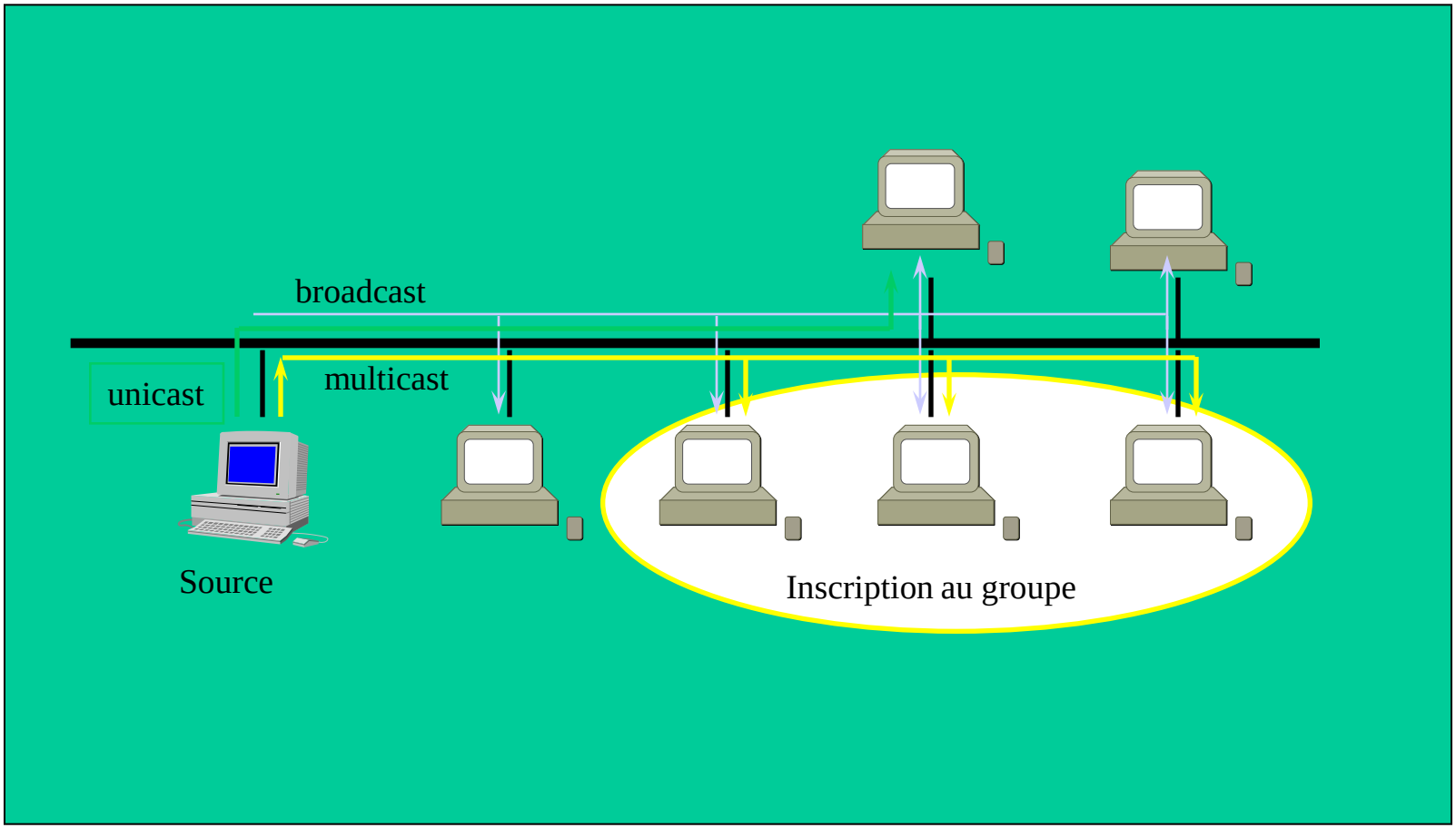
Adresse IP et *cast

- Les adresses IP de 224.0.0.0 à 239.255.255.255 sont de type multicast
- Les adresses plus petites sont de type unicast
- La dernière adresse de chaque segment de réseau représente son adresse de broadcast

IP Multicast → Ethernet

- Toutes les adresses IP de type Multicast sont associées à une plage d'adresses MAC spécifique
- La plage d'adresse est de 01:00:5E:00:00:00 à 01:00:5E:7F:FF:FF
- Pour compléter l'adresse, copier les 23 bits de poids faible de l'adresse IP multicast dans les 23 bits de poids faible de l'adresse MAC
- Une adresse MAC de type multicast peut servir jusqu'à 32 adresses IP de type multicast

Multicast IP: principe de fonctionnement



Interfaces Ethernet et *cast

- Habituellement, chaque NIC (network interface card == carte réseau) présente exactement une **adresse MAC** de type unicast

- un NIC peut présenter de 0 à N **adresse IP** unicast

- un NIC peut aussi rejoindre de 0 à M adresses (IP ou MAC) multicast

Rappel: Internet Group Management Protocol

- Le protocle IGMP permet de délivrer du traffic IP multicast par l'intermédiaire de routeur IP standards

- Les machines envoient aux routeurs des messages de "join" IGMP pour se joindre à un groupe IP multicast

Internet Group Management Protocol

- Les routeurs gardent une trace des segments et des machines qui ont rejoint ou quitté les groupes multicast

- Certains switches ethernet peuvent interpréter ces messages et ne transmettre les datagrammes que sur les ports où des machines sont effectivement à l'écoute de traffic de type multicast

Abbreviations

- ATM - Asynchronous Transfer Mode
- DHCP - Dynamic Host Configuration Protocol
- DNS - Domain Name System
- EDIFACT - Electronic Data Interchange for Administration, Commerce, Transportation
- FDDI - Fibre Distributed Data Interchange
- HTTP - Hypertext Transfer Protocol
- HTTPS - HTTP Secure
- HTML - Hyper Text MarkUp Language
- IAB - Internet Architectural Board
- ICMP - Internet Control Message Protocol
- IMAP - Internet Message Access Protocol
- IP - Internet Protocol
- ISO - International Standardization Organization
- Isoc - Internet Society
- ISP - Internet Service Provider
- LAN - Local Area Network

Abbréviations (2)

- MAC - Media Access Control
- MAN - Metropolitan Area Network
- MIME - Multipurpose Internet Mail Extensions
- MTA - Mail Transport Agent
- OSI - Open Systems Interconnection
- P2P - Peer to peer
- PAN - Personal Area Network
- PC - Personal Computer
- POP - Post Office Protocol
- PPP - Point to Point Protocol
- QoS - Quality of Service
- SMTP - Simple Mail Transfer Protocol
- TCP - Transfer Control Protocol
- UDP - User Datagram Protocol
- WAN - Wide Area Network
- WLAN - Wireless Local Area Network

Bridge, Hub, Switch, Router…

Révisions:

What is the difference between an Ethernet hub and a switch?

Quelles sont les différences entre un concentrateur et un commutateur ethernet ?

stephane.frati@unice.fr

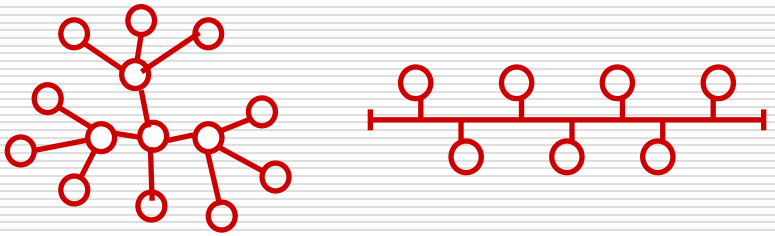
Outline

- MAC address definition
- Simplex/Duplex – Half/Full
- Ethernet Hub
- Cross-over cable
- Bridge
- Ethernet Switch
  - VLAN architecture
  - VLAN Colors
- Router
- Wrap-up

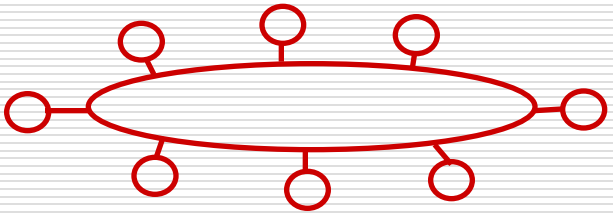
Le niveau liaison de données

Trois grandes technologies dites “ à média partagé” dominent le secteur des réseaux locaux :

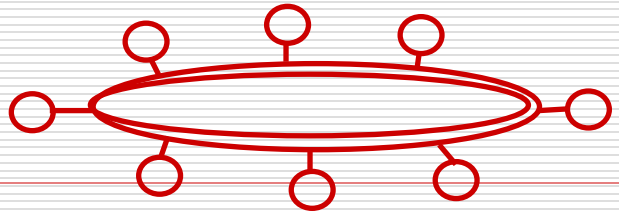
Ethernet :
Conçu à l’origine pour fonctionner en bus logique. Chacun parle quand il veut, le protocole gère les collisions. Fonctionne à 10, 100 Mbps, 1 Gbps, et même 10Gbps
S’universalise sur le marché.



Token Ring :
Anneau à jeton, chacun parle à son tour, quand il obtient le jeton. Fonctionne à 4 et 16 Mbps. Tend à disparaître.



FDDI (Fiber Distributed Data Interface)
Double anneau à jeton, inspiré du Token Ring, mais plus rapide, avec possibilité de traffic synchrone et asynchrone et de garantie de la bande passante. Fonctionne à 100 Mbps sur fibres optiques. Tend à disparaître, et fut longtemps la structure de choix pour les backbones de LAN.



Ces 3 technologies utilisent le **même système d’adressage**

What is an Ethernet MAC address ?

- **MAC = Media Access Control**
- Each and every Ethernet device → a **unique** MAC address, which is "burned" into the hardware when it is manufactured (*Burn-In Address*)
- MAC addresses uniquely identify each node in a network (in a segment of a network)
- Consists of **six bytes** which are usually displayed in hexadecimal
  e.g., *00-0A-CC-32-FO-FD*

- NB: The MAC address/station ID **may be printed on the NIC**

Le niveau liaison de données: Système d'adressage

MAC Address (Medium Access Control)

L'adresse de niveau 2 d'un élément de réseau

Format : 6 octets exprimés en hexadécimal séparés par ":" ou "–"

- l'**OUI (Organization Unique Id)** 3 octets
- l'adresse matérielle spécifique **(Product ID)** 3 octets.

Source MAC Address

L'adresse MAC de la station émettrice

Destination MAC Address

L'adresse MAC de la station destinataire

Unicast MAC Address

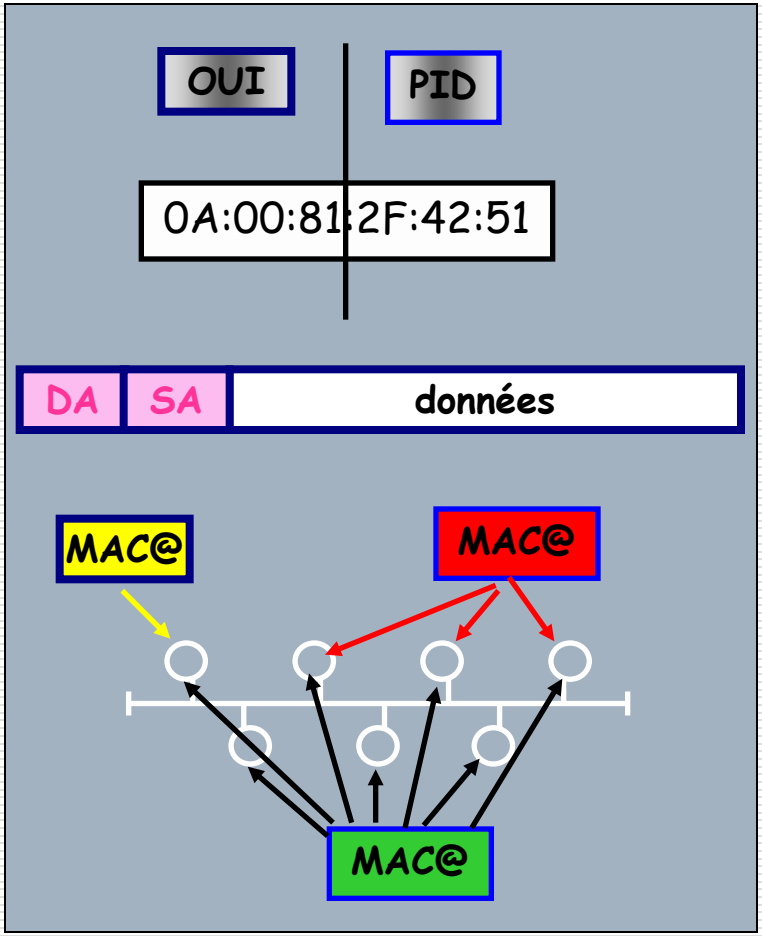
Une adresse MAC désignant une seule station

Multicast MAC Address

Une adresse MAC désignant plusieurs stations (un groupe)

Broadcast MAC Address

Adresse MAC de diffusion qui désigne l'ensemble des stations du domaine de collision concerné..



What is an Ethernet MAC address ?

- The first three bytes (e.g., *00-0A-CC*) are the manufacturer's code
- A vendor/Ethernet MAC address lookup service is available at:
  → http://coffer.com/mac_find/
- MAC address according to the IANA Ethernet-number assignment database
  →http://www.iana.org/assignments/ethernet-numbers

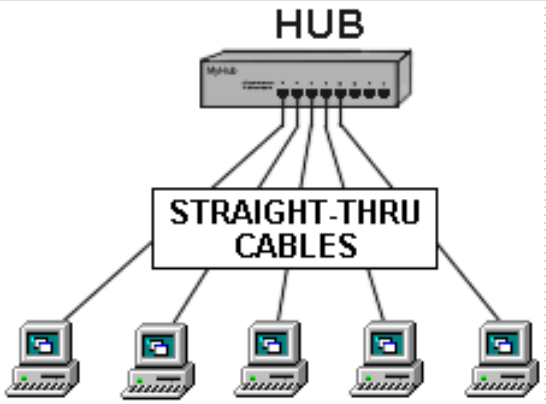
- on Windows 9X/Me: `winipcfg, arp -a`
- on Windows NT, 2000, and XP: `ipconfig /all`
- on Linux: `ip maddr, ip neigh, arp`

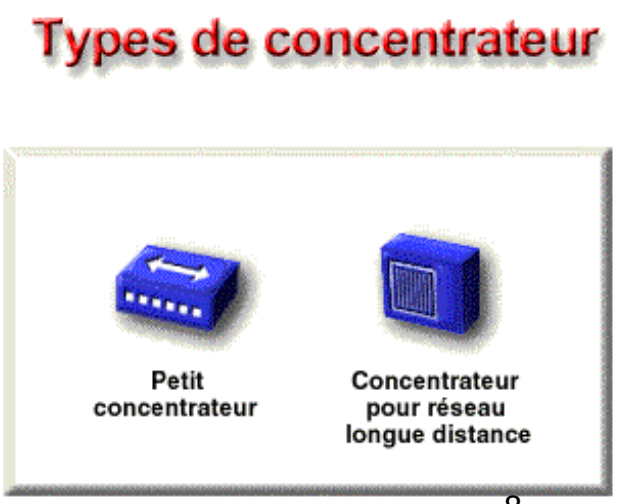
Simplex/Duplex – Half/Full

- **Simplex** transmission: **only one** device transmits – the other receives
- **Duplex** transmission: **both** ends can transmit
  - **Full-duplex** transmission: both ends can transmit at the same time (usually thanks to two parallel channels)
  - **Half-duplex** transmission: only one transmitter at a time
    (Citizen's band - CB radio)

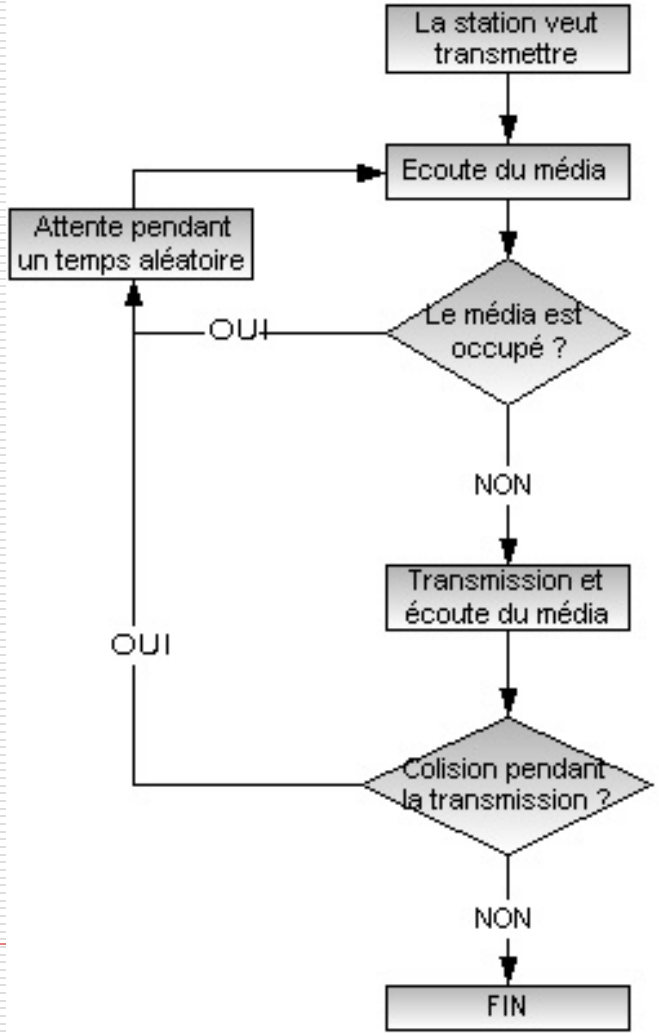
Ethernet Hub

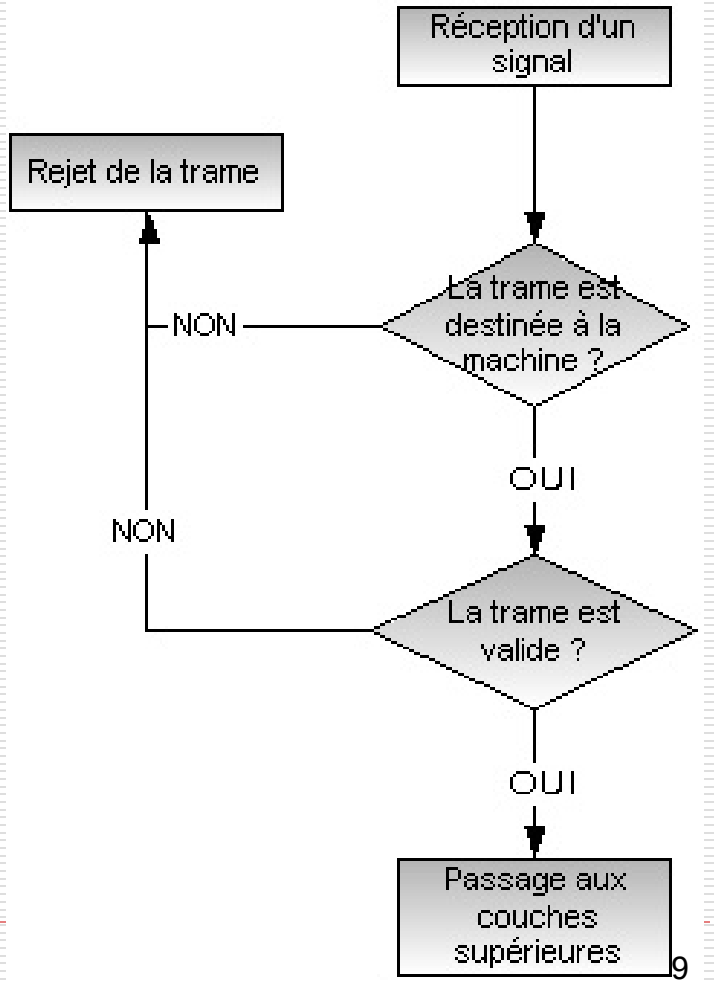
- **same ethernet segment**
- If one sends an ethernet frame, the hub transmits (**repeats**) to **all other**
- If two in the same time ➔ ***collision***
  - hosts must resolve the conflict
  - Each Ethernet Adapter has both a receiver and a transmitter
  - Ethernet Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**) protocol



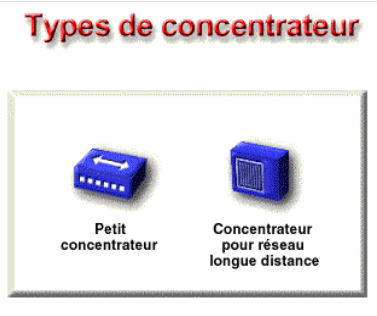


Le fonctionnement de CSMA/CD
Carrier Sense Multiple Access/Colision Detection



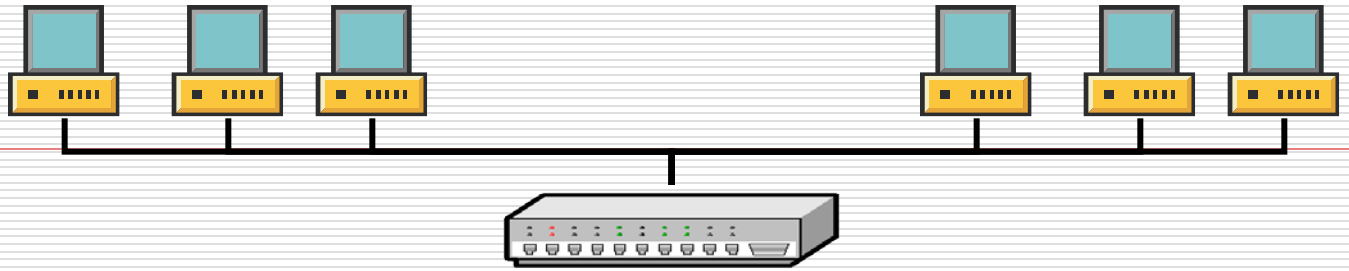


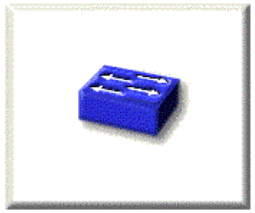
Ethernet Hub



- If collisions are avoided, adapters would be able to send data at the same time they are receiving it (full-duplex)

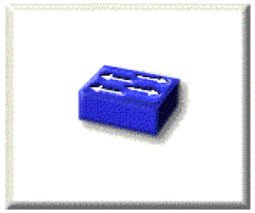
- If the maximum bandwidth (rate!) is 100Mbps and that the rate is shared by all of the PC's connected to the hub, guess...





Ethernet Switch

- Switch == **link between several segments** of network using same or different layer 1
- Operates at **layer 2** (it only watches the ethernet header)
- Progressively builds an **address table** (or MAC table) with port numbers and corresponding connected MAC addresses



Ethernet Switch

- When a switch receives a frame:
  - Looks at the destination MAC address
  - Looks for the corresponding port to send the frame out in its address table
  - Sends out the frame only through this port
- Allows full-duplex mode because it precludes collisions
- Can operate at 1 Gbps
- Device does not need an IP address
- Be careful of loops
  - Standard → **Spanning Tree protocol**
  - Proprietary → **Hirschmann HyperRing**
    http://www.industrialnetworking.com/Flash/Ring_Redundancy.html

Bridging

- Bridge == **switch** with only 2 ports

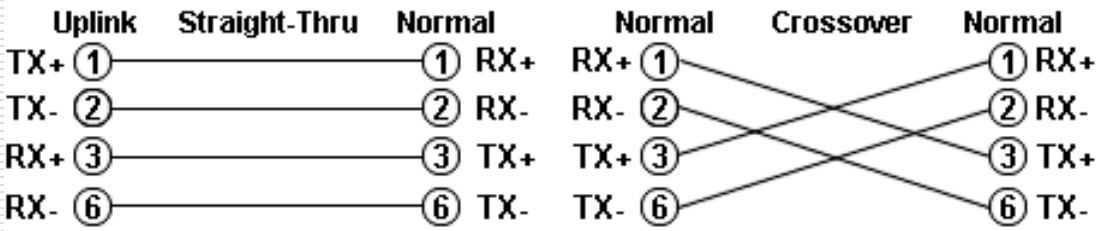
Crossover and Straight-through cables

- 2 categories of equipments:

MDI { workstations, routers

MDIX { hubs, switchs

- Possible cables:



- Connections required:

Straight-through cable

MDI ⟷ MDIX

MDIX ⟷ MDI

Crossover cable

MDI ⟷ MDI

MDIX ⟷ MDIX

Router

- A router is just barely smarter than a switch. It only gets a data packet if the destination computer isn't on the same subnet or LAN. The router then figures out where in what direction this packet must be forwarded.

- Routers use network address information (operating in the Network layer) to move data through the best path to its destination

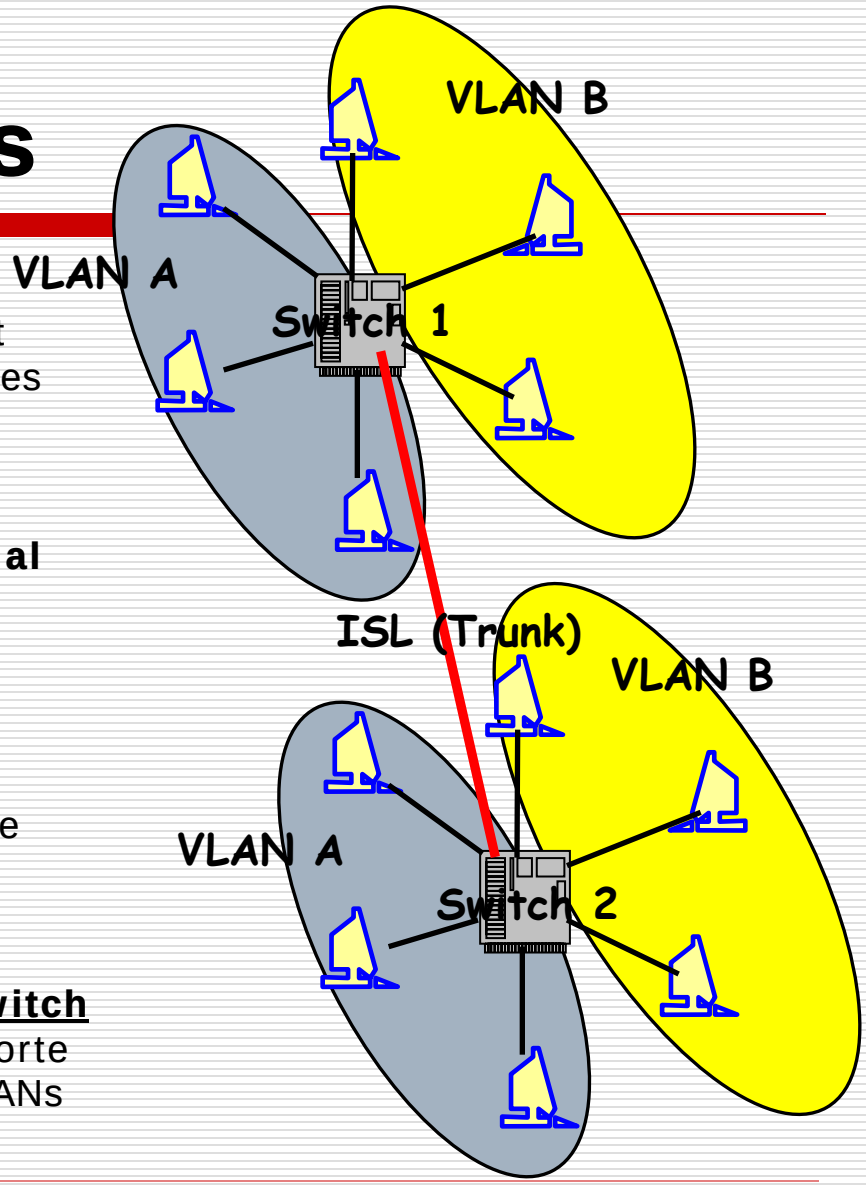
Architecture à base de switches

Fonctionne comme un pont transparent et doit donc être configuré en **Spanning Tree** avec ses collègues, pour éviter les boucles.
Permet de définir des groupes de machines formant des LAN arbitraires, changeables par logiciel au gré de la configuration : les « **Virtual LAN** » (**VLAN**)

Il existe plusieurs types de VLAN
→ voir plus loin

Plusieurs switches peuvent supporter un même ensemble de VLAN, on parle de **domaines de commutation.**

Ils sont alors reliés entre eux par un **Inter Switch Link**, aussi appelé **Trunk** (Tronçon), qui supporte sans les mélanger les trafics des différents VLANs (norme **IEEE 802.1Q** → voir plus loin)



VLAN (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*)

- Le VLAN permet de s'affranchir des limitations de l'architecture physique
  - contraintes géographiques,
  - contraintes d'adressage,
  - …
- en définissant:
  - une **segmentation logique** (logicielle)
    → un domaine de broadcast de niveau 2 indépendant du LAN physique
  - basée sur un regroupement de machines grâce à des critères :
    - adresses MAC,
    - numéros de port,
    - protocole,
    - etc…

Typologie de VLAN

Définition de VLAN selon
le critère de commutation
et le niveau auquel il s'effectue :

- Un **VLAN de niveau 1**
  (**VLAN par port**, ***Port-Based VLAN***)
  - définit un réseau virtuel en fonction des ports de raccordement sur le commutateur

- Un **VLAN de niveau 2**
  (**VLAN MAC**, **VLAN par adresse IEEE** ou ***MAC Address-Based VLAN***)
  - consiste à définir un réseau virtuel en fonction des adresses MAC des stations
  - beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station

Typologie de VLAN

Un **VLAN de niveau 3** : plusieurs types de VLAN de niveau 3 :

- Le **VLAN par sous-réseau** (***Network Address-Based VLAN***)
  - associe des sous-réseaux selon **l'adresse IP source** des datagrammes
  - apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station
  - mais une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- Le **VLAN par protocole** (***Protocol-Based VLAN***)
  - permet de créer un réseau virtuel par type de **protocole** (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau

Les avantages du VLAN

- Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :
  - Plus de **souplesse pour l'administration** et les modifications du réseau car toute l'architecture peut être modifiée par simple paramètrage des commutateurs
  - **Gain en sécurité** car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées →Les VLANs ne peuvent pas se parler entre eux, sans l'intervention d'un routeur
  - **Réduction de la diffusion** du traffic sur le réseau

- Les VLAN sont définis par les standards IEEE:
  - 802.1d,
  - 802.1p,
  - 802.1q
  - et 802.10

"VLAN Colors"

- Le VLAN switching est accompli par le "frame tagging"
- Le trafic issu et contenu dans une topologie de VLAN particulière transporte un **identifiant unique** de VLAN (VLAN ID) quand il cheminera sur un backbone ou un **trunk**

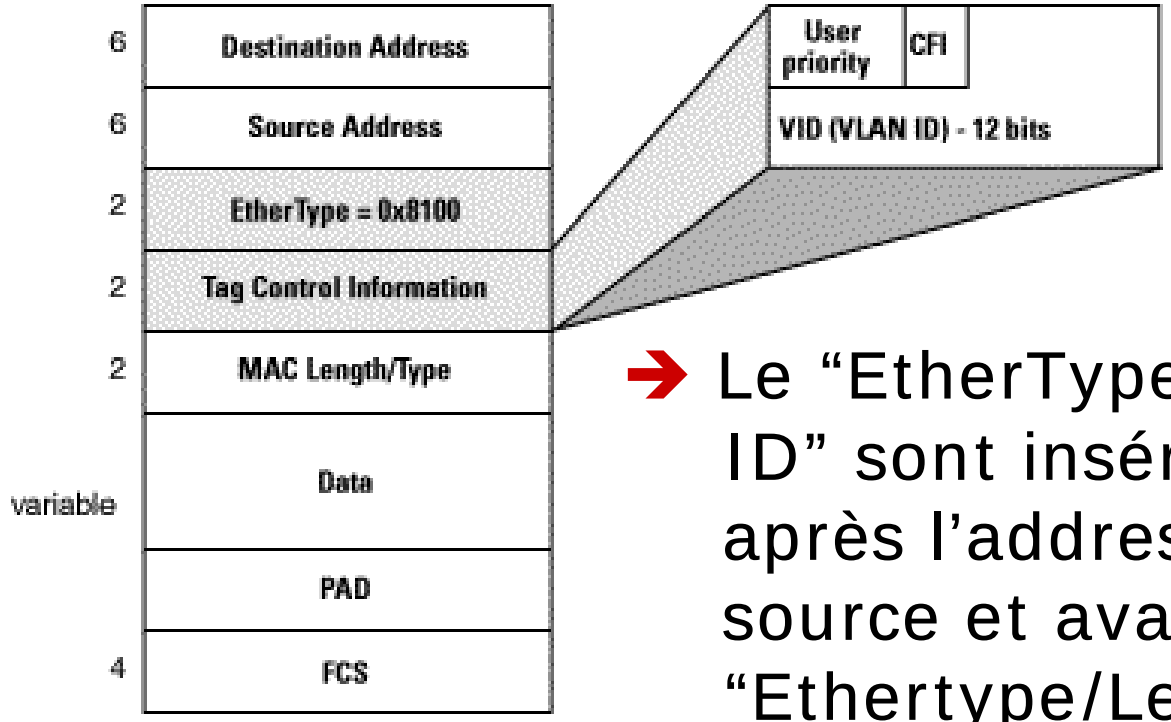
- Chaque VLAN est differentié par une **couleur** ou **VLAN Id**entifier

- Le VLAN ID permet aux éléments de commutation de VLAN de prendre des décisions de transfert intelligentes ("**intelligent forwarding""**) basées sur le **VLAN ID** embarqué dans chaque trame

“VLAN Colors”

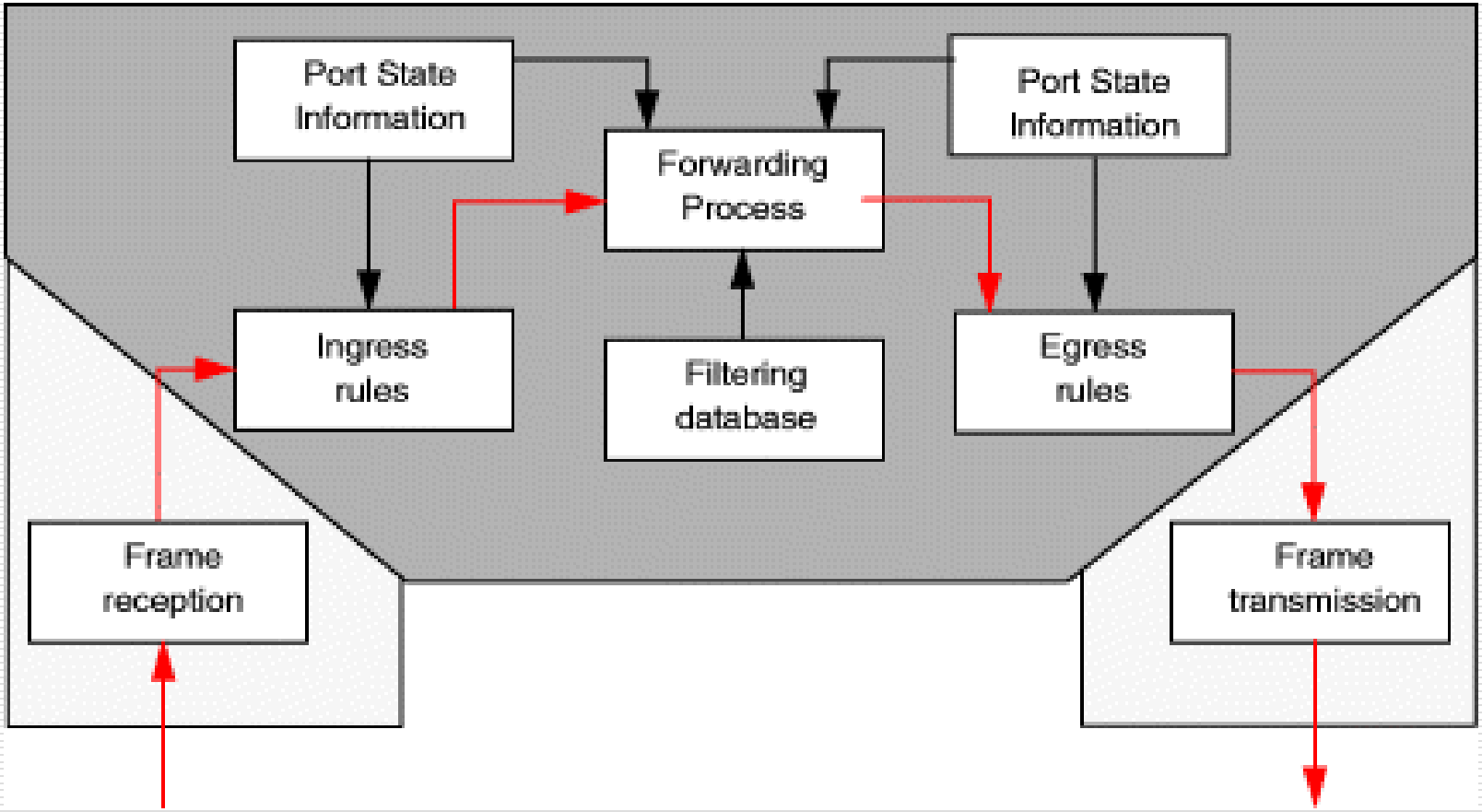
- Le VLAN ID permet aux commutateurs de VLAN et aux routeurs de sélectivement **autoriser le transfert des trames** aux ports destinataires appropriés affichant le même VLAN ID
- Le switch qui reçoit une trame d’une station source devra y insérer le VLAN ID et commuter ce paquet ainsi “coloré” sur le backbone partagé ➔ **VLAN TAG**
- Quand la trame sortira du réseau local commuté, le dernier switch en retirera le VLAN ID de l’en-tête pour la transférer sur les interfaces qui correspondent à cette couleur de VLAN
- Pour communiquer entre VLAN, les routeurs s’appuient sur le protocole IEEE 802.1Q pour effectuer leurs décisions de routage

802.1Q – Où est le Tag ?



➔ Le “EtherType” et le “VLAN ID” sont insérés juste après l’addresse MAC source et avant le champ “Ethertype/Length” ou “Logical Link Control (LLC)”

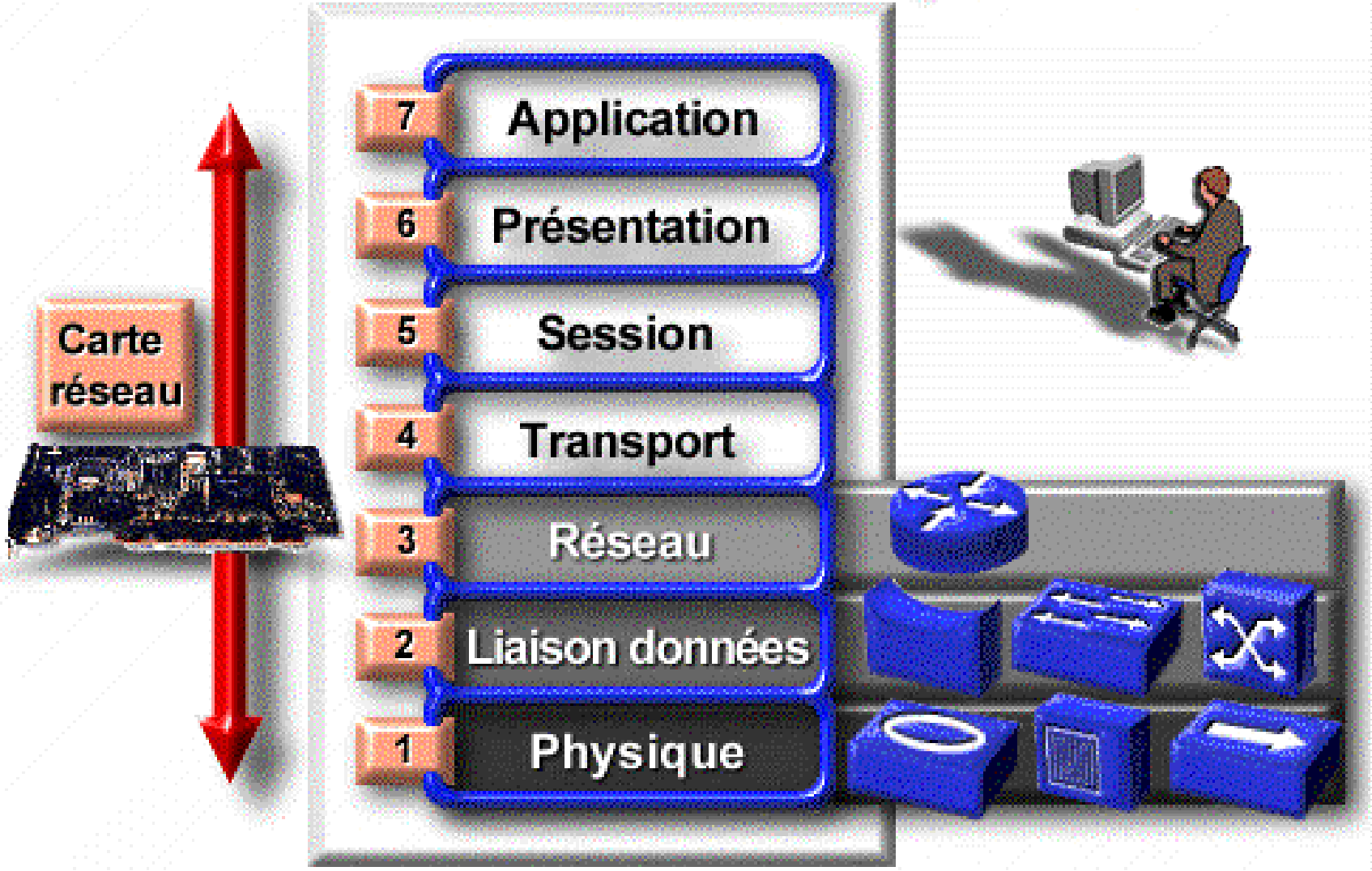
Que se passe-t-il dans le switch effectuant du VLAN tagging ?



Wrap-up in simple words…

- **HUB**: plug some computers into this, and all traffic is shared. In other words, if computer 1 talks to computer 3, computer 2 will also hear what computer 1 says. Usually computer 2 just discards traffic not meant for it, but it does tend to burden your network.
- **SWITCH**: if computer 1 talks to computer 3, computer 2 hears nothing. On high-traffic networks, this means downloads & uploads go a little faster for everyone. On low-traffic networks (home networks) users typically do not notice a difference.
- **BRIDGE**: joins two segments at layer 2
- **ROUTER**: at the border of different networks. Add filtering and you build a firewall.

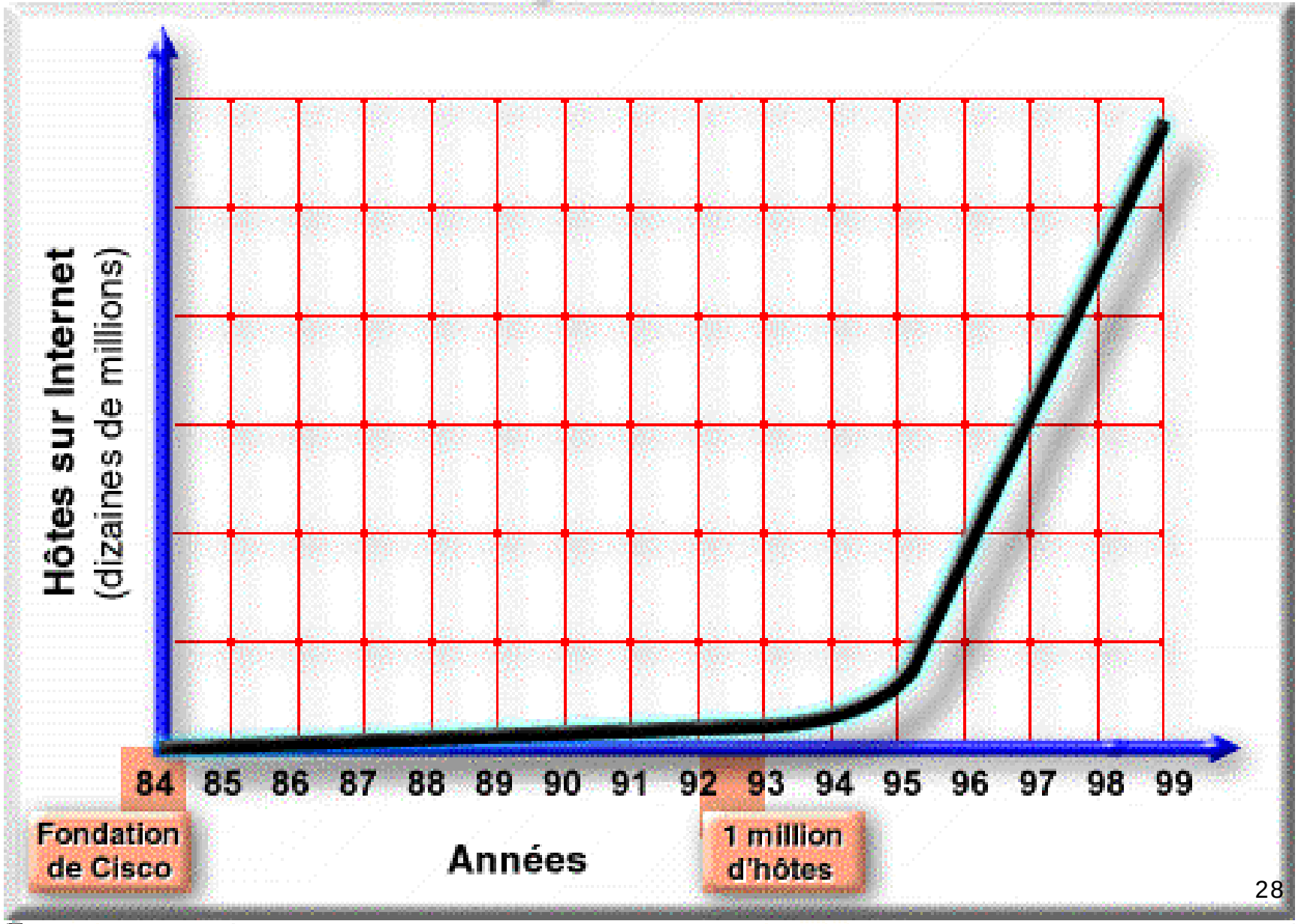
Unités et couches correspondantes



Dates importantes en communication de données

Avant 1900	Communications longue distance par messager, cavalier, signaux de fumée, pigeon voyageur, télégraphe optique, télégraphe électrique
189x	Bell invente le téléphone; le service téléphonique s'étend rapidement
1901	Première transmission transatlantique sans fil de Marconi
192x	Radio AM
1939	Radio FM
194x	2e guerre mondiale favorise le développement de la radio et des micro-ondes
1947	Shockley, Barden et Grittain inventent le transistor en solide (semi-conducteur)
1948	Claude Shannon publie " A Theory of Electronic Communication ", peut-être l'article le plus important
195x	Invention des circuits intégrés
196x	Informatique sur gros ordinateur
1962	Paul Baran de RAND travaille sur les " réseaux à commutation de paquets "
1967	Larry Roberts publie le premier article sur ARPANET
1969	ARPANET est établi à UCLA, UCSB, Stanford et université de l'Utah
1972	Ray Tomlinson crée un programme pour envoyer des messages électroniques (courriel)
197x	Emploi généralisé des circuits intégrés numériques; apparition des ordinateurs personnels numériques
1973	Bob Kahn et Vint Cerf commencent à travailler sur ce qui est plus tard devenu TCP/IP
1981	Le terme Internet est attribué à une série de réseaux en connexion
198x	Utilisation répandue des ordinateurs personnels et des mini-ordinateurs fondés sur Unix
1982	L'ISO publie le modèle et les protocoles OSI; les protocoles disparaissent mais le modèle est très influent
1984	Introduction de DNS (Domain Name Service - service de nom de domaine)
1984	Fondation de Cisco Systems
1991	Tim Berners-Lee développe le code pour le Web
1993	Introduction de Mosaic, le premier navigateur à interface graphique
1994	Introduction de Netscape Navigator
Fin 198x	Le nombre d'utilisateurs Internet double tous les six mois (croissance exponentielle) jusqu'à maintenant
1998	Cisco réalise 70 % de ses ventes via Internet; lancement de Networking Academy
1999	Course des grandes entreprises à la convergence données, voix et vidéo

Croissance exponentielle d'Internet

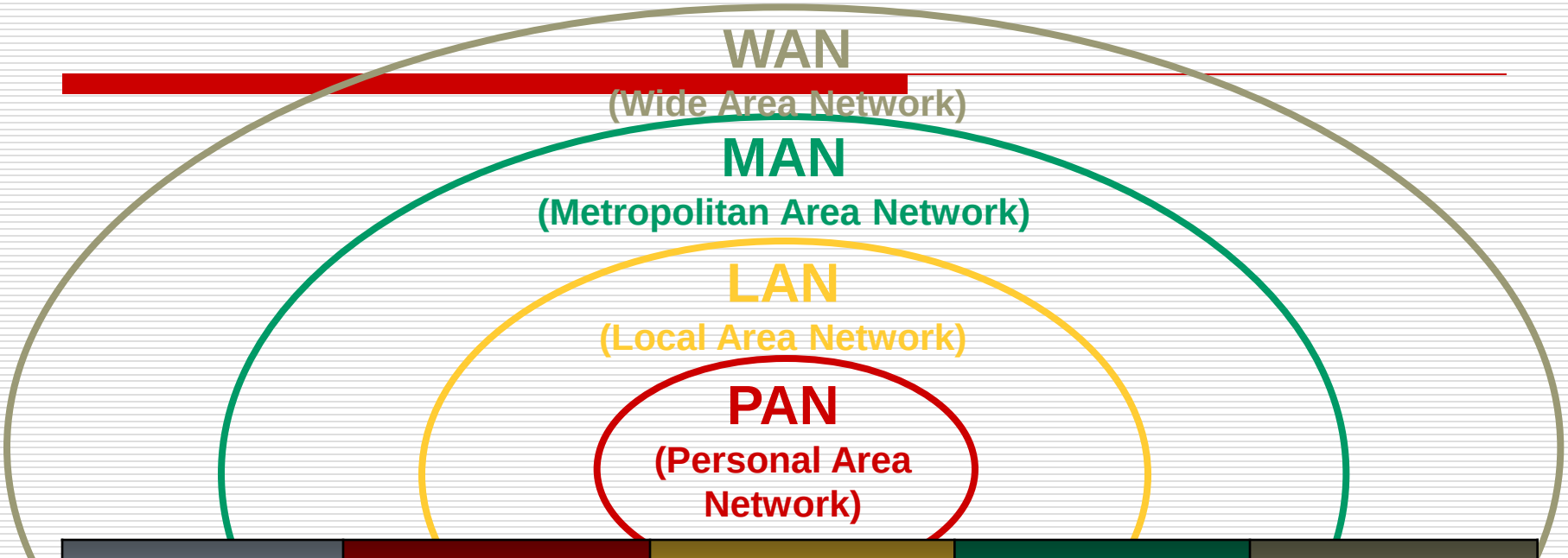


Wireless Networks
Réseaux sans-fil

Tour d'horizon des technologies sans fil

stephane.frati@unice.fr

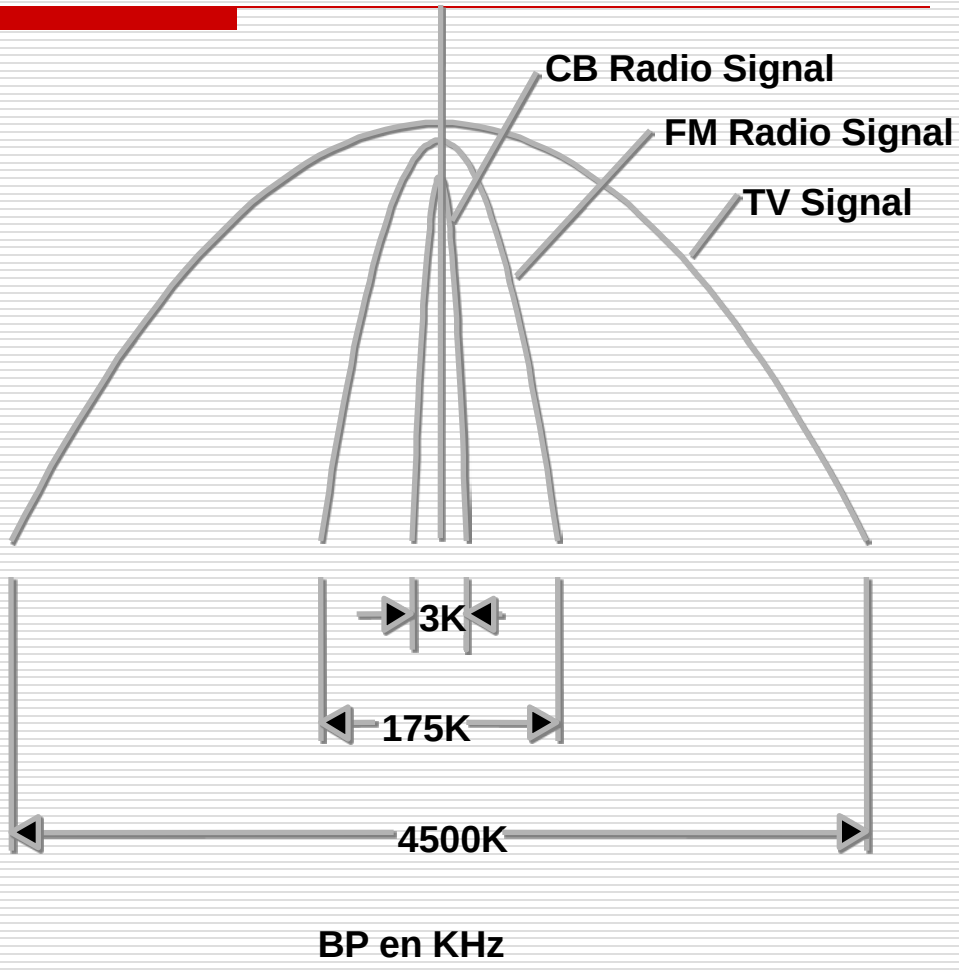
Technologies Sans-fil



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, b, g, n HiperLAN2	802.11, 802.16 WiMAX	GSM, GPRS, CDMA, 2.5-3G
Vitesse	< 1 Mbps	2 à 200 Mbps	75 Mbps	10 Kbps à 7 Mbps
Couverture	Faible	Moyenne	Moyenne-Etendue	Etendue
Applications	Point-à-point Equipement-à-equipement	Réseaux d'Entreprises	Fixe, accès au dernier kilomètre	PDA, GSM, ...

