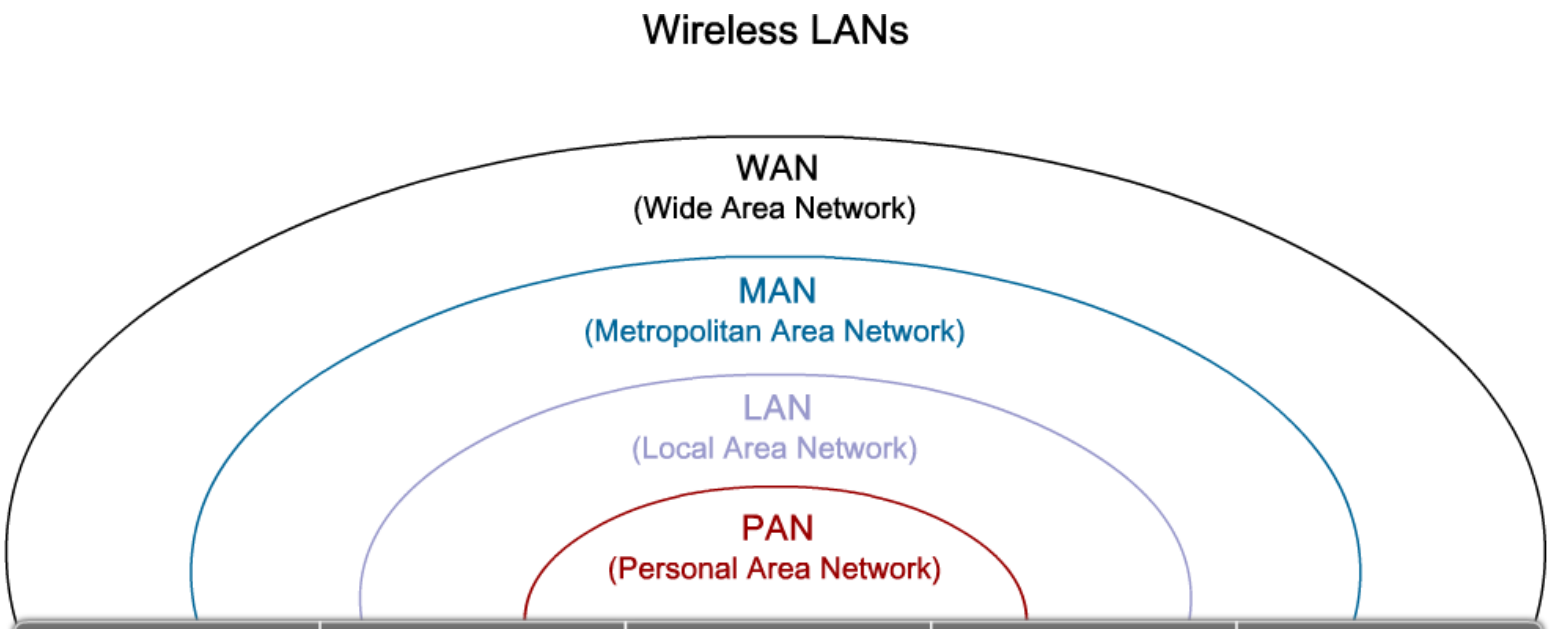
Les Wireless LAN

Les Wireless LAN

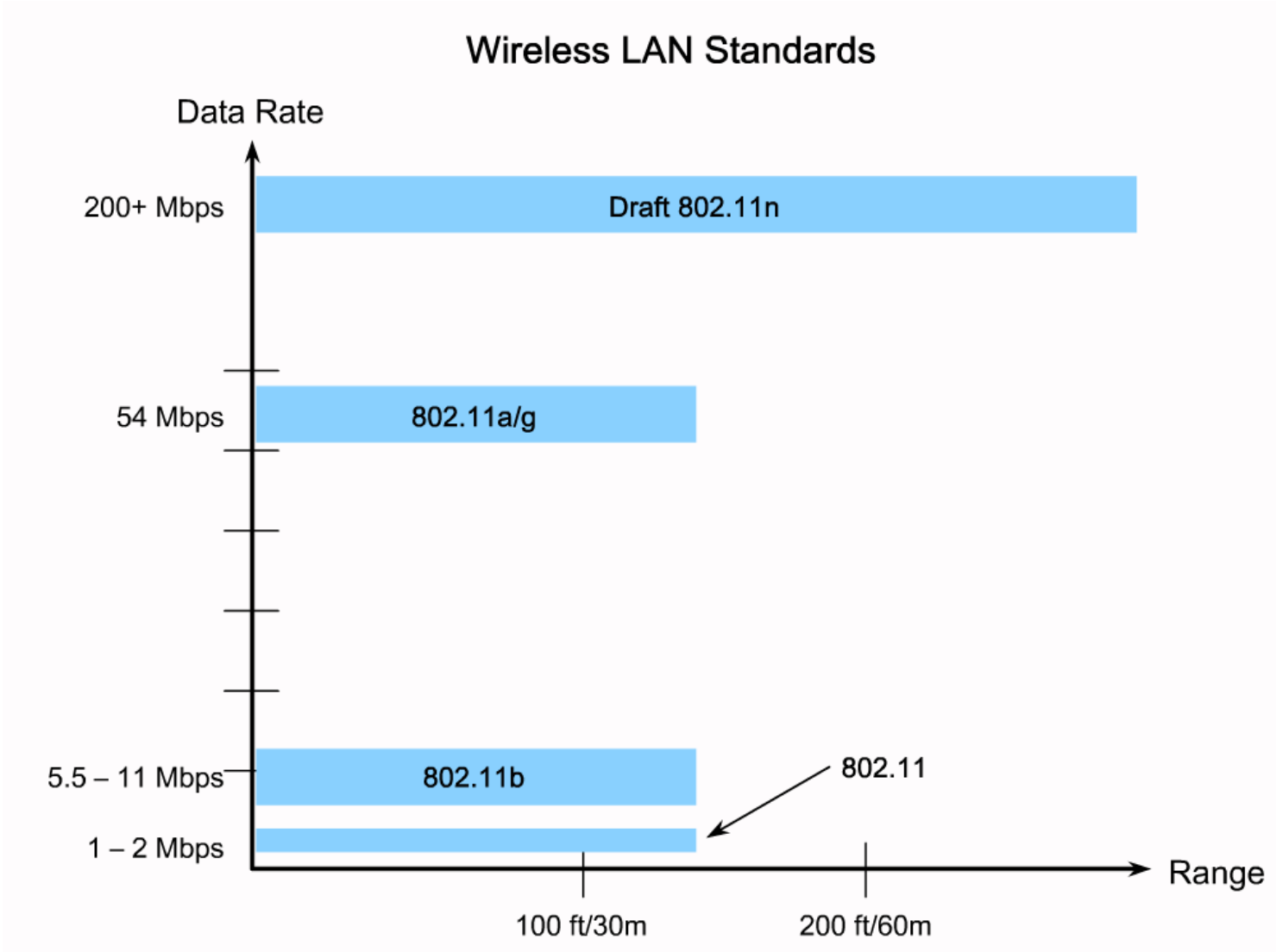
Introduction

Les réseaux Wireless ?



	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

Débit et distance maximale



Comparaison

Wireless LAN Standards

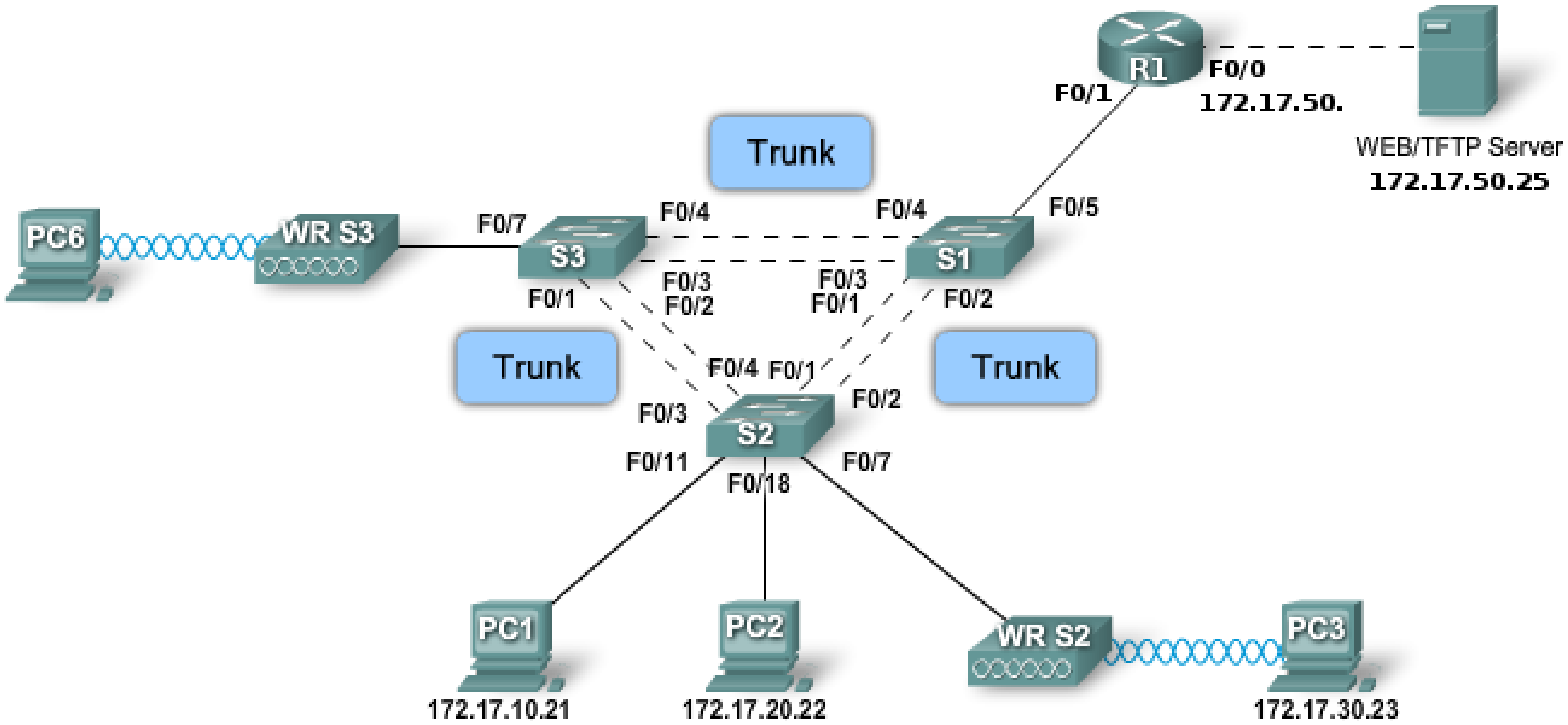
	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		5.7 GHz 2.4 GHz
Channels*	Up to 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps	Speculated to be 400 Mbps for two MIMO streams
Range	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Release Date	October 1999	October 1999	June 2003		September 2009
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed		Very good data rates, improved range
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band		