Bande passante en fréquence nécessaire à la transmission de l'information

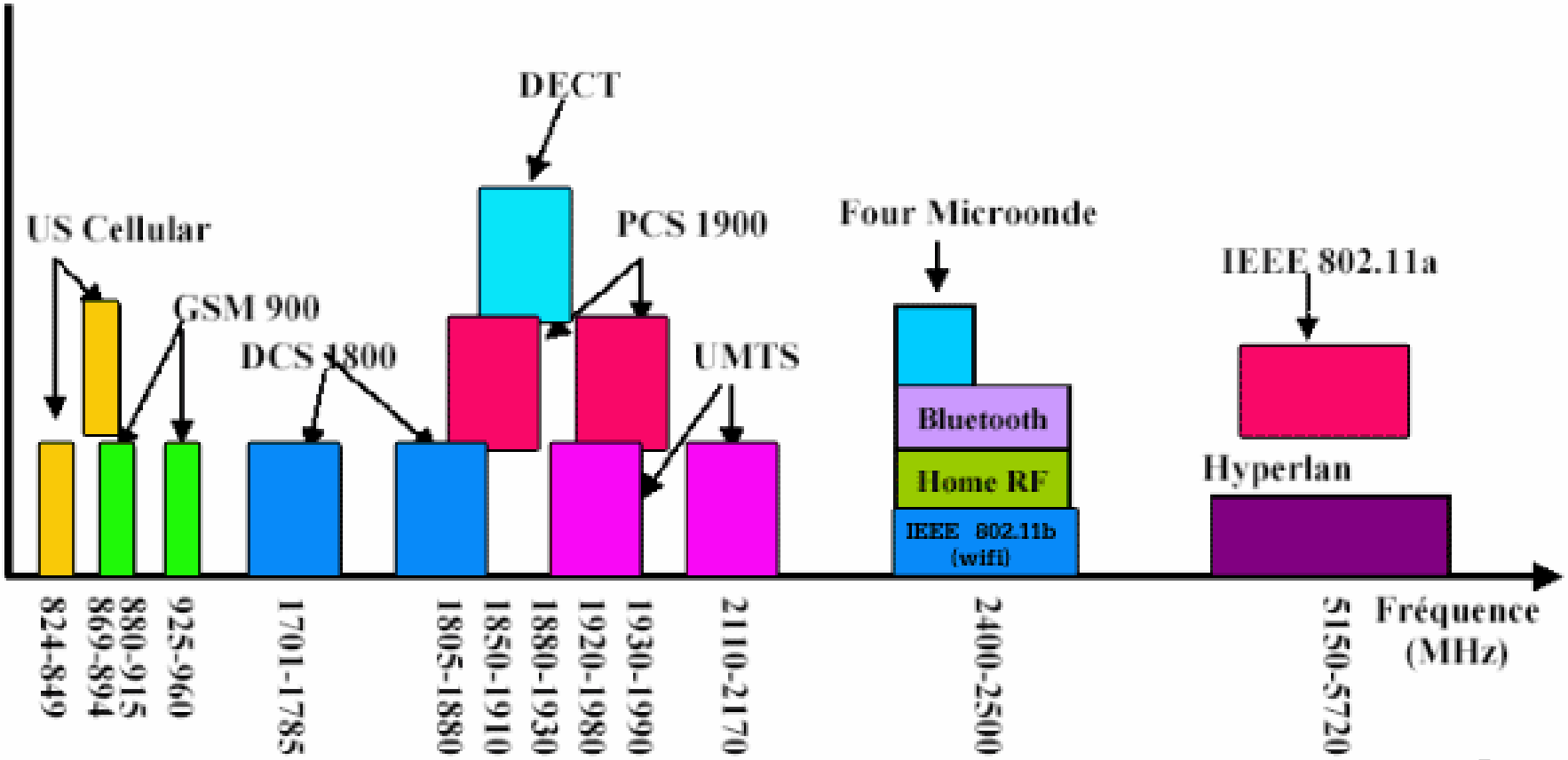
- Une largeur de bande plus grande permet un débit plus élevé.



Critères de choix

- Distance (couverture)
- Débits : 0,1 → 100 Mbps
- Mobilité
  - Indoor: stationnaire, marche
  - Outdoor: stationnaire , marche, motorisé
- Prix

Bandes de fréquences utilisées

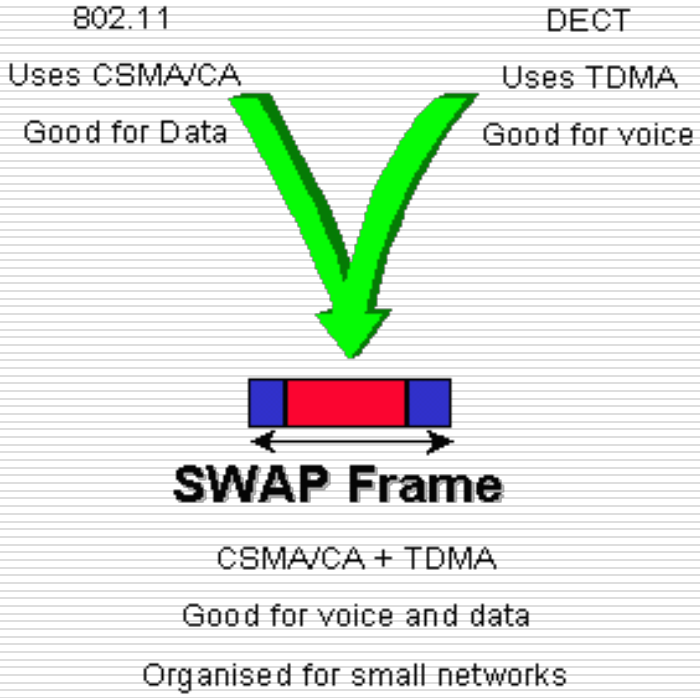


Les technologies WPAN

- Objet:
  échange d'information entre deux équipements proches

- **Home RF**

  - lancé en 1998
  - débit théorique: 1.6Mbps
  - utilisations actuelles:
  faibles en Europe, concurrencé par Wifi



Les technologies WPAN

- **Bluetooth:** IEEE 802.15.1

- lancé en 1994, précurseur des réseaux WPAN
- fréquence: 2402-2480 MHz
- FHSS, GFSK
- débit: 1-3 Mbps théorique
- portée: 10 à 30 m
- low power: 2.5 mW
- utilisations actuelles: échange données sur téléphone, PDA pour synchronisation
- number of nodes: 7

Les technologies WPAN

- **ZigBee:** IEEE 802.15.4

- low cost, low power (energy detection)
- range: 100m
- low data rates: 250 Kbps
- self-organizing mesh networks: WSN, AODV
- frequency: Europe- 868 MHz, USA- 915 MHz,
  2.4 GHz elsewhere
- number of nodes: 65000

Les technologies WLAN

IEEE 802.11

Protocole	Date de normalisation	Fréquence	Débit typique	Débit max	Portée en intérieur	Portée en extérieur
802.11a	1999	5.18-5.8 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~35 m	~100 m
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11n	2009	2.4 ou 5 GHz	200 Mbit/s	540 Mbit/s	~50 m	~125 m

Les technologies WLAN

- Objet:
  échange d'information entre deux ou plusieurs équipements locaux

- **Hiperlan**
  - lancé en 1991
  - fréquence: 5Ghz
  - bande passante théorique: 20/54Mbps
  - portée: + 30 m
  - utilisations actuelles: faibles en Europe, concurrencé par Wifi

Les technologies Cellulaires

GSM

- lancé en 1987
- technologie numérique
- fréquence 900/960-1700/1880MHz
- traitement voix (et données)
- débits de données: 43 Kbps fixe, 10Kbps mobile
- utilisations actuelles: téléphonie mobile

Les technologies Cellulaires

- GPRS/2.5G - UMTS

- pour le transfert de données

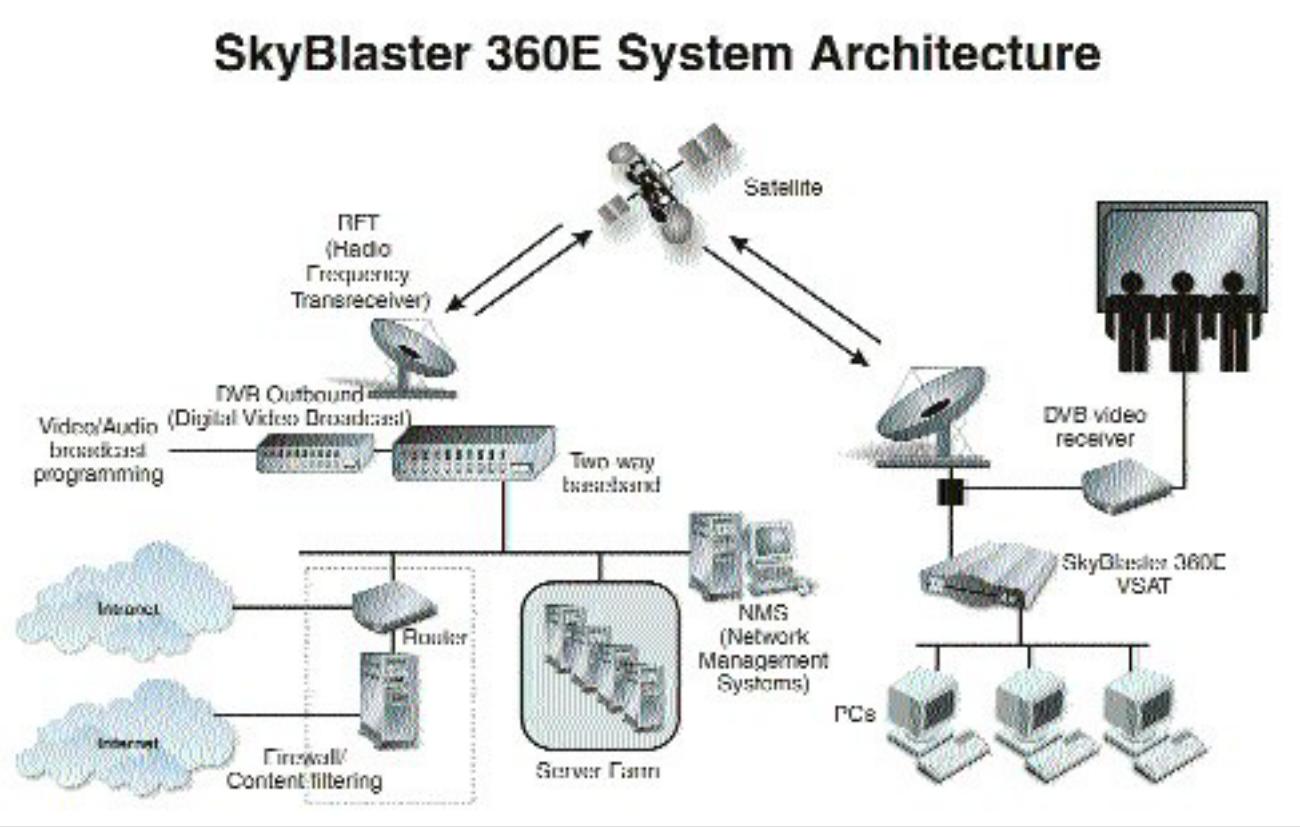
- lancement 2003

- débit théorique données:
    - GSM avec GPRS (2.5G): débit <56Kbps
    - Edge: débit de 100 à 200 Kbps
    - UMTS (3G): 384Kps
        - 3G+ HSDPA: 1.8Mbps -> 7.2 Mbps
        - 3G+ HSUPA: 1.4 Mbps

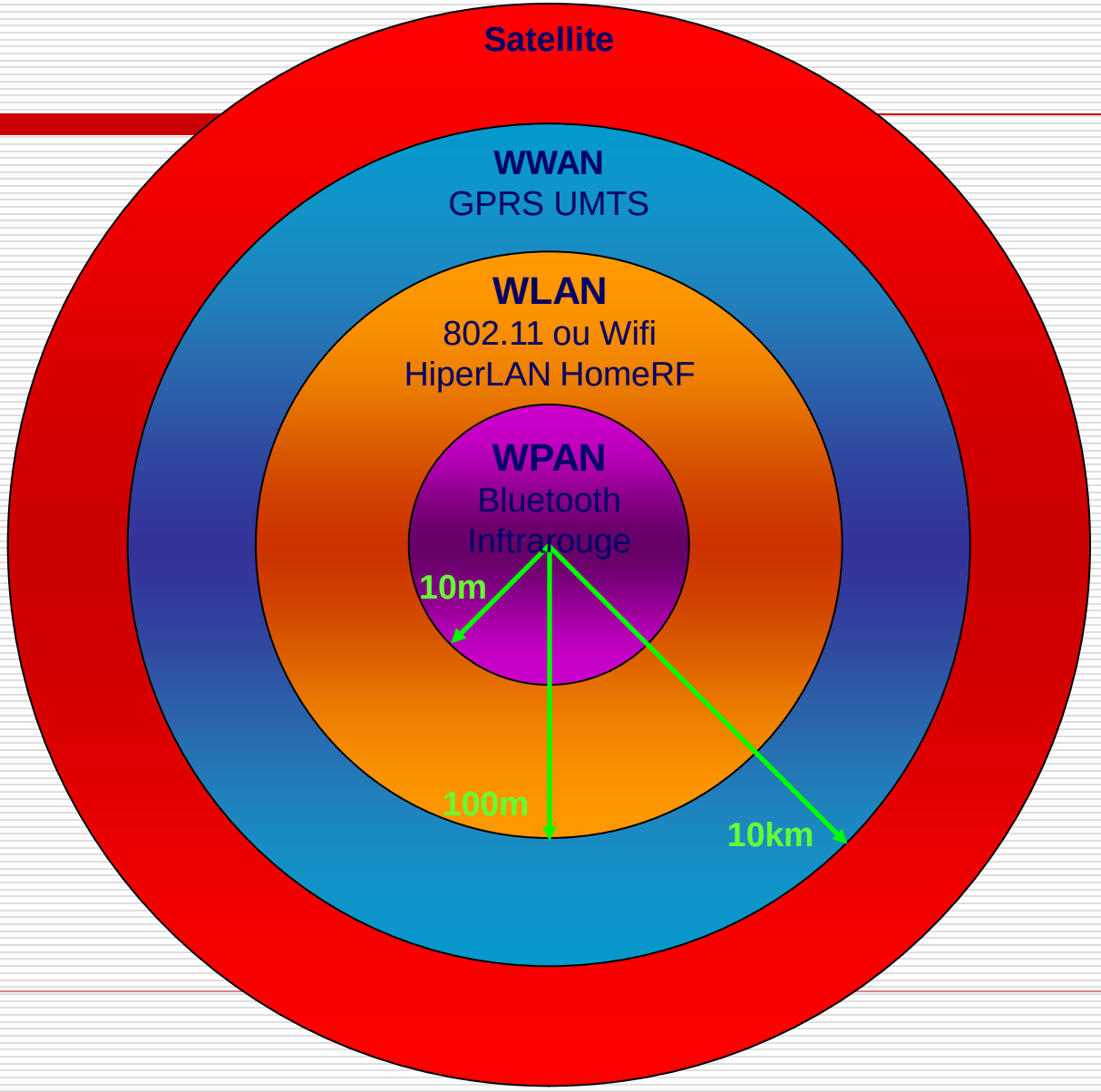
Les technologies satellite

- **Internet par satellite:**
  - pour zones rurales où les connexions câblées ou DSL ne sont pas disponibles
  - Antenne parabolique pour communications de données bidirectionnelles.
  - La vitesse uplink représente environ 1/10^{e} de la vitesse downlink qui est de 500 Kbits/s.
  - Les connexions câble et DSL présentent des vitesses de chargement plus élevées, mais les systèmes par satellite sont dix fois plus rapides qu'un modem analogique.
  - Pour accéder: antenne parabolique, deux modems (liaison montante et liaison descendante), et des câbles coaxiaux reliant l'antenne au modem.

Les technologies satellite



Positionnement du Wireless



Wi-Fi

bases théoriques

et pratiques

Patrick VINCENT
pvincent@erasme.org

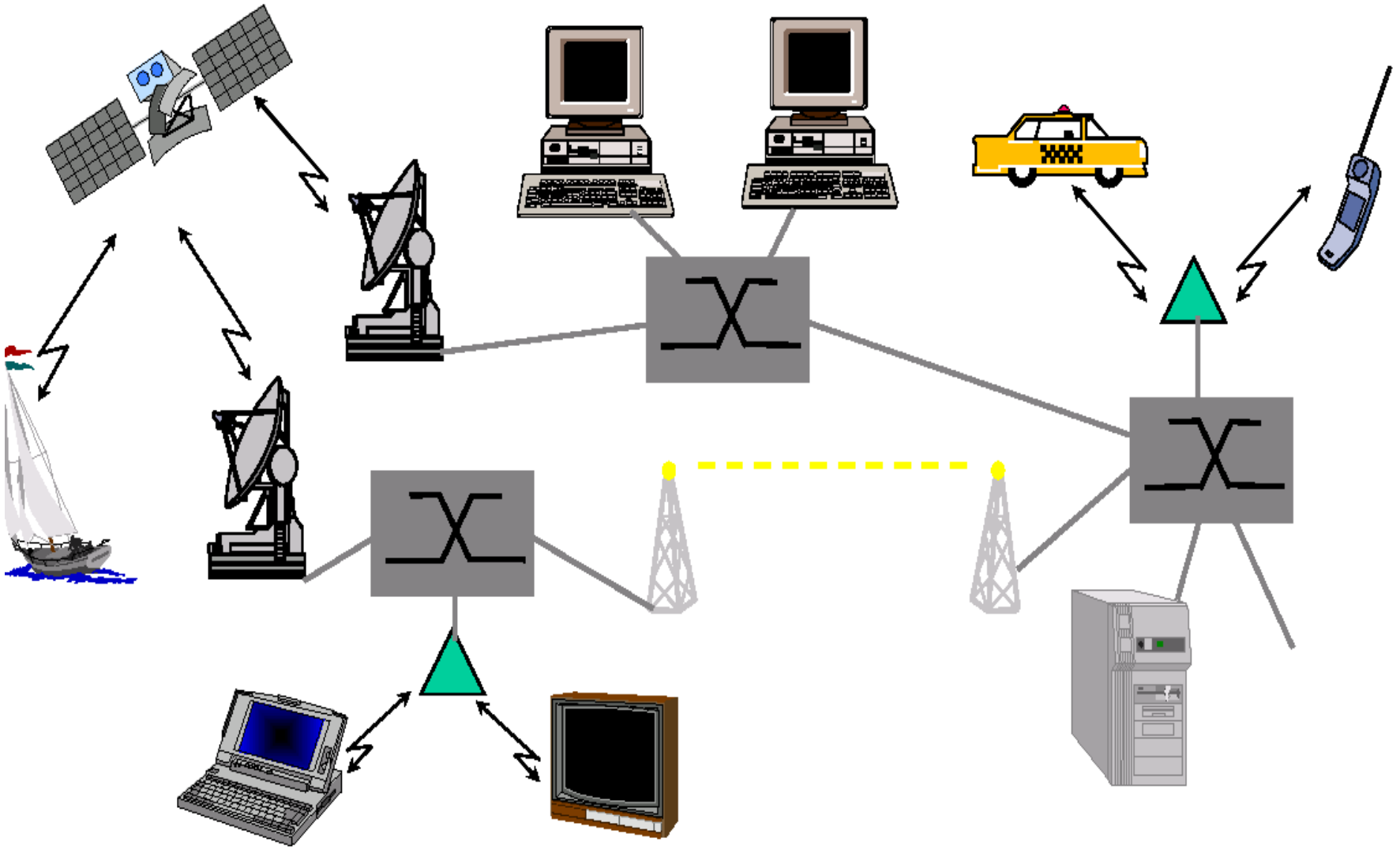
Objectifs

- Maîtriser les aspects théoriques de la norme WiFi et les notions de propagation radio
- Être capable de configurer un réseau sans fil local simple : aspects réseau (IP) et radio (WiFi)
- Être capable d'analyser une problématique de desserte sans fil et de dimensionner une solution
- Maîtriser les aspects liés à la sécurité des configurations

Partie 1

Les réseaux sans fil

Le sans fil omniprésent ?



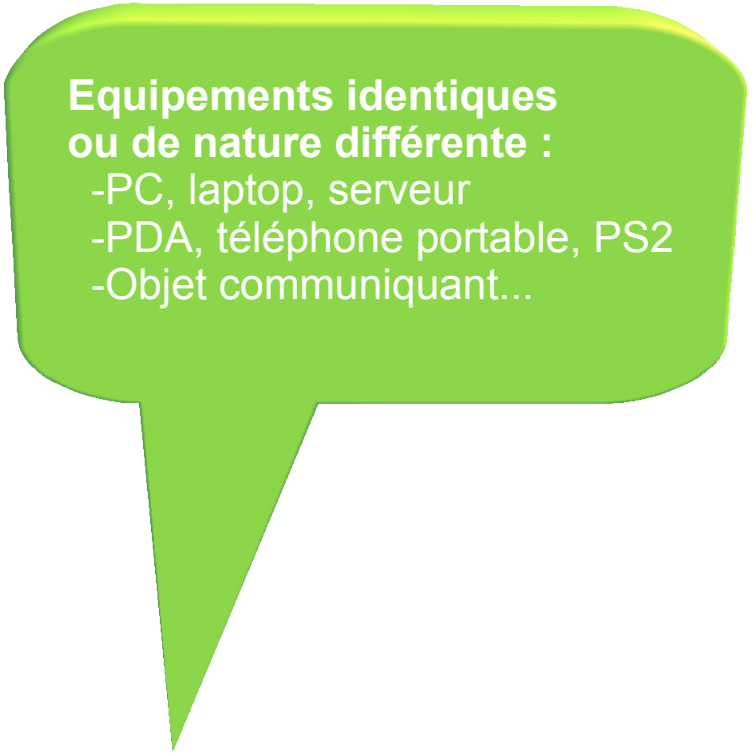
Source : anonyme sur Internet

Définition

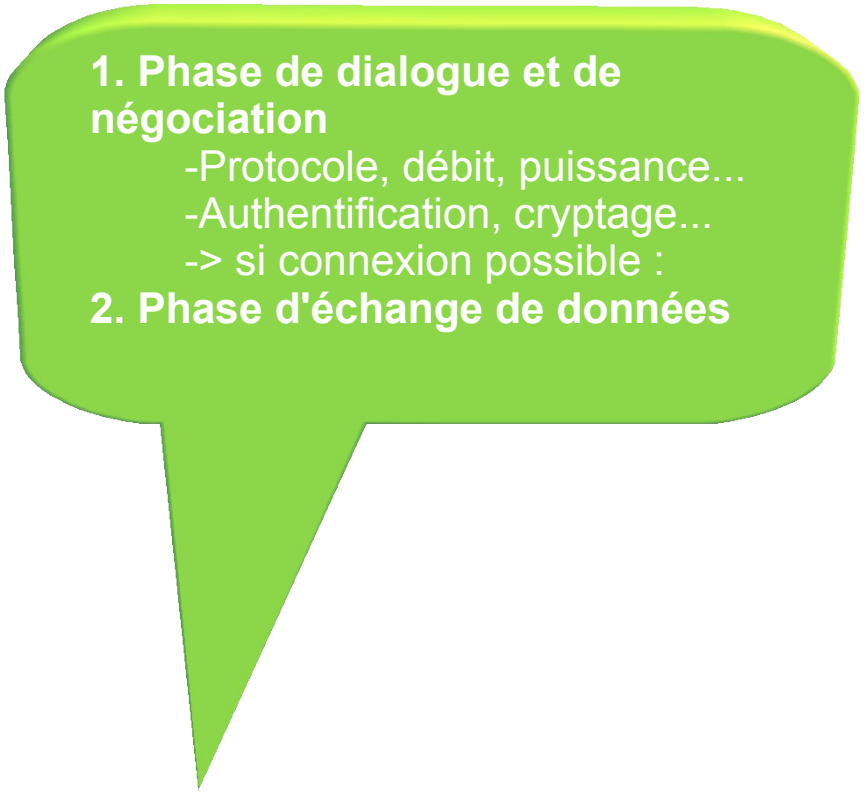
- Des protocoles sans fils connus... et inconnus :
  - IR, Bluetooth, RFID, Zigbee
  - GPS, GPRS, UMTS (3G), Satellite
  - WiFi, Wimax

- Définition d'un réseau sans fil :

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

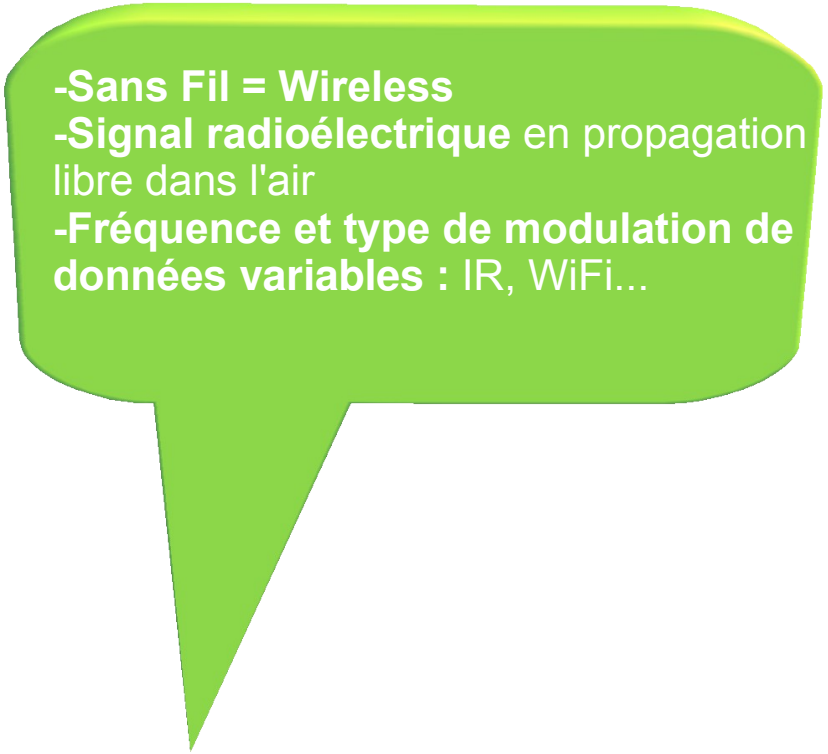


« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »



« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »



« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

Distinction récente pour caractériser une liaison selon :

-la vitesse de déplacement

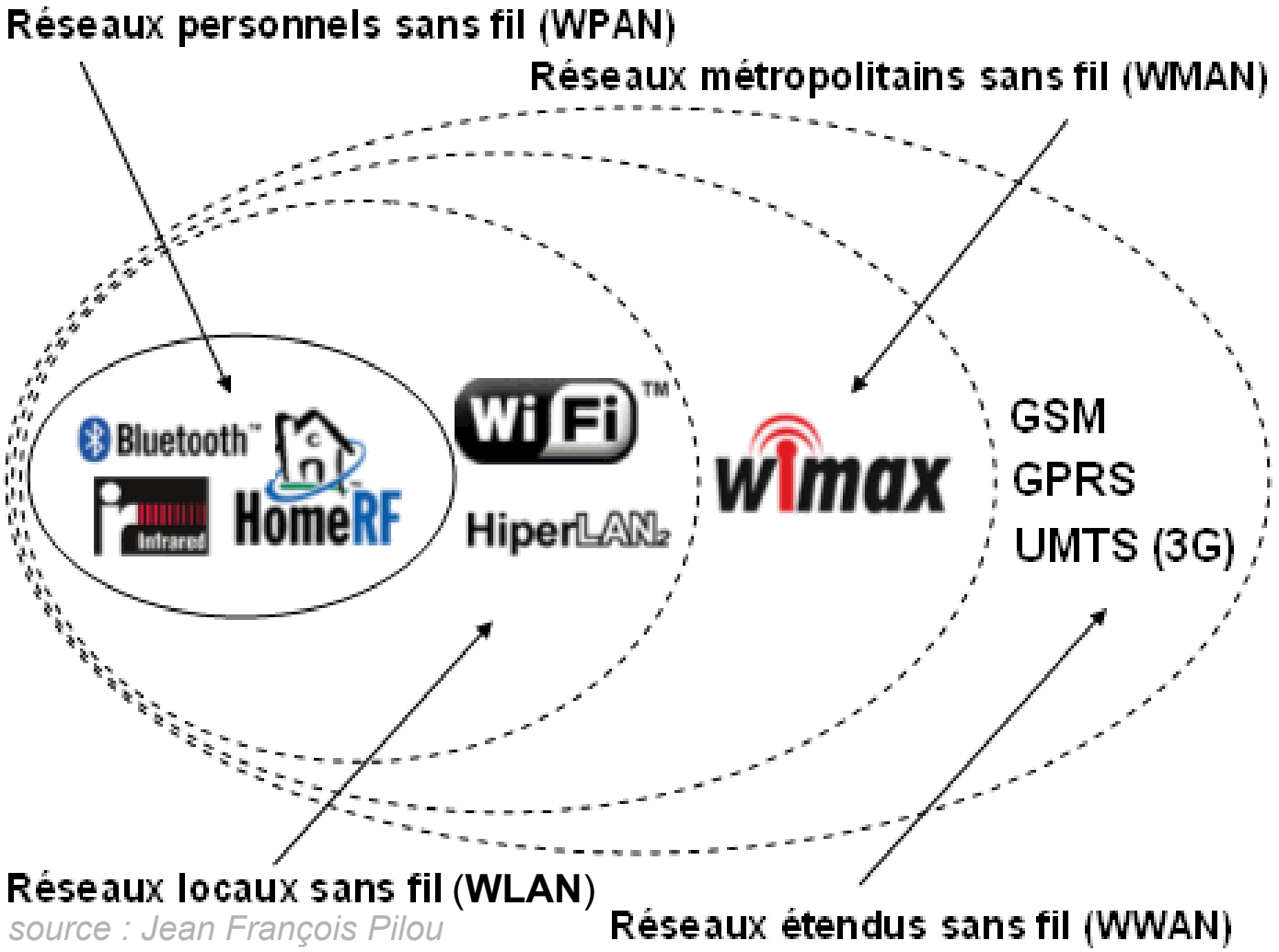
-la zone de couverture

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement... en permettant un déplacement du terminal »

Critères de classification

- Radio : fréquence, modulation et puissance
- Protocole de communication et de sécurité
- Terminaux supportés
- Architecture (topologie) du réseau
- Débit
- Portée
- Coût

Les catégories de réseau sans fil



source : Jean François Pilou

Intérêt du sans fil

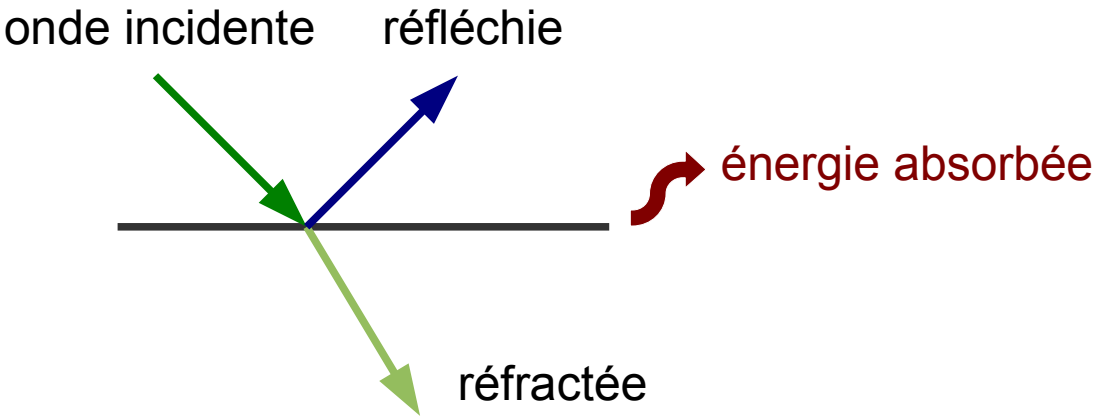
- Facilité de déploiement
- Interopérabilité avec les réseaux filaires
- Débits adaptés à un usage professionnel
- Grande souplesse et faiblement structurant (chantier, exposition, locaux temporaires)
- Non destructif (monuments historiques, sites classés)
- Grande mobilité
- Coût

... et contraintes

- Limites des ondes radio
  - sensibles aux interférences (micro-ondes, autre réseau...)
  - occupation progressive des bandes de fréquence : autorégulation
- Sécurité : données circulant librement
  - nécessite de déployer des solutions de sécurité adaptées
- Réglementation
  - fréquences et puissances d'émission contrôlées par l'Etat
- Débit : mutualisé et variable
  - Partagé entre les utilisateurs et dépendant des conditions d'usage
  - Globalement dix fois inférieur au filaire
- Aspects sanitaires

Notions de propagation radio

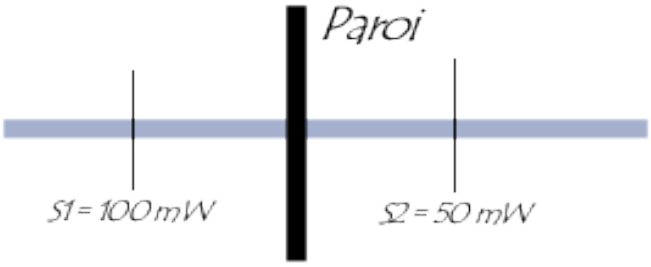
- Les ondes radio se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
- Leur vitesse dans le vide est de 3.10^8 m/s
- Lorsqu'elle rencontre un obstacle, l'onde est divisée et son énergie est répartie :



Gain et atténuation

- Atténuation
  - Lorsqu'elle traverse un obstacle, une partie de l'énergie de l'onde est absorbée
- Amplification
  - Lorsqu'il est capté par une antenne, la puissance du signal de l'onde est amplifié
- L'atténuation (ou le gain) est le rapport entre la puissance du signal avant et après modification

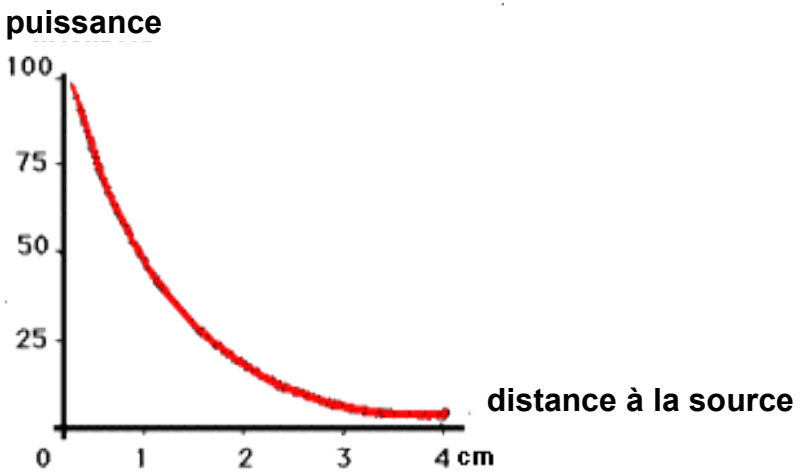
Atténuation (dB) = (10) * log (S2/S1)



$$R\,(dB) = 10 \log \left(\frac{S2}{S1} \right) = -3\,dB$$

Absorption des ondes

- L'énergie d'une onde électromagnétique est progressivement dégradée au cours de sa propagation dans l'air
  - L'onde électromagnétique qui voyage rencontre des électrons qu'elle va exciter. Ceux-ci vont ré émettre à leur tour du rayonnement ce qui perturbera le signal et donc l'atténuera.
- Les signaux se dégradent avec la distance et avec les obstacles, limitant ainsi la portée et le débit de la liaison



Cas perturbants liés au WiFi

- Fréquence
  - La **fréquence** moyenne de la porteuse du WiFi est de **2,437 Ghz**
  - La fréquence de résonance de l'eau est de **2,45 Ghz**
- Longeur d'onde
  - La longueur d'onde du WiFi est de 12,31 cm
  - **Le quart d'onde** (taille des objets absobant l'énergie de cette onde) est de **3,05 cm**
- Les éléments contenant de l'eau et / ou de taille proches de 3 cm absorbent facilement l'énergie du signal du Wi-Fi (feuilles par exemple)

L’eau n’absorbe pas les microondes !

The Nonexistent Microwave Absorption Peak of Water

Spread spectrum was patented in the early 1940s by Austrian-born actress Hedy Lamarr. She was certainly better known for other reasons: appearing in the first nude scene on film in the Czech film *Ecstasy*, her later billing as "the most beautiful woman in the world" by Hollywood magnate Louis Mayer, and as the model for Catwoman in the Batman comics.

It is often said that microwave ovens operate at 2.45 GHz because it corresponds to a particular excitation mode of water molecules. This is sometimes even offered as a reason why 802. 11 cannot be used over long distances. If atmospheric water vapor would severely attenuate any microwave signals in rain or in humid climates, then 802.11 is not suitable for use over long distances.

The existence of a water excitation mode in the microwave range is a myth. If there was an excitation mode, water would absorb a significant amount of the microwave energy. And if that energy was absorbed effectively by water, microwave ovens would be unable to heat anything other than the water near the surface of food, which would absorb all the energy, leaving the center cold and raw. An absorption peak would also mean that atmospheric water vapor would disrupt satellite communications, which is not an observed phenomenon. NASA Reference Publication 1108(02), *Propagation Effects on Satellite Systems at Frequencies Below 10 GHz*, discusses the expected signal loss due to atmospheric effects, and the loss is much more pronounced at frequencies above 10 GHz. The absorption peak for water, for example, is at 22.2 GHz.

Microwave ovens do not work by moving water molecules into an excited state. Instead, they exploit the unusually strong dipole moment of water. Although electrically neutral, the dipole moment allows a water molecule to behave as if it were composed of small positive and negative charges at either end of a rod. In the cavity of a microwave oven, the changing electric and magnetic fields twist the water molecules back and forth. Twisting excites the water molecules by adding kinetic energy to the entire molecule but does not change the excitation state of the molecule or any of its components.

802.11® Wireless Networks The Definitive Guide By Matthew Gast

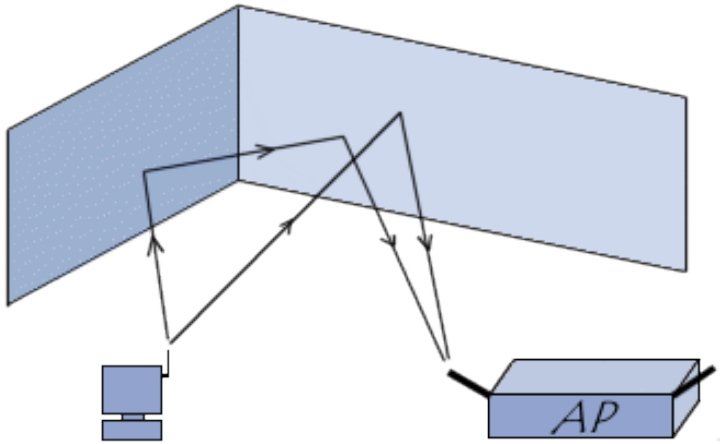
Ondes, fréquences et couverture

- Plus la fréquence est élevée plus le phénomène d'absorption est élevé, donc plus la distance de couverture est faible.
  - C'est pour cela que les communications radio se font sur des fréquences d'une centaine de MHz.
  - Pour le WiFi, par exemple on peut difficilement faire plus de 10km avec du matériel « classique ».

- Plus la fréquence est élevée, plus le débit de de données peut être important mais plus la couverture est faible.
- Puissance élevée : couverture plus grande mais durée

Chemins multiples (multipath)

- Par réflexions successives, une onde peut atteindre une station en empruntant des chemins multiples et générer des interférences
- La présence de deux antennes sur un point d'accès permets de contrôler et de séparer les signaux



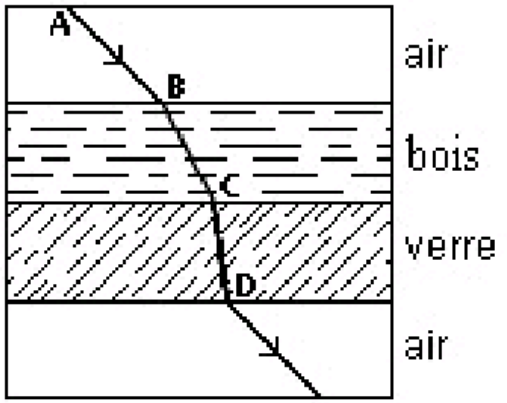
source : Jean François Pilou

En fonction du milieu traversé

Affaiblissement pour le 2.4 GHz

Matériaux	Affaiblissement	Exemples
Air	Négligeable	Champ libre
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Etres vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Elevé	Carrelage
Papier	Elevé	Rouleaux de papier
Béton	Elevé	Murs porteurs, étages, piliers
Verre blindé	Elevé	Vitres pare-balles
Métal	Très élevé	Béton armé, miroirs, armoire métallique, cage d'ascenseur

Réfraction pour le 2.4 GHz



Partie 2

La norme 802.11 (IEEE)

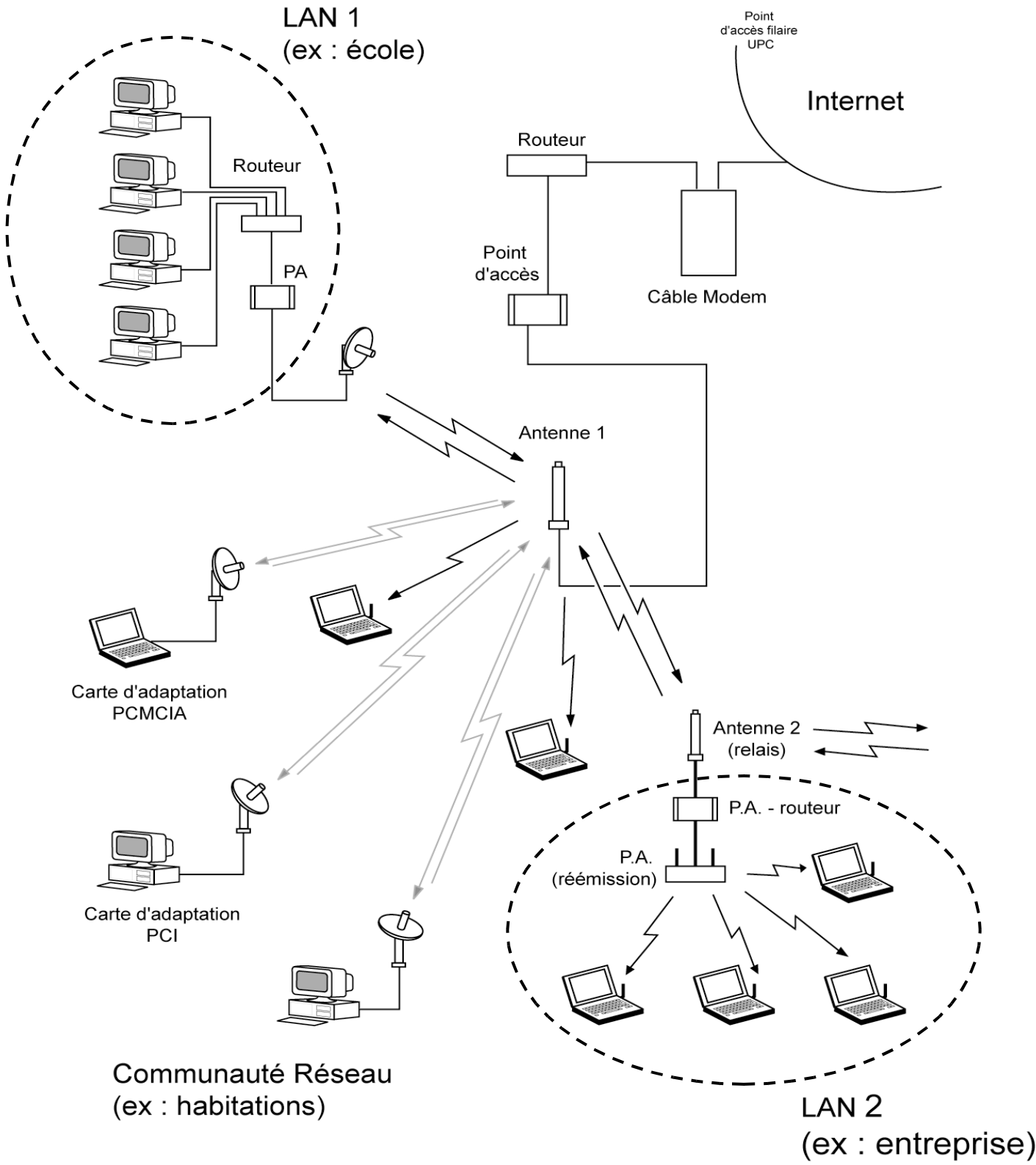
Présentation du Wi-Fi

Définition

- Le Wi-Fi
  - permets à des équipements informatiques de se connecter et d'échanger des données par voie radio
  - s'intègre dans la pile IP (sous-couche)

- Un WLAN
  - est un réseau sans fil local. Il regroupe les équipements associés entre eux utilisant le même nom de réseau
  - fonctionne en architecture cellulaire : chaque **cellule** possède sa zone de couverture et ses caractéristiques d'association

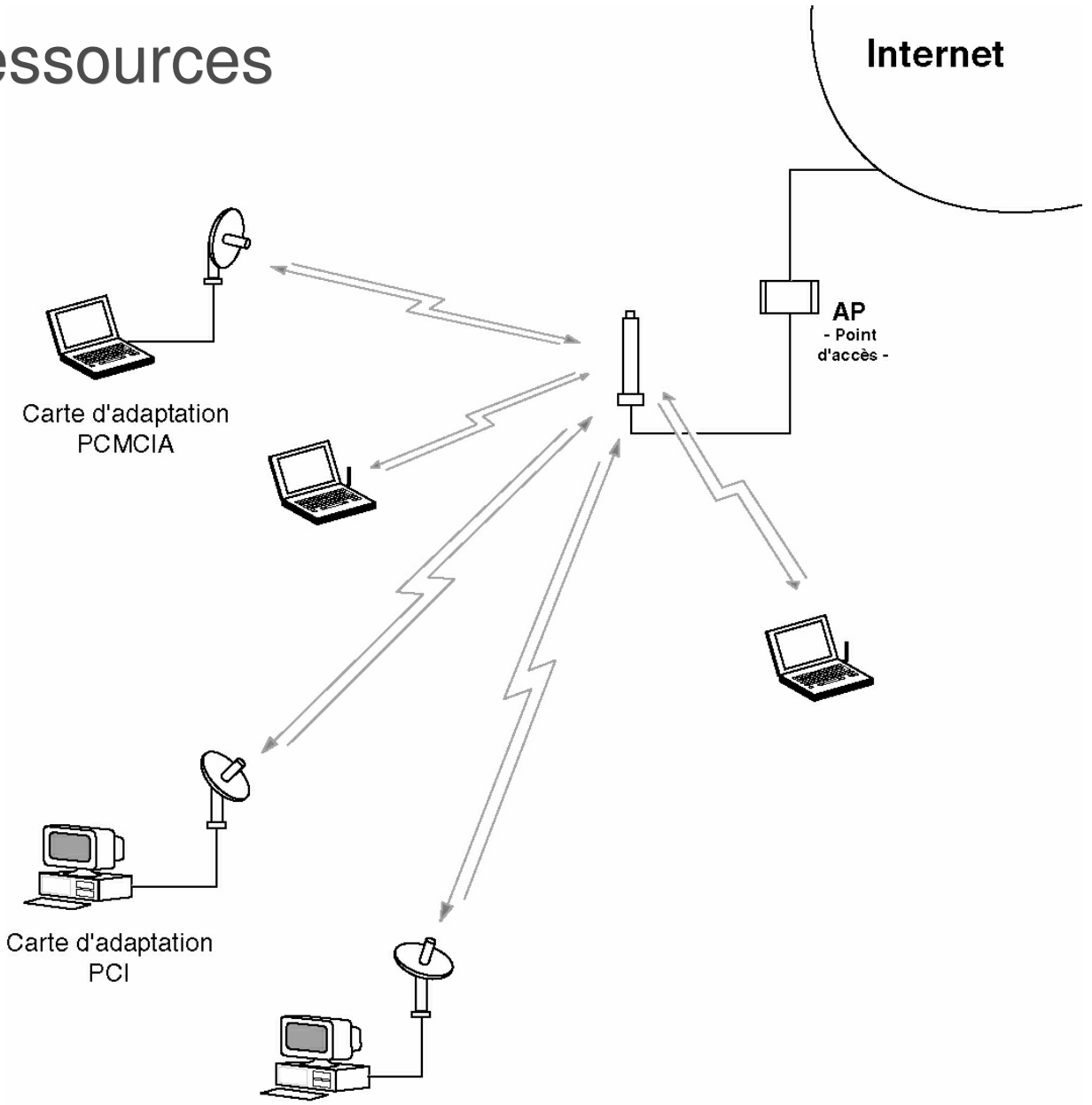
Des possibilités variées



Source : Centre Erasme

Usages

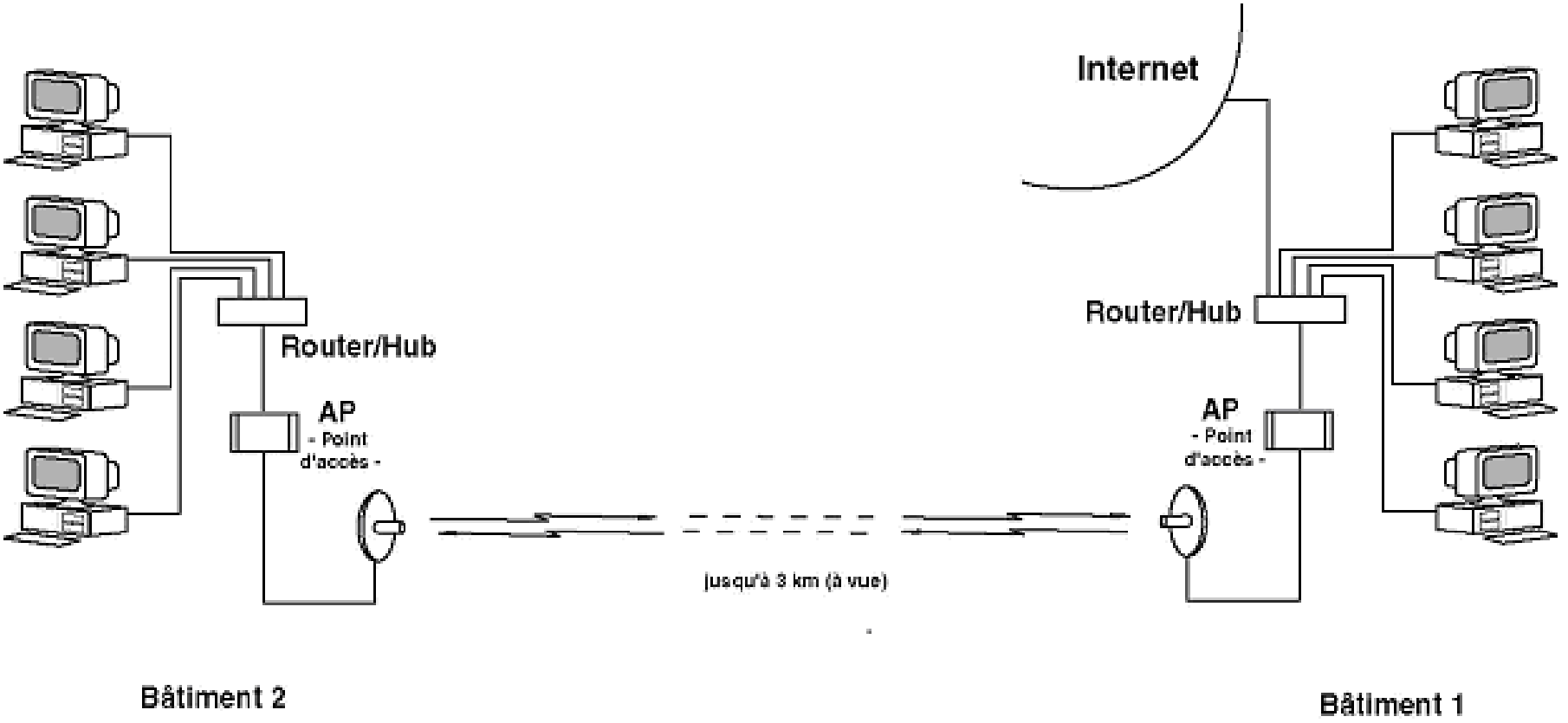
- Partager des ressources



Source : Centre Erasme

Usages

- Étendre un réseau existant



Source : Centre Erasme

Usages du Wi-Fi

- Étendre un réseau existant
  - Pont WiFi
- Partager une ressource
  - Switch / Accès Internet, Imprimante, serveur
- Réaliser un portail d'accès authentifié
  - Hot-Spot
- Utiliser des objets communiquants
  - Lecteur de flux RSS, Nazbatag, localisation
- Accéder à une ressource en mobilité
  - Hopitaux
- Déployer un réseau urbain alternatif aux opérateurs
  - Les villes Internet

Quelques données

- **Débit** : Association de 1 à 54 Mbps. 50 % de débit effectif.
- **Portée** : de quelques centaines de mètres à plusieurs km.

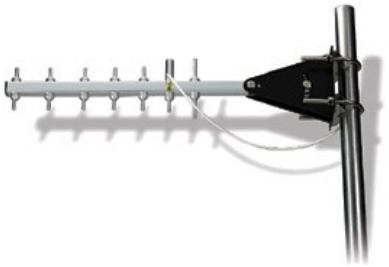
  Ce résultat sera fonction de :
  - la **puissance**$_{em}$: couples AP + antennes choisis
  - la **sensibilité**$_{rec}$: inv proportionnelle au débit choisi
  - **affaiblissement**$_{ligne}$: masques radio et interférences
- **Puissance autorisée par l'ART** : 100 mW en sortie d'antenne pour les réseaux privés et indépendants.
- **Santé** : rayonnement 10 fois inférieur à celui d'un téléphone portable.

Le matériel employé

- **Points d'accès (eq. switch)**

- **Cartes clientes (éq. carte réseau)**

- **Antennes et connectiques**



- **Matériel Ethernet**

Etat des autorisations en France

1- Création ou extension d'**un réseau privé** par technologie WiFi 2.4 Ghz libre dans le Rhône depuis le mois de Janvier 2003.

réseau privé (ou indépendant) = pas de vocation à commercialiser un service de télécommunication ou activité pas assimilée à celle d'un opérateur.

2- Utilisation du WiFi dans le but de **fournir un accès Internet payant à un tiers** : demande de licence expérimentale auprès de l'ART.

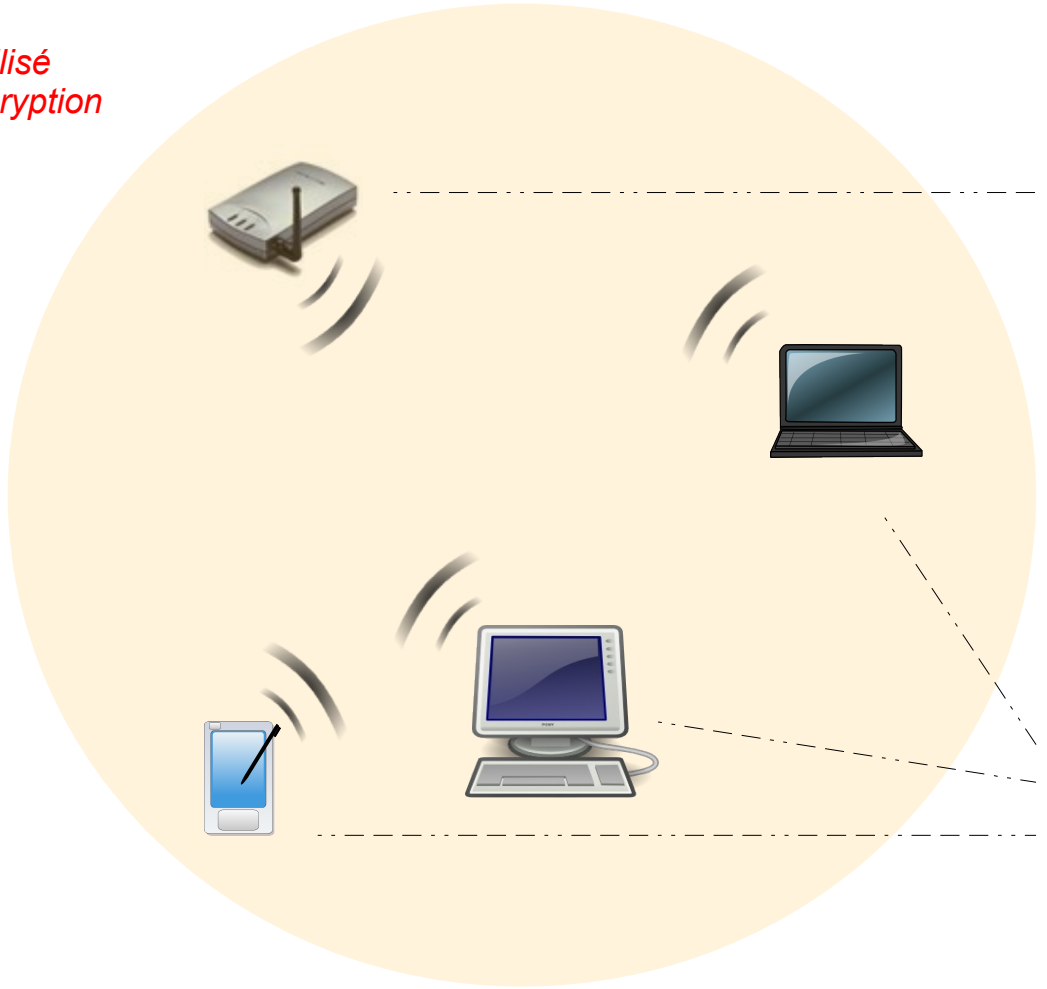
Ces deux procédures sont soumises au respect de normes européennes et françaises **d'utilisation des fréquences** et **des puissances** émises (ETSI) :

Fréquences en MHz	Intérieur	Extérieur
2400 2454	**100 mW**	**100 mW**
2483,5		**10 mW et 100 mW avec accord Défense sur propriétés privées**

Une architecture cellulaire

Un équipement Wi-Fi
= 2 interfaces

Cellule
(zone de couverture)
-ID
- Débit
- Canal utilisé
- Mode d'encryption

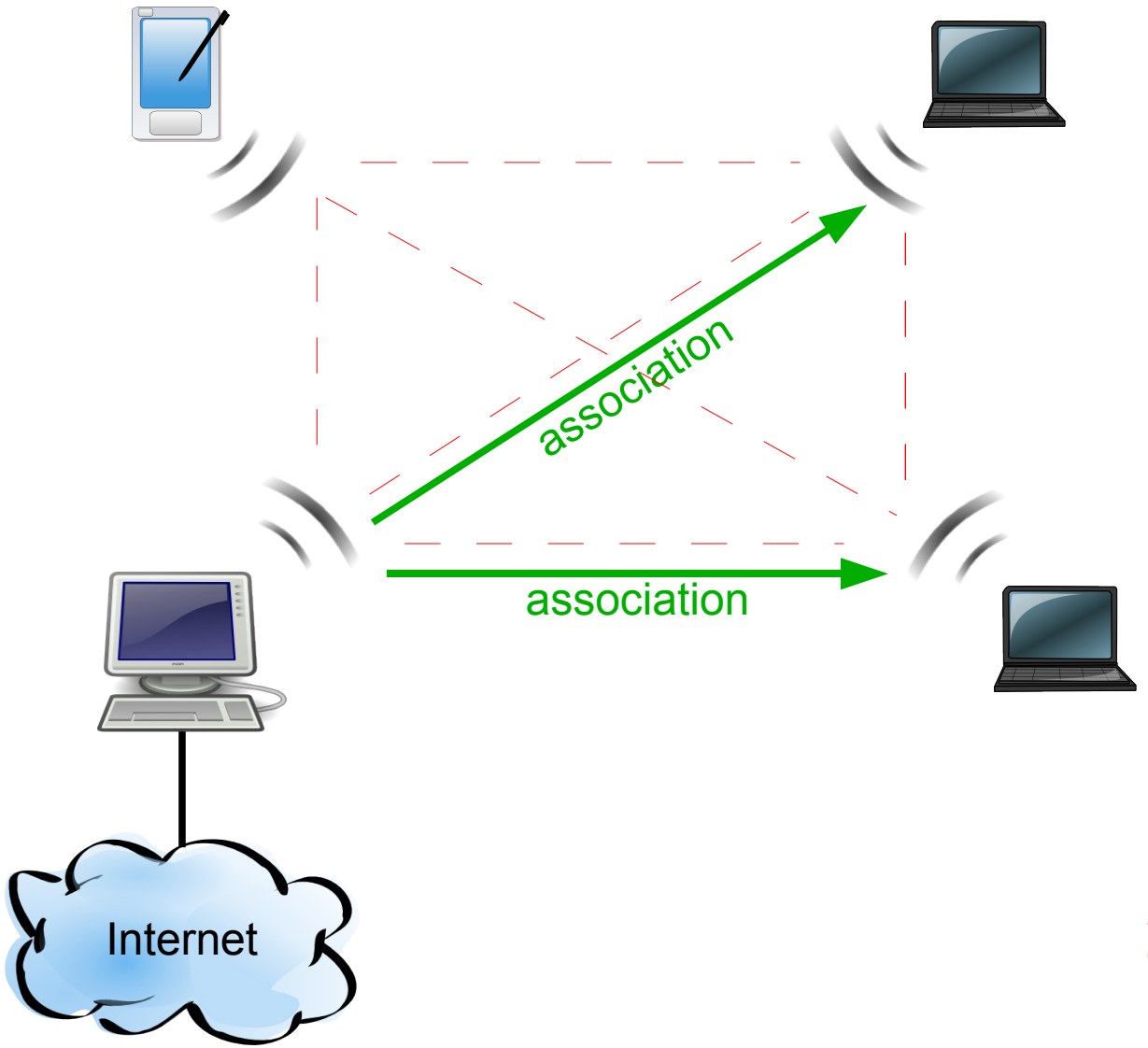


Point d'accès
module WiFi
&
module Ethernet

Adaptateur WiFi
module WiFi
&
module PCI, PCMCIA,
CompactFlash ou USB

Topologies

Topologie ad-hoc

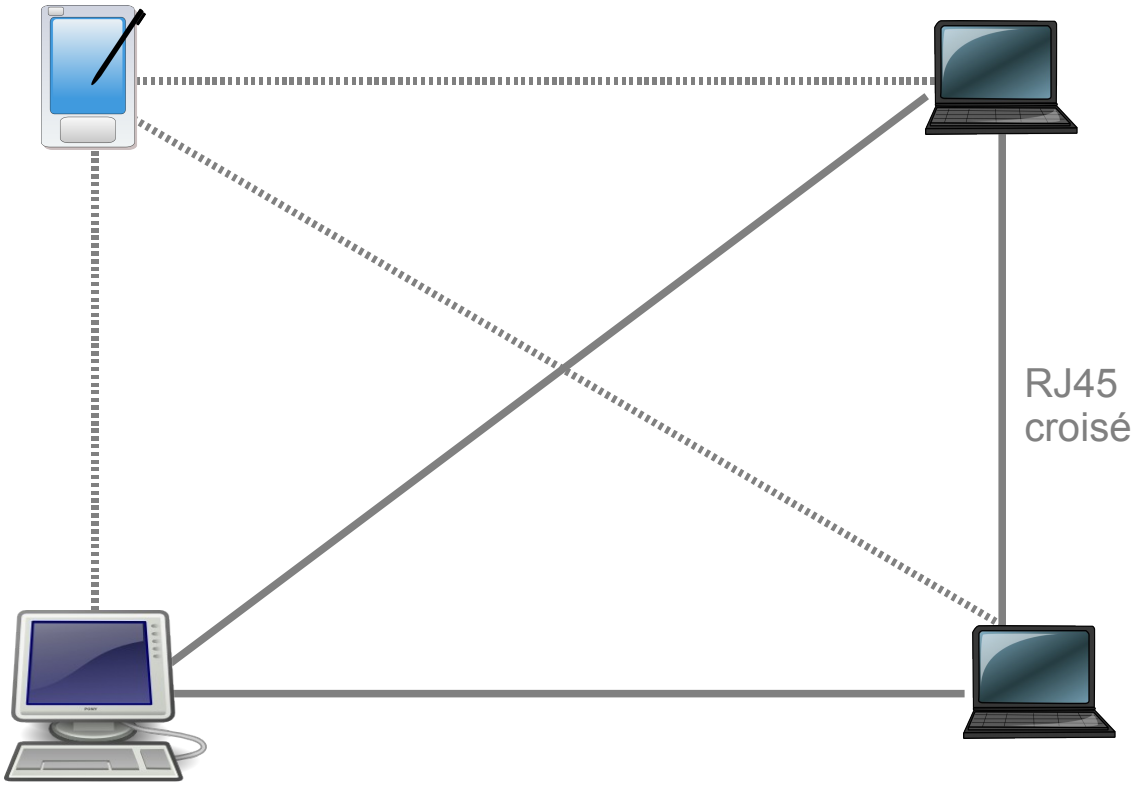


IBSS

Ensemble de services de base indépendant

... équivalent

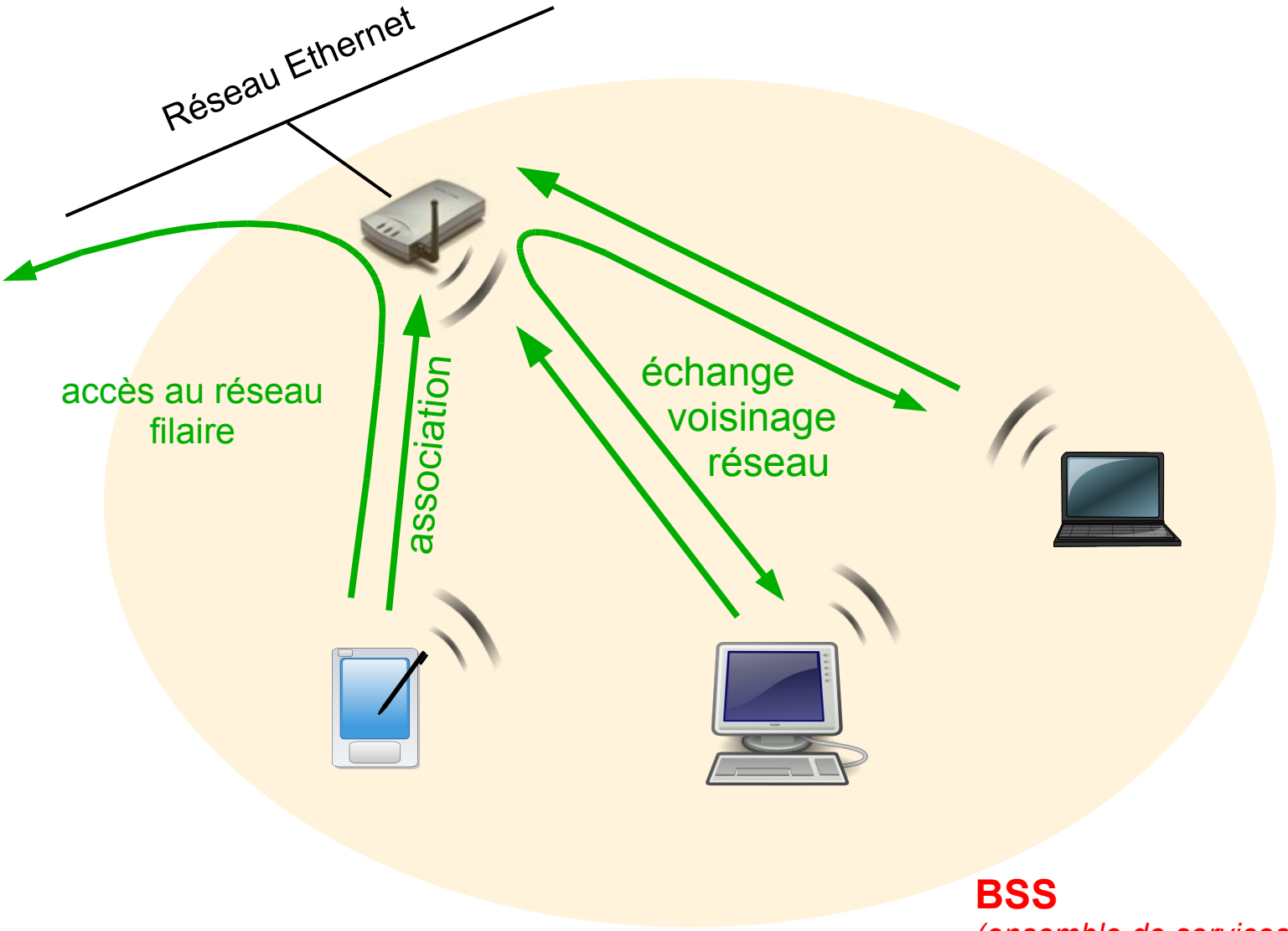
à un câble croisé en Ethernet



Topologie ad-hoc

- Des stations équipées d'adaptateurs WiFi en mode ad-hoc forment un réseau Mesh (ad-hoc)
  - Chaque adaptateur joue successivement le rôle d'AP et de client. Les machines communiquent ensemble en point à point (peer to peer).
  - Ce système n'intègre pas nativement de protocole de routage. Une norme IEEE en étude le prévoit.
  - La portée du réseau est limité aux portées de chaque paire.
- Cet ensemble de services de base indépendants (IBSS) est adapté aux réseaux temporaires lorsqu'aucun AP n'est disponible

Topologie Infrastructure

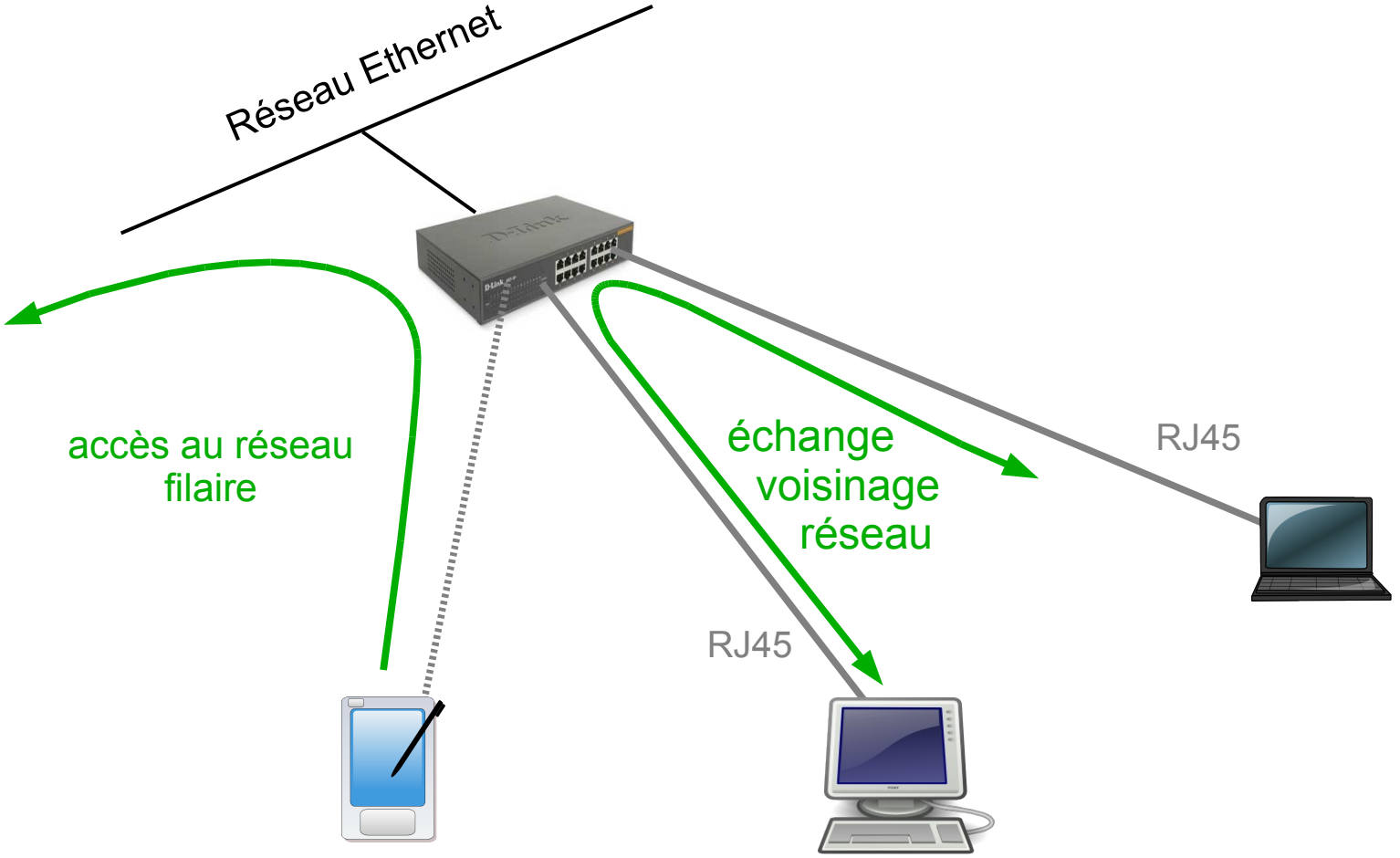


BSS

(ensemble de services de base)

BSSID = @Mac du point d'accès

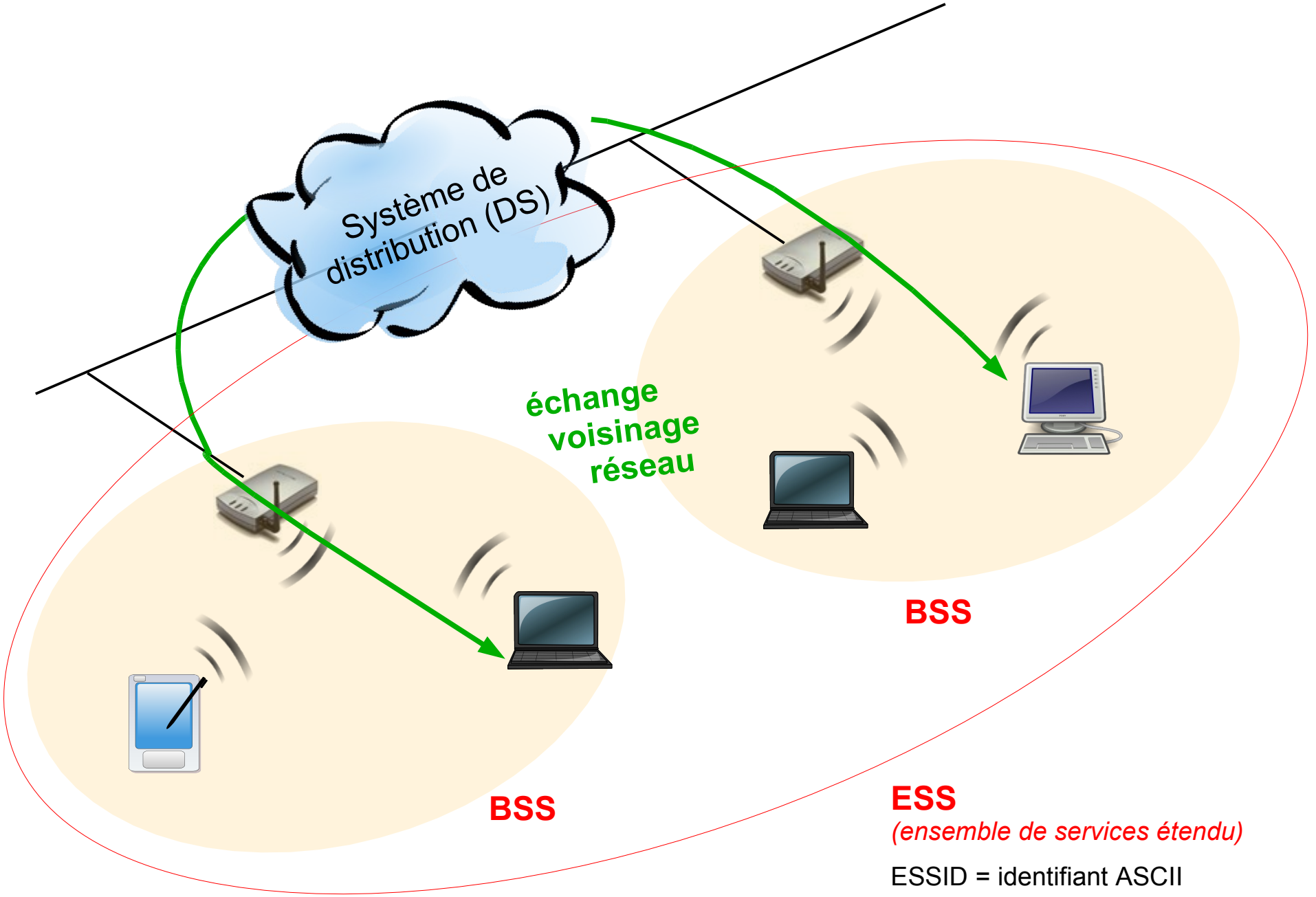
... équivalent à un hub en Ethernet



Topologie infrastructure

- Chaque station se connecte à un point d'accès qui lui offre un ensemble de services de base (BSS)
  - association et ev. authentification
  - connexion à la ressource Ethernet (bridge IP)
  - communication avec les autres stations (IP)
  - BSS caractérisé par son **BSSID** = @Mac du point d'accès
- A un point d'accès peuvent être associées jusqu'à 100 stations
- Le support de transmission est partagé entre les stations, de même que le débit radio
- Le point d'accès est mode **AP** (parent) et les stations en mode **client** (enfant)

Topologie infrastructure étendue

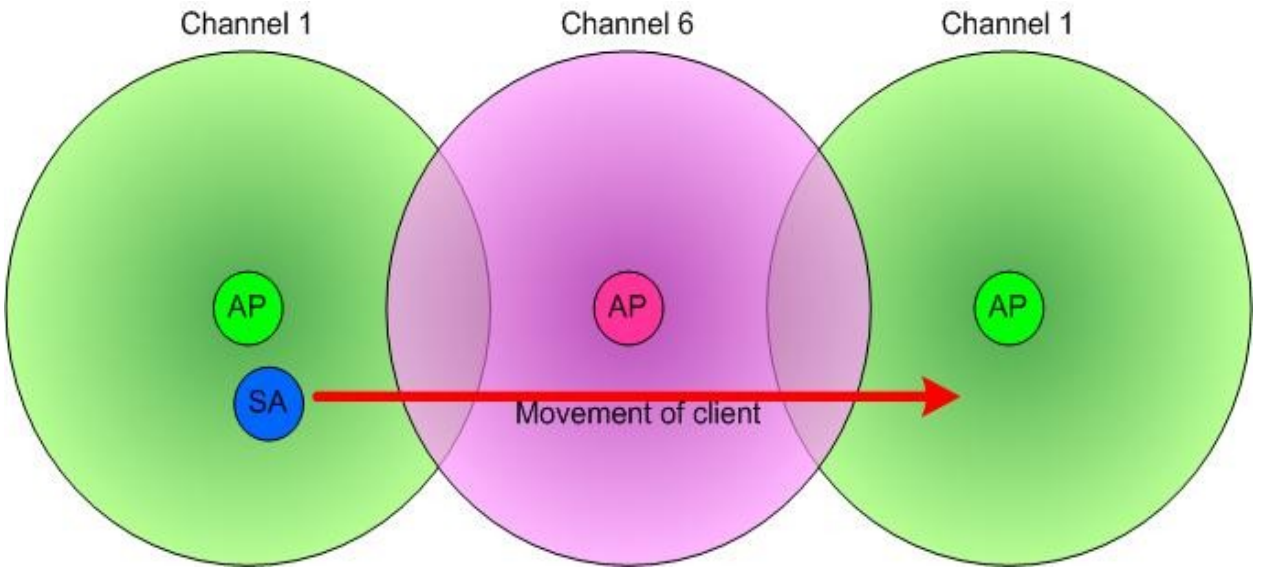


Topologie infrastructure étendue

- En reliant plusieurs points d'accès par un service de distribution (DS) on obtient un ensemble de services étendu (ESS)
  - le ESS est repéré par un (E)**SSID** = identifiant à 32 caractères au format ASCII nécessaire pour s'y associer
  - tous les AP du réseau doivent utiliser le même **SSID**
  - les cellules de l'ESS peuvent être disjointes ou se recouvrir pour offrir un service de mobilité (802.11f)
- Le service de distribution est la dorsale ou le backbone du réseau
  - réseau Ethernet
  - pont WiFi

Mobilité : notion de Roaming

- En fonction de l'organisation spatiale des canaux, on pourra offrir un service continu en mobilité : c'est le roaming (802.11f).
- Ex : flux streamé non coupé en réception
- Lors de la configuration, il faudra être vigilant quant au recouvrement des canaux



Association
et transfert de données

Les modes d'association

- Le mode d'association configuré sur un module WiFi détermine ses possibilités de connexion avec les autres :
  - **mode *AP*** (access point) : fonction d'association parent (diffuse un SSID, fonction switch et répartition de charge, gère la sécurité)
  - **mode *client* ou *managed*** : fonction d'association enfant
  - **mode *ad-hoc*** et **mode *bridge*** : pont réseau
  - **mode *repeater*** : réémission des trames
  - **mode *monitor*** : écoute et enregistrement des trames

Mode Matériel	AP (parent)	client (enfant)	Ad-Hoc	Bridge	Répéteur	Monitor
Point d'accès	X	X		X	X	(X)
Adaptateur WiFi		X	X			(X)

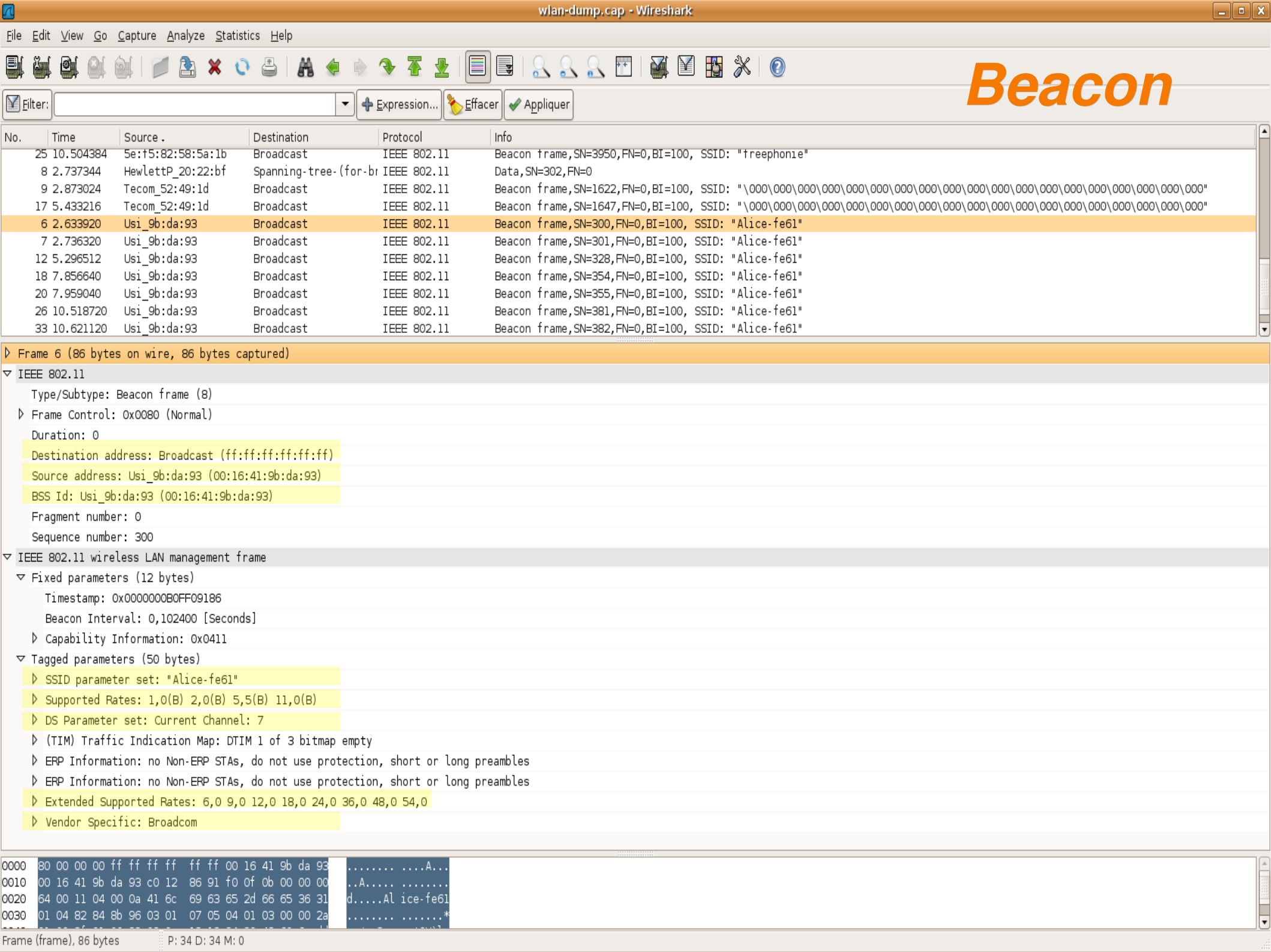
Mécanisme d'association (1)

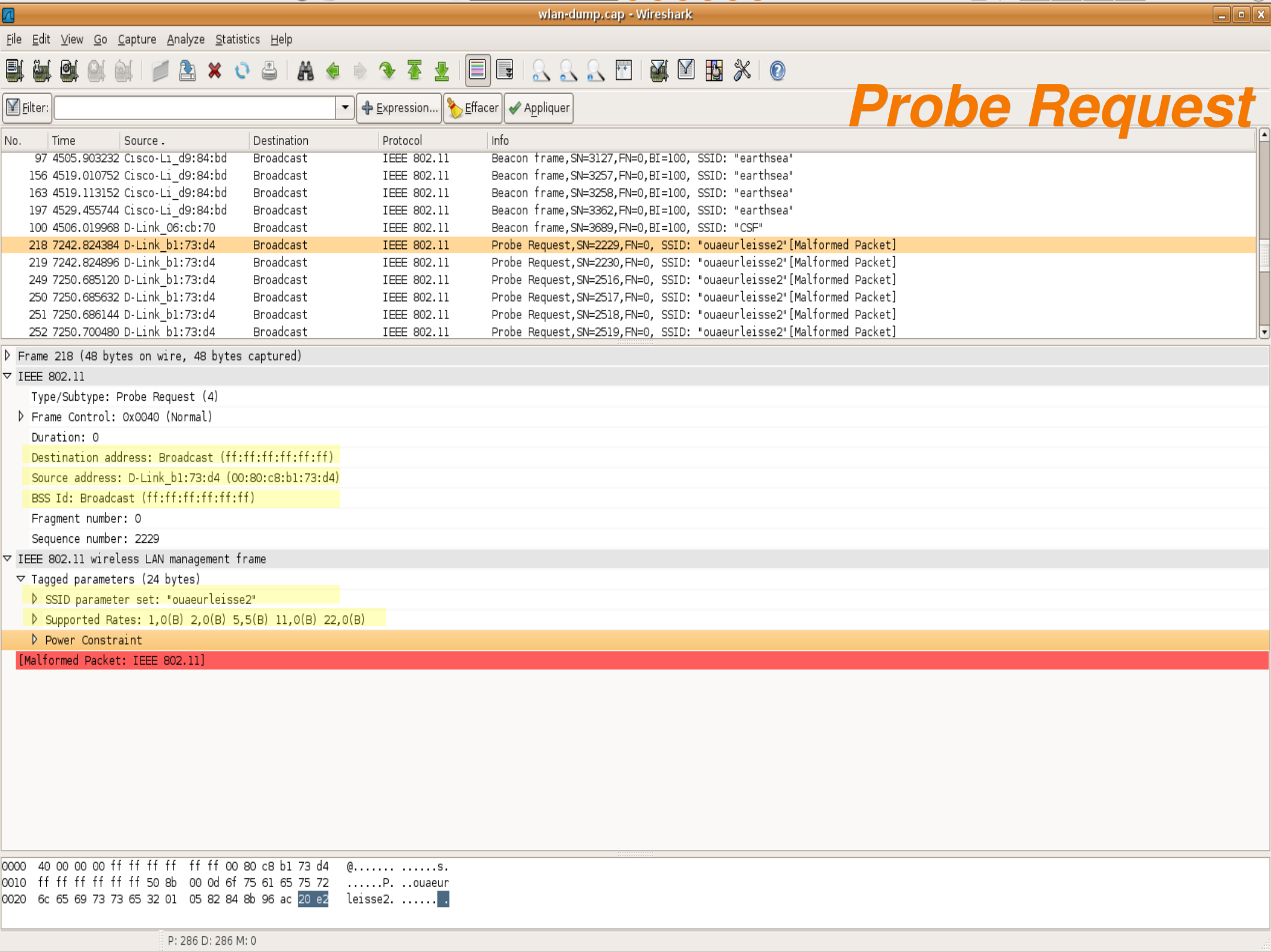
- Le point d'accès
  - diffuse régulièrement (0,1s) une **trame balise** (*beacon*) avec
    - son **BSSID** (ex : 00:16:41:9B:DA:93)
    - ses **caractéristiques radio** (ex : canal 2 / 54 Mbps / ENC)
    - optionellement son E**SSID** en clair (ex : tsunami)

- L'adaptateur client
  - lorsqu'il détecte son entrée dans une cellule, il diffuse une **requête de sondage** (*probe request*) avec
    - l'E**SSID** sur lequel il est configuré (ex : tsunami)
    - ses **caractéristiques radio** (ex : 11 Mbps)
  - autrement, ou si aucun ESSID n'est configuré
    - il écoute le réseau à la recherche d'un ESSID en clair

Mécanisme d'association (2)

- Le point d'accès
  - lorsqu'il reçoit une **requête de sondage** (probe request) vérifie
    - le E**SSID**
    - les **caractéristiques radio** proposées
  - si les données sont compatibles, il envoie une réponse avec
    - les informations sur sa charge
    - des données de synchronisation (puissance / débit)
- L'adaptateur client
  - évalue la qualité du signal émis et la distance du PA
  - choisit le PA avec le meilleur débit et la plus faible charge en cas de propositions multiples
  - envoie une demande d'association au PA choisi


wlan-dump.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Beacon
Filter: Expression... Effacer Appliquer
No. Time Source Destination Protocol Info
25 10.504384 5e:f5:82:58:5a:1b Broadcast IEEE 802.11 Beacon frame,SN=3950,FN=0,BI=100, SSID: "freephonie"
8 2.737344 HewlettP_20:22:bf Spanning-tree-(for-br IEEE 802.11 Data,SN=302,FN=0
9 2.873024 Tecom_52:49:1d Broadcast IEEE 802.11 Beacon frame,SN=1622,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000"
17 5.433216 Tecom_52:49:1d Broadcast IEEE 802.11 Beacon frame,SN=1647,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000"
6 2.633920 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=300,FN=0,BI=100, SSID: "Alice-fe61"
7 2.736320 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=301,FN=0,BI=100, SSID: "Alice-fe61"
12 5.296512 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=328,FN=0,BI=100, SSID: "Alice-fe61"
18 7.856640 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=354,FN=0,BI=100, SSID: "Alice-fe61"
20 7.959040 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=355,FN=0,BI=100, SSID: "Alice-fe61"
26 10.518720 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=381,FN=0,BI=100, SSID: "Alice-fe61"
33 10.621120 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=382,FN=0,BI=100, SSID: "Alice-fe61"
Frame 6 (86 bytes on wire, 86 bytes captured)
IEEE 802.11
Type/Subtype: Beacon frame (8)
Frame Control: 0x0080 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Usi_9b:da:93 (00:16:41:9b:da:93)
BSS Id: Usi_9b:da:93 (00:16:41:9b:da:93)
Fragment number: 0
Sequence number: 300
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Timestamp: 0x0000000B0FF09186
Beacon Interval: 0,102400 [Seconds]
Capability Information: 0x0411
Tagged parameters (50 bytes)
SSID parameter set: "Alice-fe61"
Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
DS Parameter set: Current Channel: 7
(TIM) Traffic Indication Map: DTIM 1 of 3 bitmap empty
ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
Extended Supported Rates: 6,0 9,0 12,0 18,0 24,0 36,0 48,0 54,0
Vendor Specific: Broadcom
0000 80 00 00 00 ff ff ff ff ff ff 00 16 41 9b da 93 ....A...
0010 00 16 41 9b da 93 c0 12 86 91 f0 0f 0b 00 00 00 ..A..... ....
0020 64 00 11 04 00 0a 41 6c 69 63 65 2d 66 65 36 31 d.....Al ice-fe61
0030 01 04 82 84 8b 96 03 01 07 05 04 01 03 00 00 2a ....*
Frame (frame), 86 bytes
P: 34 D: 34 M: 0


wlan-dump.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Effacer Appliquer
Probe Request
No. Time Source Destination Protocol Info
97 4505.903232 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3127,FN=0,BI=100, SSID: "earthsea"
156 4519.010752 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3257,FN=0,BI=100, SSID: "earthsea"
163 4519.113152 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3258,FN=0,BI=100, SSID: "earthsea"
197 4529.455744 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3362,FN=0,BI=100, SSID: "earthsea"
100 4506.019968 D-Link_06:cb:70 Broadcast IEEE 802.11 Beacon frame,SN=3689,FN=0,BI=100, SSID: "CSF"
218 7242.824384 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2229,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
219 7242.824896 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2230,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
249 7250.685120 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2516,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
250 7250.685632 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2517,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
251 7250.686144 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2518,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
252 7250.700480 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2519,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
Frame 218 (48 bytes on wire, 48 bytes captured)
IEEE 802.11
Type/Subtype: Probe Request (4)
Frame Control: 0x0040 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: D-Link_b1:73:d4 (00:80:c8:b1:73:d4)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
Fragment number: 0
Sequence number: 2229
IEEE 802.11 wireless LAN management frame
Tagged parameters (24 bytes)
SSID parameter set: "ouaeurleisse2"
Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 22,0(B)
Power Constraint
[Malformed Packet: IEEE 802.11]
0000 40 00 00 00 ff ff ff ff ff ff 00 80 c8 b1 73 d4 @..... ......s.
0010 ff ff ff ff ff ff 50 8b 00 0d 6f 75 61 65 75 72 ......P. ..ouaeur
0020 6c 65 69 73 73 65 32 01 05 82 84 8b 96 ac 20 e2 leisse2. ......
P: 286 D: 286 M: 0

Mécanisme d'association

Station

Point d'accès

Broadcast

Beacons

-BSSID
-Radio (canal, débit, puiss)
-(ESSID)

Découverte du réseau

Probe Request

-ESSID
-Débit

Probe Response

-Débit
-Charge

Authentification

Authentification

-Clefs

-Réponse du processus d'authentification

Association

Association Request

Association Response

Mécanisme de roaming

Station

Point d'accès (nouveau)

Point d'accès (ancien)

Re-association Request

Handover

Handover Request

Handover Response

Authentification

Authentification

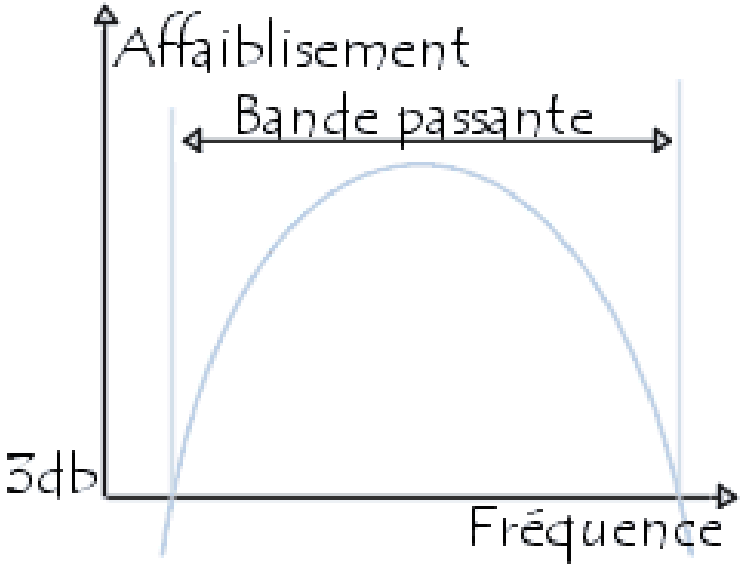
Association

Re-association Response

Gamme de fréquence et canaux

Les canaux de transmission

- Un **canal de transmission** est une bande de fréquence étroite utilisable pour une communication
- La largeur du canal (**bande passante**) est en général proportionnelle au débit de la communication
- Des canaux peuvent se recouvrir en partie générant une dégradation de la qualité du signal et du débit



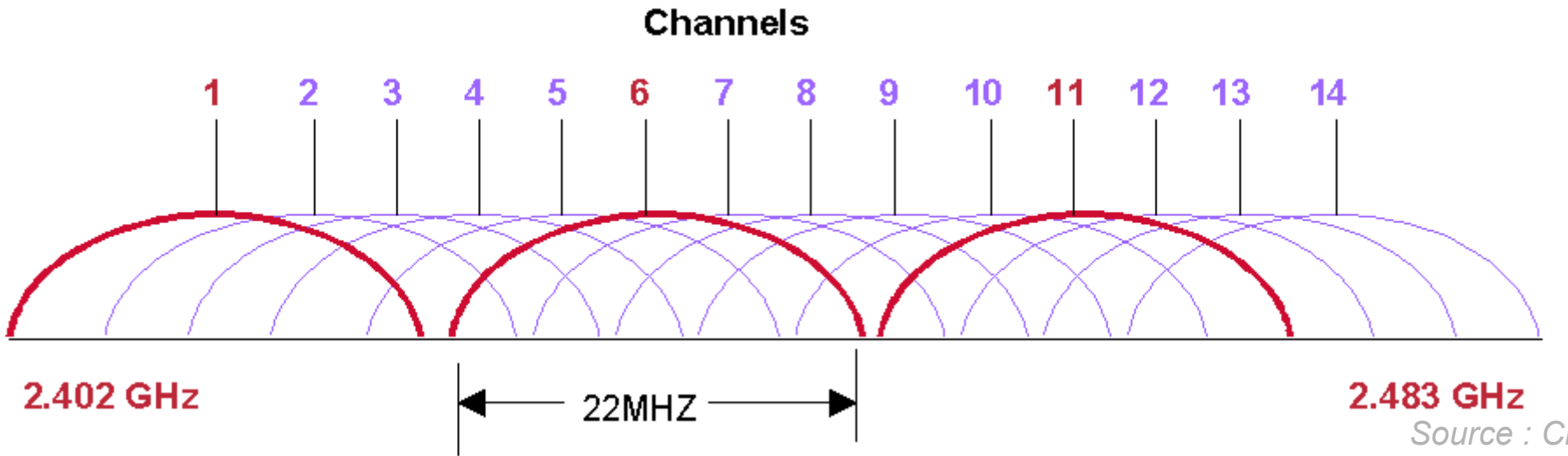
Source : Jean François Pilou

La bande ISM

- Dans chaque pays le gouvernement est le régulateur de l'utilisation des bandes de fréquence
  - ETSI en Europe
  - FCC aux Etats-Unis
- En 1985, les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine (ISM)
  - 902 à 928 Mhz
  - 2.4 à 2.483 Ghz <- **802.11b** et **g**
  - 5.725 à 5.850 Ghz <- **802.11a**
- En Europe, la première bande est utilisée par le GSM, seules les deux autres sont disponibles

Les canaux du 802.11b et g

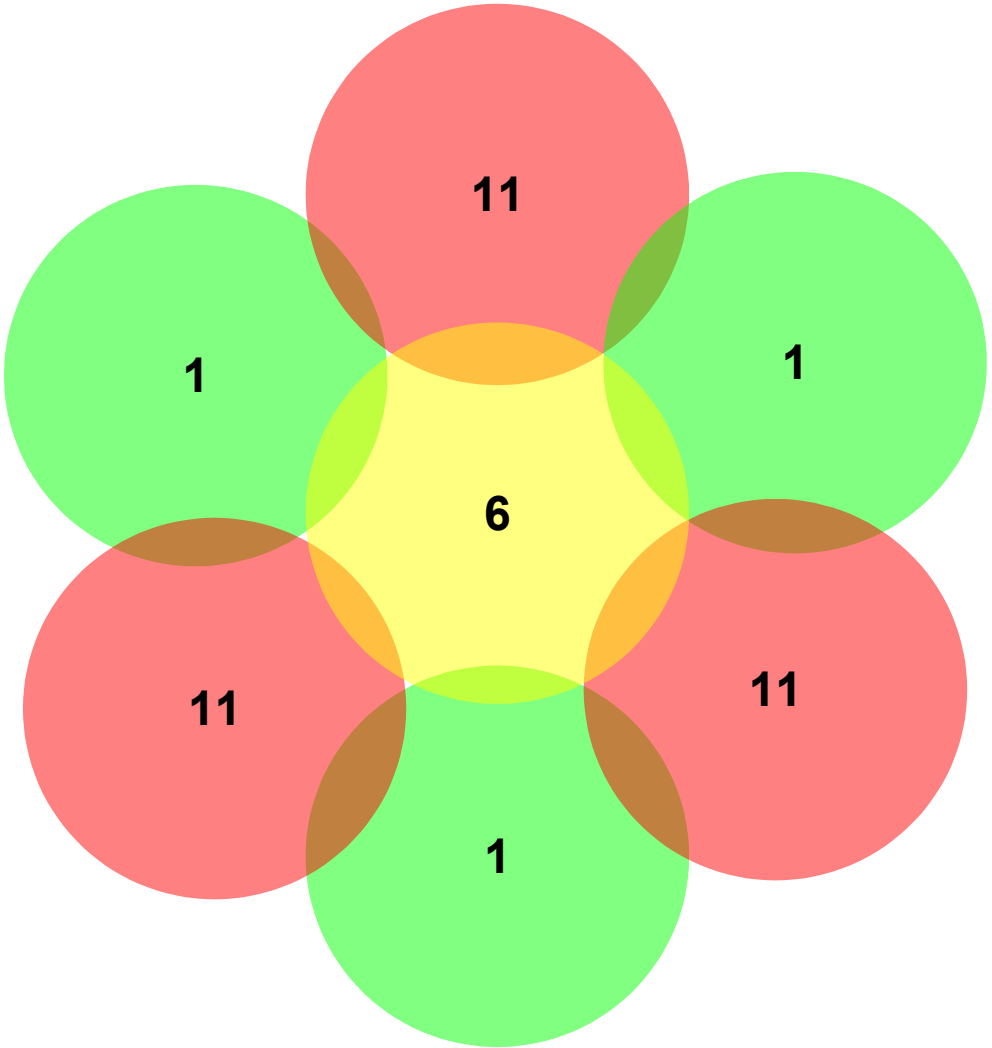
- La bande de fréquence du WiFi (802.11b et g) est divisée en 13 canaux se recouvrant partiellement
- Chaque BSS communique sur **un** canal fixé lors de la configuration de l'AP (Infrastructure) ou de l'adaptateur (ad-hoc)
- Trois canaux seulement sont utilisables simultanément et à proximité : 1, 6 et 11
- Les canaux bas sont réputés plus stables



Source : Cisco

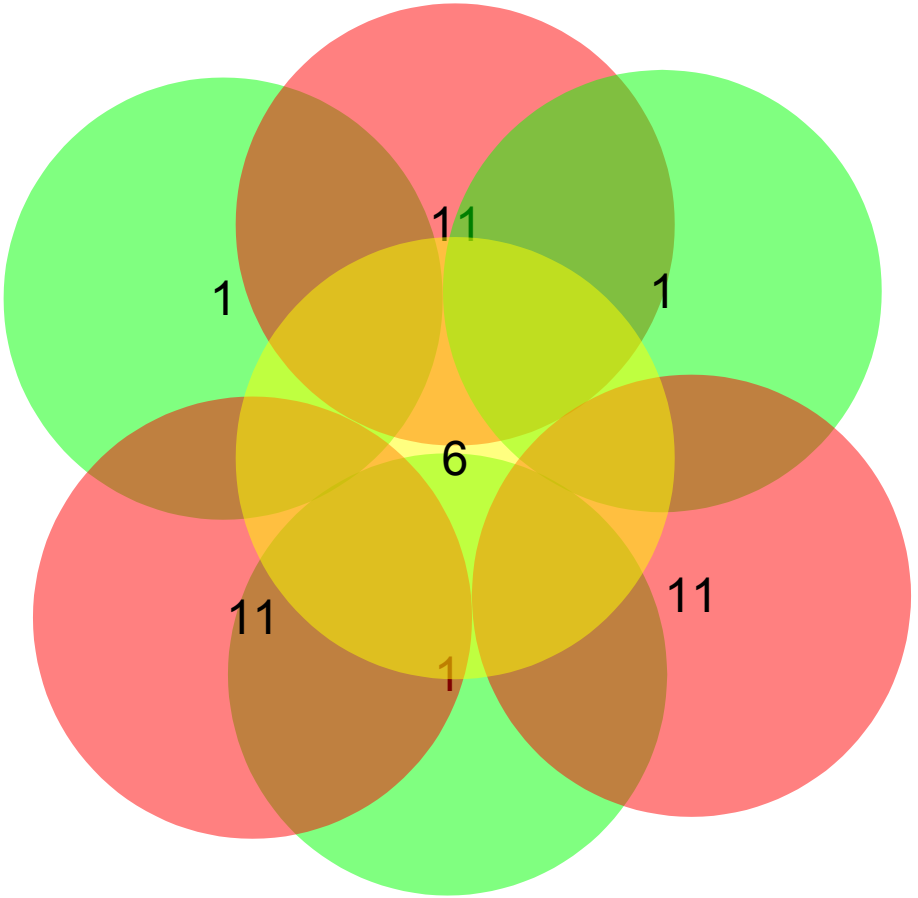
Affectation des canaux

- Affectation de trois canaux qui ne se perturbent pas (cas limite - interférences et réflexions) :

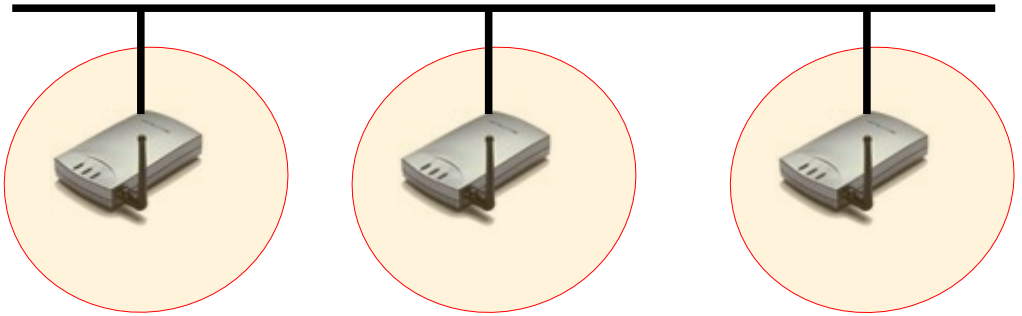


Affectation des canaux

- Affectation de trois canaux qui ne se perturbent pas (cas obligatoire) :

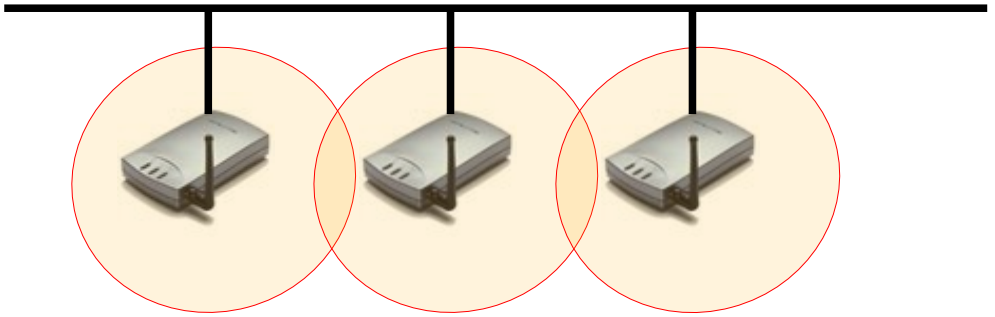


Choix de la topologie



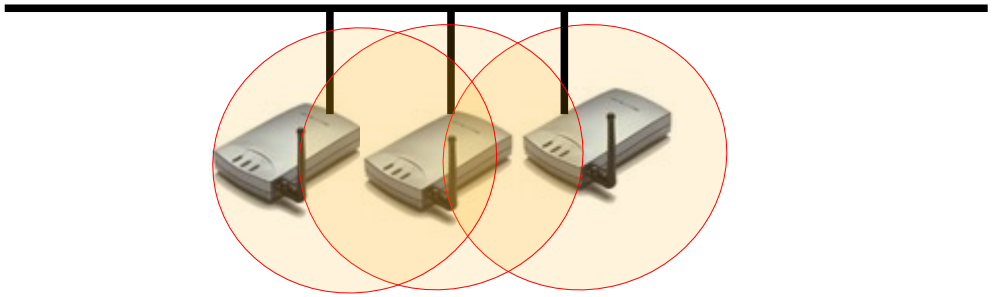
les cellules sont disjointes

- faible nombre de canaux
- pas d'interférence
- pas de mobilité



les cellules sont jointes

- service de mobilité
- exploitation de l'espace
- ev gestion des canaux
- éq réseaux sans fils



les cellules se recouvrent

- densification : nombre important d'utilisateurs
- gestion des canaux
- gestion de l'affectation

Normes et standards

La norme IEEE 802.11

- 802.11
  - Norme technique du IEEE décrivant les caractéristiques d'un réseau local sans Fil (WLAN)
  - Définit le fonctionnement des couches basses d'une liaison WiFi : couche physique et couche liaison de données
- IEEE (Institute of Electrical and Electronics Engineers / www.ieee.org)
  - Organisation professionnelle à but non lucratif regroupant 360 000 membres scientifiques de 175 pays.
  - Organise la publication de normes dans le domaine de l'ingénierie électrique :
    - IEEE 802.3 : Fonctionnement d'Ethernet
    - IEEE 1394 : Fonctionnement du Bus série (FireWire)
    - IEEE 1284 : Port parallèle

Le label Wi-Fi

- Le label Wi-Fi (Wireless-Fidelity)
  - Certification d'un consortium industriel (WiFi Alliance) attestant de la conformité des produits au standard 802.11 et de leur interopérabilité
  - Label industriel et commercial
  - Les produits bénéficiant de la certification peuvent appliquer le logo WiFi (Wireless Fidelity)
- La «Wi-Fi Alliance»
  - Regroupe 260 entreprises : http://www.wifialliance.com/our_members.php
  - Proposent des labels complémentaires marquant les évolutions techniques de sécurité : WEP, WPA2

Le standard 802.11

	Débit théorique maximum	Bande de fréquence	Portée maximale	Observations
802.11b	11 Mbps	2,4 GHz	– intérieur : 50 m – extérieur : 200 m (11 Mbps)	– sensible aux interférences (bluetooth, téléphone sans fil, four micro-ondes...) – faible coût (répandue) – non réglementée (1999) – bonne pénétration pour la majorité des matériaux
802.11a	54 Mbps	5 GHz	– intérieur : 20 m	– réglementée – fréquences radio élevées (couverture plus faible tributaire des obstacles) – plus chère – pas d'interférence avec les appareils électroniques
802.11g	54 Mbps	2,4 GHz	– intérieur : 20 m – extérieur : 50 m (54 Mbps)	- compatible avec 802.11b - s'imposera devant le 802.11b

Les différentes normes

- **Origine**
  - **802.11** : 2 Mbits/s (1997)
- **Amendements**
  - **802.11b** : 2,4 Ghz - 11 Mbits/s (bande ISM) - FSSS
  - **802.11a** : 5 Ghz - 54 Mbits/s (bande UN-II) - OFDM
  - **802.11g** : 2,4 Ghz - 54 Mbits/s (bande ISM) - OFDM
  - **802.11e** : Qualité de service
  - **802.11f** : Itinérance (roaming)
  - **802.11h** : Norme européenne pour les fréquences et la gestion d'énergie
  - **802.11i** : Sécurité - chiffrement et authentification AES
- **A venir**
  - **802.11n** : WwiSE ou Super-WiFi - avril 2007 - 540 Mbps - technologie MIMO (multiple-input multiple-output)
  - **802.11s** : Réseau Mesh, en cours d'élaboration. Mobilité sur les réseaux de type adhoc avec routage dynamique OLSR. Débit de 2 Mbps.