* Non-overlapping channels.

Quelques autres normes 802.11

- 802.11c : Bridge Operations Procedures
- 802.11d : Global Harmonization
  - Adresse les problèmes légaux
- 802.11e : MAC Enhancements for QoS
- 802.11f : Inter Access Point Protocol
  - Améliore la qualité de service (QoS) pour les utilisateurs itinérants
- 802.11h : Spectrum Managed 802.11a
  - Dédié aux problèmes légaux européens liés à l'utilisation de la bande des 5 Ghz
- 802.11i : MAC Enhancements for Enhanced Security
  - Amélioration de la sécurité des protocoles utilisés en 802.11b

Exemple Wireless LANs



Avantages du WiFi

- Norme internationale maintenue par l'IEEE et indépendante d'un constructeur en particulier
- Fonctionnement similaire à Ethernet
  - Évite le développement de nouvelles couches réseaux spécifiques
- Rayon d'action important (jusque 300m, en champ libre)
- Débit acceptable
- Mise en œuvre facile
  - Pas de travaux, pas de nouveau câblage
  - Pas de déclaration préalable dans la plupart des pays
  - Pas de licence radio à acheter
  - Coût d'une installation faible : environ 30 € pour une carte wifi et 100 € pour une borne.

Quelques inconvénients

- Des constructeurs proposent des normes propriétaires
  - 802.11b+ (Dlink) ou Turbo (3Com/US Robotics) : Extension à 22Mb/s dans la bande des 2,4Ghz
  - 802.11g Turbo à 100Mbps (annoncé en Mai 2003)
  - Intégration de nouvelles extensions, incompatibles avec les normes actuelles
- Pourquoi ?
  - Délai de ratification des normes importantes
  - Pour le 802.11n : 8 ans de travaux. Ratifié le 11 Septembre 2009. Début des travaux en 2002. Document final de cette norme : 560 pages

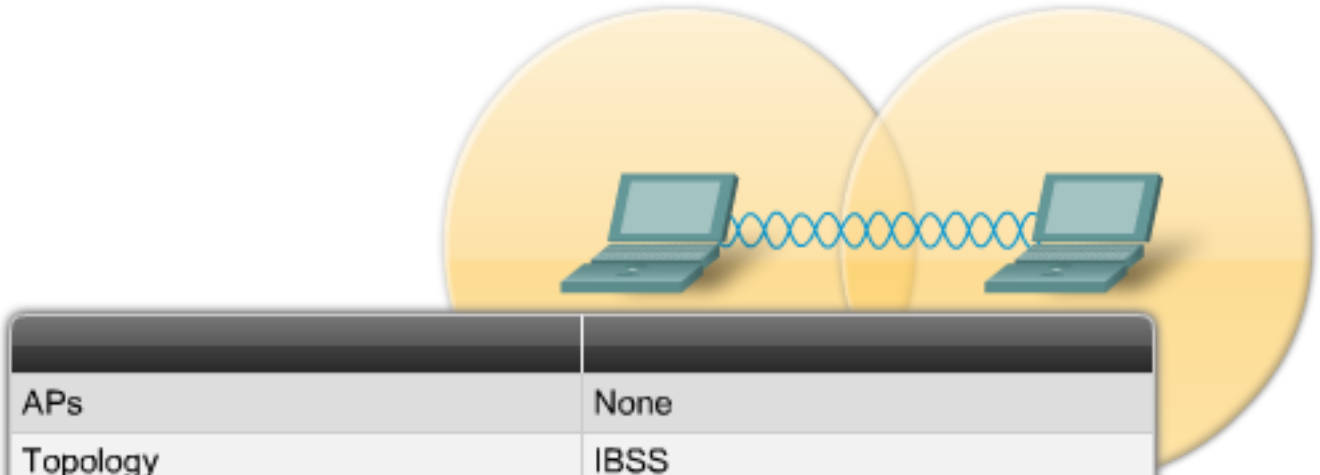
WLAN et LAN ?