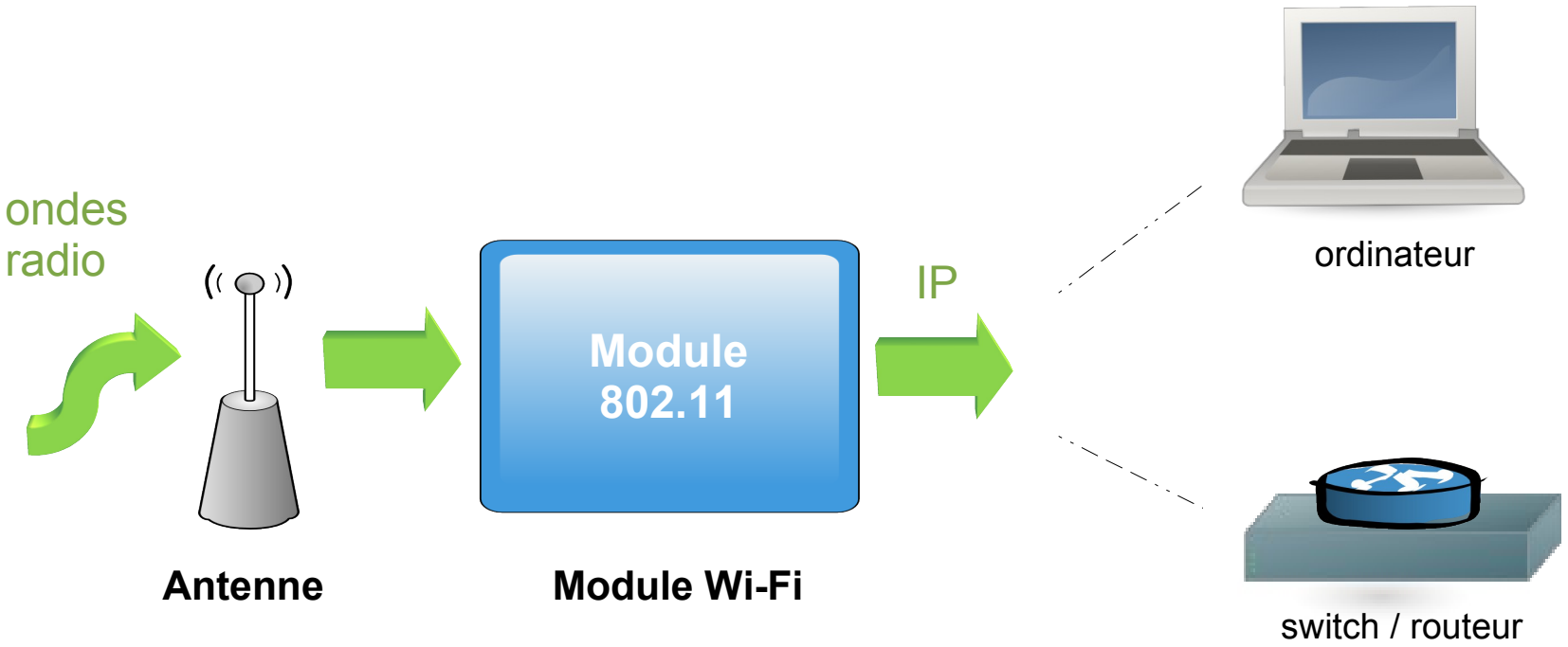
Fonctionnement

Couche 802.11

Fonctionnement

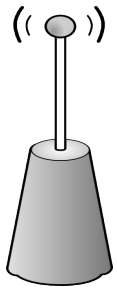
- Tous les équipements WiFi sont équipés d'une antenne et d'un module chargé de la commutation

  ondes radio <-> trames IP

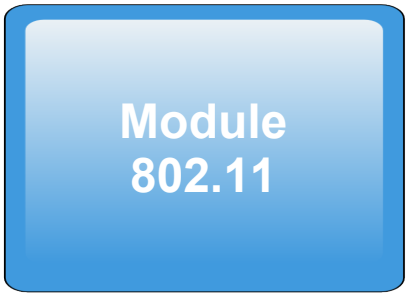


Fonctionnement

ondes radio

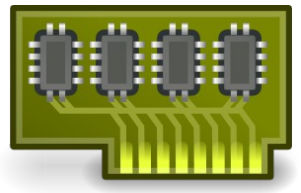


Antenne



Module Wi-Fi

paquet IP



Connexion PCMCIA

port PCMCIA

Fonctionnement

ondes radio

paquet IP

Module 802.11

port PCI

Antenne

Module Wi-Fi

Connexion PCI

Fonctionnement

ondes radio

Antenne

Module 802.11

Module décapsulation Wi-Fi

paquet IP

Module 802.3

Module d'encapsulation Ethernet

trame Ethernet

cablage Ethernet

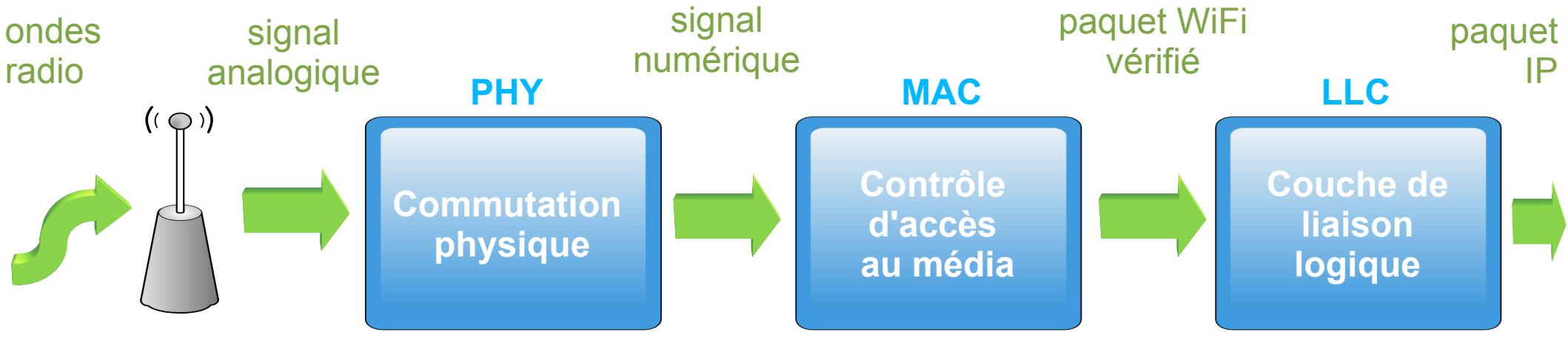
switch / routeur

Le module WiFi

- Modulation

ondes radio <-> trames IP

niveau 1 <-> niveau 3 de la couche OSI



Convertit le signal (gamme de fréquence, puissance et modulation) et **décode l'information**

DSSS / FHSS / ODPM

Gère l'accès au média et s'assure de la transmission des trames

CSMA/CA

- Mode d'association
- Authentification et sécurité
- Fragmentation
- Roaming
- Économie d'énergie

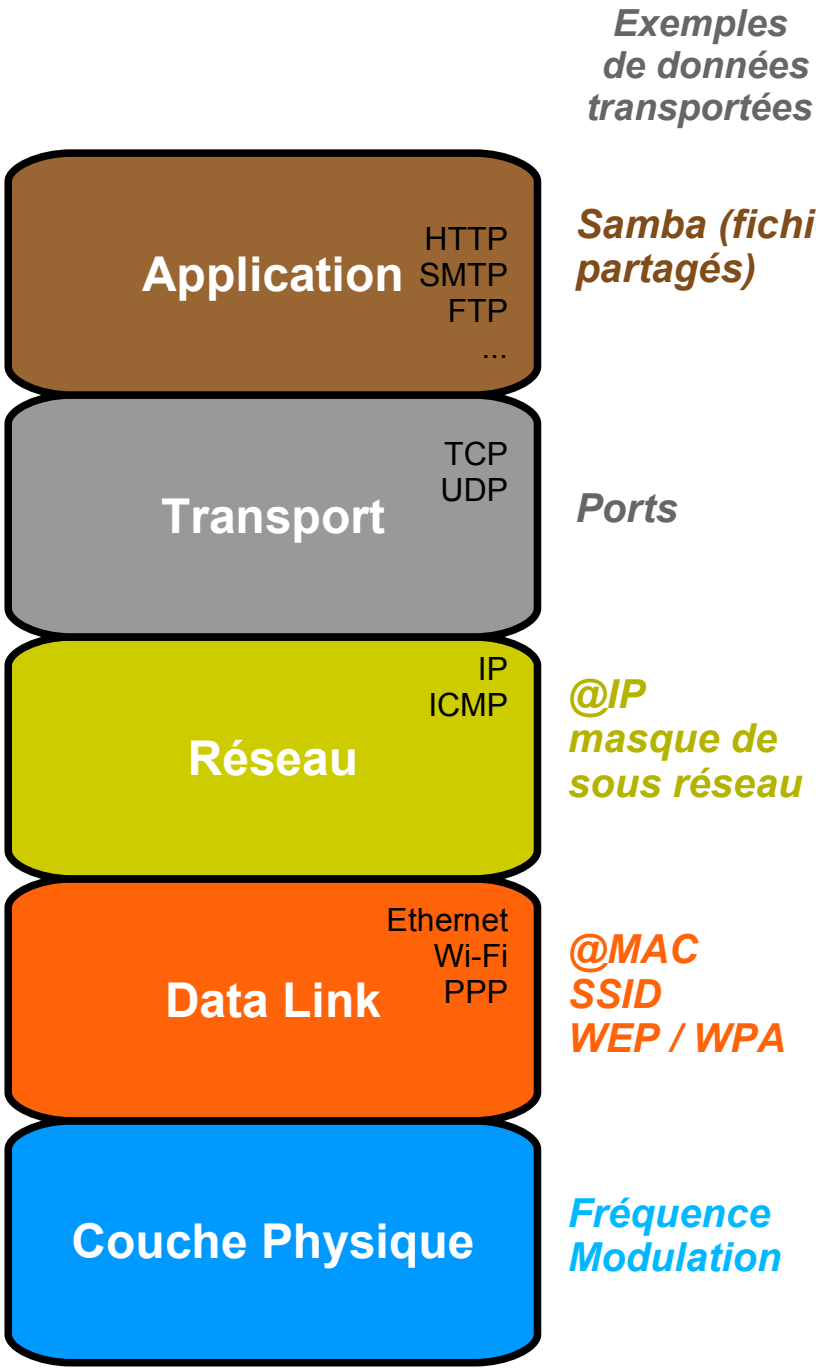
Lien WiFi

Partie 3

Configuration d'un réseau Wi-Fi

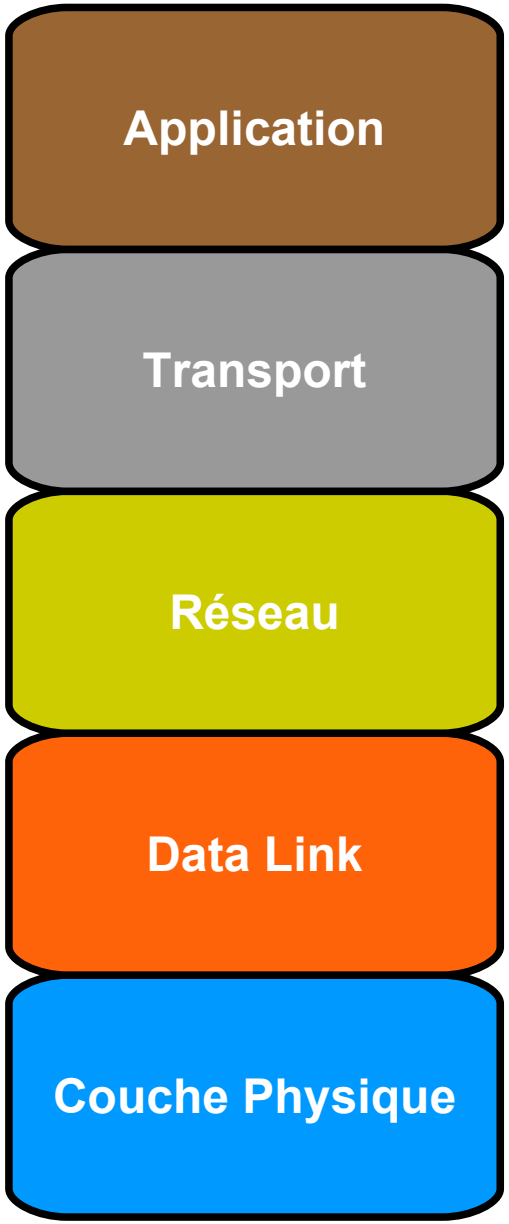
Le modèle OSI

Modèle TCP/IP en couches



- Les réseaux sont généralement organisés en "piles protocolaires"
- chaque couche de la pile offre un niveau d'abstraction supplémentaire à la couche supérieure
- chaque couche offre un service supplémentaire par rapport à la couche inférieure

Les couches 802.11



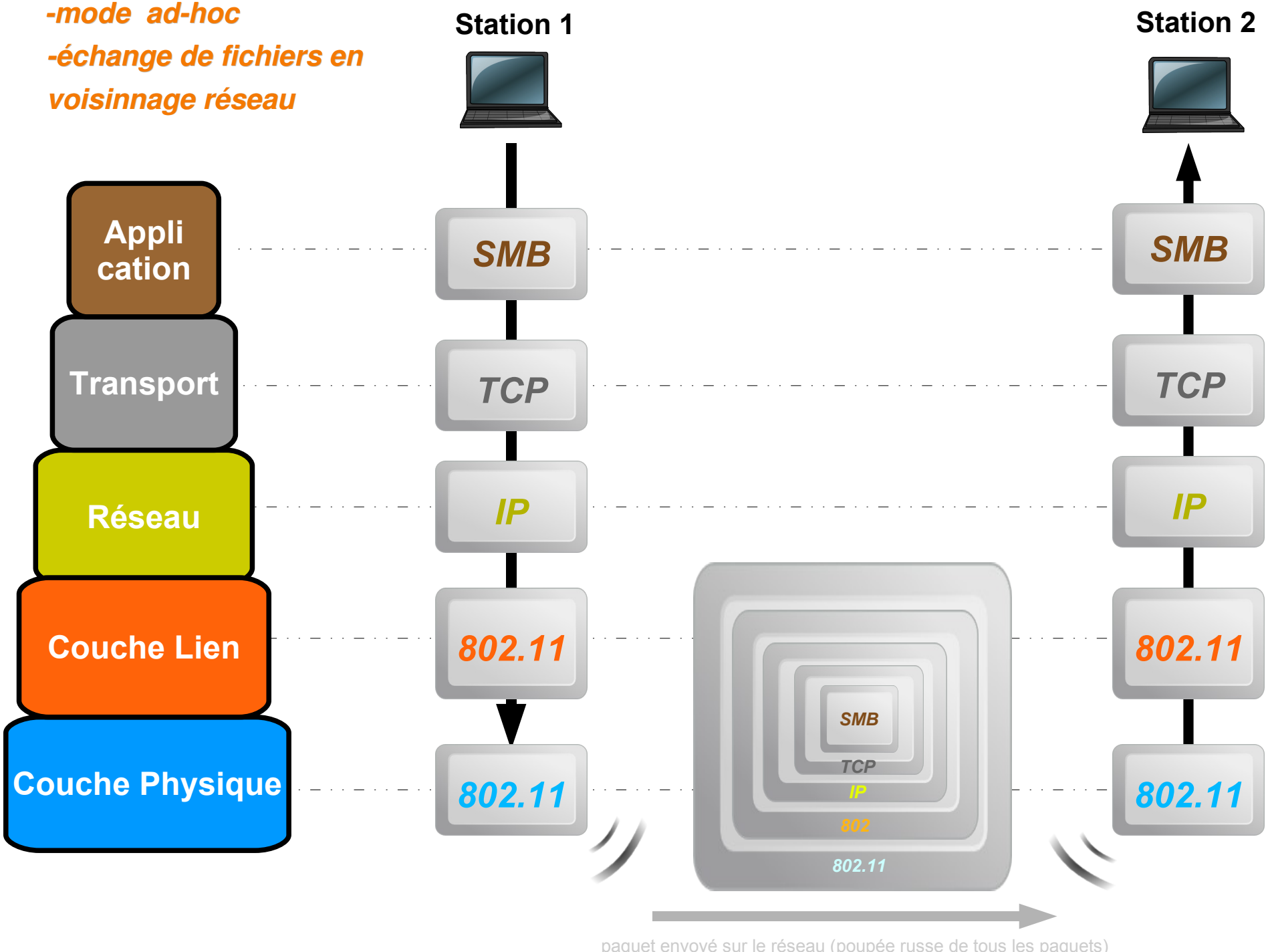
Couches Wi-Fi (802.11 - 802.2)

- **Logical Link Control (LLC)**
  Couche de liaison logique
  lien WiFi
- **Medium Acces Control (MAC)**
  Contrôle d'accès au média
  CSMA/CA (DCF)
- **Couche Physique (PHY)**
  Modulation de données
  IR / DSSS / FHSS / OFDM

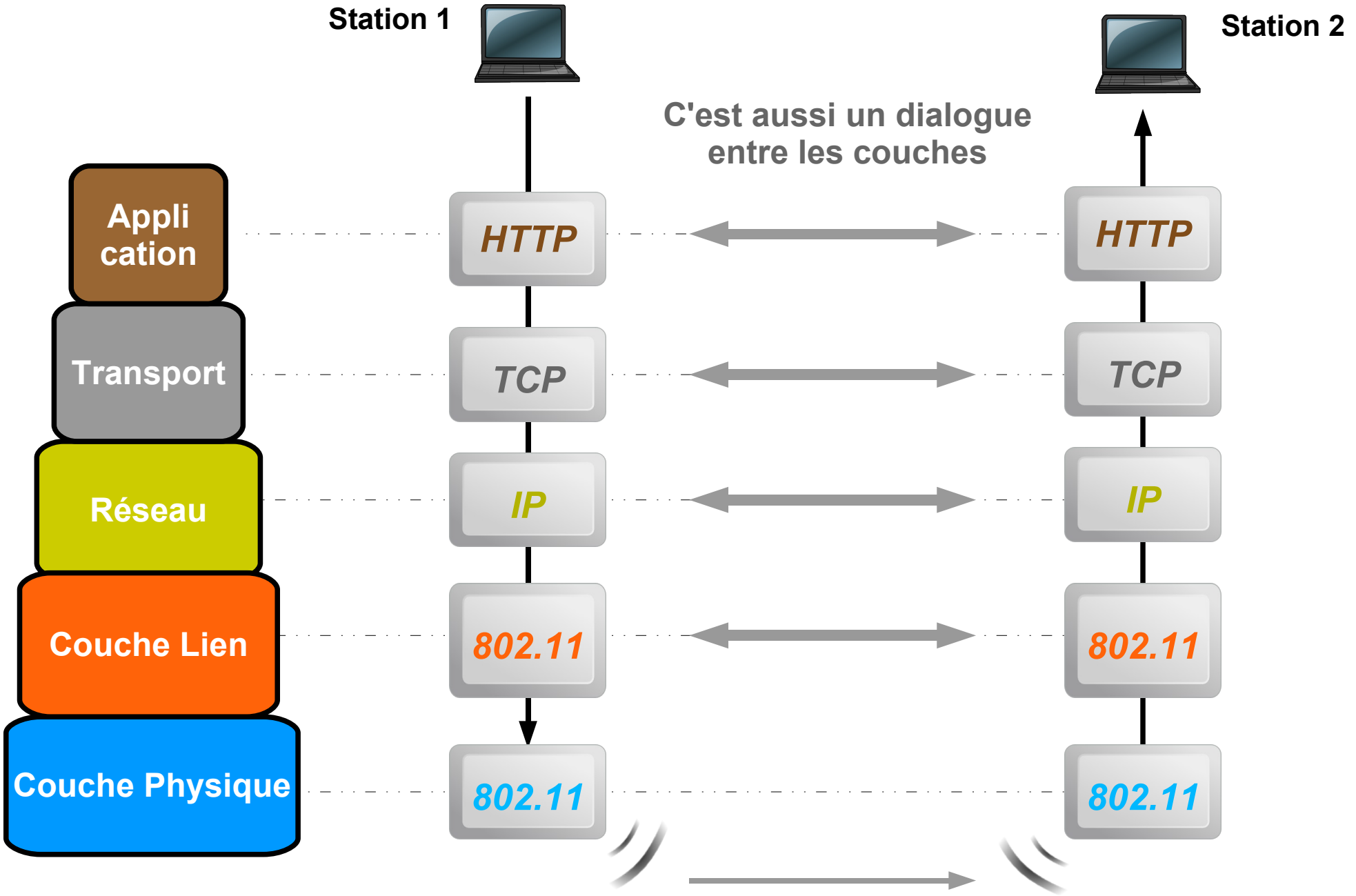
Communication entre deux stations

-mode ad-hoc

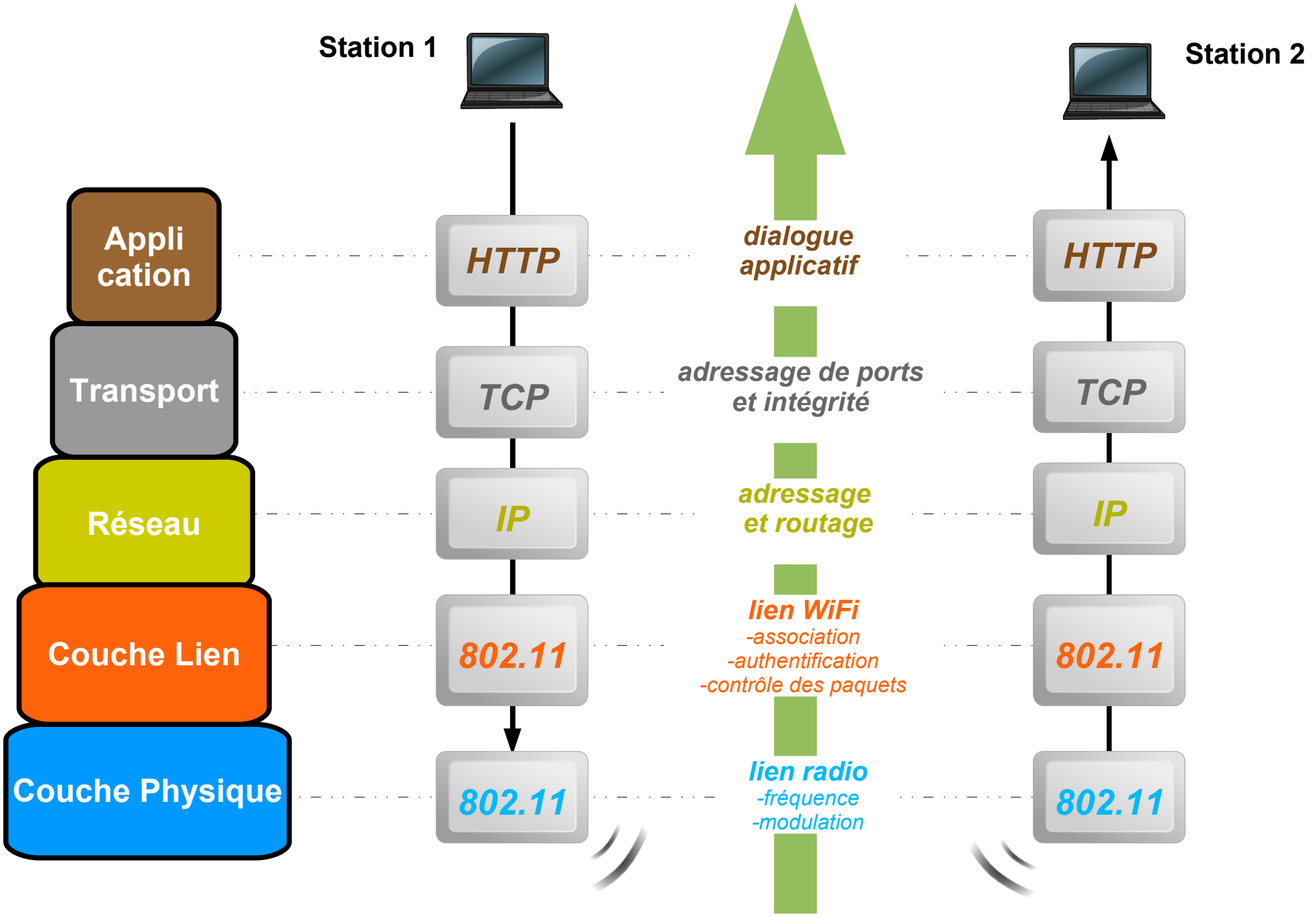
-échange de fichiers en voisinnage réseau



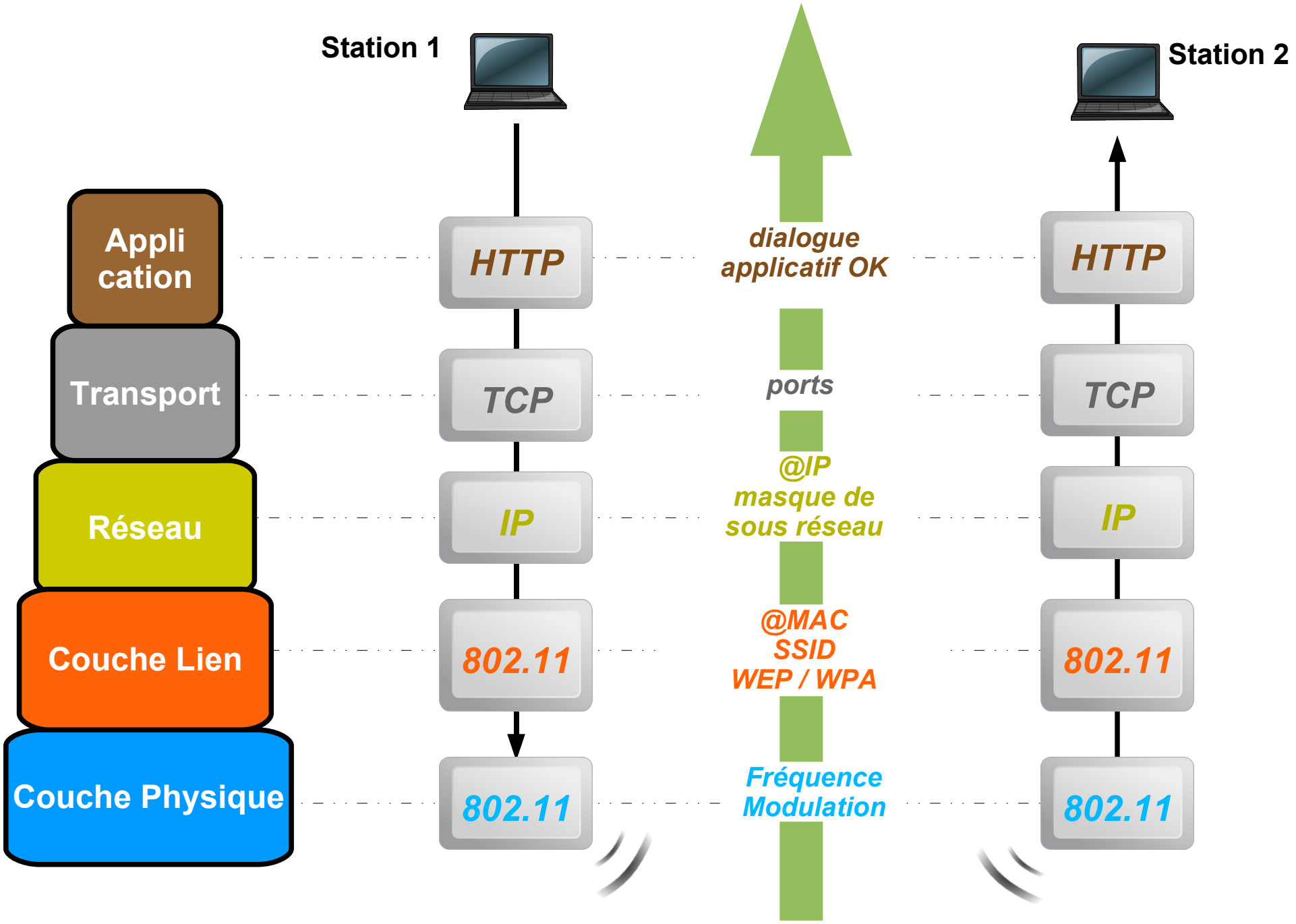
Un dialogue transversal



Des services successifs

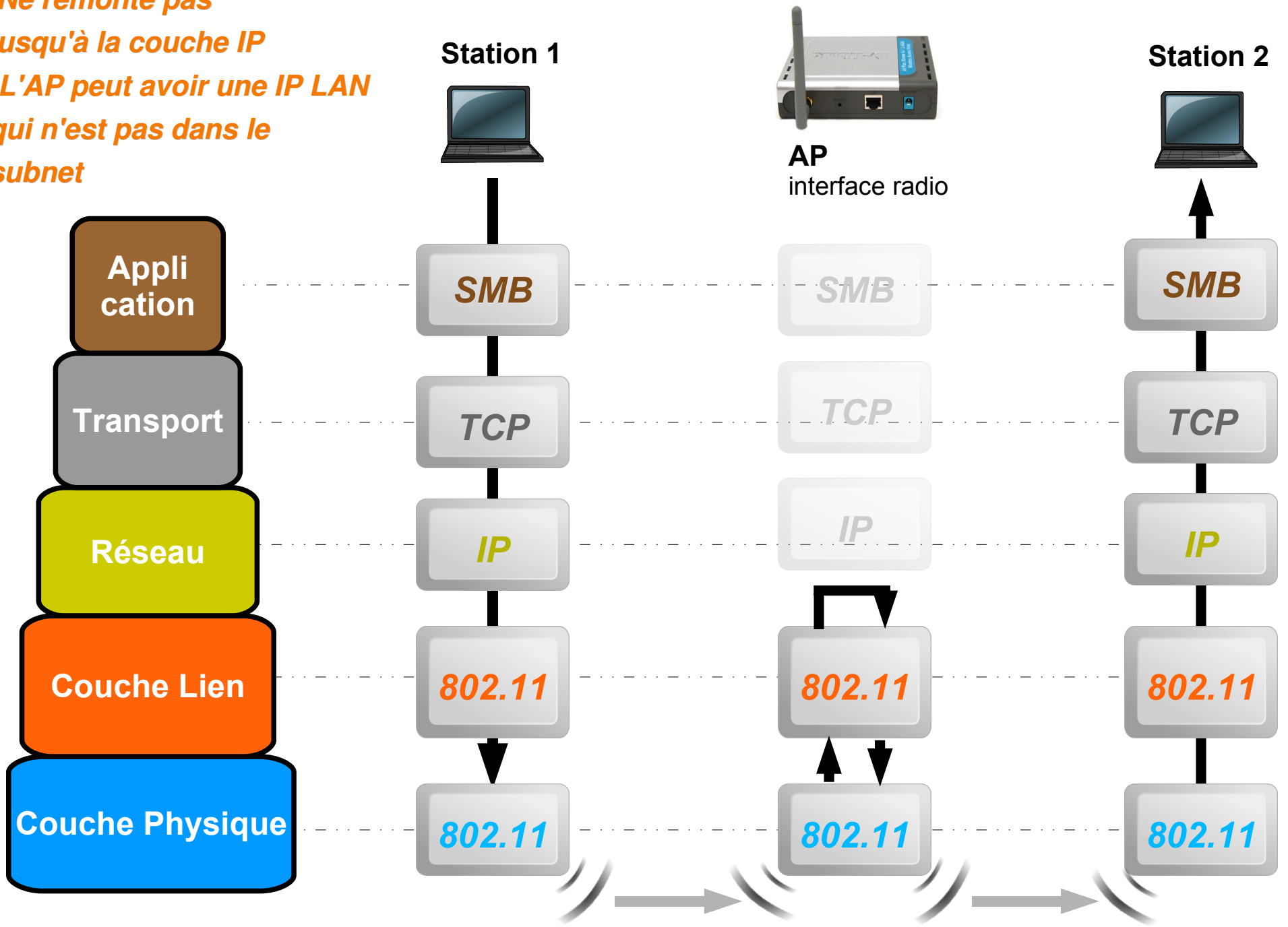


Des filtres successifs



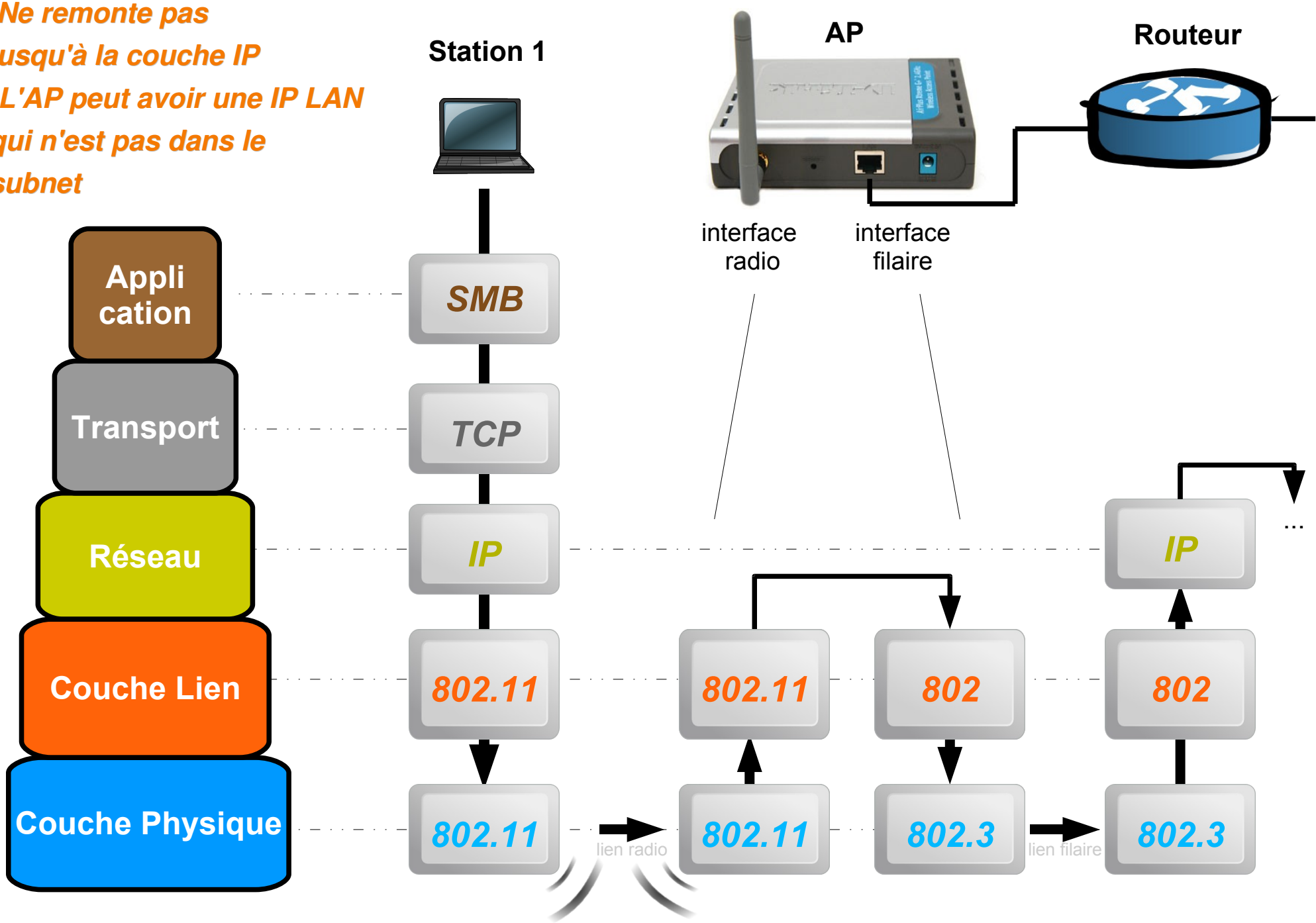
Mode Infrastructure

-Ne remonte pas jusqu'à la couche IP
-L'AP peut avoir une IP LAN qui n'est pas dans le subnet

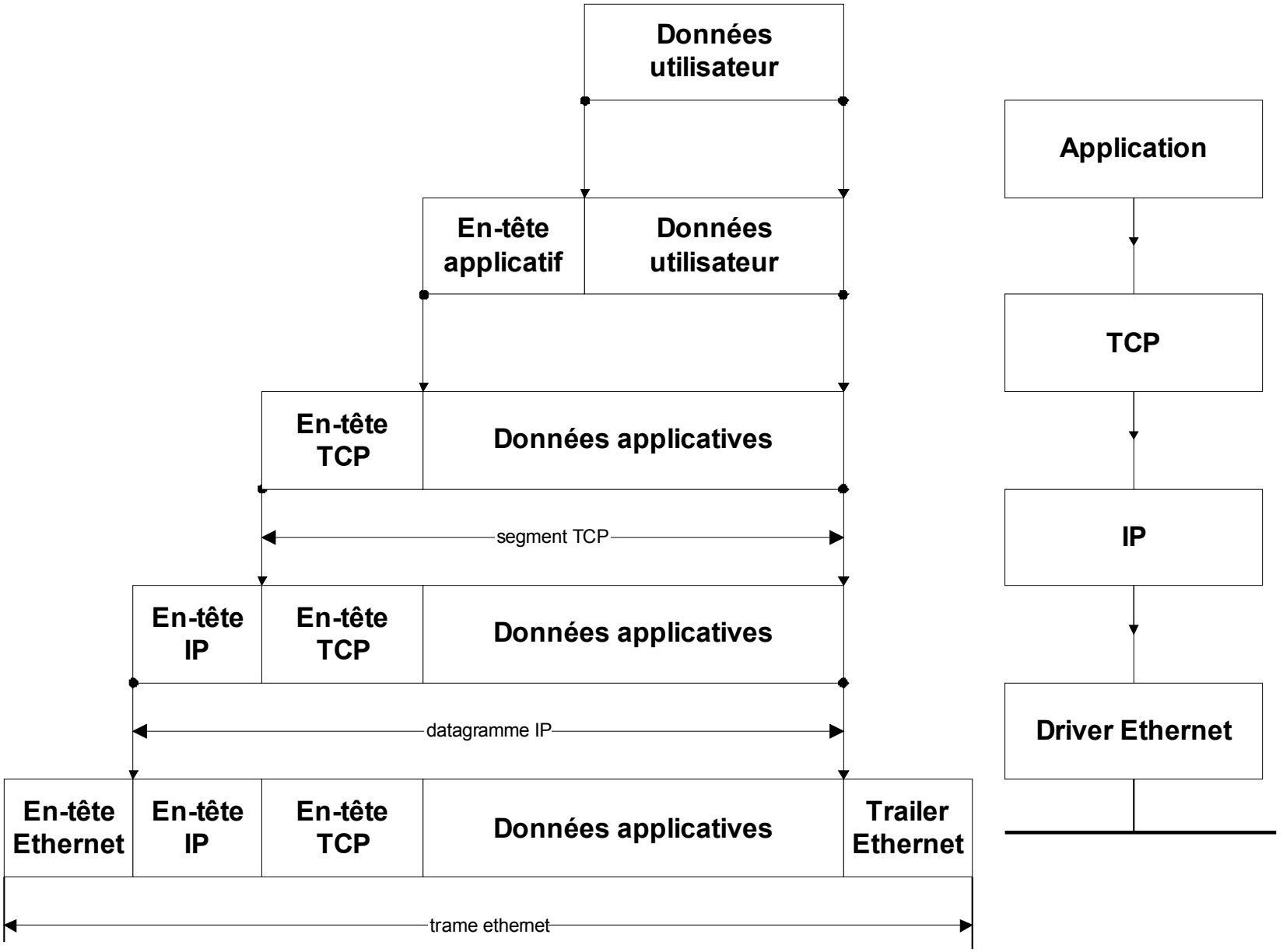


AP = Bridge de niveau 2

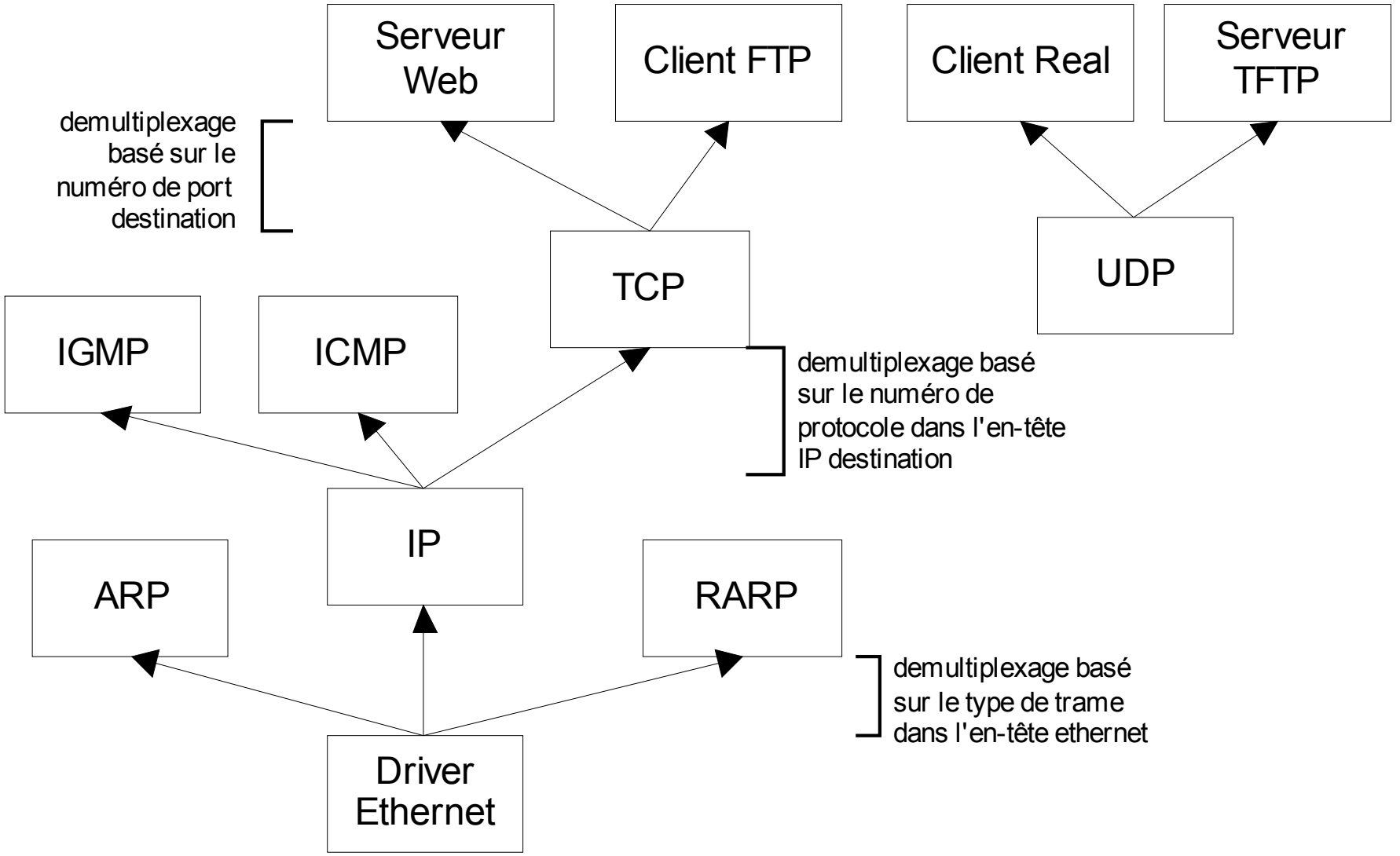
-Ne remonte pas jusqu'à la couche IP
-L'AP peut avoir une IP LAN qui n'est pas dans le subnet



Réseau TCP/IP - Encapsulation



Démultiplexage



Ce qu'il faut retenir

- La couche Wi-Fi (802.11) est indépendante de la couche IP. Elle est préalable à son fonctionnement dans la communication réseau.
- Lors de la configuration du réseau, ces deux aspects sont traités séparément et nécessaires pour la communication entre les équipements :
  - paramètres radio
  - paramètres réseau

Réseau TCP/IP

Les adresses IP

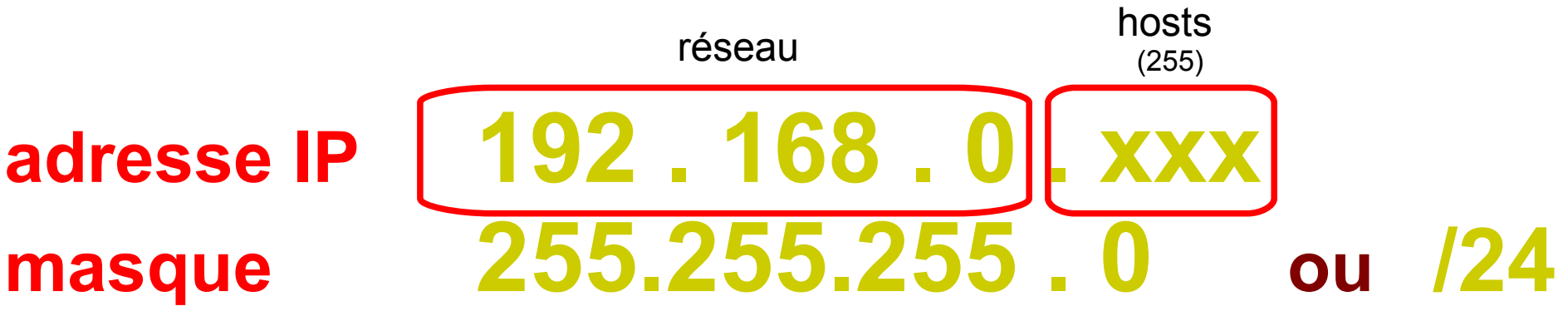
- Dans un réseau, chaque machine est identifiée par une adresse IP, qui doit être unique à l'intérieur du réseau (les réseaux étant délimités par les routeurs).
- Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux.
- Chaque machine ne dispose que d'une adresse par réseau, à l'exception des machines passerelles (routeurs, proxy, gateway) qui possèdent plusieurs interfaces.
- Ces adresses sont composées de 4 nombres entiers (4 octets) entre 0 et 255, notées : xxx.xxx.xxx.xxx
  - De 0.0.0.0 à 255.255.255.255
  - Par exemple : 194.153.205.26

Les adresses IP

- Les 4,3 Milliards d'adresses sont subdivisées en **adresses privées** et en **adresses publiques**.
- Les adresses privées
  - concernent les machines des réseaux locaux (LAN)
  - elles se situent derrière au moins un routeur NAT
  - elles sont d'usage libre / Intranet
  - elles se divisent en trois catégories
    - classe A : **10.0.0.0** à **10.255.255.255** (16387064 @)
    - classe B : **172.16.0.0** à **172.31.255.255** (1032256 @)
    - classe C : **192.168.0.0** à **192.168.255.255** (64516 @)
- Les adresses publiques
  - concernent les machines directement reliées à l'Internet
  - attribuées et contrôlées par l'ICANN

Les masques de sous réseau

- Une adresse IP est constituée de deux parties :
  - A gauche, une partie désigne **le réseau** (netID)
  - A droite, une partie désigne **les ordinateurs** (host-ID)
- Le masque fixe la limite entre ces deux parties.
- Se présente sous la même forme: xxx.xxx.xxx.xxx ou /xx
- Les valeurs non nulles désignent la partie réseau.
  La notation CIDR désigne le nombre de bits du réseau :
  24 -> 3 octets



Les masques de sous-réseau

- Les équipements qui veulent communiquer entre eux, doivent utiliser la **même adresse réseau** (masque) et une **adresse d'ordinateur** (host)

Adresse IP de l'ordinateur 1	Adresse IP de l'ordinateur 2	Masque de sous réseau
192.168.0.1	192.168.0.2	255.255.255.0
192.168.10.1	192.168.0.3	255.255.0.0
192.56.78.98	81.63.75.17	0.0.0.0

Masque de sous réseau	Notation CIDR	Nombre de machines
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1022
255.255.248.0	/21	2046
255.255.240.0	/20	4094
255.255.224.0	/19	8190
255.255.192.0	/18	16382
255.255.128.0	/17	32766
255.255.0.0	/16	65534
255.254.0.0	/15	131070
255.252.0.0	/14	262142
255.248.0.0	/13	524286
255.240.0.0	/12	1048574
255.224.0.0	/11	2097150
255.192.0.0	/10	4194302

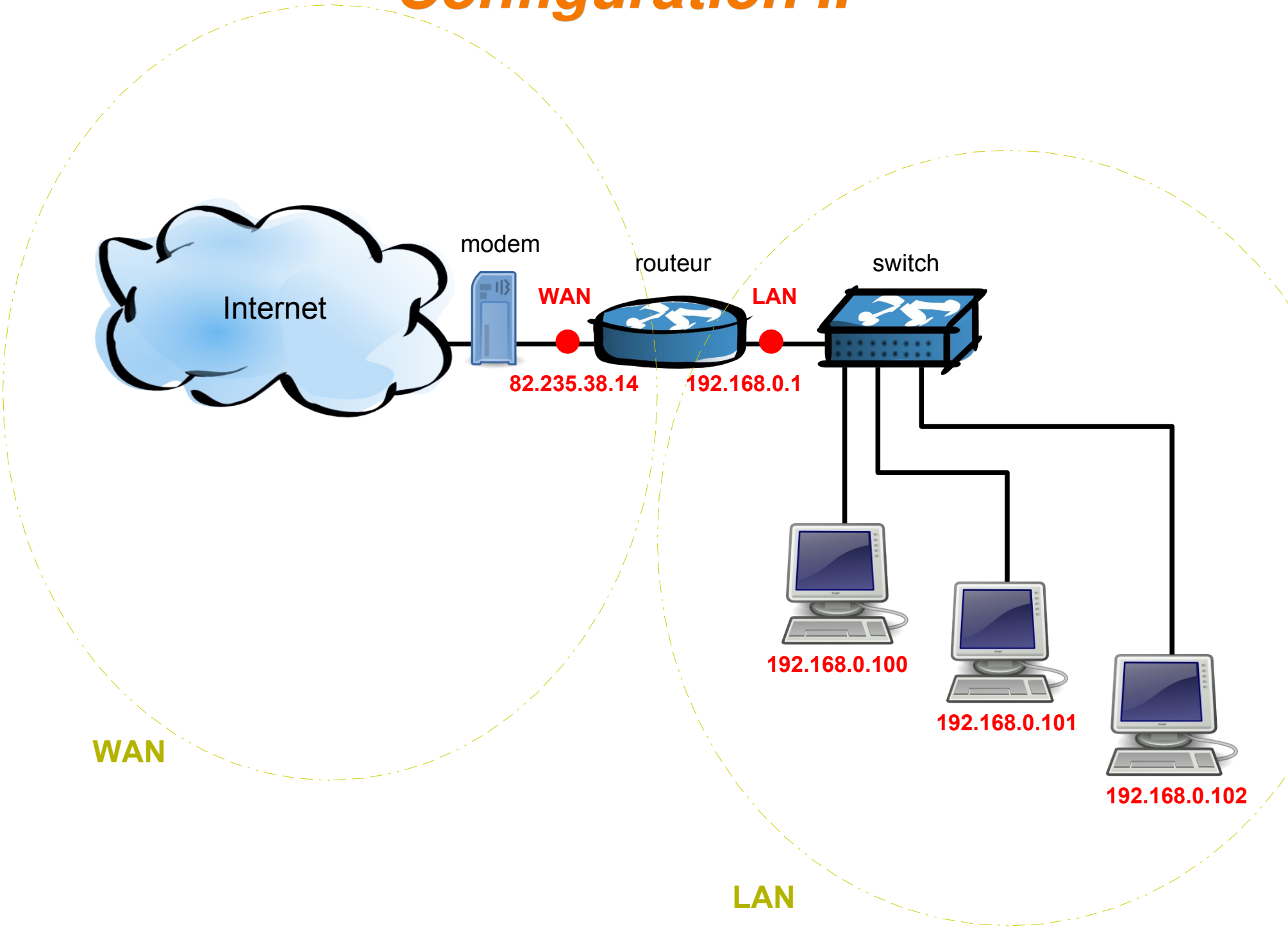
Par défaut, dans un réseau local, on utilisera :

192.168.0.xxx / 255.255.255.0 : 254 machines (/24)

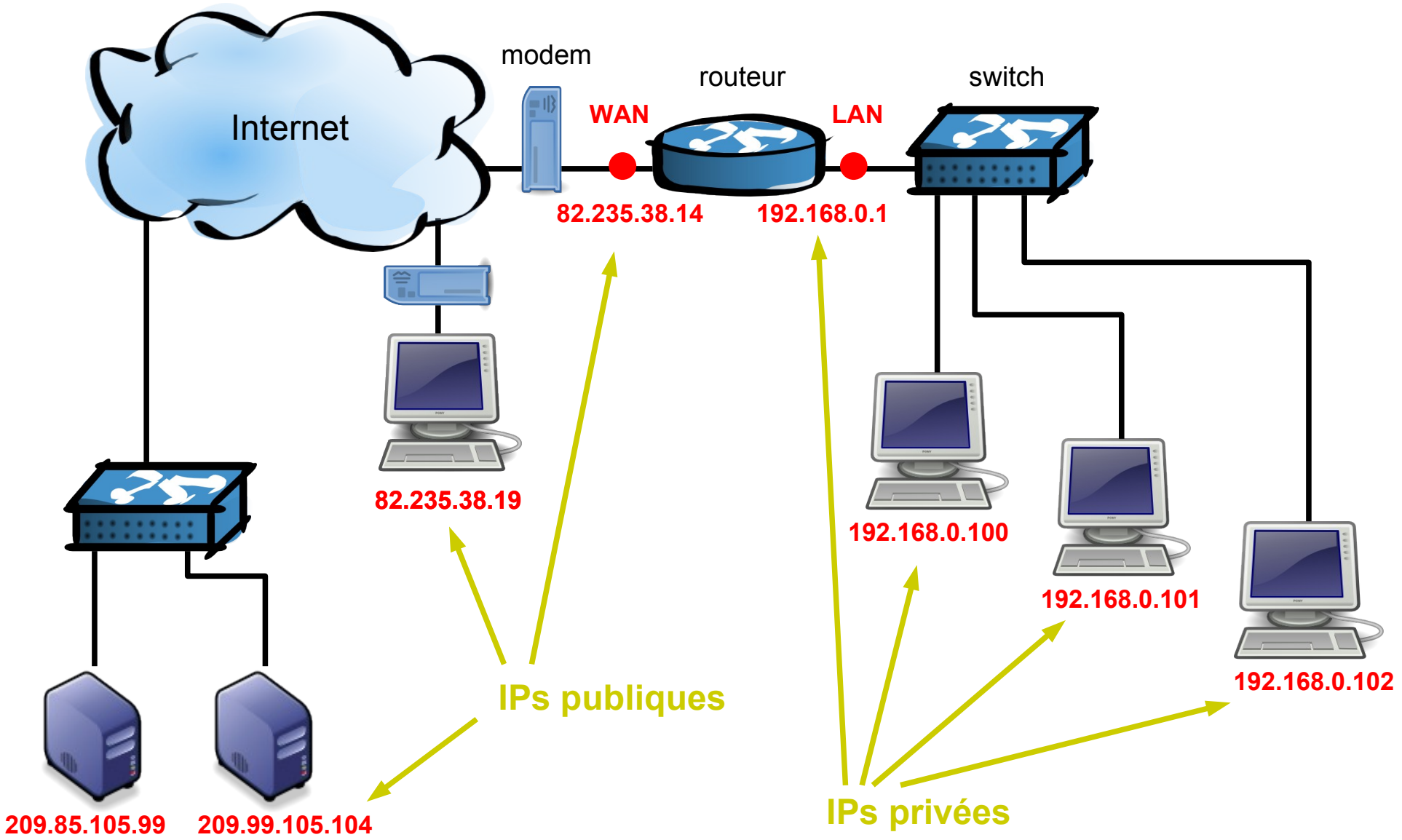
Les masques de sous-réseau

- Nombre de machines = $2^{(32\text{-CIDR})}-2$
- Les deux adresses en moins sont :
  - **l'@ broadcast** : dernière valeur de l'host-ID (ex : 192.168.0.255 / 24)
  - **l'@ réseau** : première valeur de l'host-ID (ex : 192.168.0.0 / 24)
- Des @IP apparemment compatibles peuvent correspondre à des réseaux différents (et donc être non joignables) :
  - **192.168.0.1 / 255.255.255.0** : 254 machines (/24)
  - **192.168.0.2 / 255.255.255.240** : 15 machines (/28)
  - **192.168.0.3 / 255.255.0.0** : 65534 machines (/16)

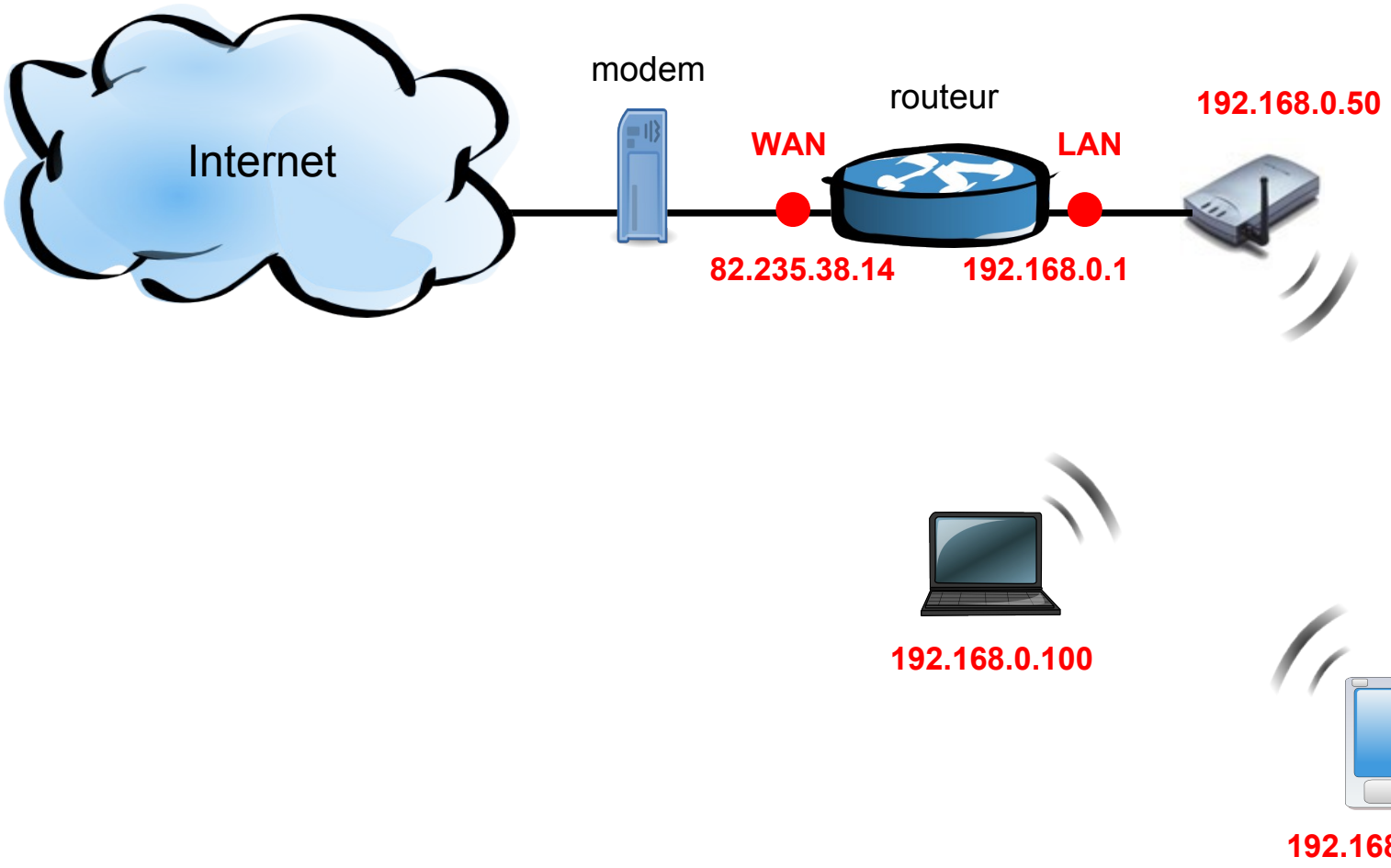
Configuration IP



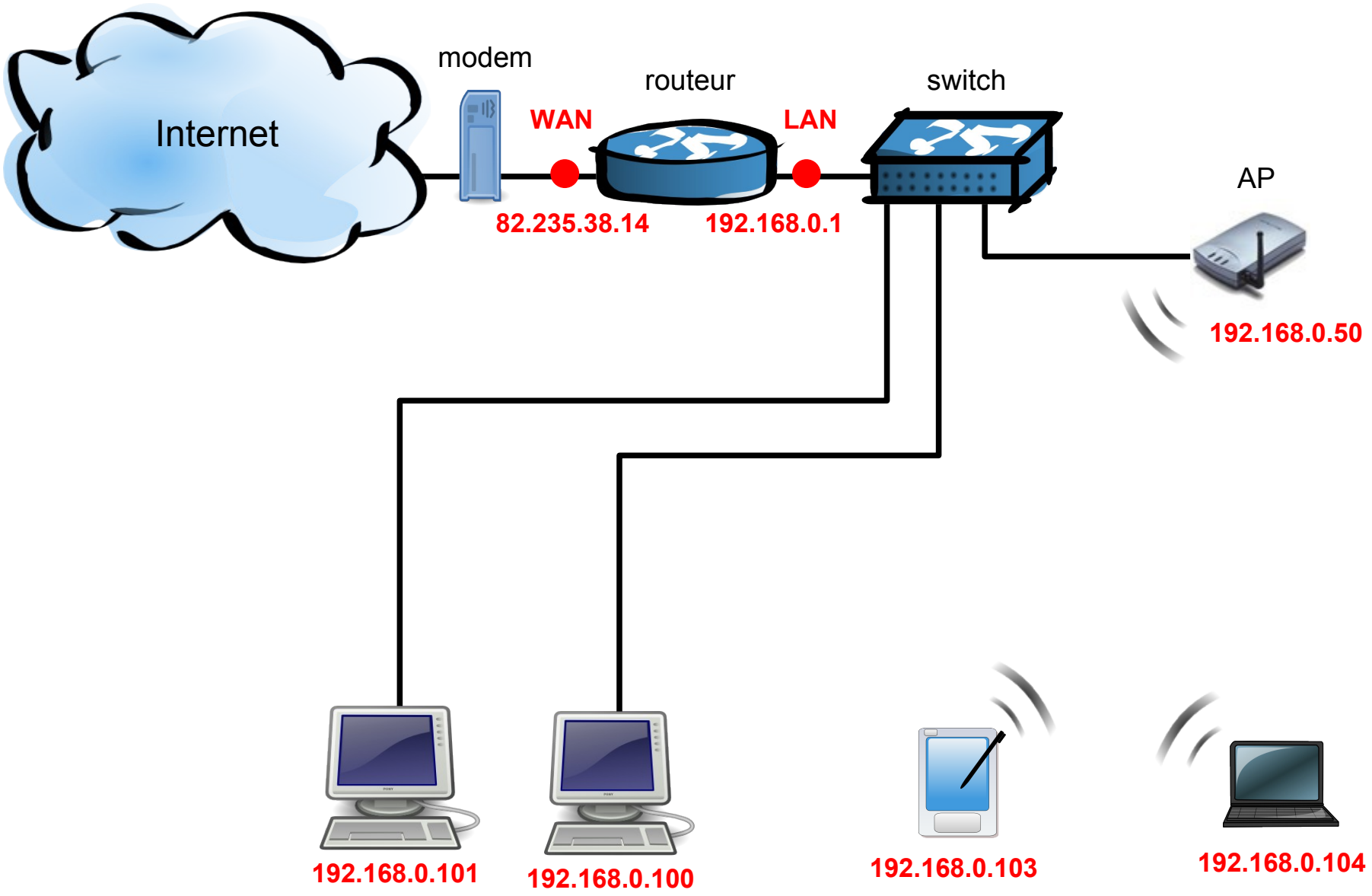
Configuration IP



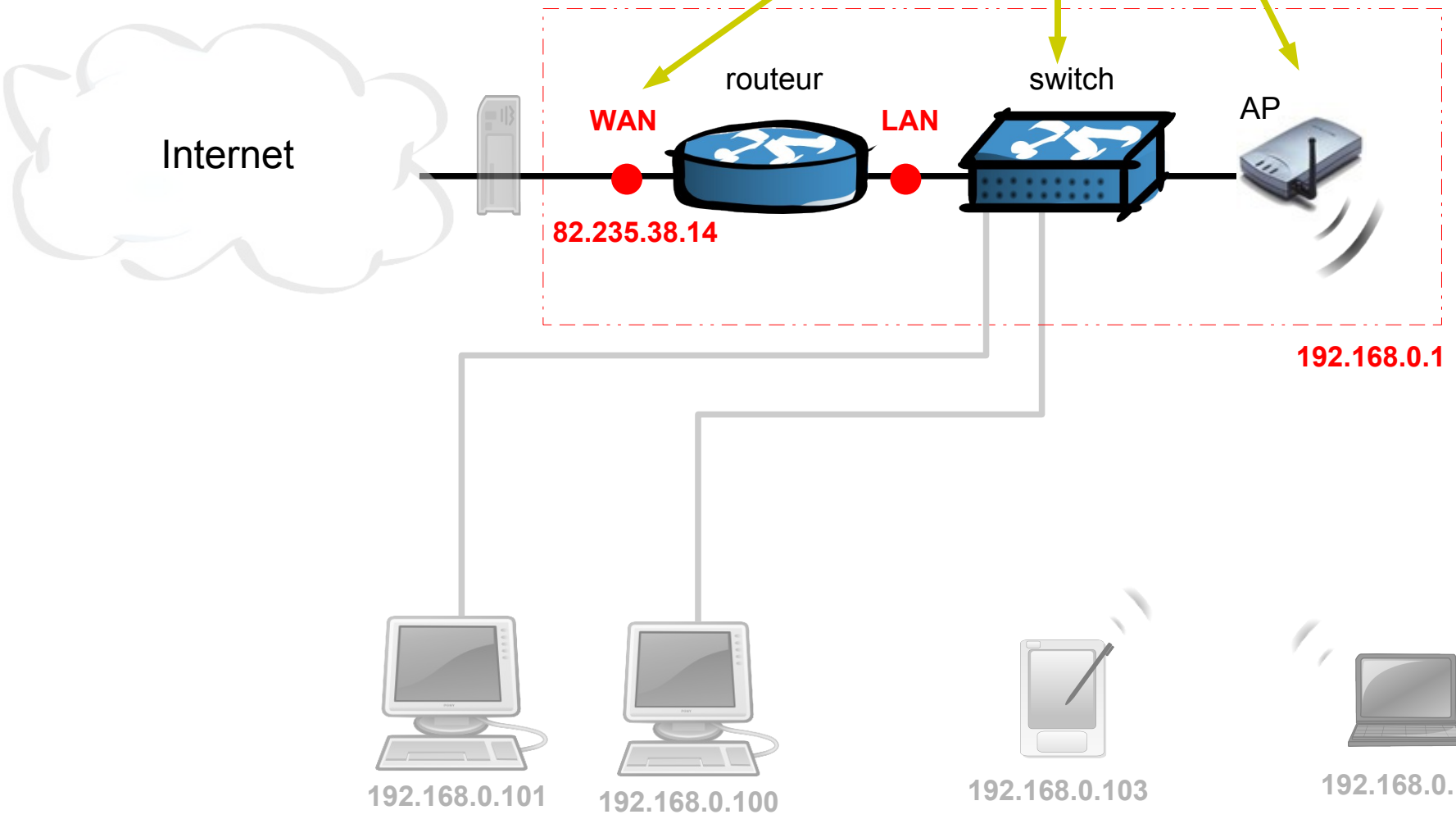
Topologie Infrastructure



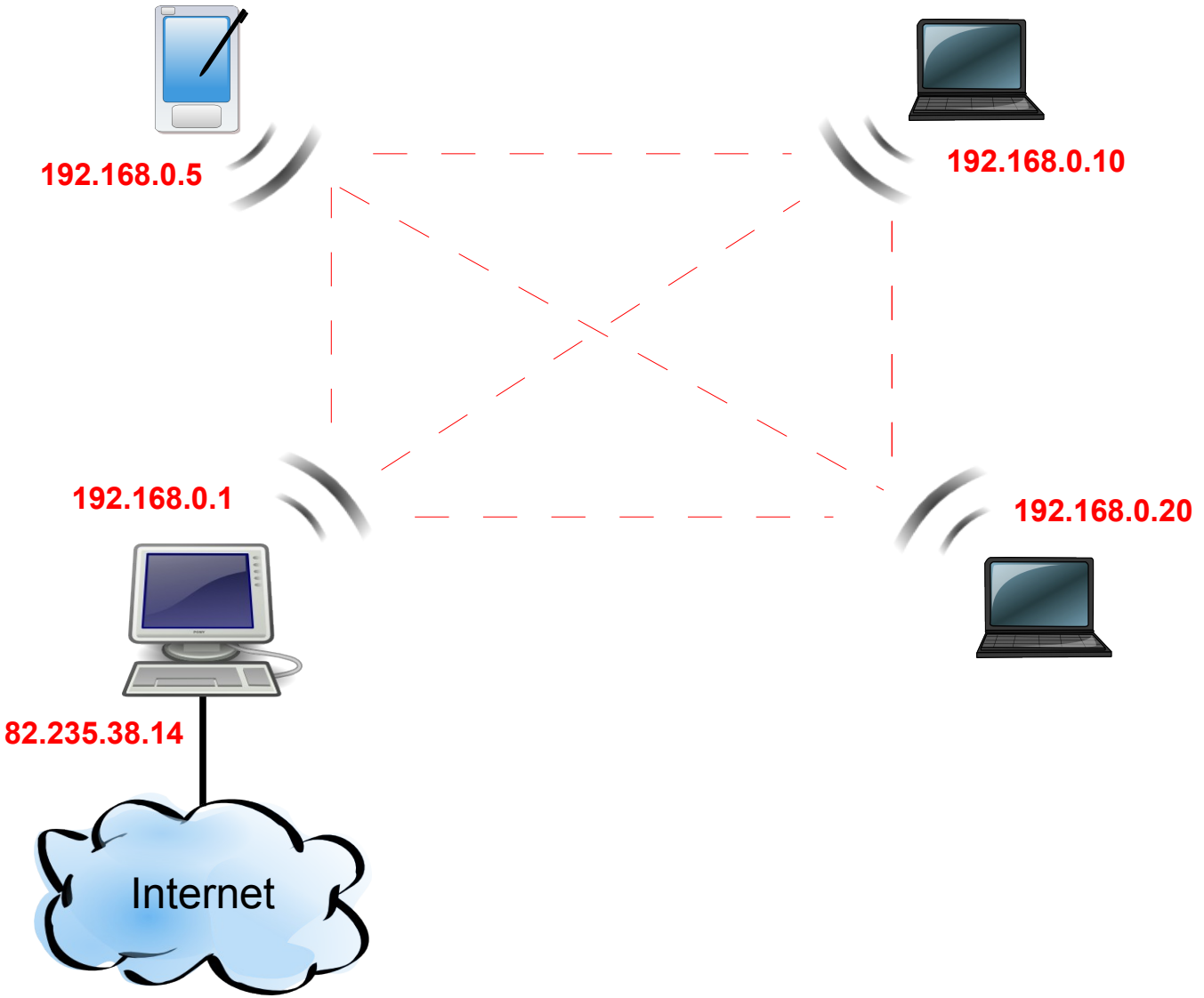
Topologie Infrastructure



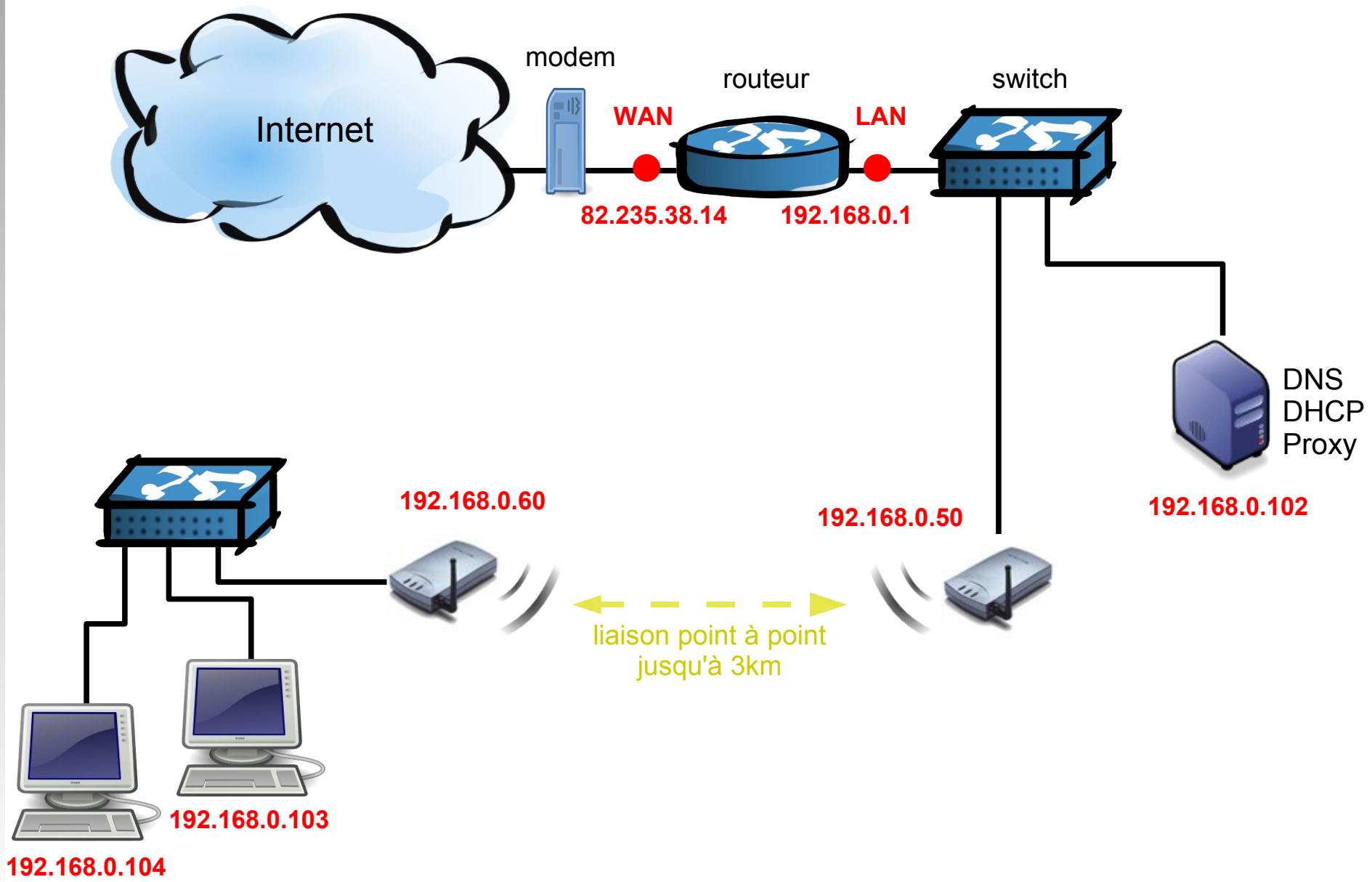
= 3 en 1


Internet
WAN
routeur
LAN
switch
AP
82.235.38.14
192.168.0.1
192.168.0.101
192.168.0.100
192.168.0.103
192.168.0.104

Topologie ad-hoc



Etendre un réseau existant



Configurations nécessaires

- Pour communiquer dans le cadre du LAN (*) les machines ont besoin de :
  - **une adresse IP** + **un masque de sous-réseau**

- Pour sortir sur Internet une machine a besoin de :
  - **une adresse IP** + **un masque de sous-réseau**
  - **une passerelle** (Gateway)
  - **un serveur de résolution de nom** (DNS)

* : échange de fichiers (SMB), ping (ICMP), FTP, Pages Web (HTTP)...

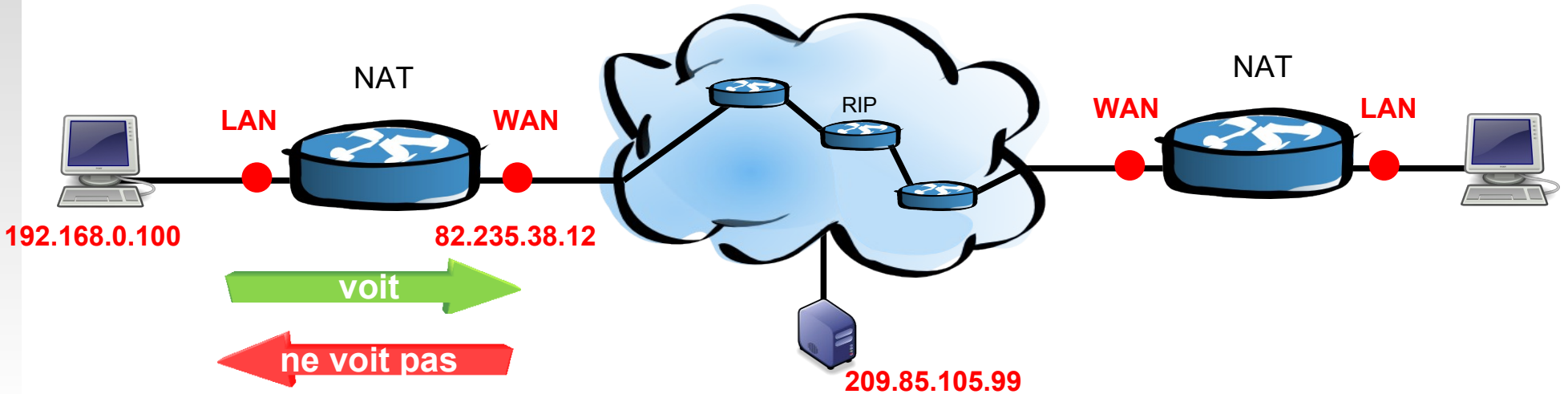
Serveur DHCP

- Distribue dynamiquement aux machines en effectuant la requête
  - une adresse IP + plage de sous réseau
  - la passerelle de sortie
  - une adresse de DNS

    -> configure automatiquement **la couche IP** du réseau
- Cette configuration dynamique est particulièrement adaptée aux réseaux de type Infrastructure.
- La plupart des AP - routeurs intègrent cette option.
- Faiblesse sécurité : paramètres IP connus.

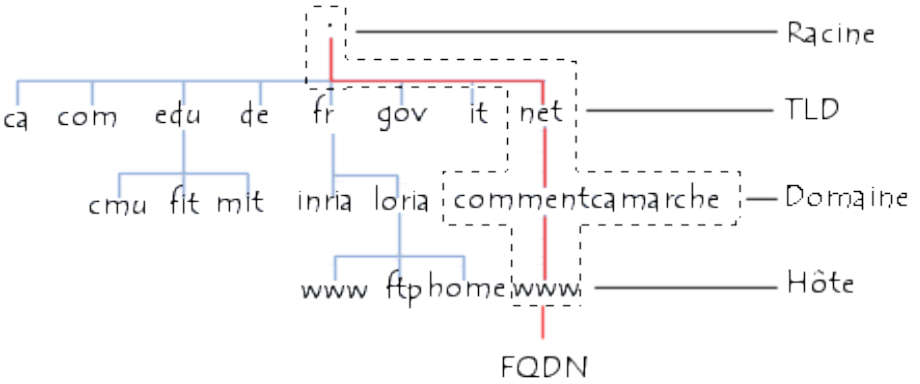
Les routeurs

- Possèdent deux interfaces. Ils transmettent leurs paquets IP d'une interface à l'autre.
- Routage NAT
  - Permets une translation d'adresse :
    une @IP publique <-> n * @IP privées
  - Le réseau public (WAN) est visible depuis le réseau privé (LAN) mais pas l'inverse.



Le serveur DNS

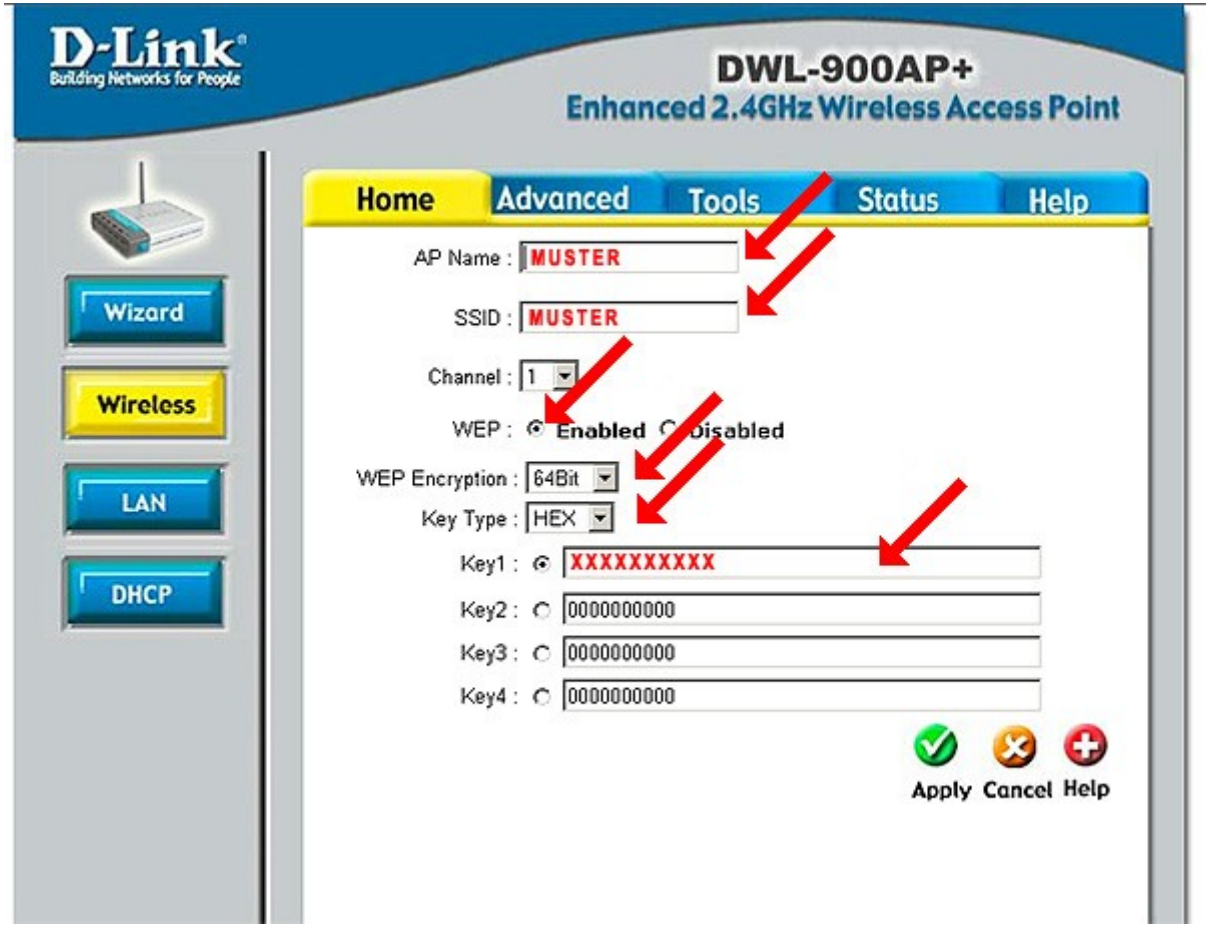
- Un DNS (Domain Name System) effectue la corrélation entre **une @IP** et **un nom de domaine** associé
  - ex : 209.85.135.99 <-> google.fr
- Le serveur qui effectue la résolution de nom est en général hébergé au niveau du FAI et son adresse est récupérée dynamiquement en même temps que l'IP publique (routeur, PC).



Configuration du réseau Wi-Fi

Réglages Radio de l'AP

- Configuration Radio
  - Nom
  - (E)SSID
  - Canal d'émission
  - SSID Broadcast
  - Topologie : AP, Client, Bridge, Repeater...

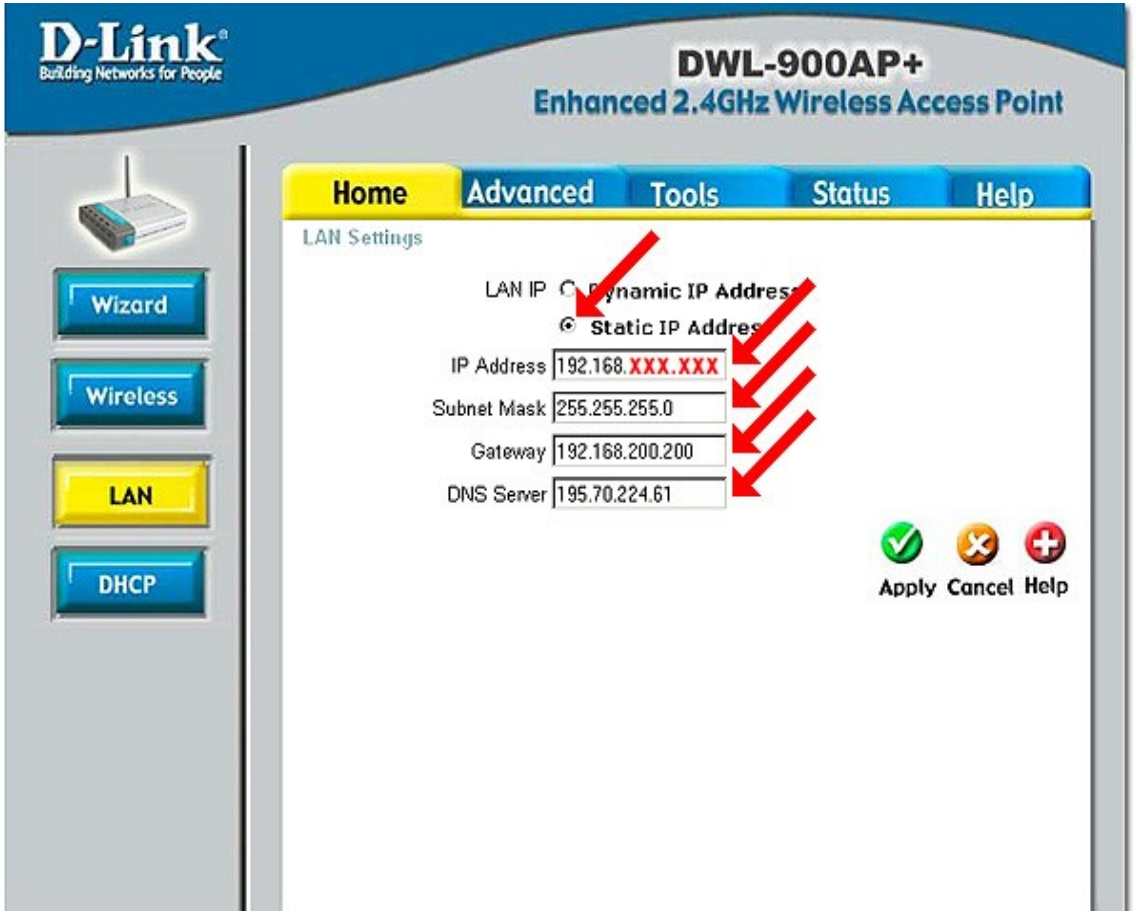


- Configuration Radio avancée
  - Puissance d'émission
  - Chiffrement et authentification : WEP / WPA
  - Filtrage des adresses MAC
  - Radio : Débits, DTIM, Fragmentation, Beacon...

Réglages TCP/IP de l'AP

- @IP WAN
  (interface Ethernet)
  - @IP / Masque
  - Passerelle
  - DNS

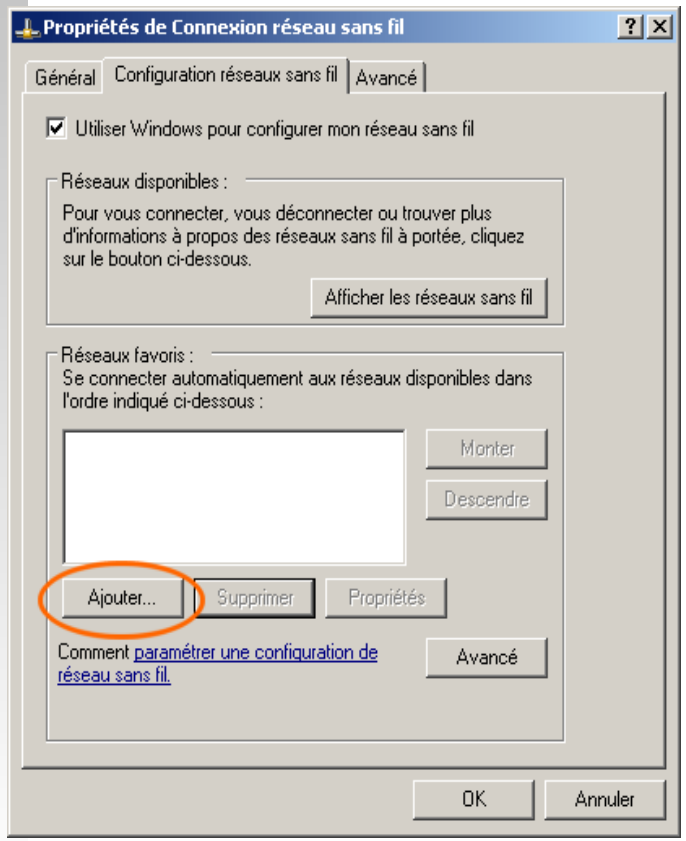
  ou
  - attribution en DHCP
- @IP LAN
  (interface Radio et Switch)
  - Activation DHCP - Plage

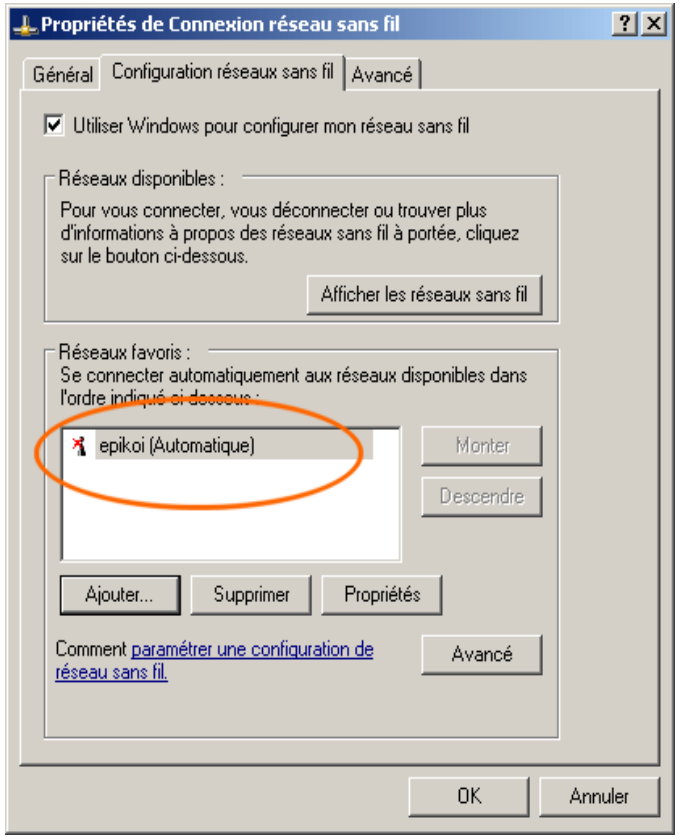


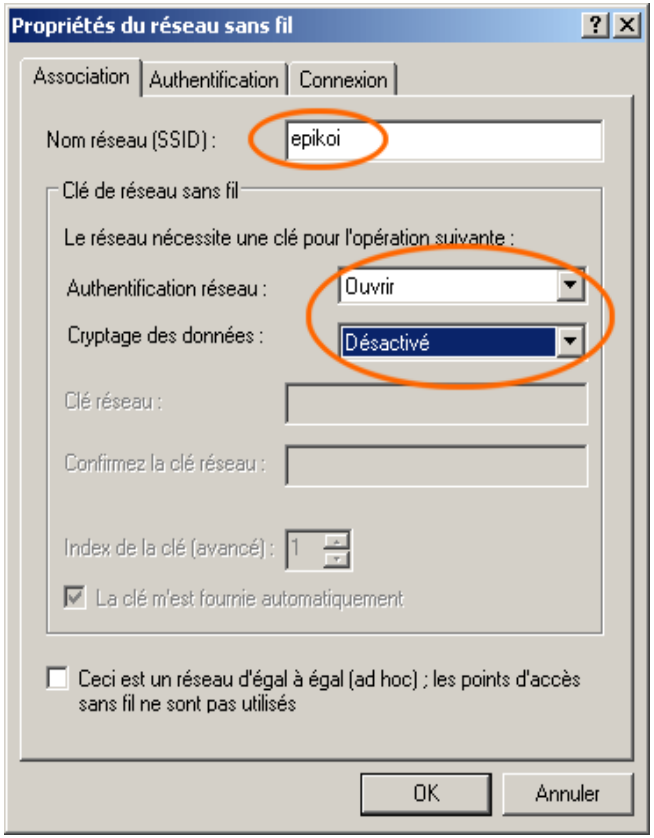
Réglages radio de l'adaptateur Wi-Fi

- Configuration Radio
  - (E)SSID
  - Topologie : Infrastructure ou ad-hoc
  - Cryptage et authentification :

CRYPTAGE ► AUTHENTIFICATION ▼	Pas de Cryptage	WEP	TKIP	TKIP
Ouverte	X	(X)		
Partagée	(X)	X		
WPA-PSK			X	
WPA-EAP (802.1x)				X





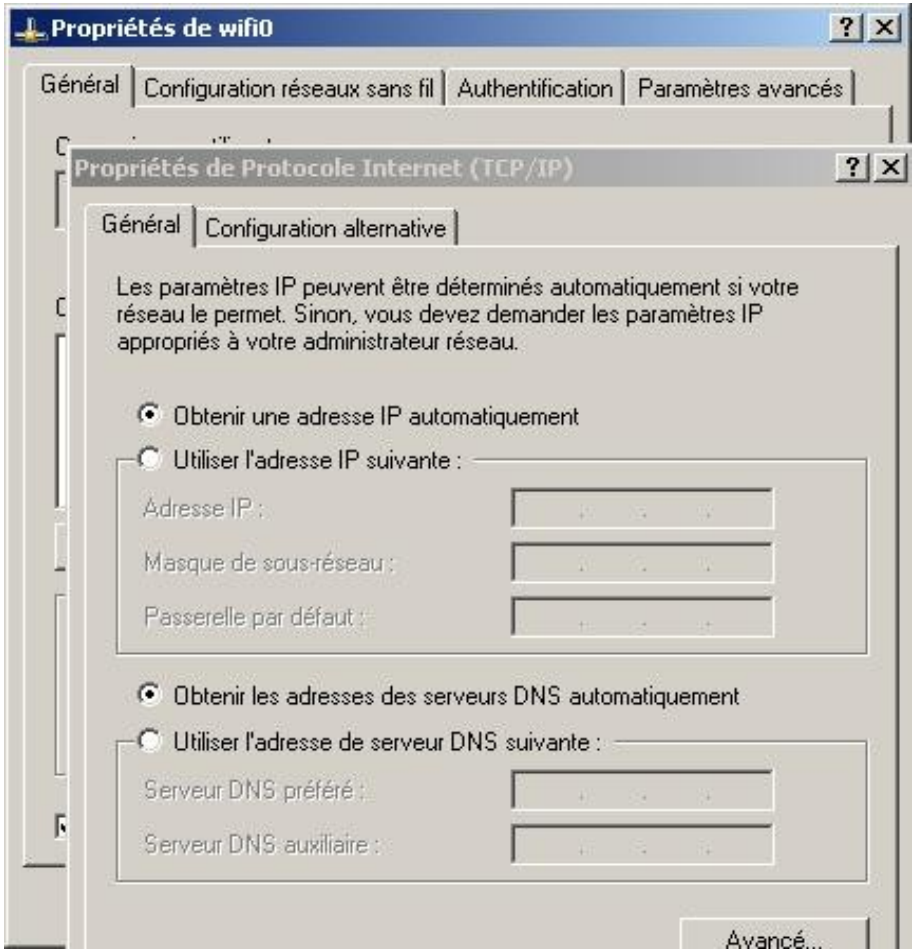


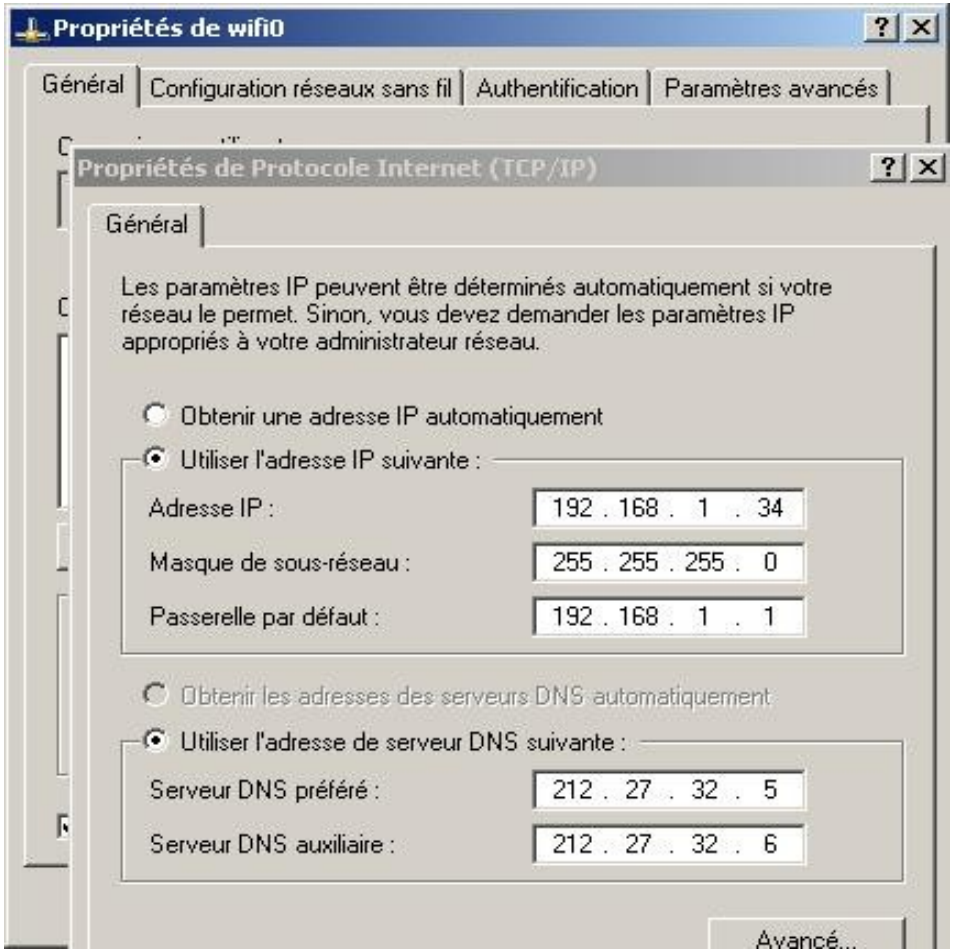
Réglages TCP/IP de l'adaptateur Wi-Fi

- DHCP

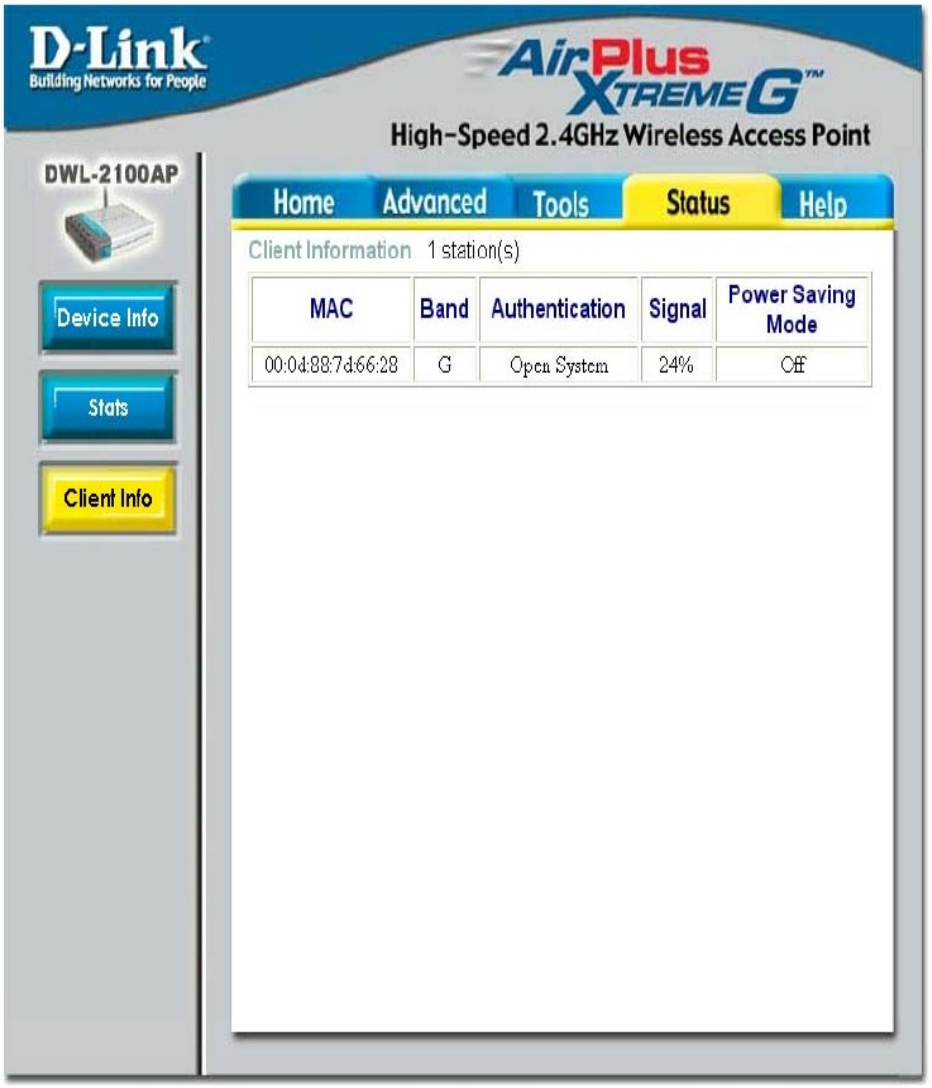
OU

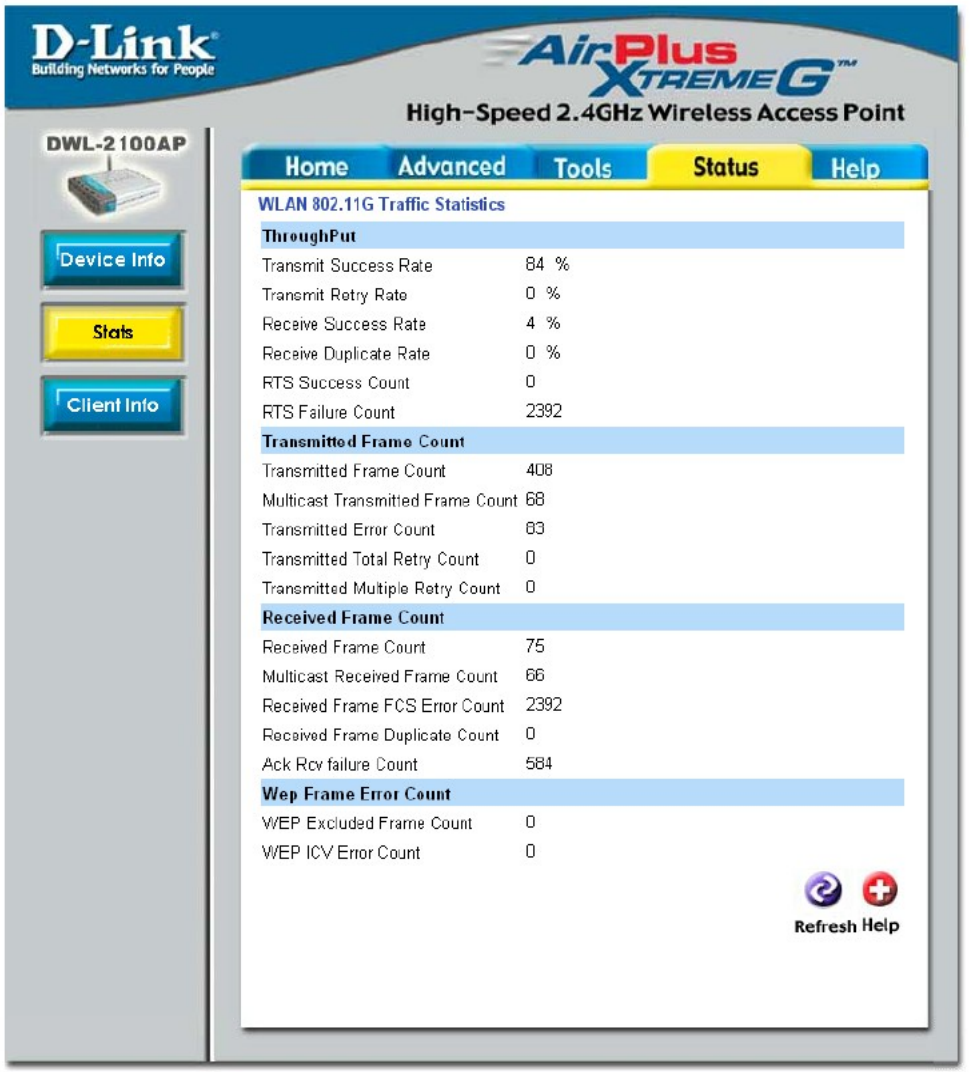
- Valeurs fixes
  - @IP / masque
  - Passerelle
  - DNS