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Les Wireless LAN

Les topologies 802.11

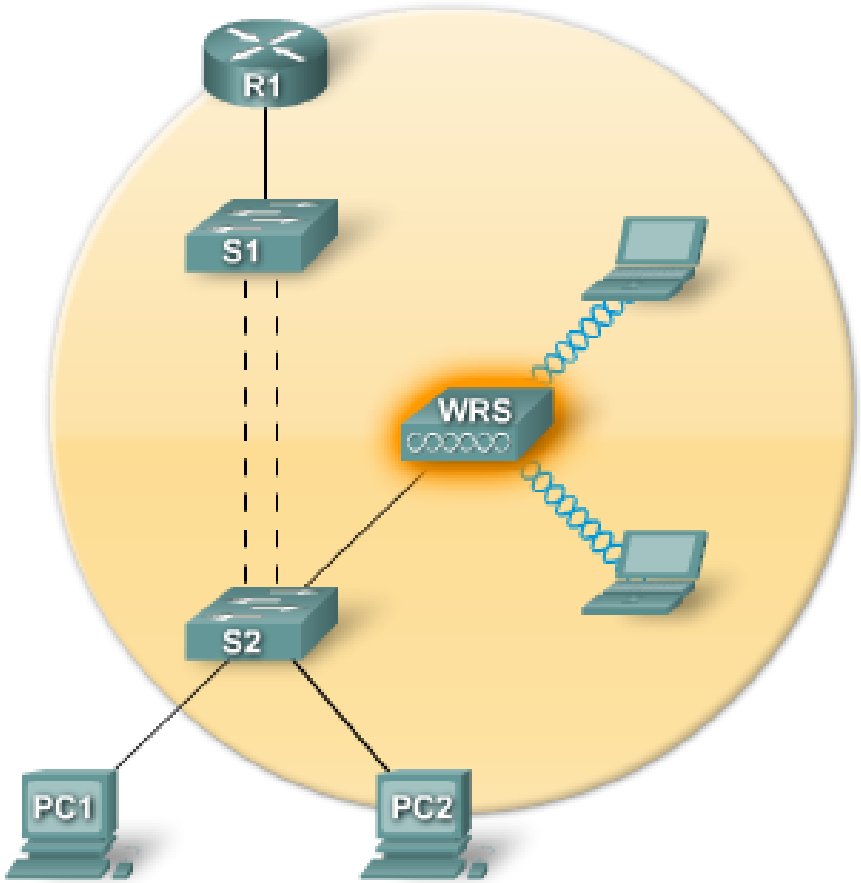
Le ad-hoc



APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Mode infrastructure

APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)