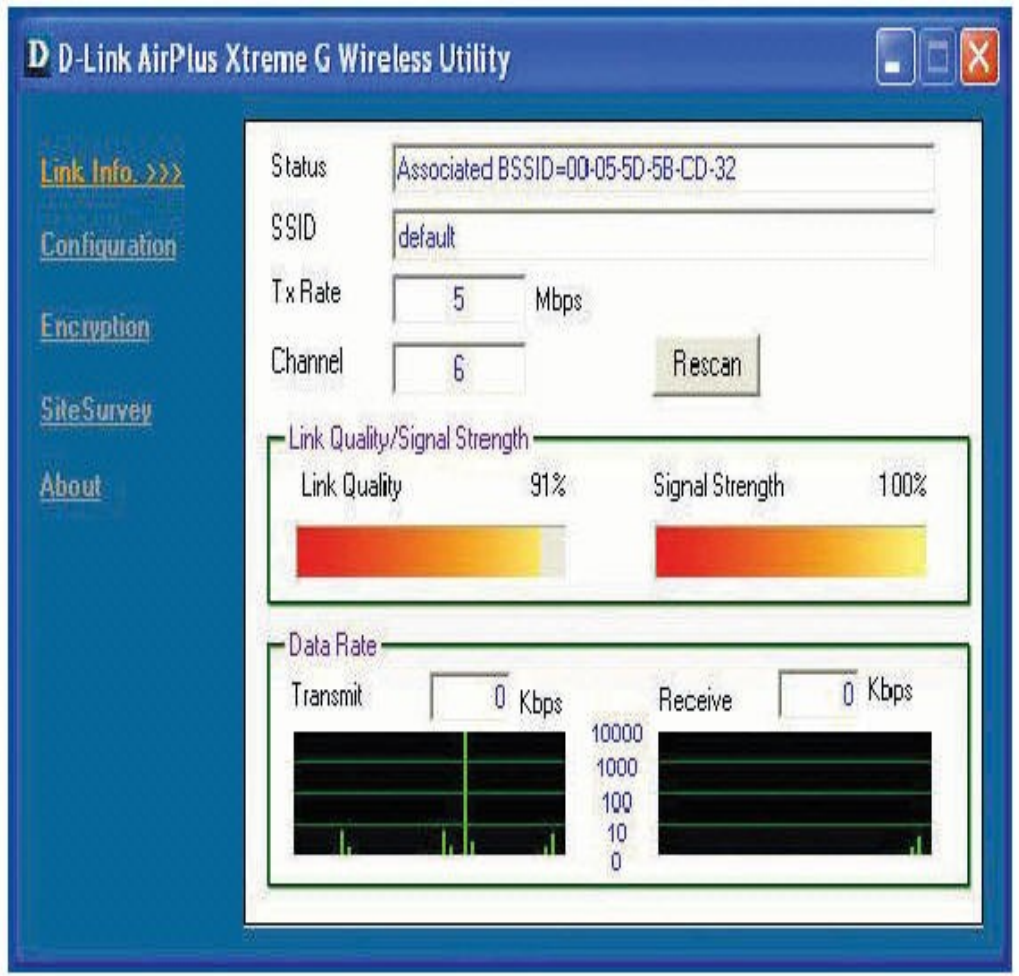


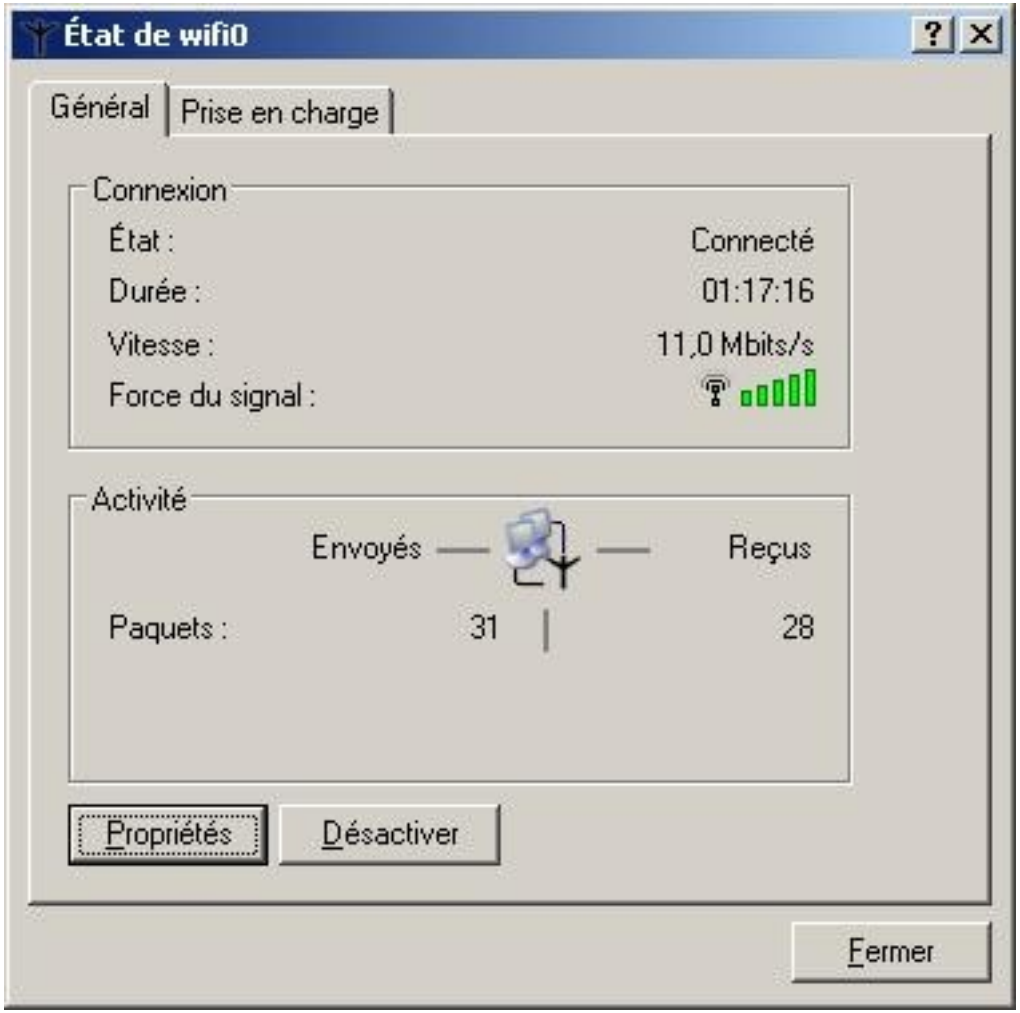
Diagnostics d'association (AP)





Diagnostics en mobilité (client)

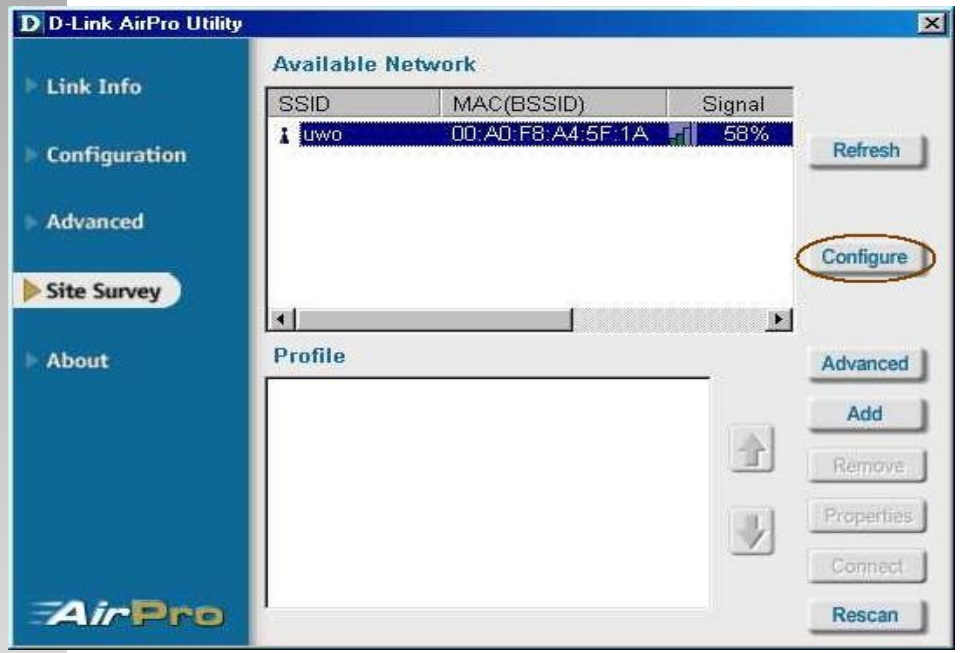


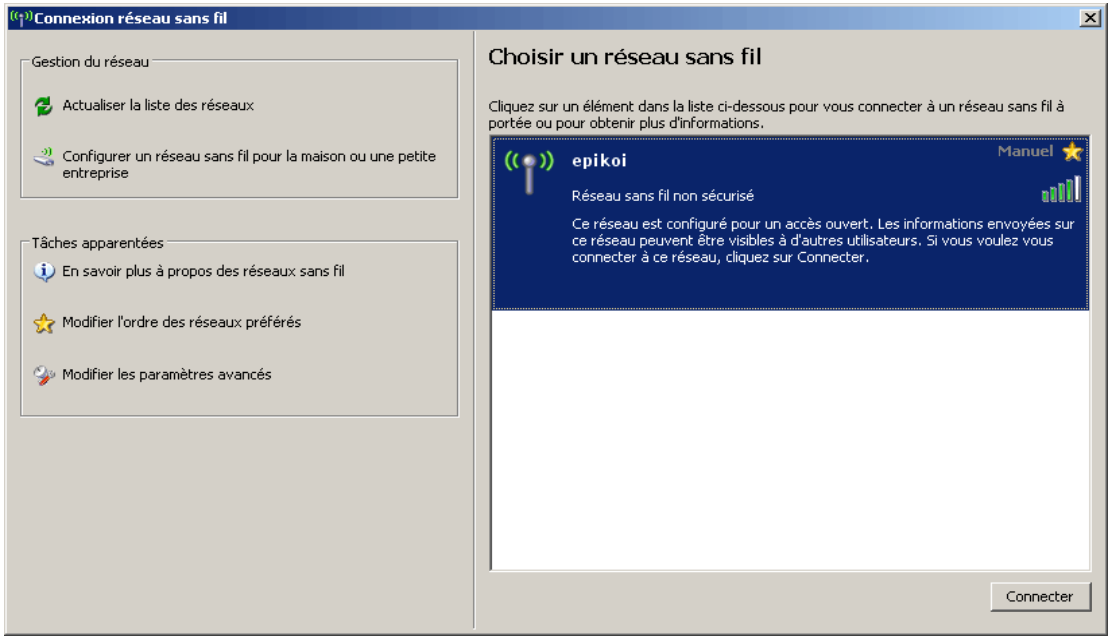


Outil Fabricant (Dlink)
-Puissance du signal
-Qualité du signal

Outil générique (Windows)
-Puissance du signal

Détection des réseaux (client)

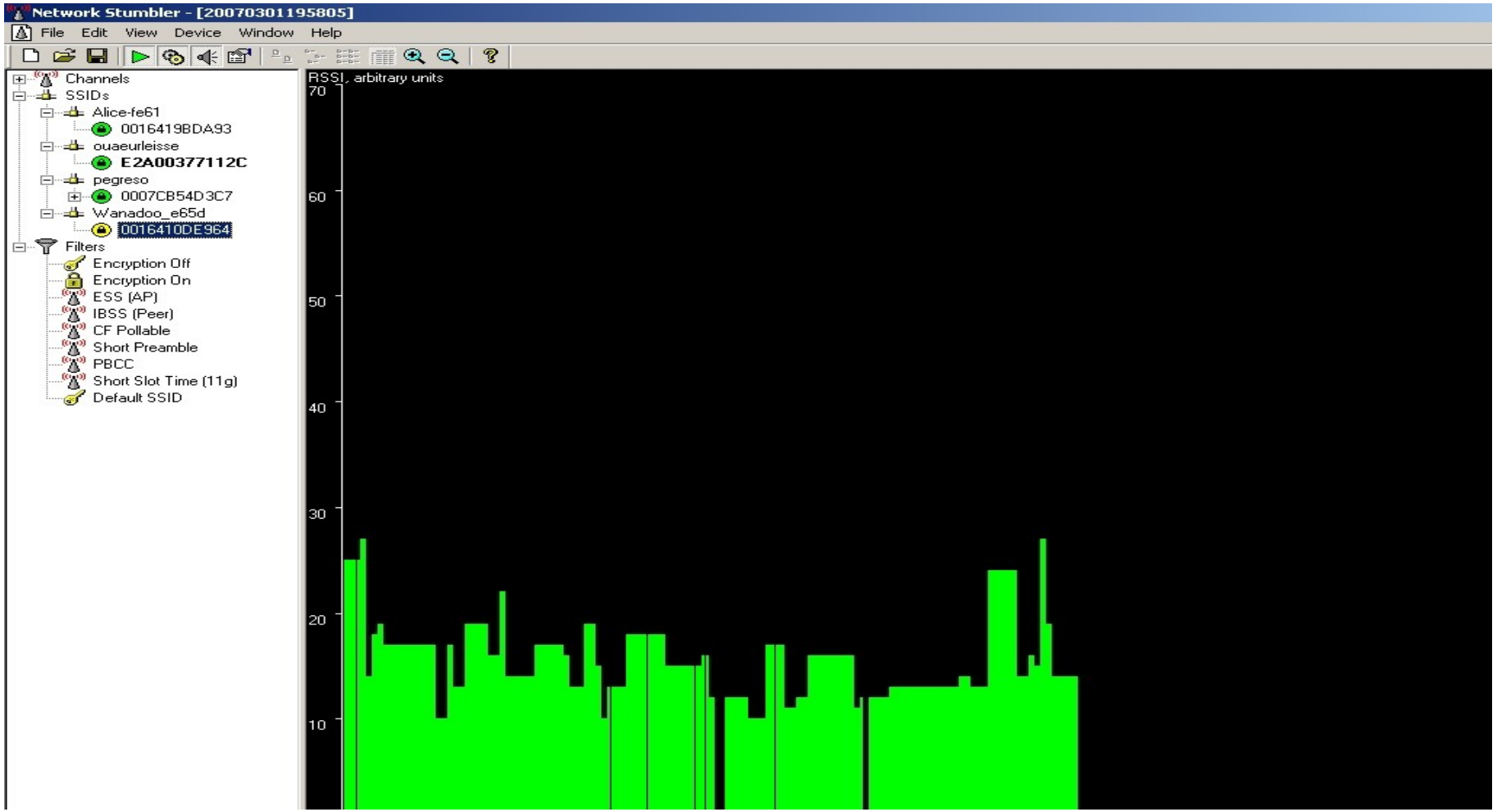




Outil Fabricant (Dlink)
-SSID
-BSSID
-Puissance du Signal

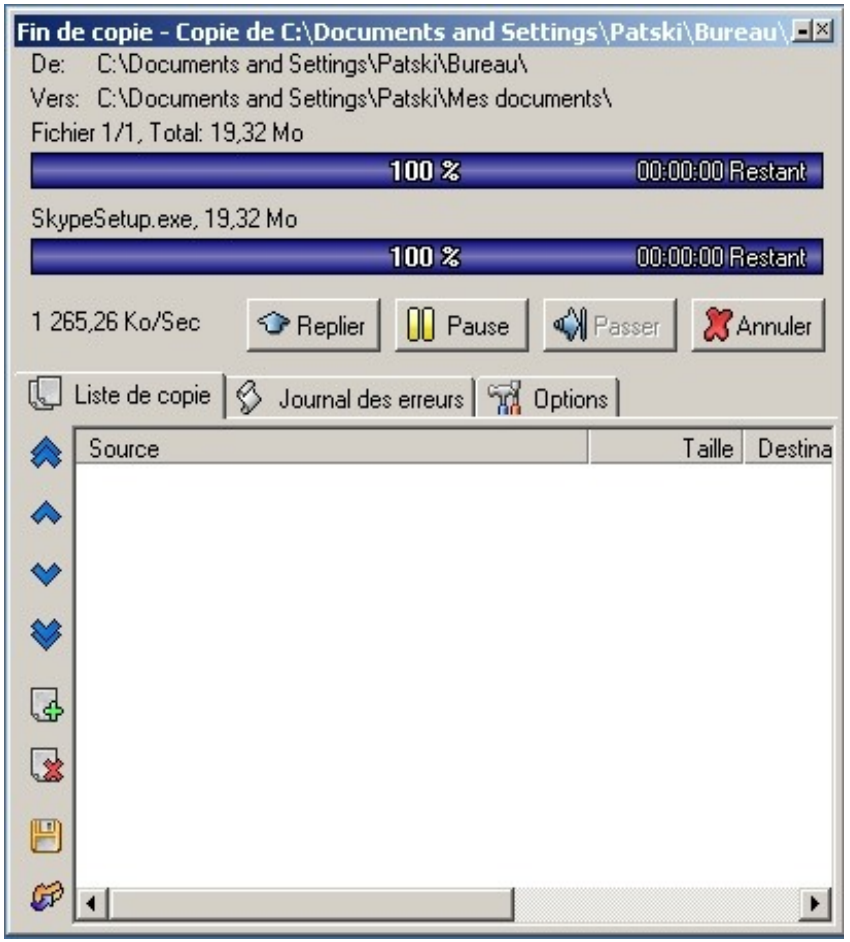
Outil générique (Windows)
-SSID
-Puissance du signal

Outils génériques (client)



NetStumbler
-SSID
-BSSID
-Puissance du Signal
-type d'encryption
-rapport S/B

Mesure de débit



SuperCopier
(Windows)

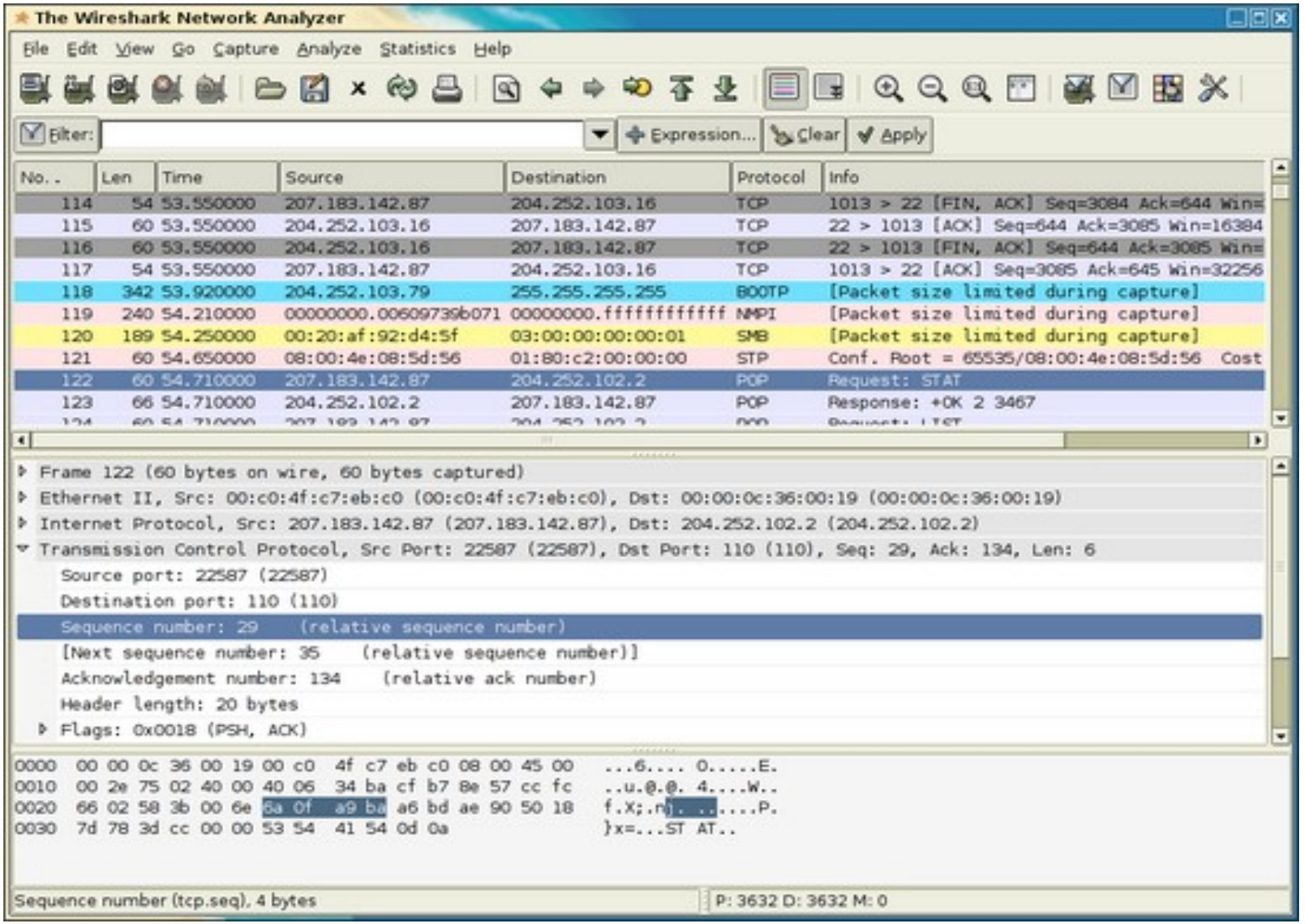
```
C:\>iperf -c 195.128.64.194 -p 4665 -t 60
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4632 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-64.3 sec   160 KBytes  20.4 Kbits/sec

C:\>iperf -c 195.128.64.194 -p 4665 -t 180
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4633 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-187.1 sec   528 KBytes  23.1 Kbits/sec

C:\>iperf -c 195.128.64.194 -p 4665 -t 60
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4667 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-65.1 sec   136 KBytes  17.1 Kbits/sec
```

Iperf
(Windows) en ligne de commande

Ecoute et enregistrement de trafic



WireShark + WinPcap (Windows)

Pour le WiFi ajouter Airpcap

Airpcap permet l'émulation du mode monitor sur l'interface radio des adaptateurs USB (Windows)

Partie 4

Matériel

-

Liens entre portée, débit et puissance

Chipsets et Fabricants

- Quelques fabricants de Chipsets recouvrent la quasi totalité des cartes
  - Prism (Interstil) : Dlink, Linksys, Netgear
  - Texas Instrument : Dlink, US-Robotics
  - Hermes : Onorico, Buffalo
  - Atheros et Broadcom: dernirères versions 54Mbps
- Certains Chipsets ne sont pas utilisables en écoute
- Le label Wi-Fi garantit l'interropérabilité du matériel et des normes vues jusque-là.
  - En cas de mélange des normes, le débit maximal sera le plus faible à savoir celui de la norme 802.11b
  - Quelques normes propriétaires rares (Dlink : 802.11+ ; Cisco : TKIP...)

Points d'accès

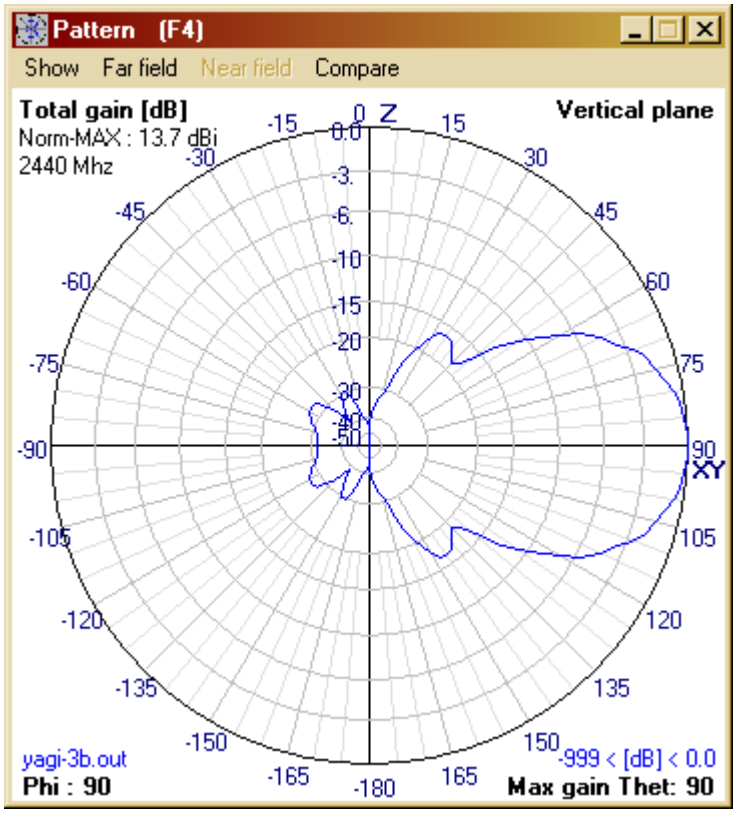
- **Points d’accès (eq. switch)**
  - Sensibilité en réception et puissance de sortie.
  - Topologies supportées (AP, Bridge, AP Client, repéteur…)
  - Services supplémentaires (DHCP, routage, filtrage des clients, 802.1x, 802.1q)
  - Exemple du Cisco et du Dlink

Adaptateurs WiFi

- **Cartes clientes (éq. carte réseau)**
  - Tous types d'adaptation : PCMCIA, PCI, USB, CF
  - Trois types de réception : directe, patch ou avec antenne extérieure
  - Bonne interopérabilité

Antennes

- Le **gain** d'une antenne est exprimé en **dBi**
  - 3 dB <-> multiplication par 2 ; 6 par 4 ; 9 par 8
- On note la répartition spatiale de ce gain sur un diagramme
- Le choix d'une antenne doit se faire sur le compromis : **ouverture angulaire/portée** (et prix)



Antennes

	Gain	Ouverture	Coût	Nom
Directionelle	12 à 19 dBi	45 à 60 °	30 à 60 euros	Yagi – Grids
Sectorielle	9 à 12 dBi	120 °	60 à 100 euros	Patch
Omni-directionelle	7 à 9 dBi	360 °	100 à 150 euros	
Ricorée	8 dBi	50 °	10 euros	Pringles
Mini-omni	2 dBi	360 °		

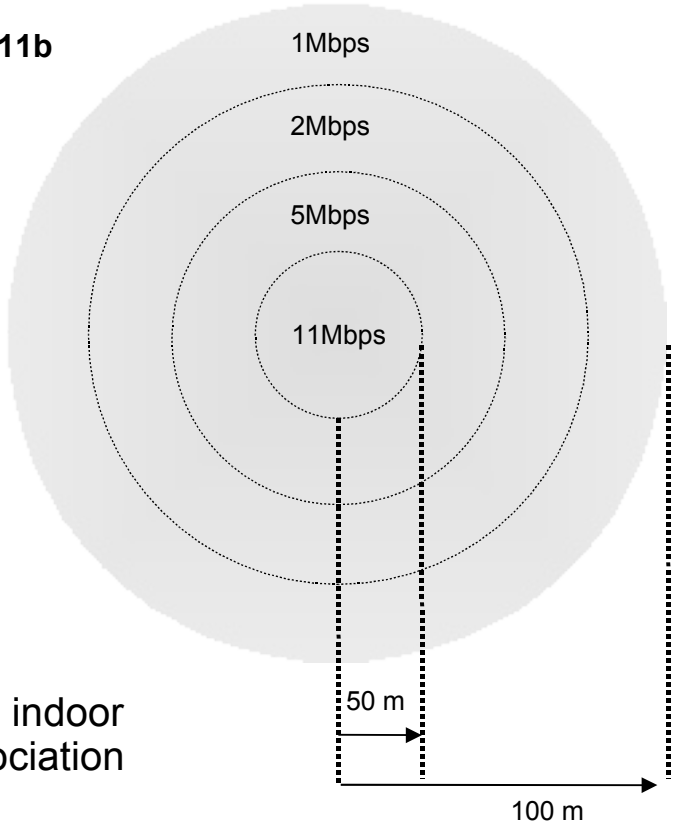
Les connectiques

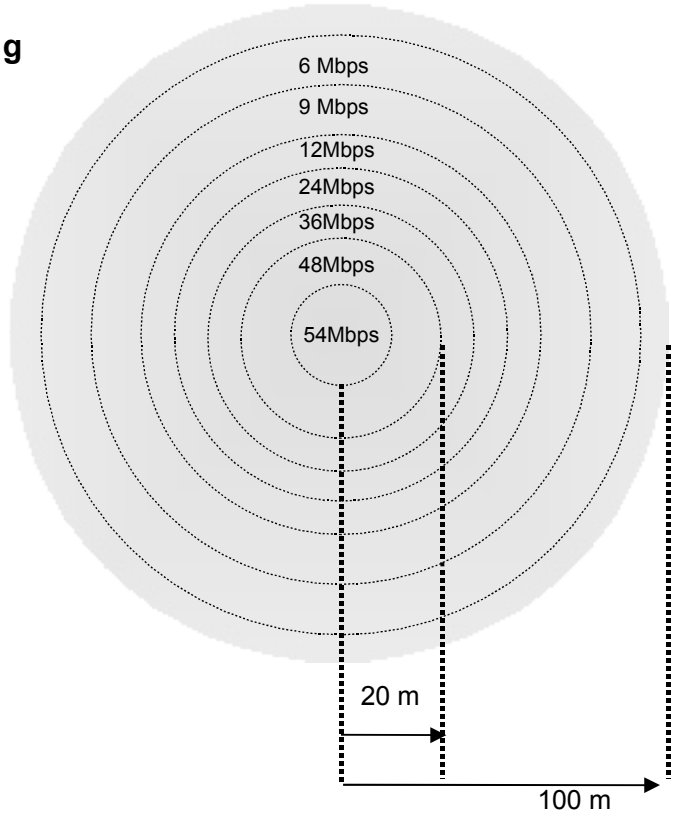
- Type N
  - La connectique d'antenne standard
- Type TNC-RP
  - Utilisée par les constructeurs Cisco et Linksys
- Type SMA
  - Répandue sur les cartes PCI et le matériel Dlink
- Type MMCX
  - Dédiées aux sorties mini-PCMCIA

Débit d'association

- Variable : 54 - 48 - 36 - 24 - 12 - 11 - 5,5 - 2 - 1 Mbit/s
- Adapté automatiquement en fonction
  - de la puissance reçue par l'appareil (distance)
  - du rapport Signal/Bruit (qualité du signal)

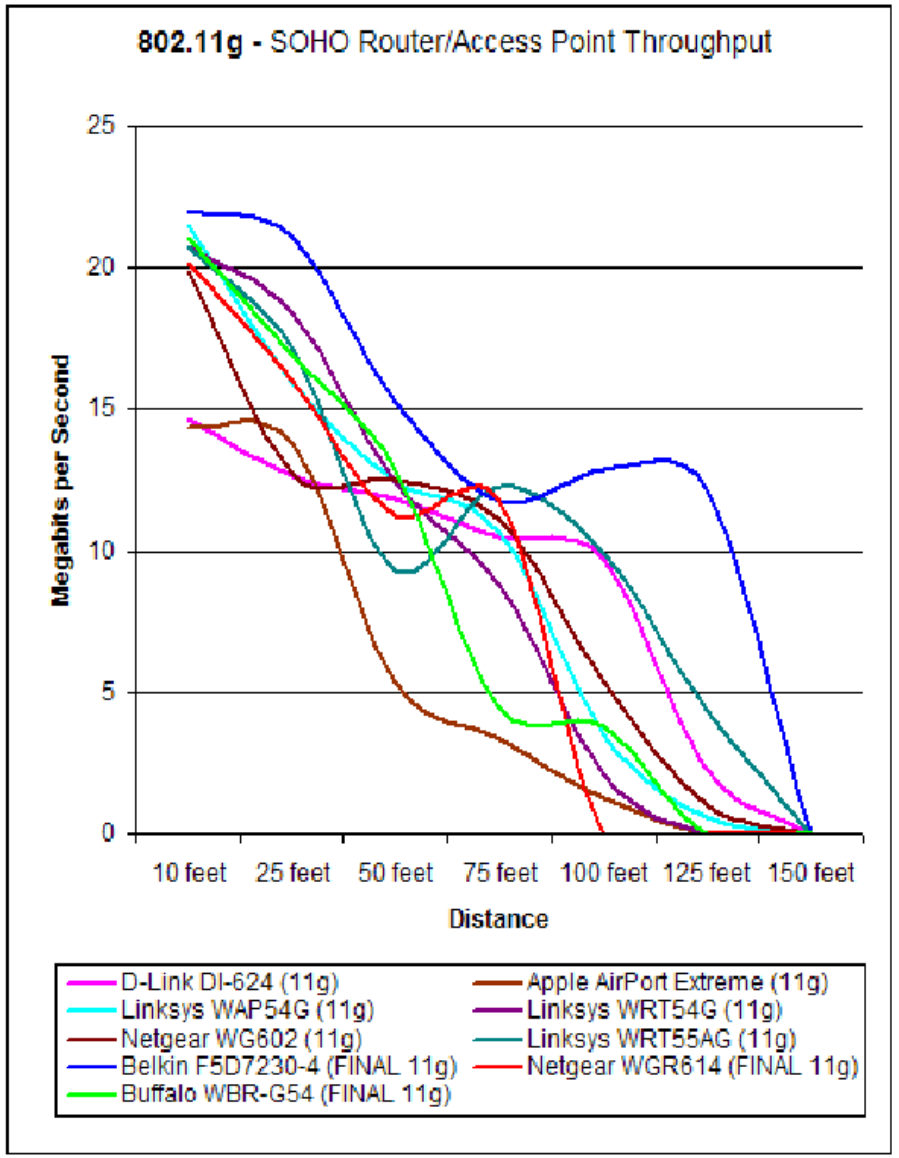
débits indoor d'association

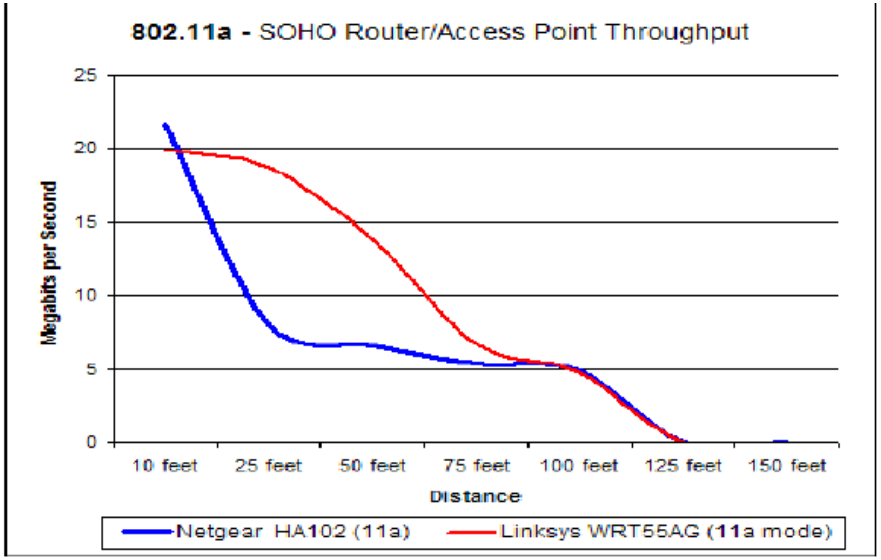


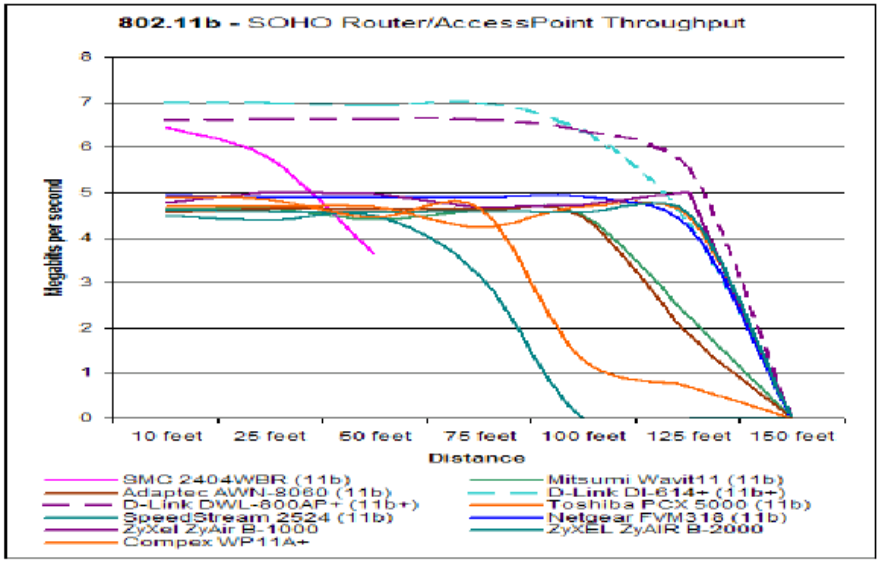


Débits effectifs

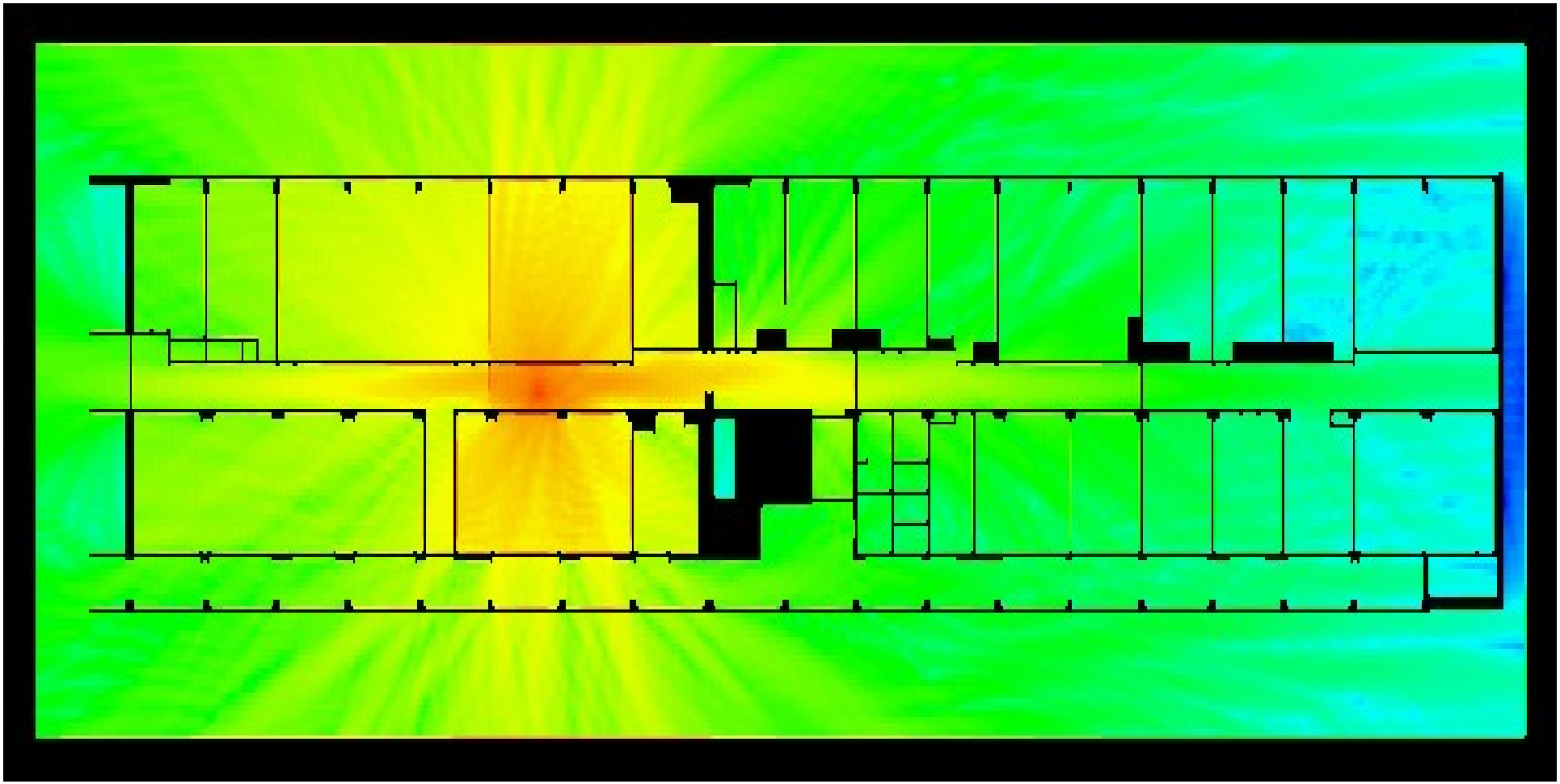
- Débit en ftp binaire ≈ 50 % du débit annoncé.







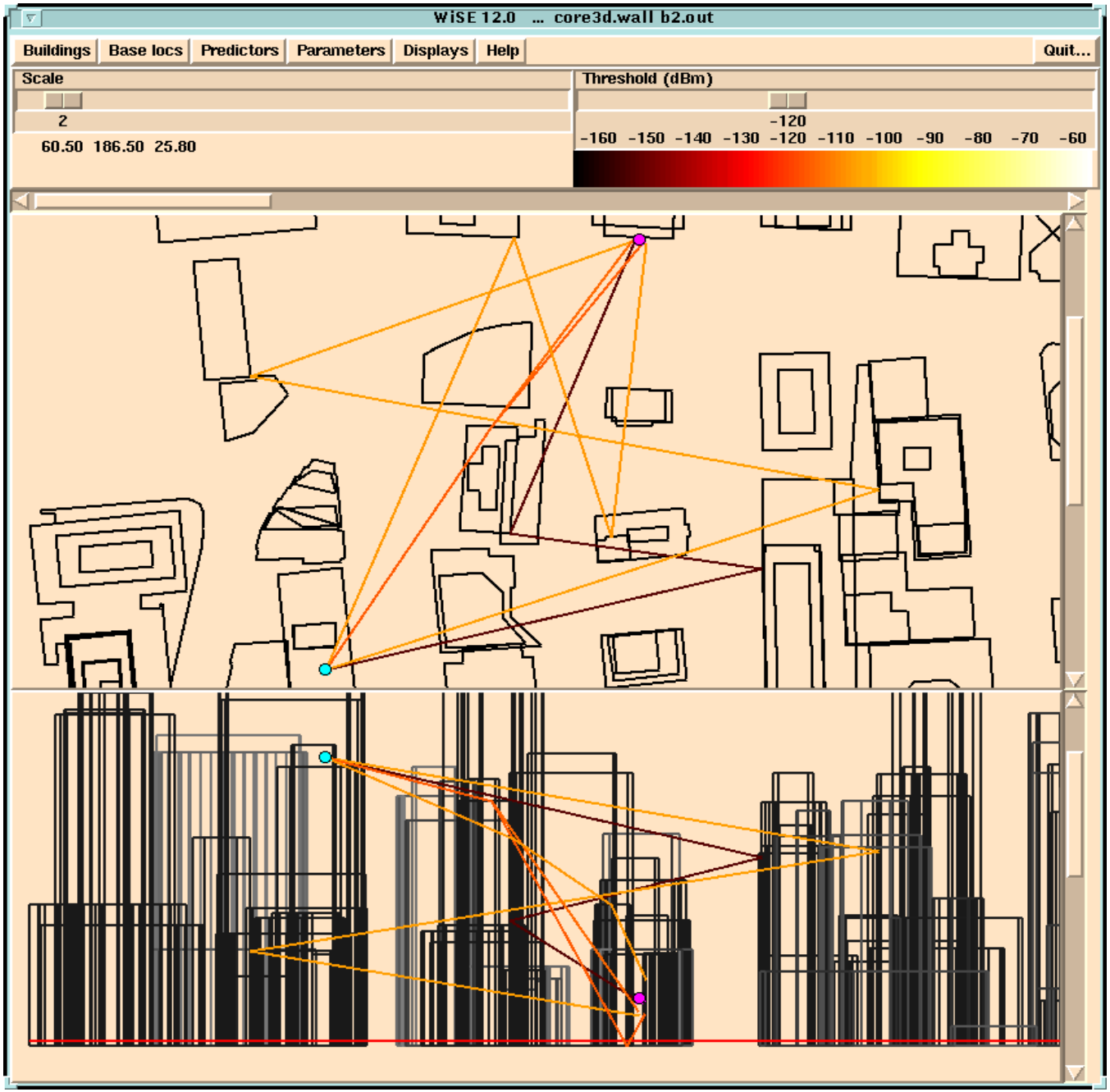
Propagation des ondes en indoor



- réflexions multiples
- diffractions multiples
- géométrie 3D
- influence de la polarisation

Références : John C. Stein

Propagation des ondes en milieu urbain



Références : John C. Stein

Calcul de la PIRE

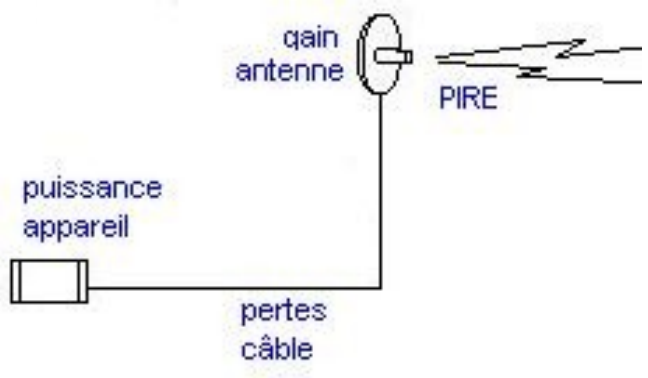
- La PIRE est la puissance effective rayonnée en sortie d'antenne
- Elle est limitée à 100 mW à l'extérieur (et à l'intérieur) en France.
- 100 mW = 20 dBm
- Compter 1 dB par mètre en moyenne pour les pertes

PIRE (dBm) =

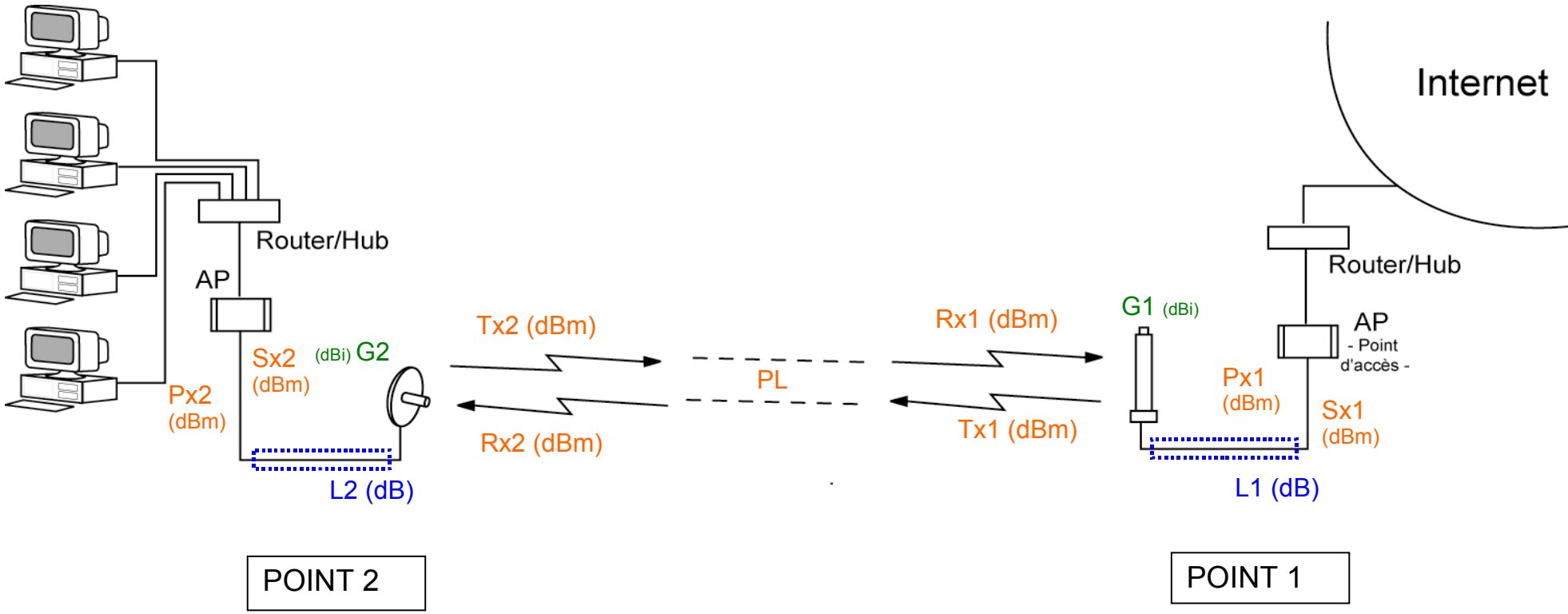
puissance en sortie AP (dBm)

– pertes câbles (dB)

+ gain d'antenne (dBi)



Théorie de portée radio



- Le champ doit être exempt de masque (bâtiment, arbres...) et doit respecter la zone de Fresnel.
- Les résultats sont très dépendants des sensibilité de réception des appareils.
- Avec 10 mW en sortie d'AP, 3m de câble et 2 Yagis à 14 dBi on peut obtenir sur un lien de 2 à 3 km.

Calcul de portée d'un lien

- Outils de calcul
  - http://reseau.erasme.org/article.php3?id_article=10
  - http://www.swisswireless.org/wlan_calc_fr.html
  - http://www.temcom.com/pages/dBCalc_fr.html

- **A retenir** : le meilleur résultat de portée est obtenu avec l'utilisation de matériel aux caractéristiques symétriques de part et d'autre
  - AP (sensibilité de réception et puissance émission)
  - Antennes (Gain)
  - Connectiques et câbles (Pertes en ligne)

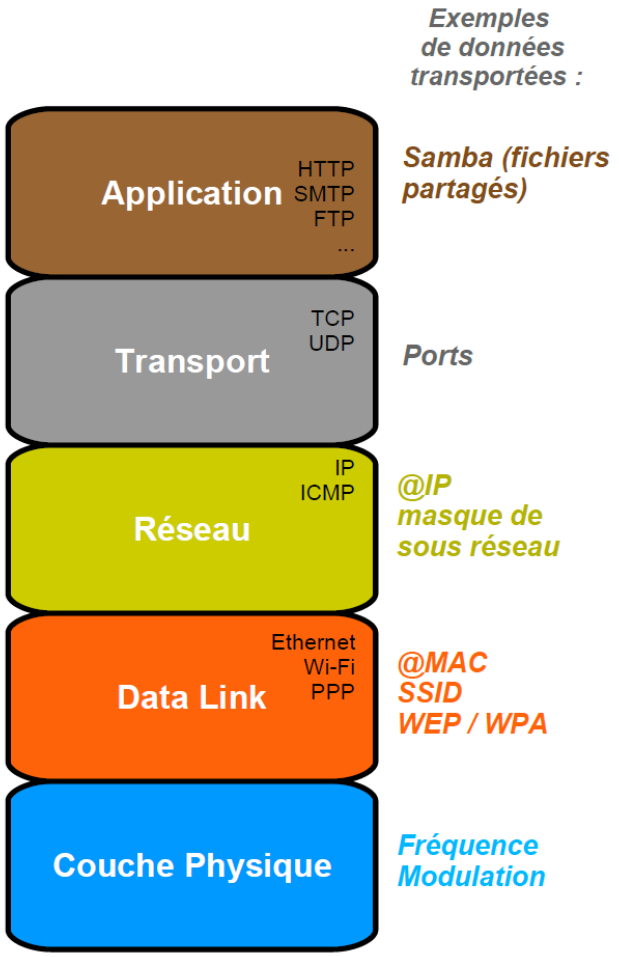
802.11 : Fonctionnement

- La sous-couche MAC
  - Challenges
  - Access Modes
  - Contention-based access
  - Fragmentation

- Les différentes couches physiques
  - Spread-spectrum principle
  - FH PHY
  - DS PHY
  - OFDM PHY
  - MIMO

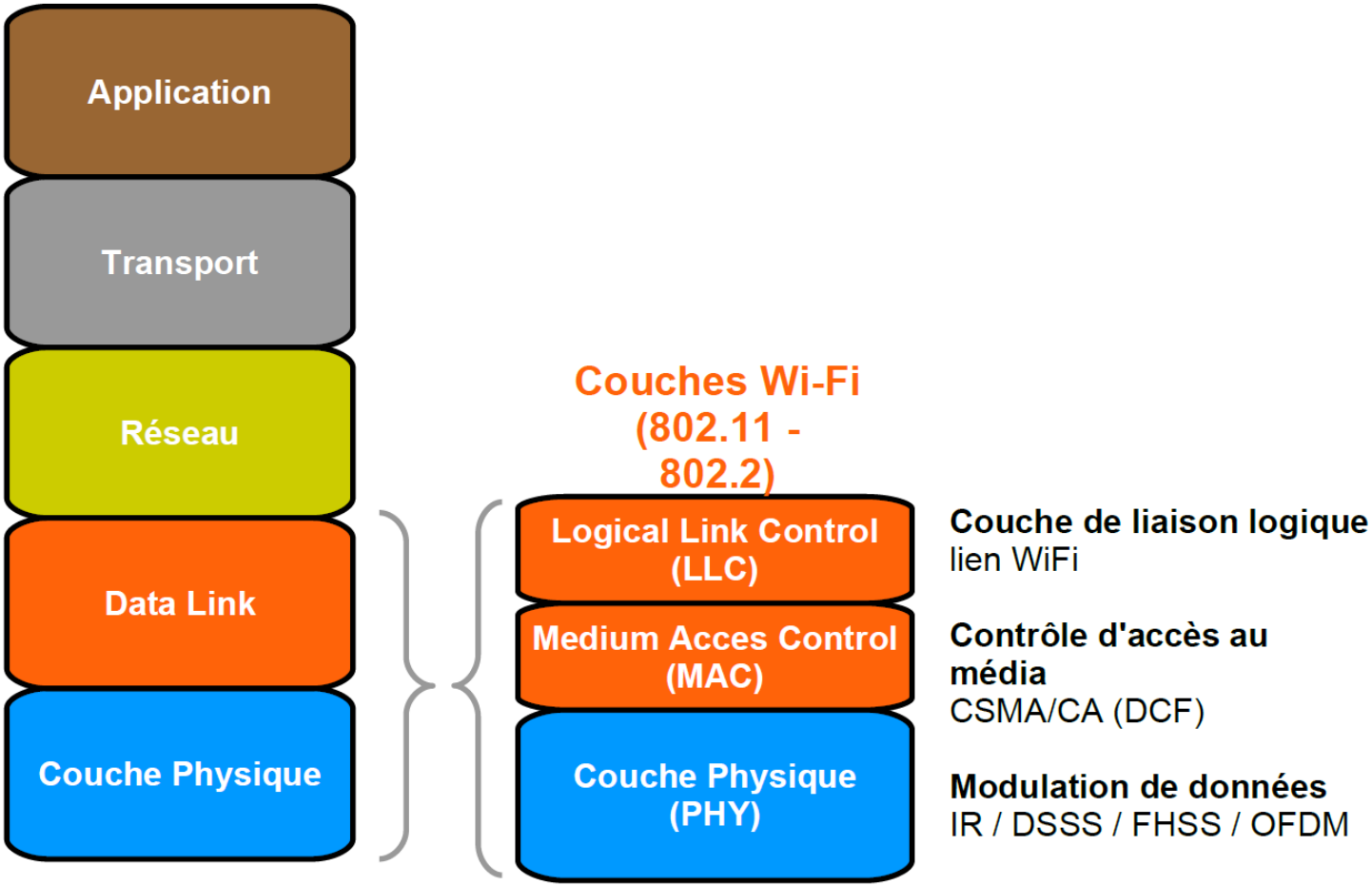
- La sécurité
- Le déploiement
- Les aspects juridiques et sanitaires

Modèle TCP/IP en couches

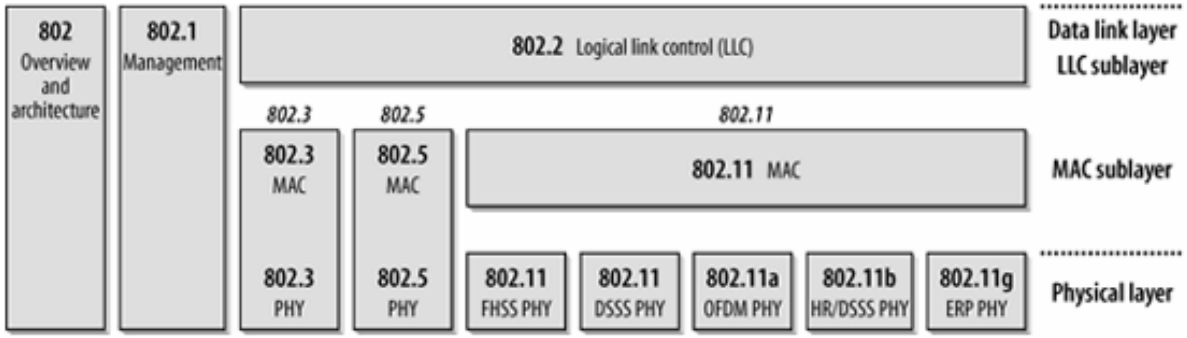


- Les réseaux sont généralement organisés en "piles protocolaires"
- chaque couche de la pile offre un niveau d'abstraction supplémentaire à la couche supérieure
- chaque couche offre un service supplémentaire par rapport à la couche inférieure

Les couches 802.11



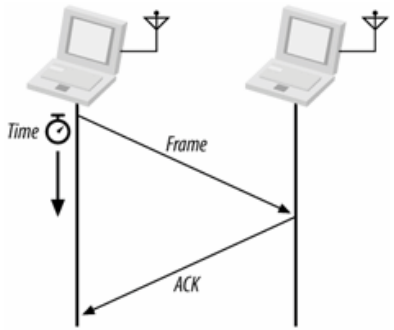
The IEEE 802 family and its relation to the OSI model



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

The 802.11 MAC: challenges

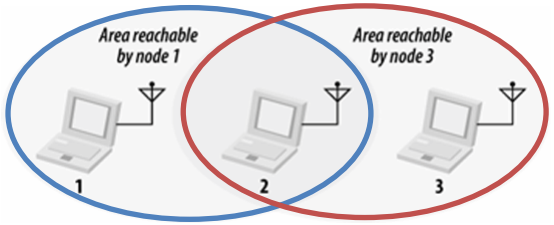
- **RF Link Quality:**
  - On a wired Ethernet, it is reasonable to transmit a frame and assume that the destination receives it correctly.
  - Radio links are different, especially when the frequencies used are unlicensed ISM bands. Even narrowband transmissions are subject to noise and interference, but unlicensed devices must assume that interference will exist and work around it.
  - Unlike many other link layer protocols, 802.11 incorporates positive acknowledgments.
  - Atomic operation: single transactional unit:
  - Atomic operations are "all or nothing."



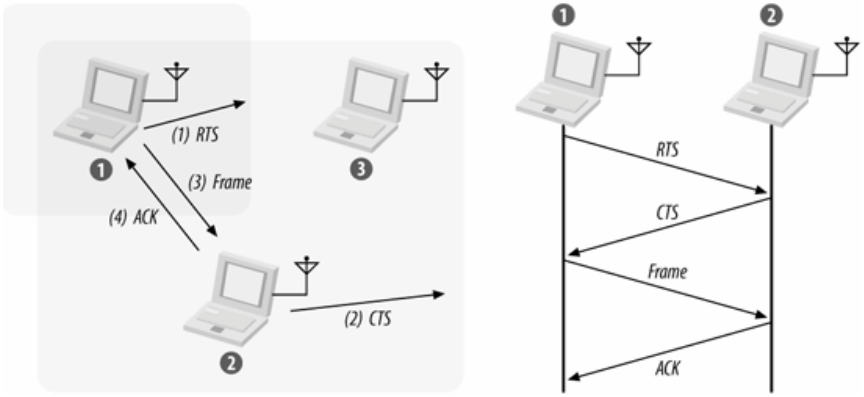
802.11® Wireless Networks The Definitive Guide
By Matthew Gast

The 802.11 MAC: challenges

- **The hidden node problem**



  - For this case: Request to Send (RTS) and Clear to Send (CTS) signals to clear out an area.



  - RTS/CTS transmission procedure consumes a fair amount of capacity, especially because of the additional latency incurred before transmission can start.

    -> Only in high-capacity environments and environments with significant contention on transmission. For lower-capacity environments, it is not necessary.

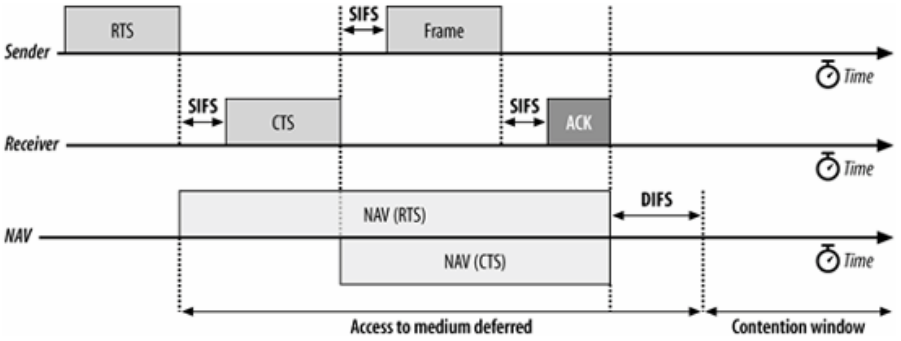
802.11® Wireless Networks The Definitive Guide
By Matthew Gast

MAC Access Modes and Timing

- **Access to the wireless medium is controlled by coordination functions**
  - DCF: *Distributed Coordination Function*
    - basis of the standard CSMA/CA access mechanism
    - first checks to see that the radio link is clear before transmitting.
    - To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the CTS/RTS clearing technique to further reduce the possibility of collisions.
  - PCF: *Point Coordination Function*
    - provides contention-free services.
    - Point coordinators reside in access points, so the PCF is restricted to infrastructure networks.
  - HCF: *Hybrid Coordination Function*
    - service quality for a step above best-effort delivery
    - allows stations to maintain multiple service queues and balance access to the wireless medium in favor of applications that require better service quality
    - 802.11e

MAC Access Modes and Timing

- **Carrier-sensing and NAV**:

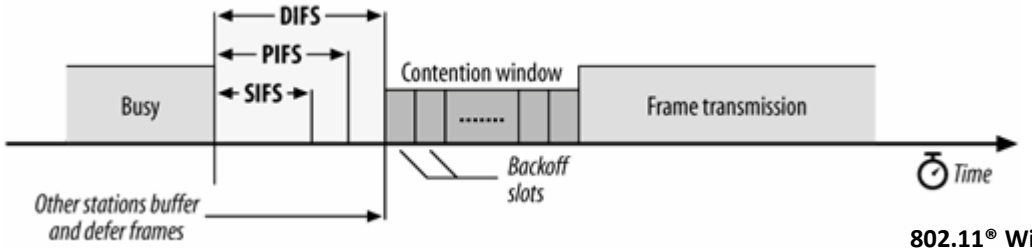


  - Physical carrier-sensing:
    - provided by the physical layer
    - but expensive and not sufficient
  - Virtual carrier-sensing:
    - Network Allocation Vector
    - The NAV is a timer (in duration field) indicating the amount of time the medium will be reserved, in microseconds.
    - Stations set the NAV to the time for which they expect to use the medium, including any frames necessary to complete the current operation. Other stations count down from the NAV to 0.
    - when the NAV is nonzero, the virtual carrier-sensing function indicates that the medium is busy
    - when the NAV reaches 0, the virtual carrier-sensing function indicates that the medium is idle.
    - By using the NAV, stations can ensure that atomic operations are not interrupted.

802.11® Wireless Networks The Definitive Guide
By Matthew Gast

MAC Access Modes and Timing

- **Interframe spacing**:
  - As with traditional Ethernet, the interframe spacing plays a large role in coordinating access to the transmission medium. 802.11 uses four different interframe spaces.
  - Varying interframe spacings create different priority levels for different types of traffic. The logic behind this is simple: high-priority traffic doesn't have to wait as long after the medium has become idle.
    - Short interframe space (SIFS): for the highest-priority transmissions, such as RTS/CTS frames and positive acknowledgments
    - PCF interframe space (PIFS): Stations with data to transmit in the contention-free period can transmit after the PIFS has elapsed and preempt any contention-based traffic.
    - DCF interframe space (DIFS): The DIFS is the minimum medium idle time for contention-based services. Stations may have immediate access to the medium if it has been free for a period longer than the DIFS.
    - Extended interframe space (EIFS): not fixed, used only when there is an error in frame transmission
  - By using the SIFS and the NAV, stations can seize the medium for as long as necessary.



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

Contention-Based Access Using the DCF

- Before attempting to transmit, each station checks whether the medium is idle. If the medium is not idle, stations defer to each other and employ an orderly exponential backoff algorithm to avoid collisions.

- For the 802.11 MAC rules, two **basic rules** apply to all transmissions using the DCF:

  1. medium idle for longer than the DIFS -> transmission can begin immediately

     by the exponential backoff procedure

     a. If the previous frame was received without errors, the medium must be free for at least the DIFS.

     b. If the previous transmission contained errors, the medium must be free for the amount of the EIFS.

  2. medium busy -> the station must wait

Contention-Based Access Using the DCF

- **Additional rules** (for particular environment or depending on the previous transmissions)

1. Error recovery is up to the station sending a frame:

   a. Positive acknowledgments are the only indication of success. Atomic exchanges must complete in their entirety to be successful.

   b. Any failure increments a retry counter, and the transmission is retried. A failure can be due to a failure to gain access to the medium or a lack of an acknowledgment.

2. Multiframe sequences may update the NAV: when a station receives a medium reservation that is longer than the current NAV, it updates the NAV.

3. Frames transmitted after the SIFS and thus receiving maximum priority: ACKs, the CTS in an RTS/CTS exchange sequence, and fragments in fragment sequences.

   a. Once a station has transmitted the first frame in a sequence, it has gained control of the channel. Any additional frames and their ACKs after the SIFS, locking out any other stations.

   b. Additional frames in the sequence update the NAV for the expected additional time the medium will be used.

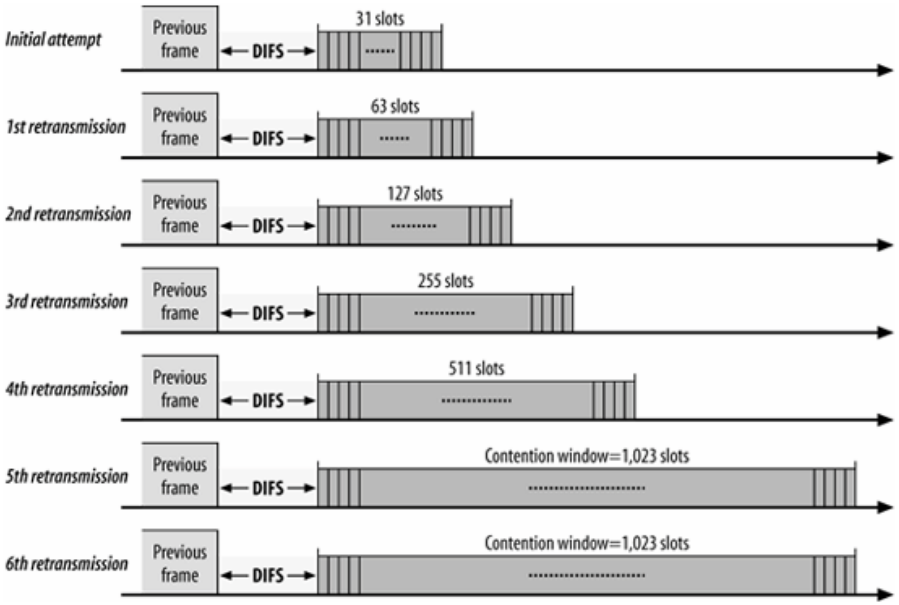
4. Extended frame sequences are required for packets longer than configured thresholds.

   a. Packets larger than the RTS threshold must have RTS/CTS exchange.

   b. Packets larger than the fragmentation threshold must be fragmented

Contention-Based Access Using the DCF

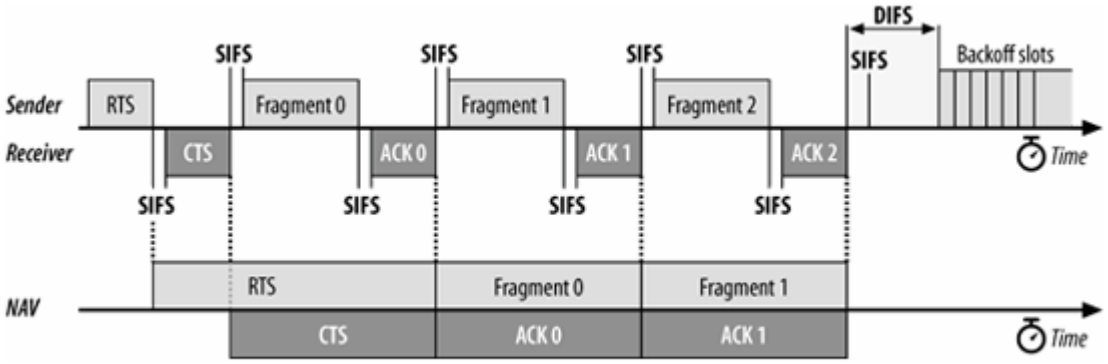
- **Backoff with the DCF**
  - After frame transmission has completed and the DIFS has elapsed, stations may attempt to transmit congestion-based data.
  - A period called the **contention window** or **backoff window** follows the DIFS. This window is divided into slots. Slot length is medium-dependent; higher-speed physical layers use shorter slot times. Stations pick a random slot and wait for that slot before attempting to access the medium
  - The station that picks the first slot wins access to the medium
  - As in Ethernet, the backoff time is selected from a larger range each time a transmission fails.



Fragmentation and reassembly

- Wireless LAN stations may attempt to fragment transmissions so that interference affects only small fragments, not large frames. By immediately reducing the amount of data that can be corrupted by interference, fragmentation may result in a higher effective throughput.

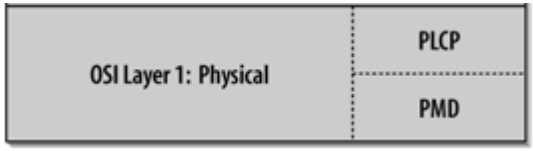
- Fragmentation takes place when the length of a higher-level packet exceeds the fragmentation threshold configured by the network administrator.



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

Physical-Layer Architecture

- Physical layer is divided into two sublayers:
  - Physical Layer Convergence Procedure (PLCP) sublayer
    - glue between the frames of the MAC and the radio transmissions in the air
    - adds its own header. Frames include a preamble to help synchronize incoming transmissions, and the preamble may depend on the modulation method
    - incorporates a clear channel assessment (CCA) function to signal to the MAC when the medium is idle
  - Physical Medium Dependent (PMD) sublayer
    - transmits any bits it receives from the PLCP into the air using the antenna



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

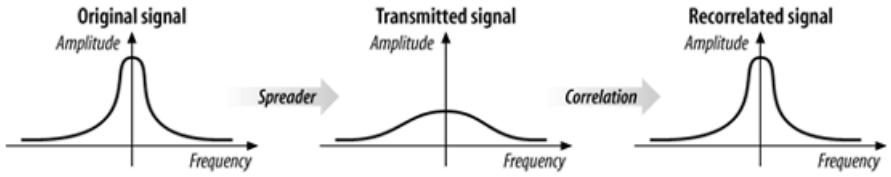
The radio link

- 3 physical layers standardized - initial revision of 802.11, 1997:
  - Frequency-hopping (FH) spread-spectrum radio PHY
  - Direct-sequence (DS) spread-spectrum radio PHY
  - Infrared light (IR) PHY

- Later, 3 further physical layers based on radio technology were developed:
  - 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) PHY
  - 802.11b: High-Rate Direct Sequence (HR/DS or HR/DSSS) PHY
  - 802.11g: Extended Rate PHY (ERP)
  - 802.11n: colloquially called the MIMO PHY or the High-Throughput PHY

Spread-spectrum techniques

- Traditional radio communications focus on cramming as much signal as possible into as narrow a band as possible.
- Spread spectrum works by using mathematical functions to diffuse signal power over a large range of frequencies.
- When the receiver performs the inverse operation, the smeared-out signal is reconstituted as a narrow-band signal, and, more importantly, any narrow-band noise is smeared out so the signal shines through clearly.
- Use of spread-spectrum technologies is a requirement for unlicensed devices.
- To minimize interference between unlicenced devices, the FCC imposes limitations on the power of spread-spectrum transmissions: 4W of ERP



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

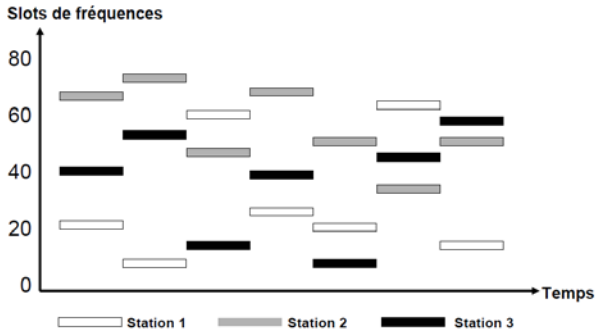
Types of spread spectrum

- The radio-based physical layers in 802.11 use three different spread-spectrum techniques:
  - Frequency hopping (FH or FHSS):
    - systems jump from one frequency to another in a random pattern, transmitting a short burst at each subchannel.
  - Direct sequence (DS or DSSS)
    - systems spread the power out over a wider frequency band using mathematical coding functions
    - 802.11b et 802.11g
  - Orthogonal Frequency Division Multiplexing (OFDM)
    - OFDM divides an available channel into several subchannels and encodes a portion of the signal across each subchannel in parallel.
    - technique is similar to the Discrete Multi-Tone (DMT) technique used by some DSL modems
    - 802.11a et 802.11g

The Frequency-Hopping (FH) PHY

- rapidly changing the transmission frequency in a predetermined, pseudorandom pattern
- Timing the hops accurately is the key to success; both the transmitter and receiver must be synchronized so the receiver is always listening on the transmitter's frequency.

- Orthogonal hopping sequences
  3 stations over 7 time slots: simultaneous emission but not on the same channel

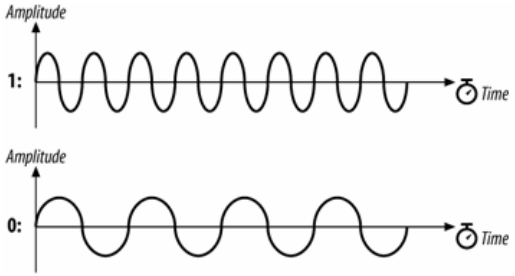


- 79 channels of 1MHz between 2.402 and 2.479 Ghz
- 802.11 divides hopping sequences into nonoverlapping sets: 26 orthogonal sequences per set

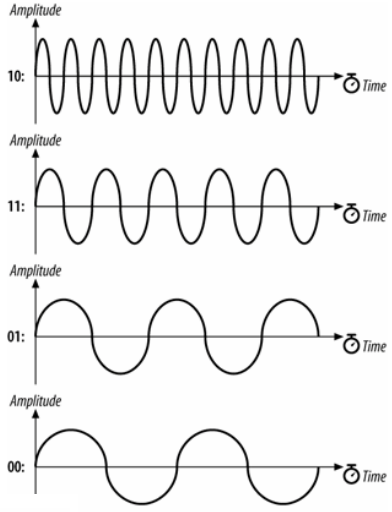
The FH PHY: GFSK modulation

- The FH PHY uses Gaussian frequency shift keying (GFSK).
- Frequency shift keying encodes data as a series of frequency changes in a carrier.
  -> resilient to noise affecting signal amplitude `M'=4D=01001101

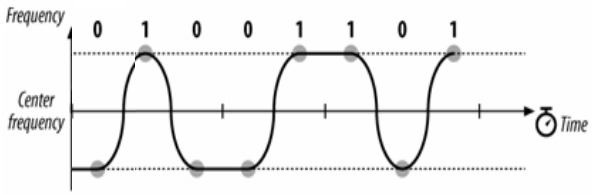
2GFSK



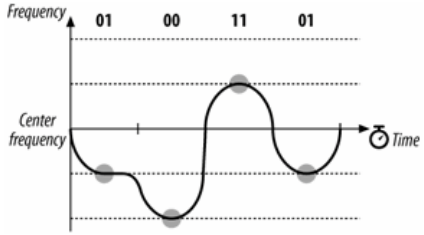
4GFSK



Modulation of `M'=4D=01001101



max 1 Mbps

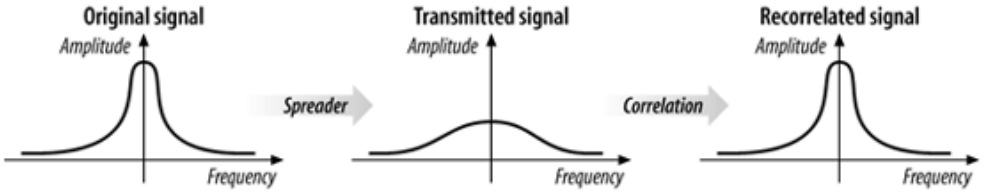


Max 2 Mbps

802.11® Wireless Networks The Definitive Guide
By Matthew Gast

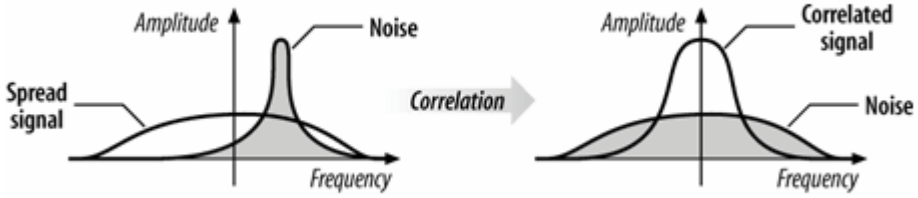
The Direct Sequence PHYs: DSSS and HR/DSSS (802.11b)

- Another SS technique
- Principle: smear the RF energy over a wide band in a carefully controlled way



- For a narrowband receiver, the transmitted signal looks like low-level noise

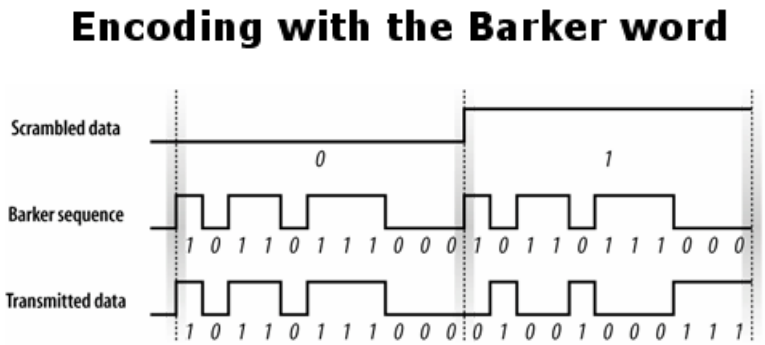
- Correlation gives direct-sequence transmissions a great deal of protection against interference. Noise tends to take the form of relatively narrow pulses that, by definition, do not produce coherent effects across the entire frequency band. Therefore, the correlation function spreads out noise across the band, and the correlated signal shines through:



802.11® Wireless Networks The Definitive Guide
By Matthew Gast

Encoding in 802.11 Direct Sequence Networks

- Direct-sequence modulation works by applying a chipping sequence to the data stream. A chip is a binary digit used by the spreading process.



- Chipping streams, which are also called pseudorandom noise codes (PN codes), must run at a much higher rate than the underlying data -> power drain in DS PHYs
- Higher spreading ratios improve the ability to recover the transmitted signal but require a higher chipping rate and a larger frequency band.

  -> in designing direct-sequence systems for the real world, the spreading ratio should be as low as possible to meet design requirements and to avoid wasting bandwidth
- Direct-sequence modulation trades bandwidth for throughput.

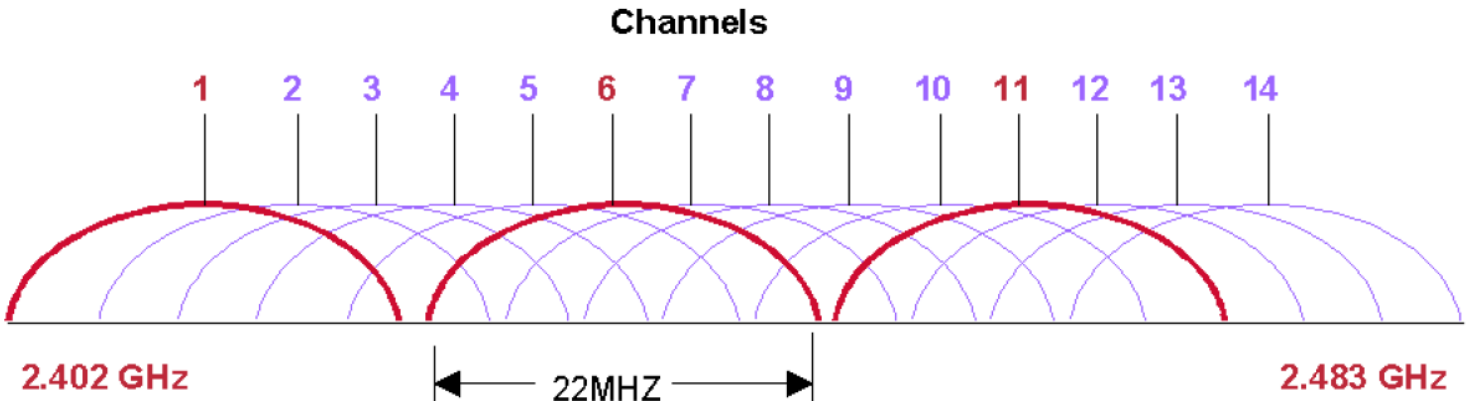
802.11® Wireless Networks The Definitive Guide
By Matthew Gast

Encoding in 802.11 Direct Sequence Networks

- 14 channels every 20MHz
- Center frequency every 5MHz

Regulatory domain	Allowed channels
U.S. (FCC)/Canada (IC)	1 to 11 (2.412-2.462 GHz)
Europe, excluding Spain (ETSI)	1 to 13 (2.412-2.472 GHz)
Spain	10 to 11 (2.457-2.462 GHz)
Japan (MIC)	1 to 13 (2.412-2.462 GHz) and 14 (2.484 GHz)

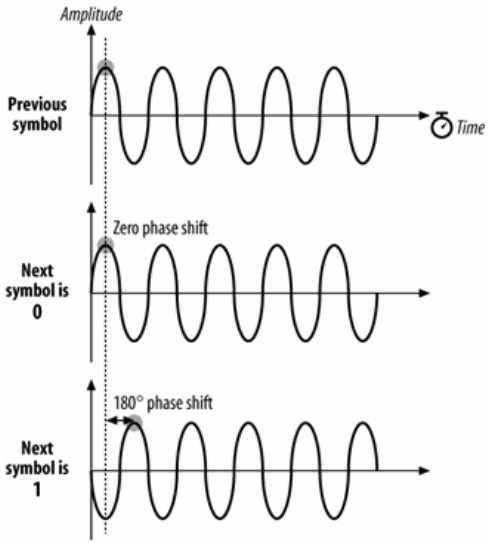
- Total bandwidth of 80 MHz
- Overlapping channels unusable simultaneously



DS PHY modulation: DPSK

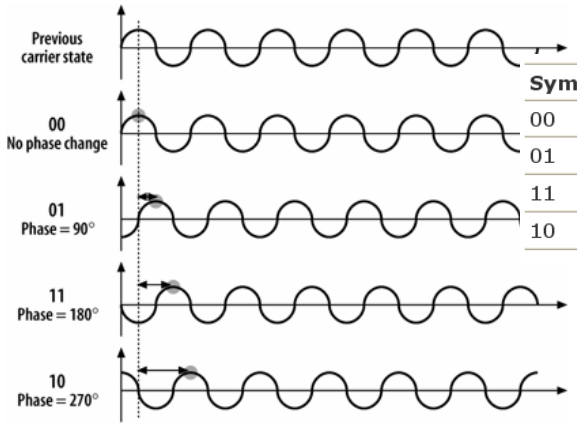
- Differential phase shift keying

DBPSK



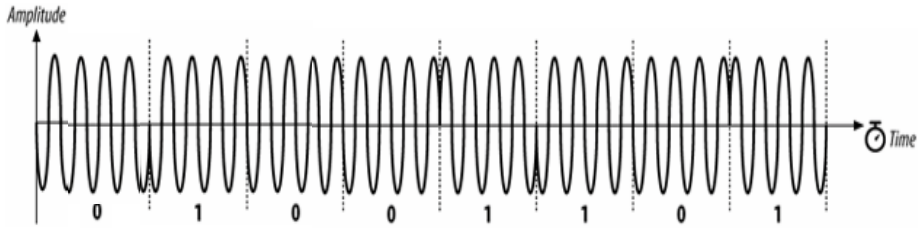
Symbol	Phase shift
0	0
1	180° (π radians)

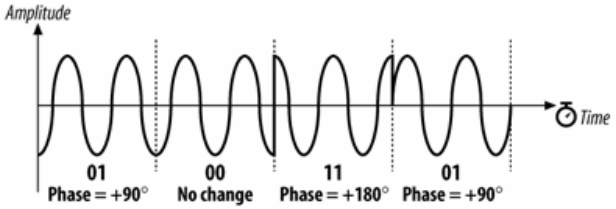
DQPSK



Symbol	Phase shift
00	0
01	90° (π/2 radians)
11	180° (π radians)
10	270° (3π/2 or -π/2 radians)

Modulation of `M'=4D=01001101





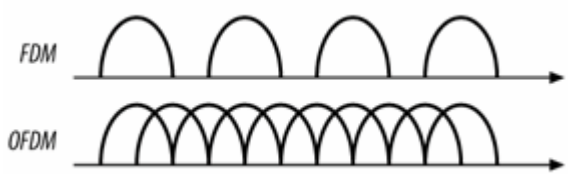
- not resilient to multipath interference -> CCK instead of Barker

OFDM PHY

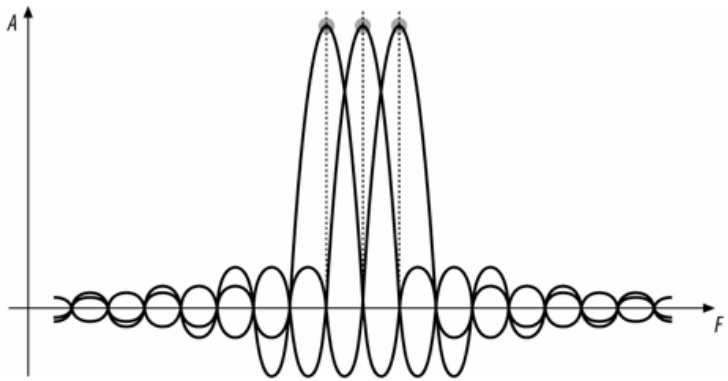
- Principle: chopping a large frequency channel into a number of subchannels.
  -> The subchannels are then used in parallel for higher throughput
- Traditional FDM was widely used by first-generation mobile telephones as a method for radio channel allocation (each user was given an exclusive channel)
  -> guard bands needed
- Pb with traditional FDM: guard bands waste bandwidth and thus reduce capacity

- To avoid wasting transmission capacity with unused guard bands, OFDM selects channels that overlap but do not interfere with each other

FDM versus OFDM



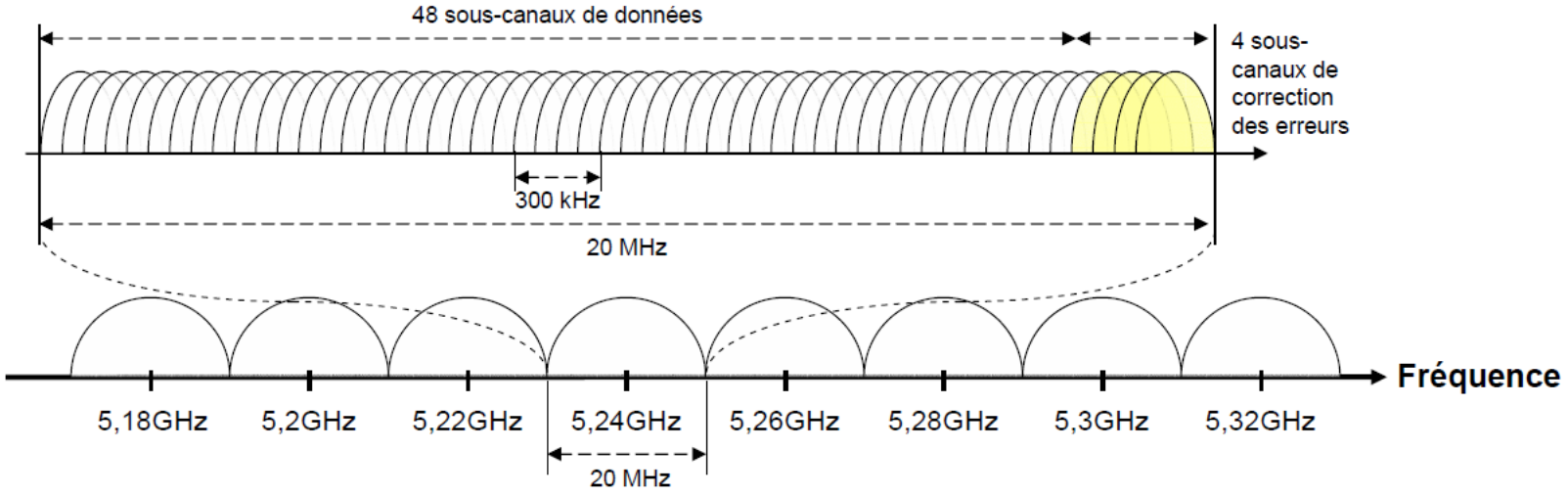
Orthogonality in the frequency domain



Resilient to ISI → up to 54 Mbps

OFDM PHY in 802.11a

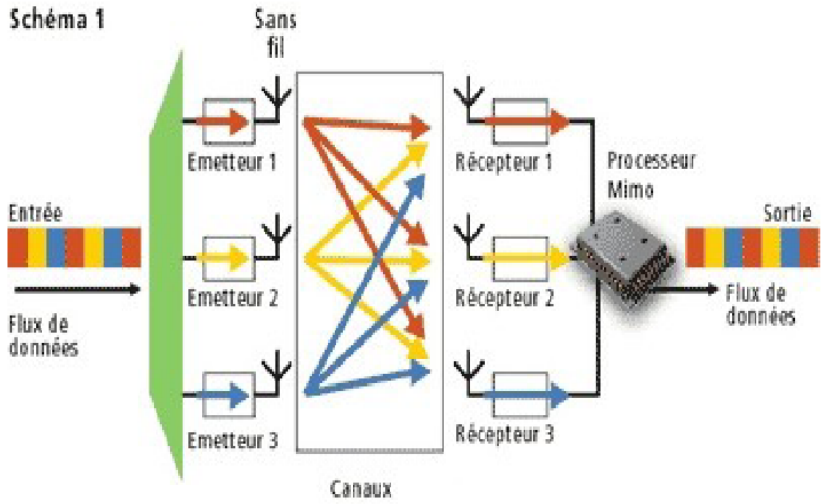
- Each channel has 52 subchannels of 300KHz each
- All subchannels are used in parallel for transmission
- Rate from 6 Mbps to 54 Mbps:
  - BPSK modulation: 0.125 Mbps per subchannel: total of 6 Mbps
  - QAM64 modulation: 1.125 Mbps per subchannel: total of 54 Mbps

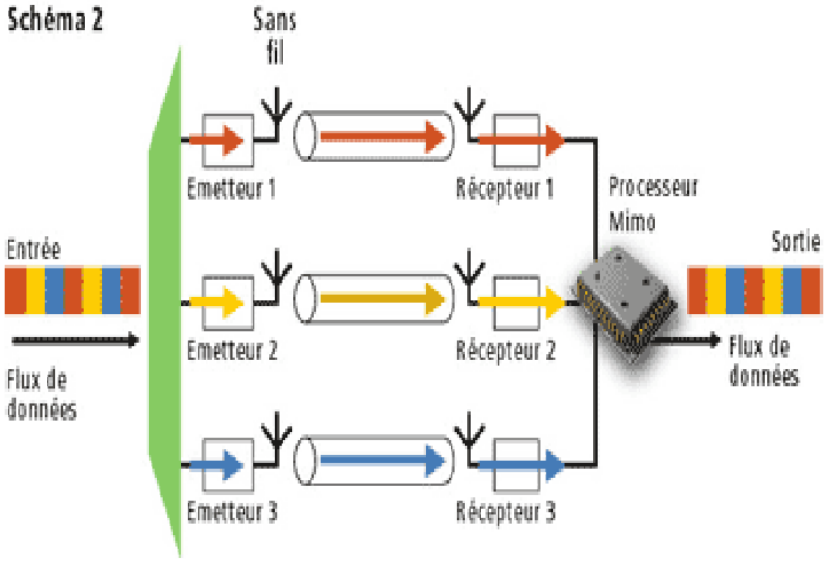


802.11g: The Extended-Rate PHY

- 802.11g offers a bit rate comparable to 802.11a while still operating in the microwave band -> backwards compatibility with 802.11b
- 802.11g is really several physical layer specifications in one
- Any device that implements 802.11g is required to support a few mandatory modes:
  - For backwards compatibility, 802.11g devices must support DSSS modulation (802.11) at 1 and 2 Mbps, and CCK modulation (802.11b) at 5.5 and 11 Mbps
  - Basic OFDM support is required, and all 802.11g stations are further required to support OFDM modulation at 6, 12, and 24 Mbps.

802.11n: The MIMO PHY





Émission

- les signaux sont émis par trois antennes distinctes
- la propagation du signal dans l'air les multiplexe vers chacun des récepteurs

Réception

- l'algorithme de traitement de chaque récepteur isole le signal d'un des émetteurs en utilisant les réflexions
- le protocole dispose donc de trois canaux virtuels
- le débit est multiplié par trois

802.11n: The MIMO PHY

- IEEE 802.11n (Oct 2009) is an amendment to IEEE 802.11-2007 (WiFi Alliance) which builds on previous 802.11 standards by adding:
  - multiple-input multiple-output (MIMO)
  - 40 MHz channels
  - frame aggregation to the MAC layer

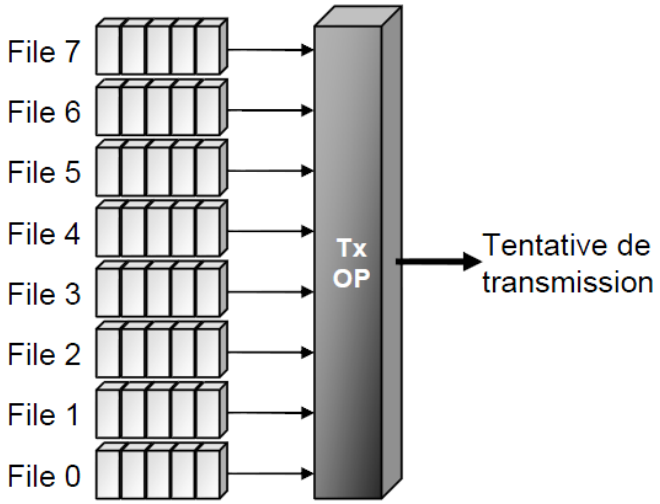
MCS Index	Spatial Streams	Modulation Type	Coding Rate	Data Rate Mb/s			
				20 MHz channel		40 MHz channel	
				800ns GI	400ns GI	800ns GI	400ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
...	3	...	...	...	...	...	...
23	3	64-QAM	5/6	195.00	216.60	405.00	450.00
...	4	...	...	...	...	...	...
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

Economie d'énergie

- Stations mobiles : optimiser l'utilisation de l'énergie disponible :
  - ***continuous aware mode*** : mode par défaut, pas d'économie d'énergie
  - ***power save polling mode*** : mode économie d'énergie
    - le point d'accès tient un enregistrement de toutes les stations en mode économie d'énergie
    - il stocke toutes les données qui leur sont adressées
    - régulièrement, les stations s'éveillent pour recevoir un trame balise indiquant si oui ou non des données leur sont adressées
    - si oui, les stations récupèrent leurs données puis retournent en mode veille jusqu'à la prochaine trame balise

Qualité de service

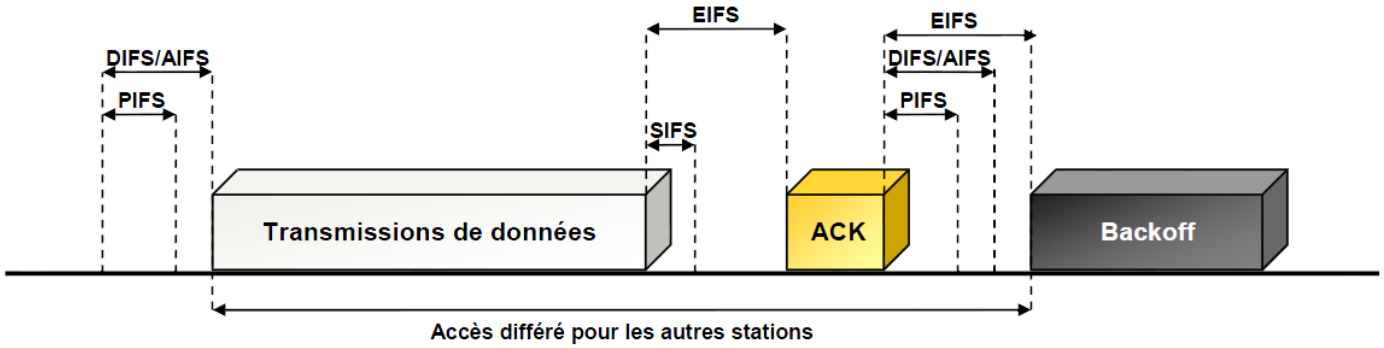
- Gestion des priorités : accès EDCF (*Extended DCF*)
  - méthode PCF jamais utilisée car non implantée par les fabricants
  - EDCF : évolution du DCF, introduite dans IEEE 802.11e
  - accès au support selon le niveau de priorité de la trame
  - 8 niveaux de priorité : 8 files d'attente de transmission
  - mécanisme TxOP : *Transmission Opportunities*



Qualité de service

AIFS : *Arbitration IFS*

- utilisé de la même manière que le DIFS
- valeur dynamique : varie en fonction du niveau de priorité requis
- valeur supérieure ou égale au DIFS
- diminue les risques de collision



L'algorithme de back-off

- sa valeur est dynamique également
- variation fonction de la taille de la fenêtre de contention : si la taille est petite, la station attend moins longtemps

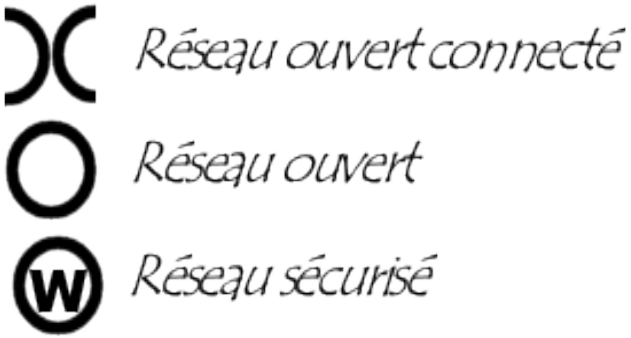
Partie 5

Sécurité

Les risques

Un manque de sécurité intrinsèque

- Propagation des ondes vaste et peu maîtrisée
  - Réseau sans fil équivalent à des câbles RJ45 qui pendent aux fenêtres ;)
- Problèmes d'usage
  - AP souvent vendus et installés sans sécurité par défault
  - AP temporaires laissés en marche à l'insu des resp. IF
- Le War-Driving
  - Un repérage des réseaux urbains accessibles :



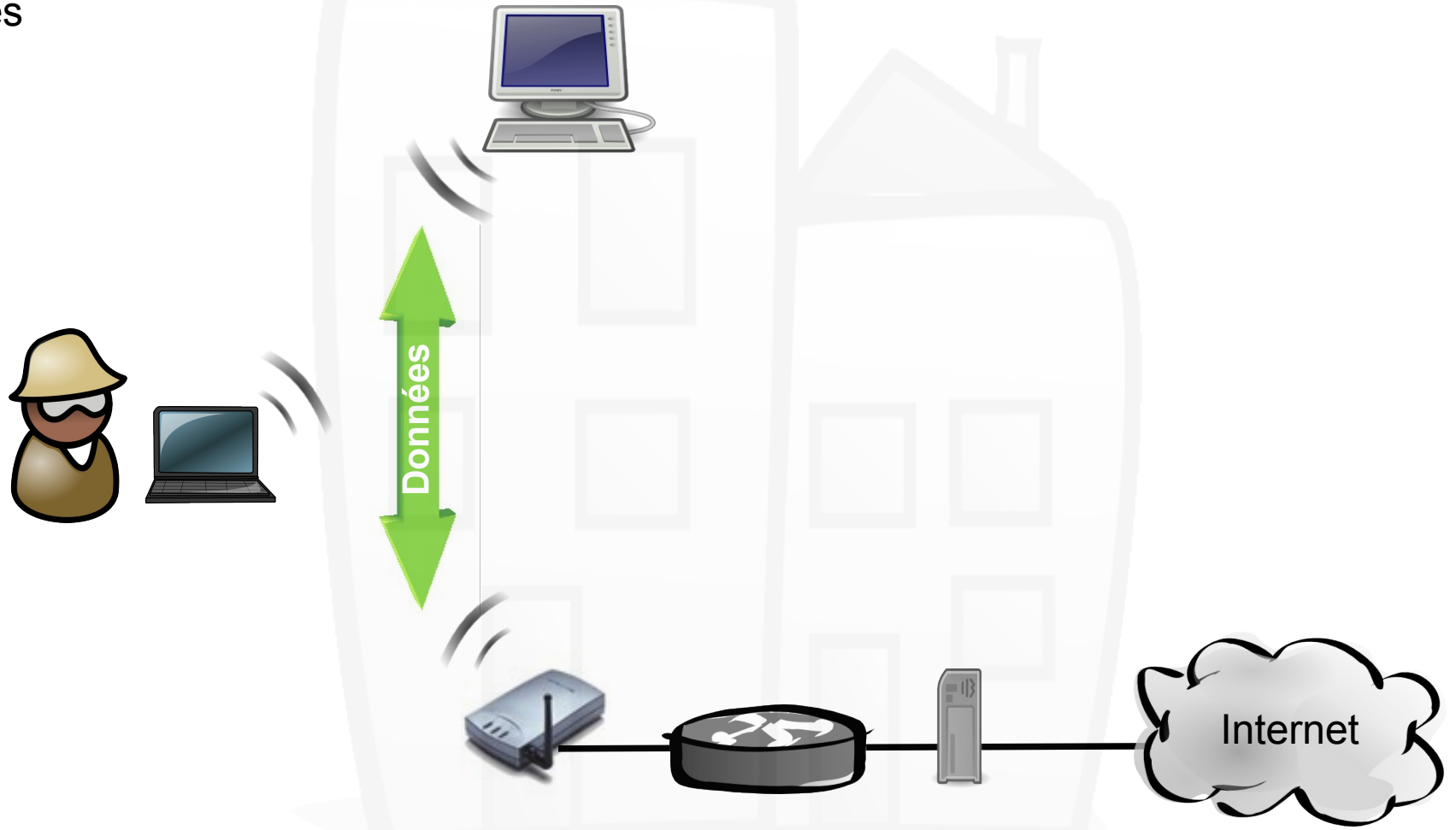
  - Voir : http://www.nantes-wireless.org/pages/wiki/index.php?pagename=WarDriving