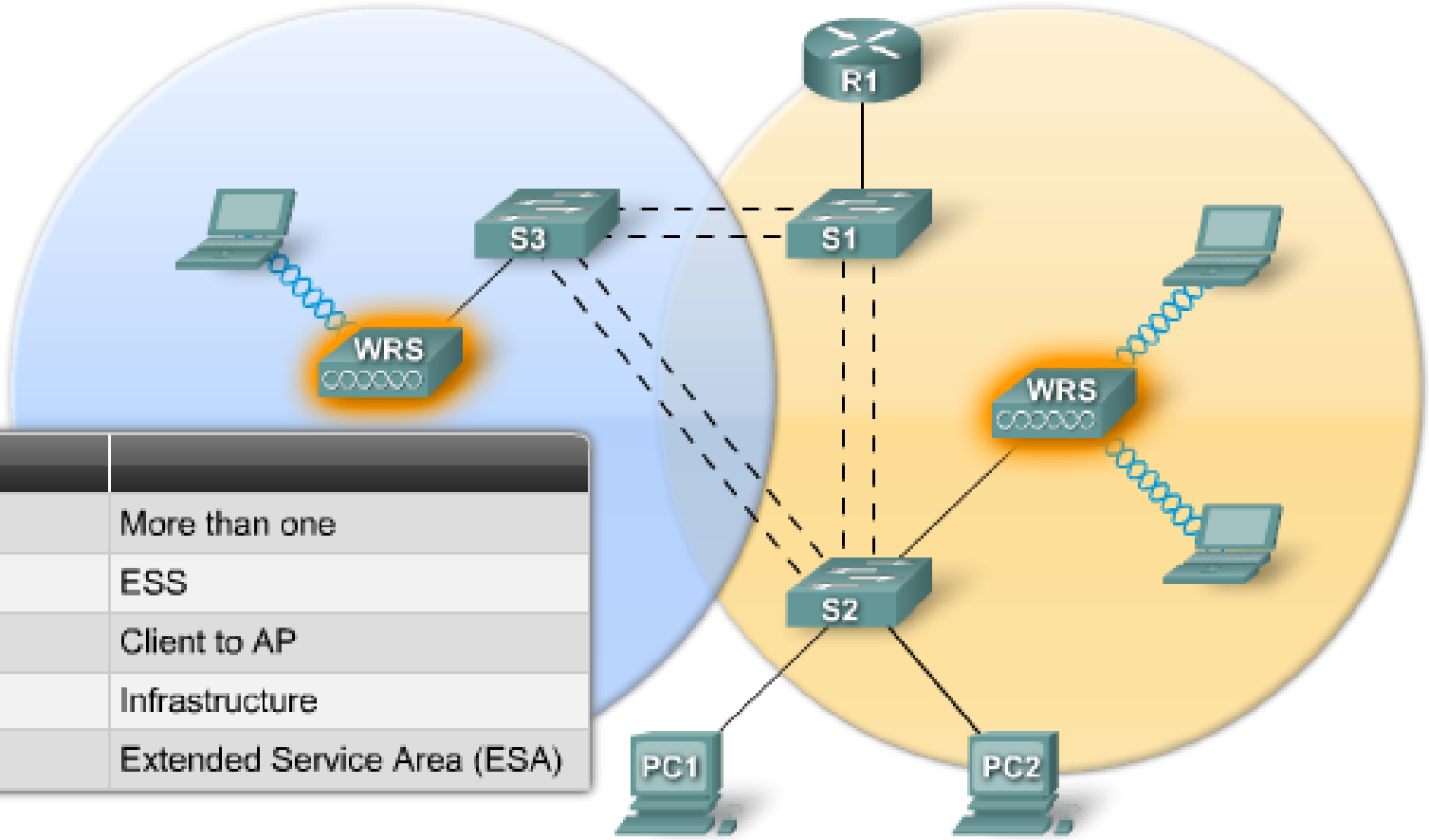
Les BSS

- Les stations qui communiquent sur les réseaux 802.11 sont regroupés dans des Basic Service Set
- Existence de 2 types de Basic Service Set (BSS)
  - Independent BSS (IBSS) ou mode ad-hoc : chaque station communique avec d'autres stations
  - Infrastructure BSS (abrégé en BSS) ou mode infrastucture : chaque station communique avec un point d'accès
- Les stations doivent être dans le même Basic Service Set pour pouvoir communiquer ensemble
- Processus de communication
  - Les stations doivent s'associer au IBSS ou au BSS
  - Objectif : éviter que quiconque, proche d'une station, puisse directement communiquer avec elle

Les SSID

- Un BSS est identifié par une valeur de 48 bit, appelé BSS Identifier
  - En mode infrastructure : le BSS est souvent l'adresse MAC du point d'accès
  - En mode ad-hoc : nombre aléatoire généré par la première station
- En wifi, il est possible de se déplacer d'un BSS à un autre, sans perdre la connexion : le roaming
  - Attention : le wifi n'est pas fait pour assurer une communication lors de déplacement comme les réseaux cellulaires
- Le regroupement de plusieurs BSS se fait dans un Extended Service Set (ESS)
- Chaque BSS dans un ESS sont identifiés par le même Service Set Identifier (SSID)
- Le SSID est unique sur un réseau, sensible à la casse, de longueur comprise entre 2 et 32 caractères

Un WLAN étendu



APs	More than one
Topology	ESS
Connection	Client to AP
Mode	Infrastructure
Coverage	Extended Service Area (ESA)

Usage des SSID

- Les SSID servent à contrôler les accès aux points d'accès
- Les stations et les points d'accès doivent avoir le même SSID pour pouvoir communiquer
- Comment connaître le SSID d'un point d'accès ?

Les Wireless LAN

Son fonctionnement

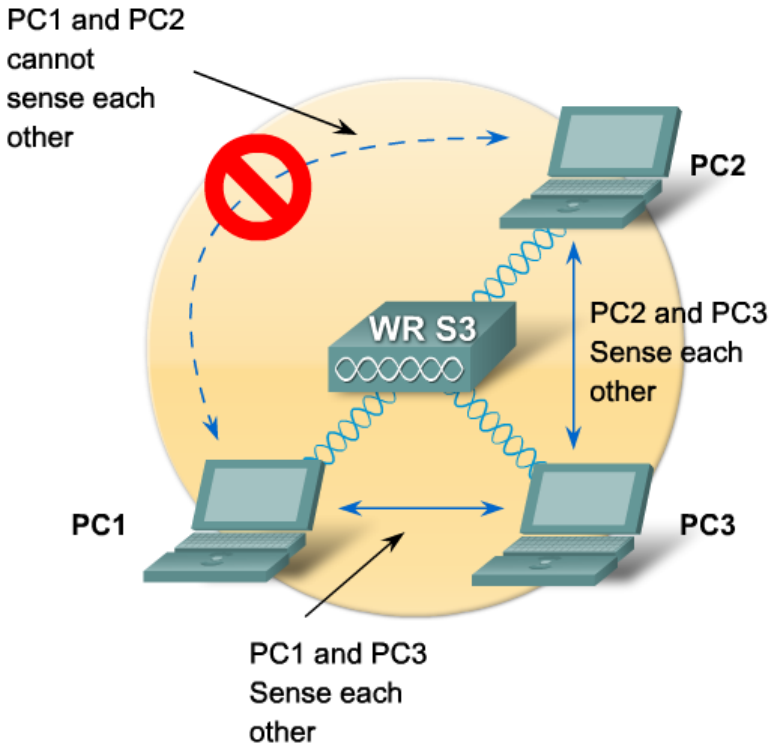
CSMA/CA ?