Attaques possibles

- L'écoute des données
- L'intrusion et le détournement de connexion
- L'occupation de la Bande Passante
- Le brouillage des transmissions
- Le dénis de service

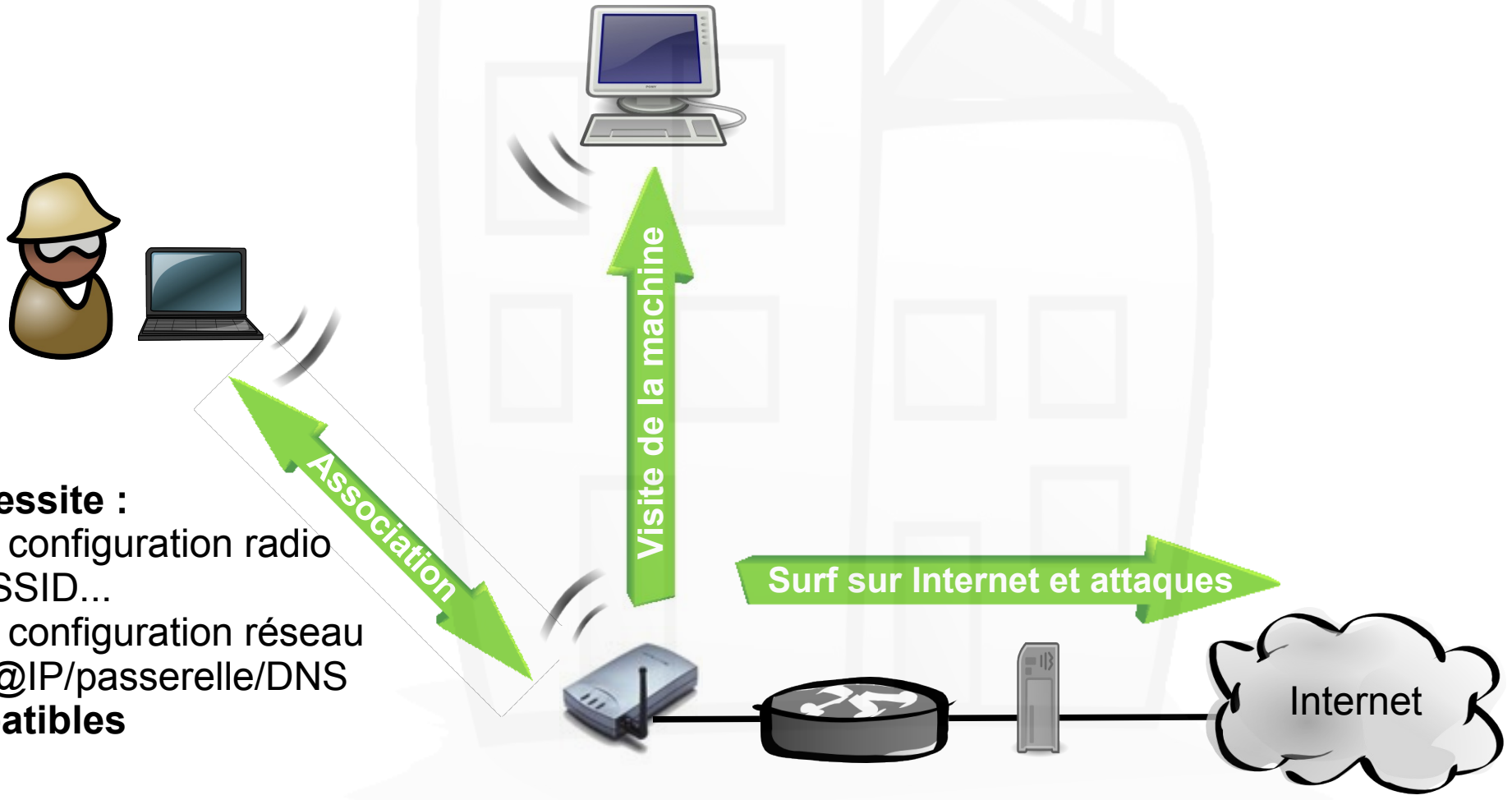
L'écoute des données

• **Solution efficace :**
le chiffrement
(ou cryptage)
des données



L'intrusion et le détournement de connexion

- **Solution efficace :**
  -restreindre l'accès radio
  -restreindre l'accès réseau
  -authentifier la personne



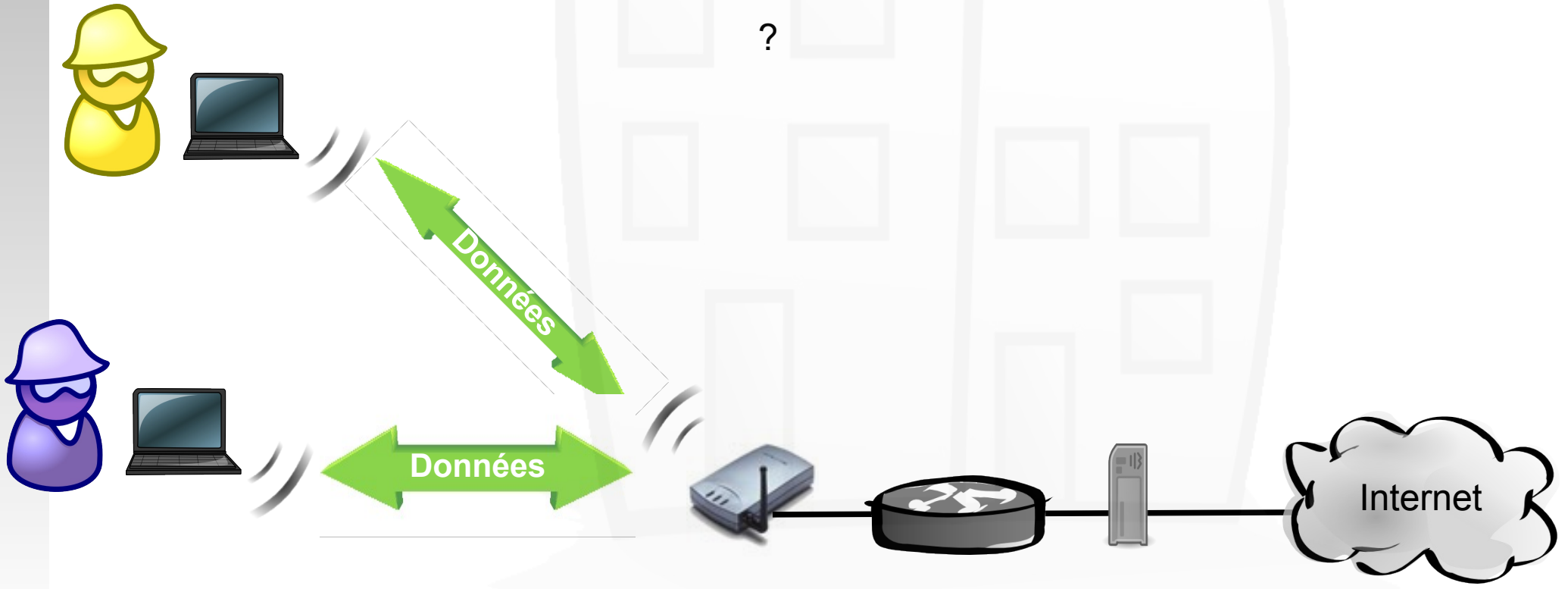
- **Nécessite :**
  -une configuration radio
    -SSID...
  -une configuration réseau
    -@IP/passerelle/DNS

compatibles

L'occupation de la bande passante

• Echange de fichiers lourds bloquant la bande passante de l'utilisateur principal. (importante de l'upload)

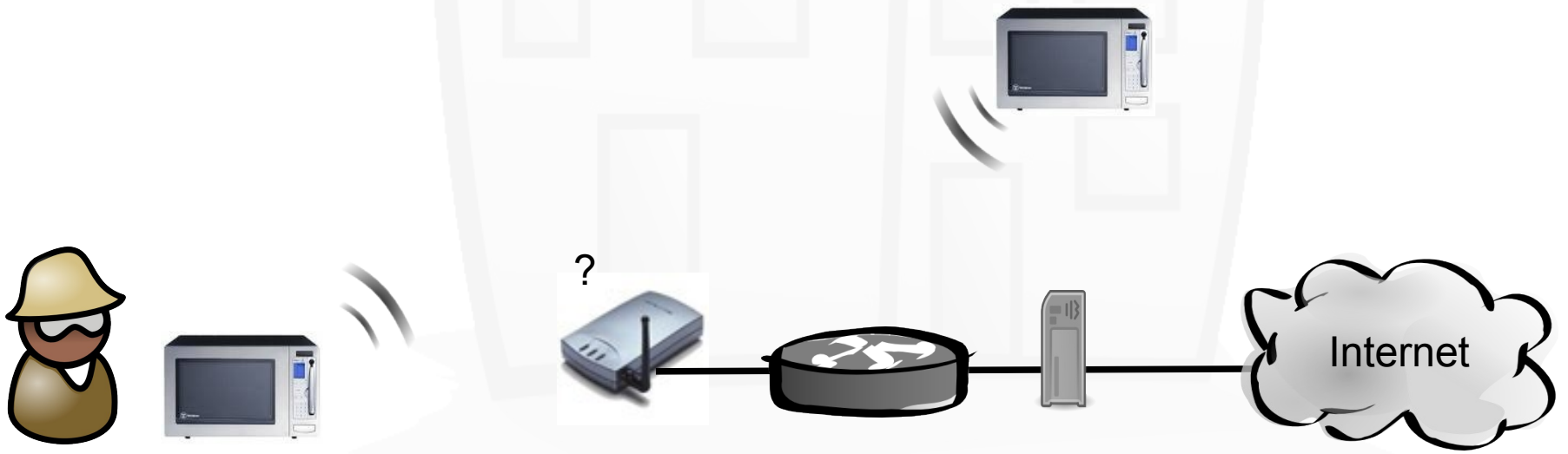
• **Prérequis et solutions :** identiques.



Le brouillage de transmission

• **Provenance :**
téléphones DETC,
fours à micro-ondes

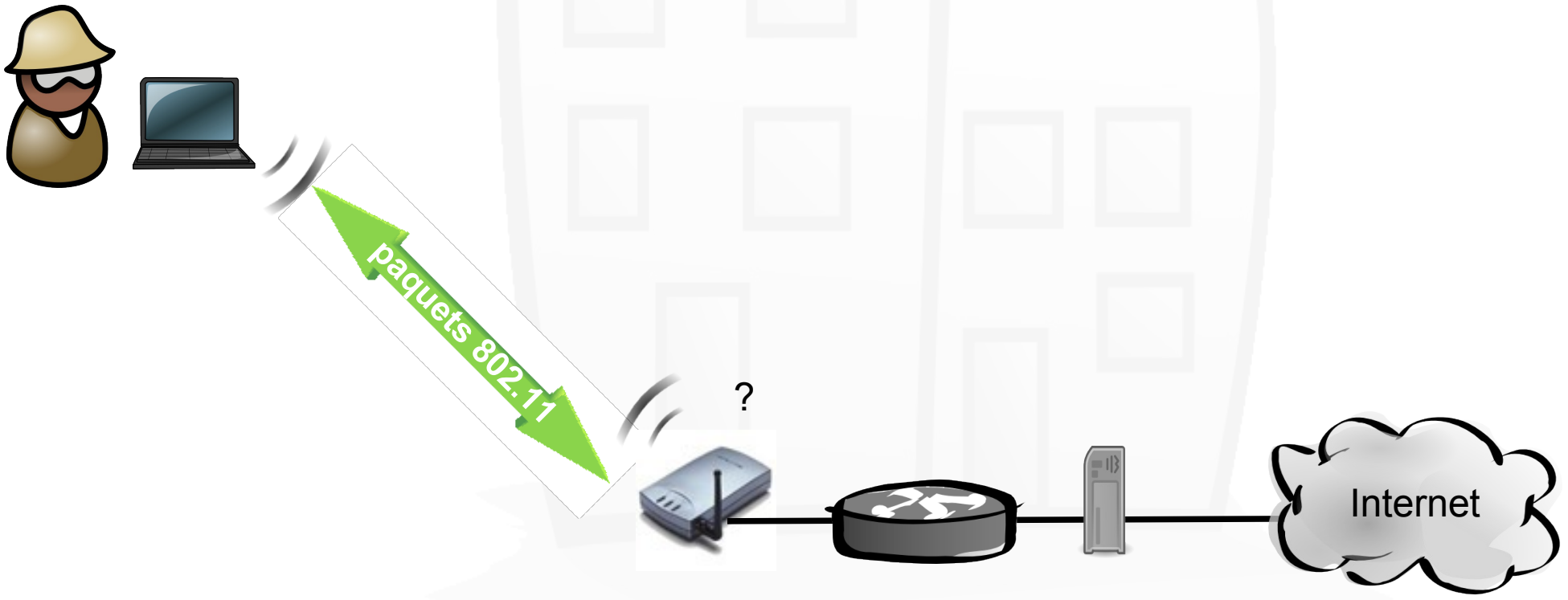
• **Solution efficace :**
couper la source
ou s'éloigner



Le dénis de service

• Utilise la connaissance du protocole CSMA/CA pour occuper le PA ou lui envoyer des paquets chiffrés pour la mettre HS

• **Solution efficace :**
-WPA

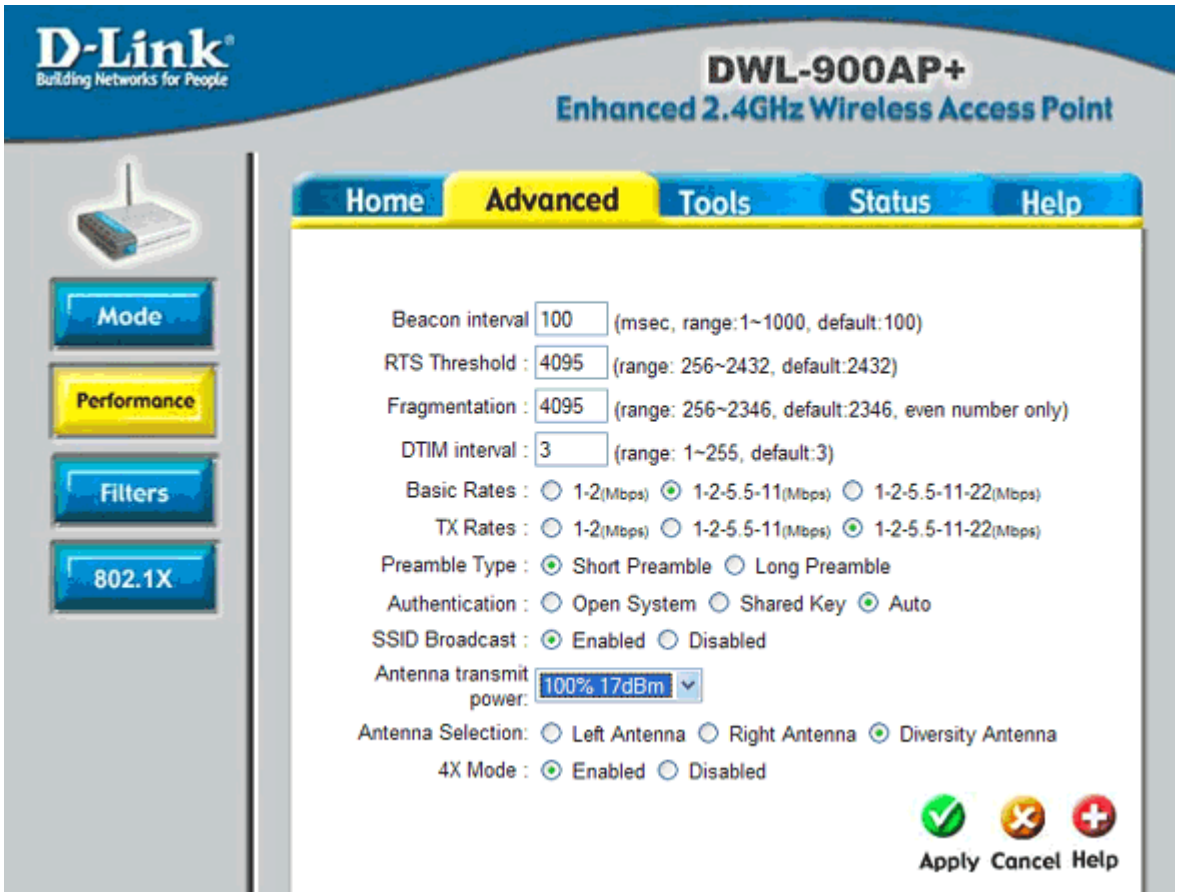


Les solutions

Une configuration radio adaptée

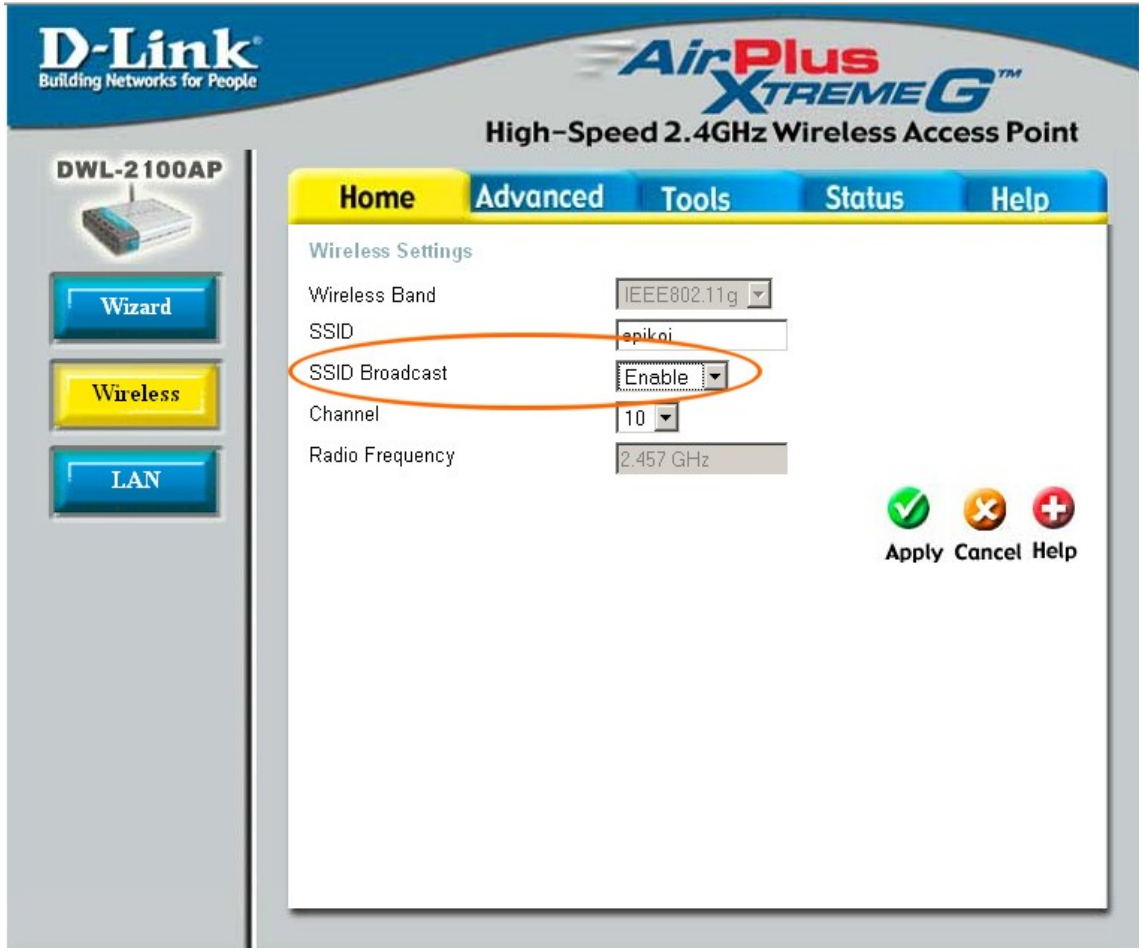
En fonction de la zone effective à couvrir :

- **Positionner les points d'accès** de manière optimale
- **Diminuer la puissance d'émission** du PA
- Faire des **tests** en situation



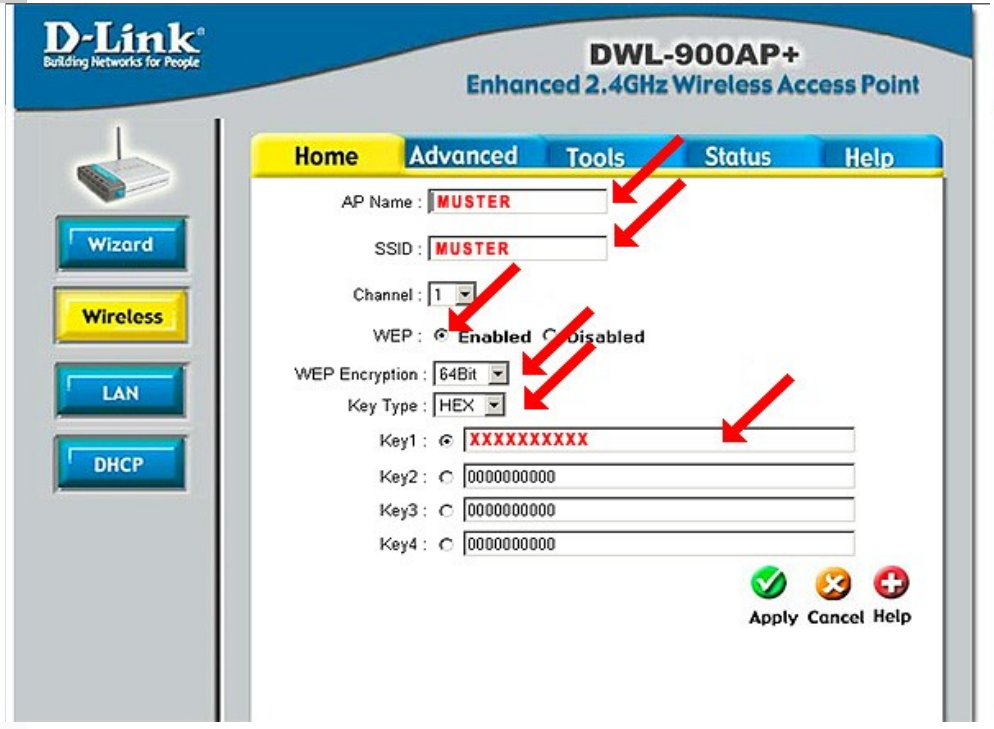
Ne pas Broadcaster le SSID

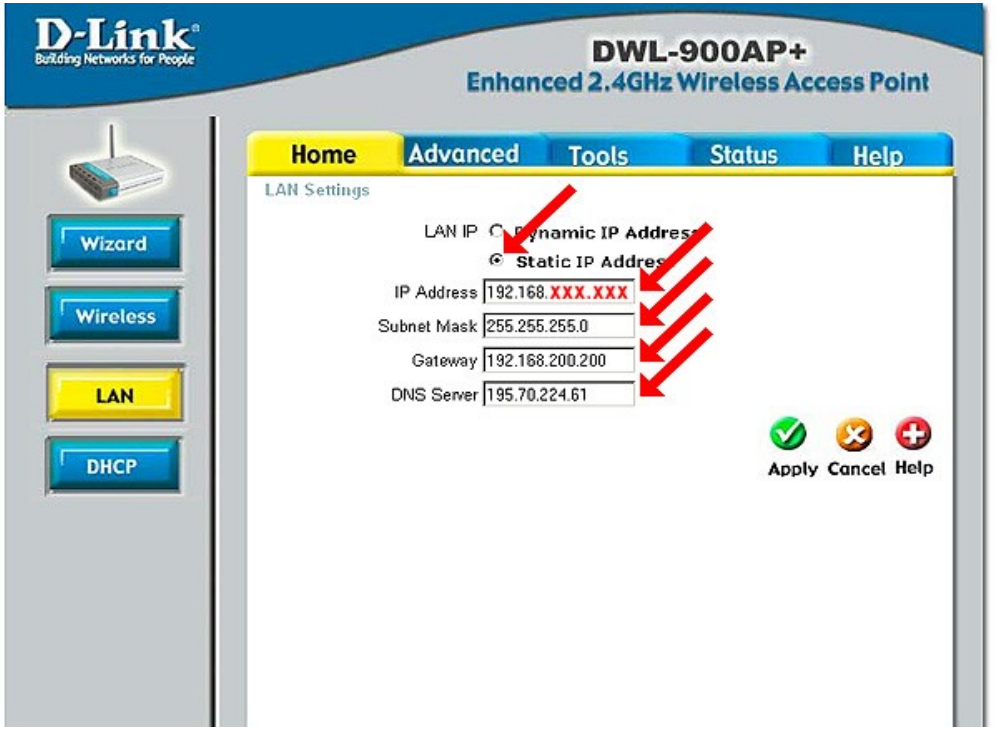
- Le SSID ne sera pas visible par défaut par les nouveaux utilisateurs.
- Les personnes utilisant des outils d'écoute pourront le détecter.
- Si le réseau n'a pas vocation à accueillir de nouveaux utilisateurs régulièrement, à mettre en place.



Modifier les valeurs par défault

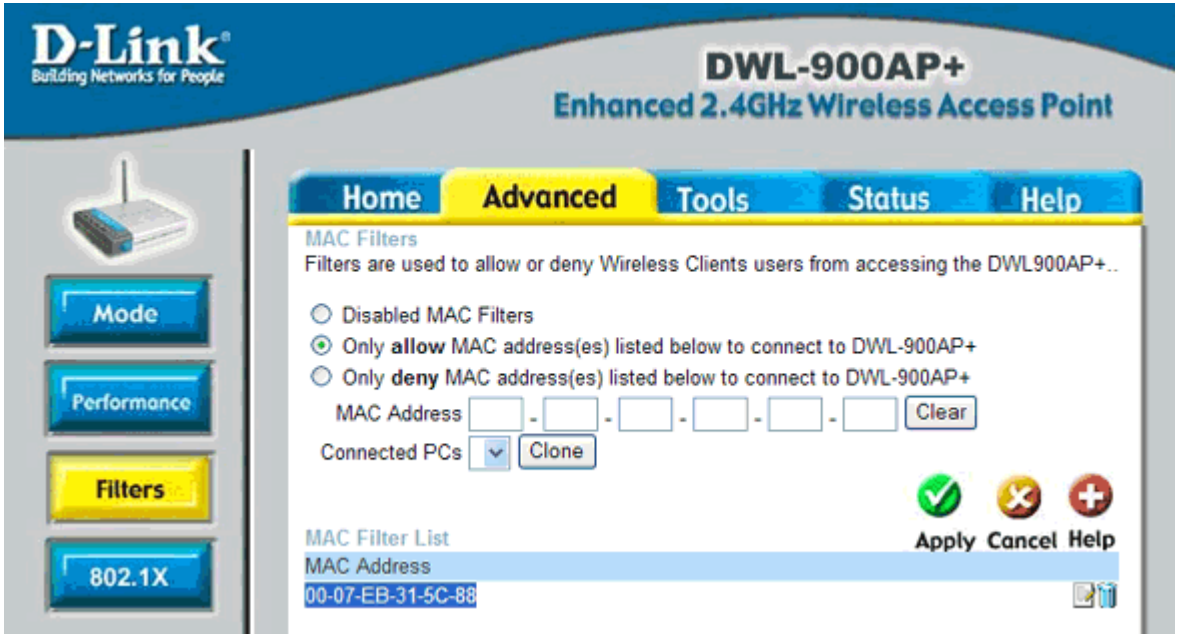
- Modifier le mot de passe d'administration
- Changer le SSID et le nom de l'AP par défault
  - donne des indications sur le modèle
- Changer l'adressage IP par défault





Filtrer les @MAC

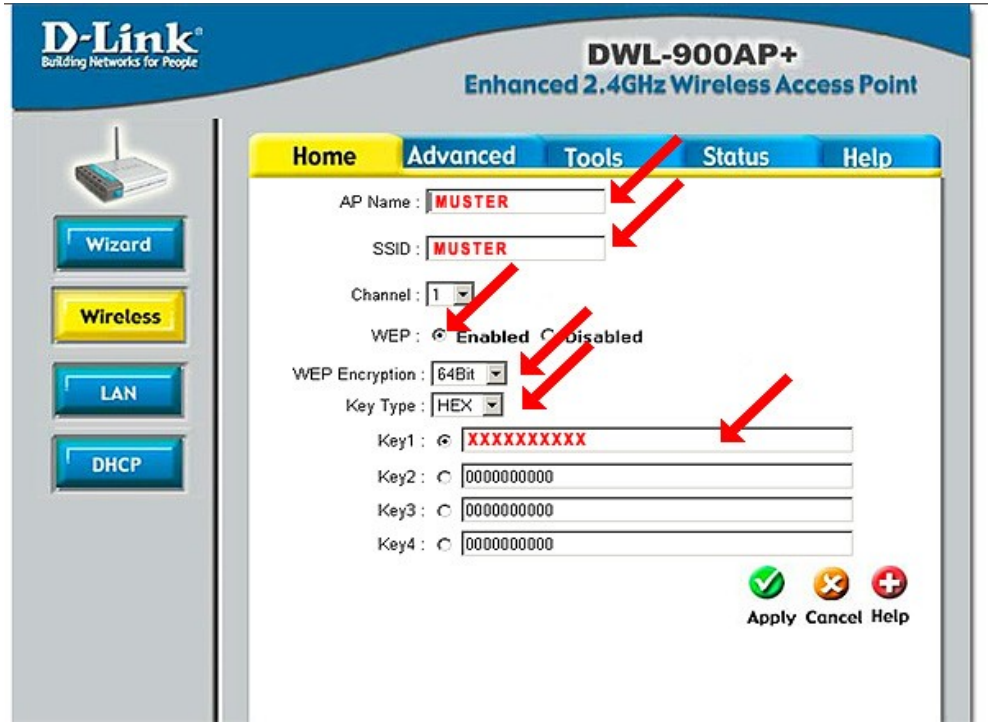
- Possibilité de lister les @Mac des stations autorisées ou interdites
- @MAC = identifiant unique de chaque interface réseau 802 (WiFi, Ethernet) : 01:23:F5:67:29:A1
  - attribuée par le fabriquant et l'IEEE (plaque d'immatriculation)
  - mais peut être falsifiée



Chiffrer les données : WEP

- WEP = Wired Equivalent Privacy
- Protocole de chiffrement utilisant une clef secrète statique de 64 ou 128 bits

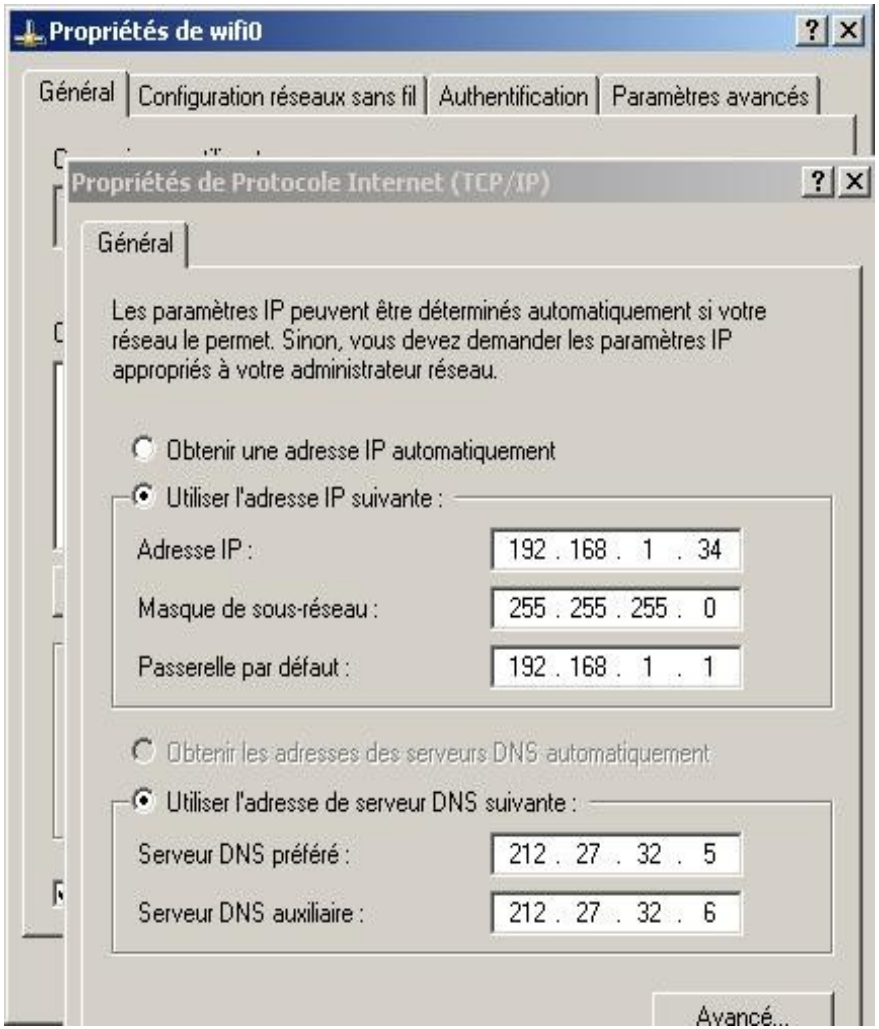
- Fiabilité
  - Une clef de 128 bits couvre 3/4 des risques pour un particulier
  - Une attaque de force brute permets de casser une clef de 64 bits
  - Une capture d'un million de paquets permets de casser une clef de 64 ou 128 bits (faille algorithmique)
- Nécessite d'être configurée sur l'AP et toutes les stations



Désactiver le serveur DHCP

- Une configuration réseau n'étant pas attribuée automatiquement rend la prospective plus dissuasive
- Néanmoins le gain de sécurité est faible et fait perdre la souplesse d'administration du DHCP

-> solution réservée aux besoins spécifiques

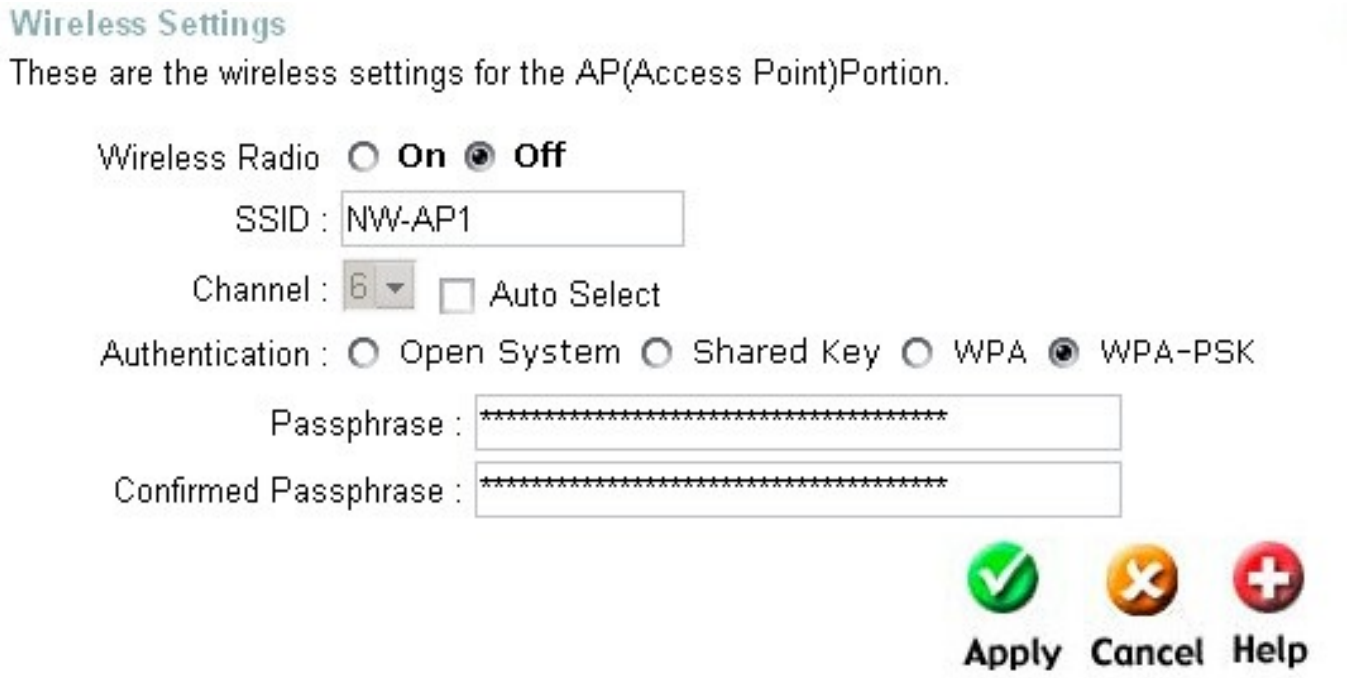


WPA : authentification + chiffrement

- Wi-Fi Protected Access (WPA et WPA2)
  - comble les lacunes du WEP
  - récent donc pas implémenté sur tous les matériels (voir maj firmware)
  - respecte la norme 802.11i (2004)
- Chiffrement : TKIP
  - Temporal Key Integrity Protocol
  - Vecteurs d'initialisation tournants et vérification d'intégrité
- Authentification
  - personnel : WPA - PSK
  - entreprise : 802.1/x - EAP avec serveur Radius

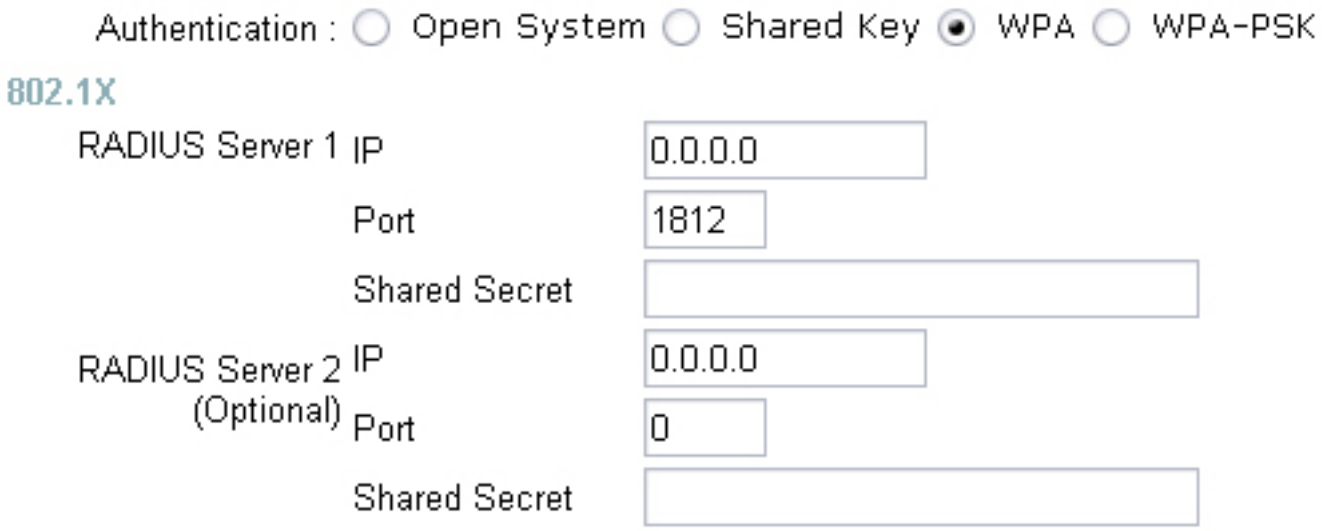
WPA – PSK (personnel)

- Nécessite une Pass-Phrase devant être saisie sur l'AP et le client
- Cette clef sert à la fois à l'authentification (Pre-Shared-Key) et au chiffrement (TKIP)



WPA – EAP / 802.1x (entreprise)

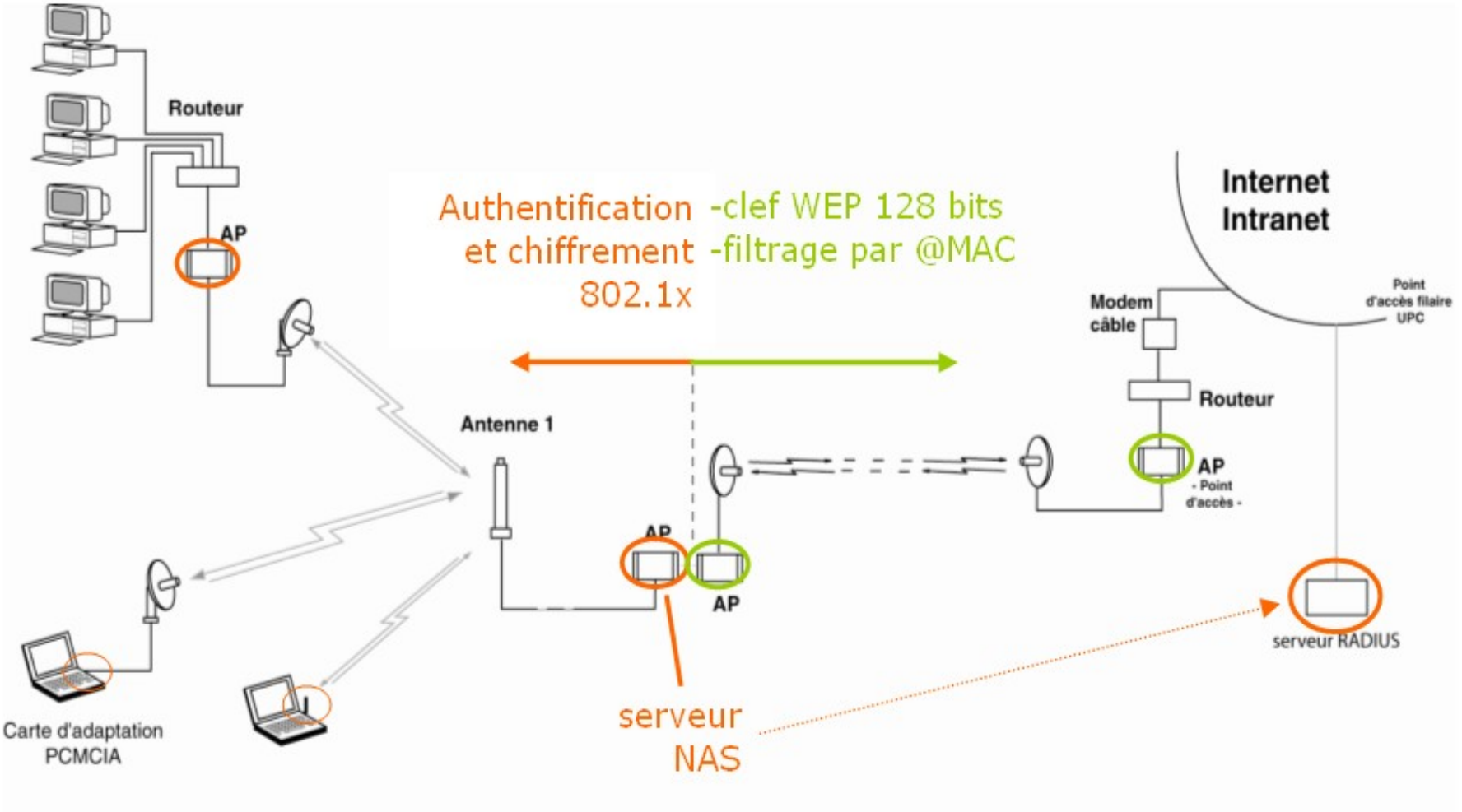
- Utilise un serveur Radius centralisé pour gérer l'authentification : robuste mais compliqué
- Cette clef sert à la fois à l'authentification (Pre-Shared-Key) et au chiffrement (TKIP)



WPA (suite et fin)

- Faiblesses
  - L'utilisation de Pass-Phrase trop courtes voire trop communes pouvant être brute-forcées.
  - La possibilité de générer des trames "DISASSOCIATE" et cela relancera ainsi le procéssus d'identification du WPA.
- Pour en savoir plus
  - http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
  - http://reseau.erasme.org/rubrique.php3?id_rubrique=15
  - http://www.freeradius.org/

Une exemple de sécurisation complet



Synthèse

Résumé des solutions

		Interception de données	Intrusion	Occupation de BP	Brouillage des transmissions	Dénis de service
Wi-FI	**Réglage de la puissance**	+	+	+	-	+
	Ne pas broadcaster le SSID	-	+	+	-	+
	Limitation des @Mac	-	+	+	-	+
	Clef WEP	++	+	+	-	+
	WPA	+++	++	+	-	+
IP	**@IP fixes**	-	+	+	-	-
	Tunnel VPN	+++	+	-	-	-

- : ne fonctionne pas
+ : fonctionne mais peu fiable
++ : recommandé
+++ : meilleure solution

Partie 6

Déployer
un réseau sans fil

Méthodologie

- Théorie
- Evaluation des besoins
- Etude de site
- Dimensionnement
- Sécurité
- Documentation
- Fonctionnement, optimisation et maintenance

Analyse des besoins

- Quel est le nombre des utilisateurs et leur perspective d'évolution ?
- Quelle est la densité des utilisateurs et leur espacement ?
- Le profil des utilisateurs (accès restreint ou public)?

- Nature et importance des données qui transiteront ?
- Quelles sont les applications utilisées actuellement, ou plus tard (dans 2 ans)?
- Quels sont les types de trafic (sporadique ou continu) et les volumes de trafic effectifs ?
- Quels sont le besoin de débit minimum des utilisateurs en accès sans fil ?

- Types des stations qui seront connectées, leurs compatibilité ?
- Quel est la topologie et le plan d'adressage du réseau filaire amont ?
- Existe t il des services réseau : DHCP, DNS, Proxy ?
- Des restrictions ? Des filtrages ?

Etude de site

- Objectif
  - Déterminer avec précision des emplacements des APs
  - Paramétrer la radio des APs et (puissance de transmission, couverture, canaux, type d'antennes)
- Procédure
  - Rassembler les plans des locaux. Y-indiquer l'emplacement des prises LAN, secteur, coupe-feu, etc.)
  - Localiser les éventuelles sources d'interférences et évaluer leur importance (cages d'ascenseur, éléments en mouvement, rayonements...)
  - Faire des tests avec un AP et un portable pour évaluer la puissance et la qualité du signal
  - Fixer l'orientation des antennes et la puissance des APs
  - Envisager des installations électriques autonomes

Dimensionnement

- Evaluer la capacité des Aps

	Exemple de type d'application	Nombre utilisateurs
802.11b	– Consultation messagerie – Navigation Internet	50
	– Téléchargement de fichier peu volumineux	25
	– Téléchargement de fichier volumineux – VoIP, vidéoconférence…	10
802.11a **802.11g**	– Téléchargement de fichier volumineux – VoIP, visé	50

- Effectuer le plan d'adressage réseau du site

Stratégie de sécurité

- Dimensionner des solutions de sécurité adaptées
  - Wi-Fi
    - Réglage de la puissance
    - Ne pas broadcaster le SSID
    - Limitation des @Mac
    - WPA à défaut Clef WEP
  - IP
    - @IP fixes
    - Tunnel VPN
  - En informer les utilisateurs
- Faire des audits sécurité régulièrement
  - notamment : log des utilisateurs et des @Mac au niveau AP(-> à rediriger éventuellement dans un fichier de log)
  - ping de toutes les adresses IP du Subnet (attribuées ou statiques)
  - évolution des débits

Documentation

- Documenter l'historique de l'installation
  - Guide d'implémentation et de mise en marche du réseau
  - Historique des interventions
- Produire un plan WiFi
    - APs et identification
    - Zone de couverture, canal, antennes, débits
    - Réglage de sécurité
- Produire un plan du réseau
    - Schéma IP des connexions et des équipements
    - Plan d'adressage
    - Distribution des adresses : DHCP, DNS, Proxy, ect
    - Anticiper le manque d'adresses

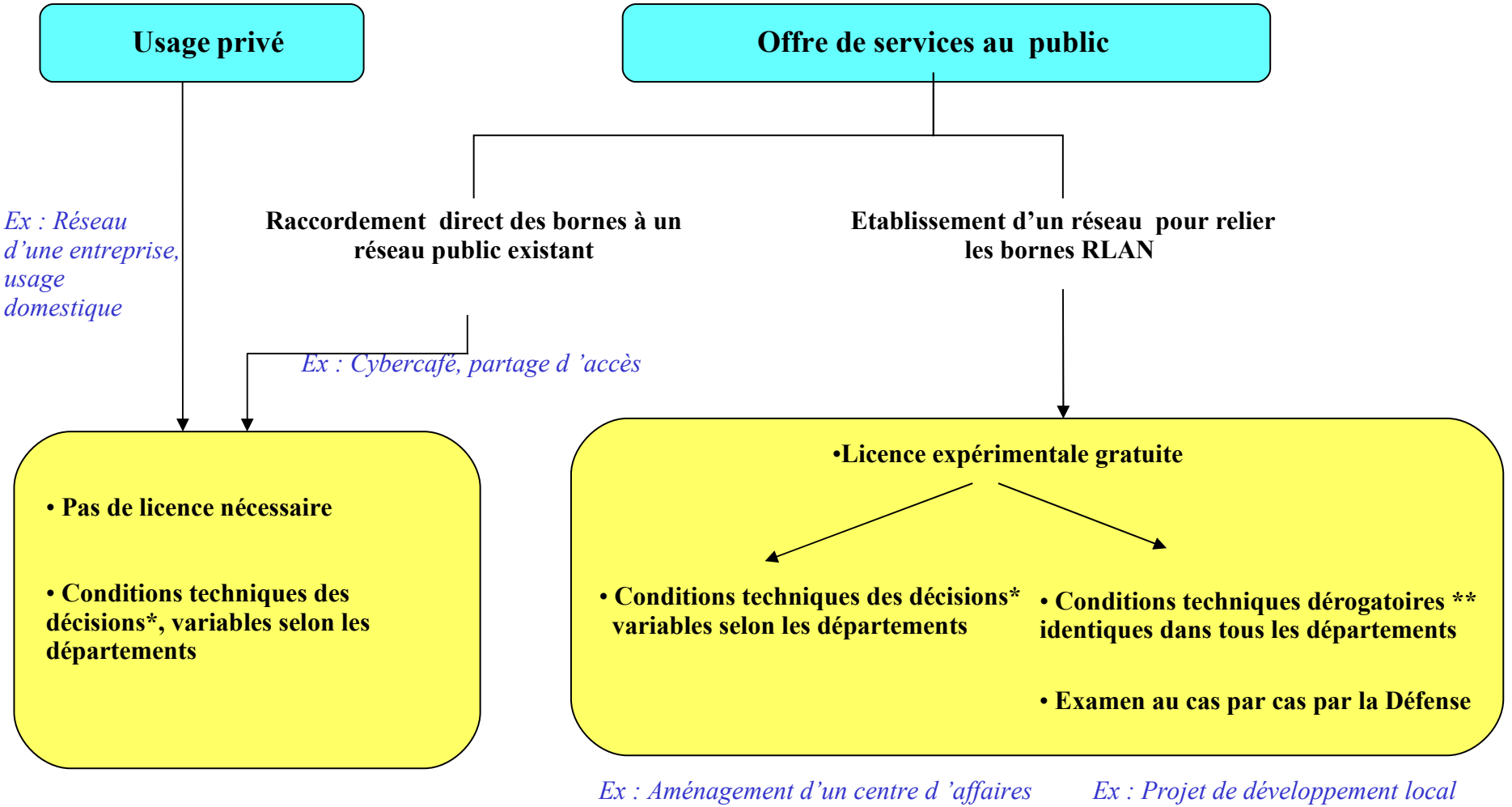
Partie 7

Compléments

Aspects juridiques

Aspects juridiques (radio)

Le cadre réglementaire pour les RLAN en 2,4 GHz



** détaillées dans le communiqué de presse du 7 novembre 2002*
*** puissance rayonnée (PIRE) de 100 mW en extérieur et en intérieur*

Source : http://www.art-telecom.fr - 19/11/2002

Aspects juridiques (contenu)

- La loi contre le terrorisme (LCT) du 29 octobre 2005 impose à tous ceux qui proposent un accès à Internet au public (particuliers, cybercafés ou des fournisseurs d'accès à Internet) de conserver les données de connexion pendant 3 ans et à les communiquer si nécessaire aux services de police.
- En pratique, le log des adresses MAC connectées suffit.
- Certains points d'accès embarquent des solutions d'enregistrement des logs.
- En cas d'utilisation de votre réseau à votre insu vous êtes responsable de ce qui est fait depuis votre connexion

Aspects sanitaires

Des éléments concrets

- Les normes européennes d'utilisation des ondes WiFi spécifient une puissance rayonnée < 100 mW.
- Le WiFi rayonne moins que la plupart des équipements quotidiens
  - Téléphone GSM : < 2W ;
  - Téléphone DTEC : < 500 mW ;
  - Antennes GSM : 20 à 50 W ;
  - four à micro-ondes : 1 kW ;
  - émetteur de la tour Eiffel : 6 MW
- La puissance d'un champ électro-magnétique décroît avec le carré de la distance.
- Un élément radio WiFi à 1 mètre revient à poser un téléphone portable en marche à 3 mètres.

... mais des questions subsistent

- L’utilisation de radio-fréquences suscite des interrogations.
- Les nombreuses études en cours, surtout au sujet de l’utilisation des téléphones mobiles, sont globalement rassurantes.
- Néanmoins l'accumulation des ondes et l'inconnu des effets à long terme incitent au principe de précaution.
- Depuis 2002, presque tous les constructeurs se sont ralliés à des utilisations de l'ordre de 30 mW en sortie d'antenne WiFi.
- Voir : http://reseau.erasme.org/article.php3?id_article=29