- Carrier Sense Multiple Access with Collision Avoidance
- Fonction du Request To Send/Clear To Send pour résoudre le problème de la station cachée

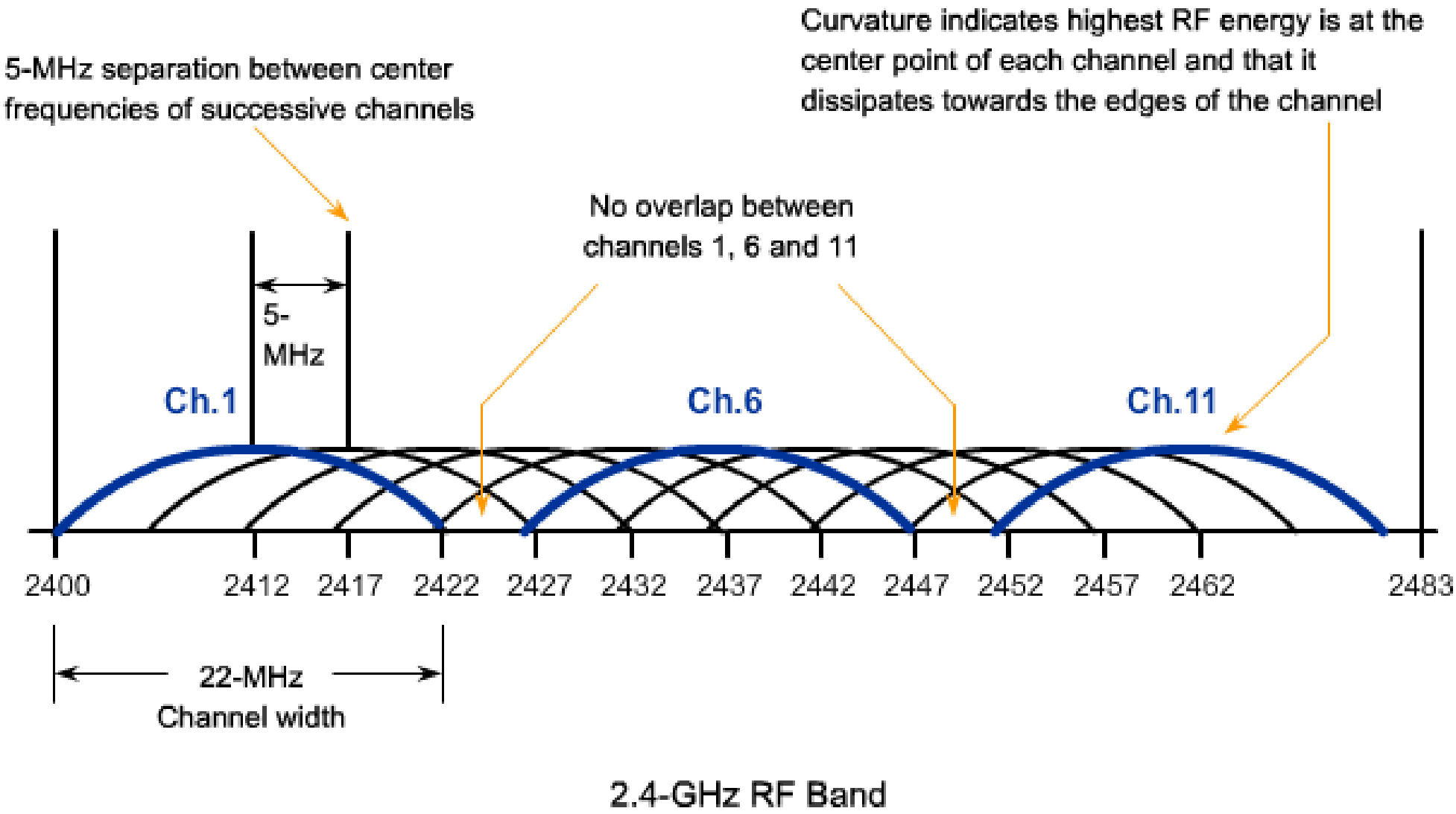
The Hidden Node Problem:

- PC1 and PC2 reach WRS3
- PC1 and PC2 cannot reach each other
- PC1 does not detect PC2 activity on the channel
- PC1 sends data while PC2 is transmitting
- A collision occurs

PC3 is sensed by both PC1 and PC2, so there are no collisions involving PC3.



Les canaux


5-MHz separation between center frequencies of successive channels
Curvature indicates highest RF energy is at the center point of each channel and that it dissipates towards the edges of the channel
No overlap between channels 1, 6 and 11
5-MHz
Ch.1
Ch.6
Ch.11
2400
2412
2417
2422
2427
2432
2437
2442
2447
2452
2457
2462
2483
22-MHz
Channel width
2.4-GHz RF Band

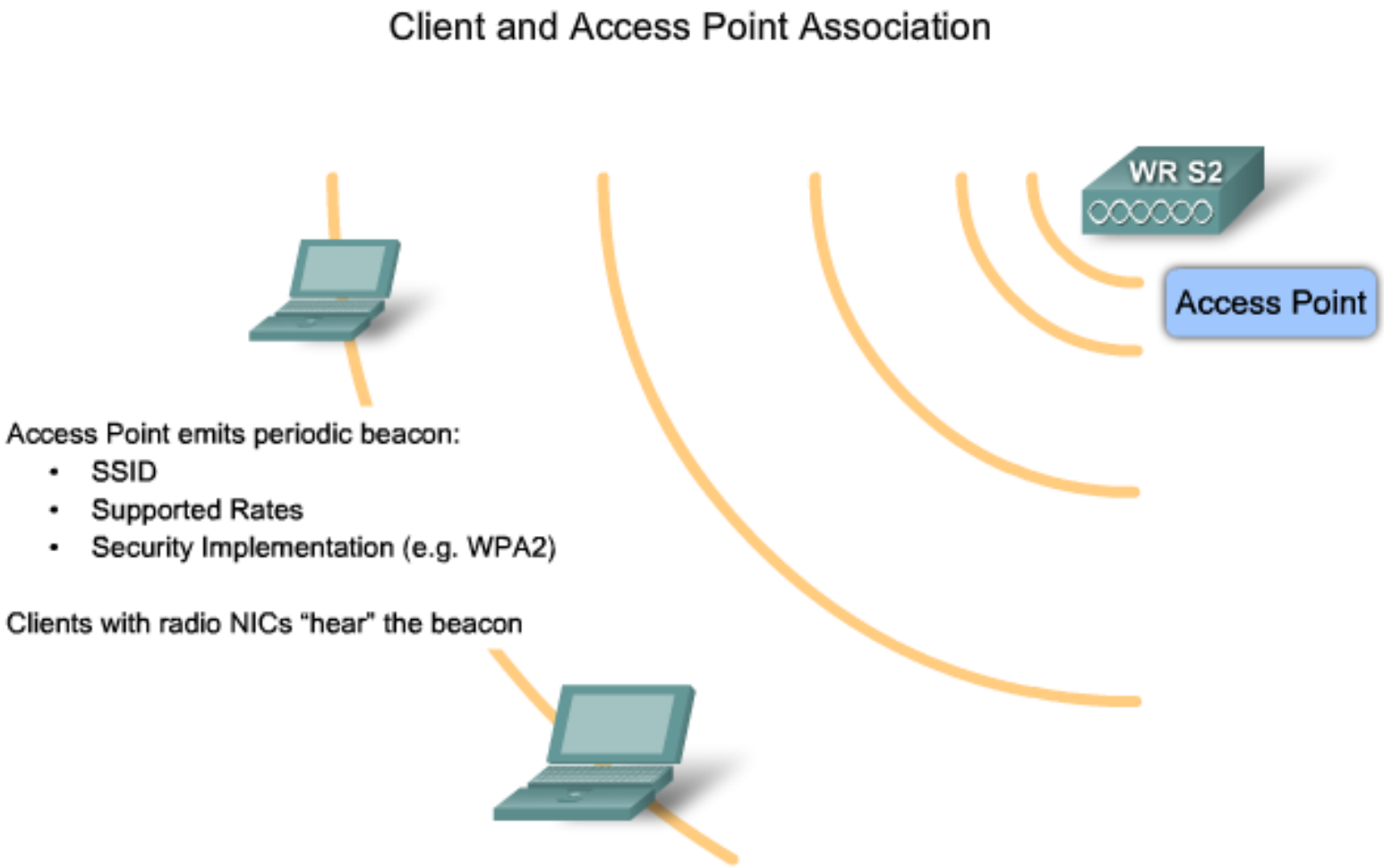
Les limites légales

- Jusqu'en 2003
  - USA : Canal 1 à 11, puissance max. 1000 mW
  - Europe (hors France) : Canal 1 à 13, puissance max 100mW
  - Japon : Canal 1 à 14, puissance max 10mW
  - France : Canal 10 à 13, puissance max 100mW
- Depuis fin 2003, en France Canal 1 à 13
- Historiquement, certains portables Wifi en importation US ne pouvaient pas fonctionner en France
  - Canaux 12 et 13 non utilisable !

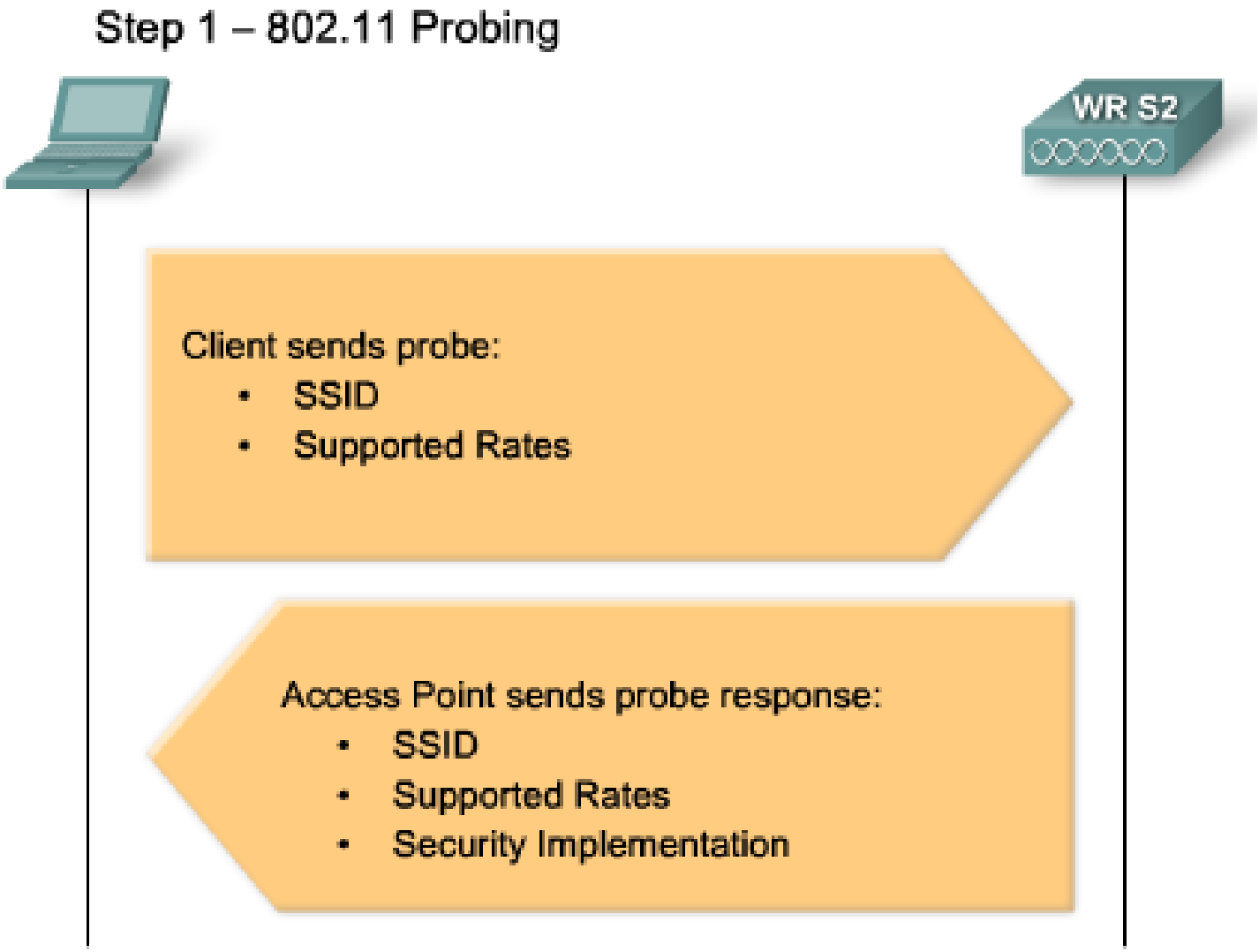
Beacon frames

- Les trames de type beacon sont expédiées régulièrement sur le réseau (en infrastructure) ou entre station (en ad-hoc)
- Ils transportent de nombreuses informations
  - Synchronisation temporelle entre la station et le point d'accès afin d'être sûr que toutes les fonctions sensibles aux temps soient correctement exécutées (saut de fréquences en FHSS, par exemple). Attention : indépendant de l'horloge du système d'exploitation
  - Paramètres spécifiques aux bons fonctionnements du FHSS ou du DSSS
  - Le SSID du réseau est inclu dans les beacon trames. Attention : la désactivation du broadcast du SSID ne stoppe pas l'émission des beacon trames.
  - Trafic Indication Map : permet de gérer les paquets en file d'attente à destination de station en veille
  - Débit supporté par le point d'accès

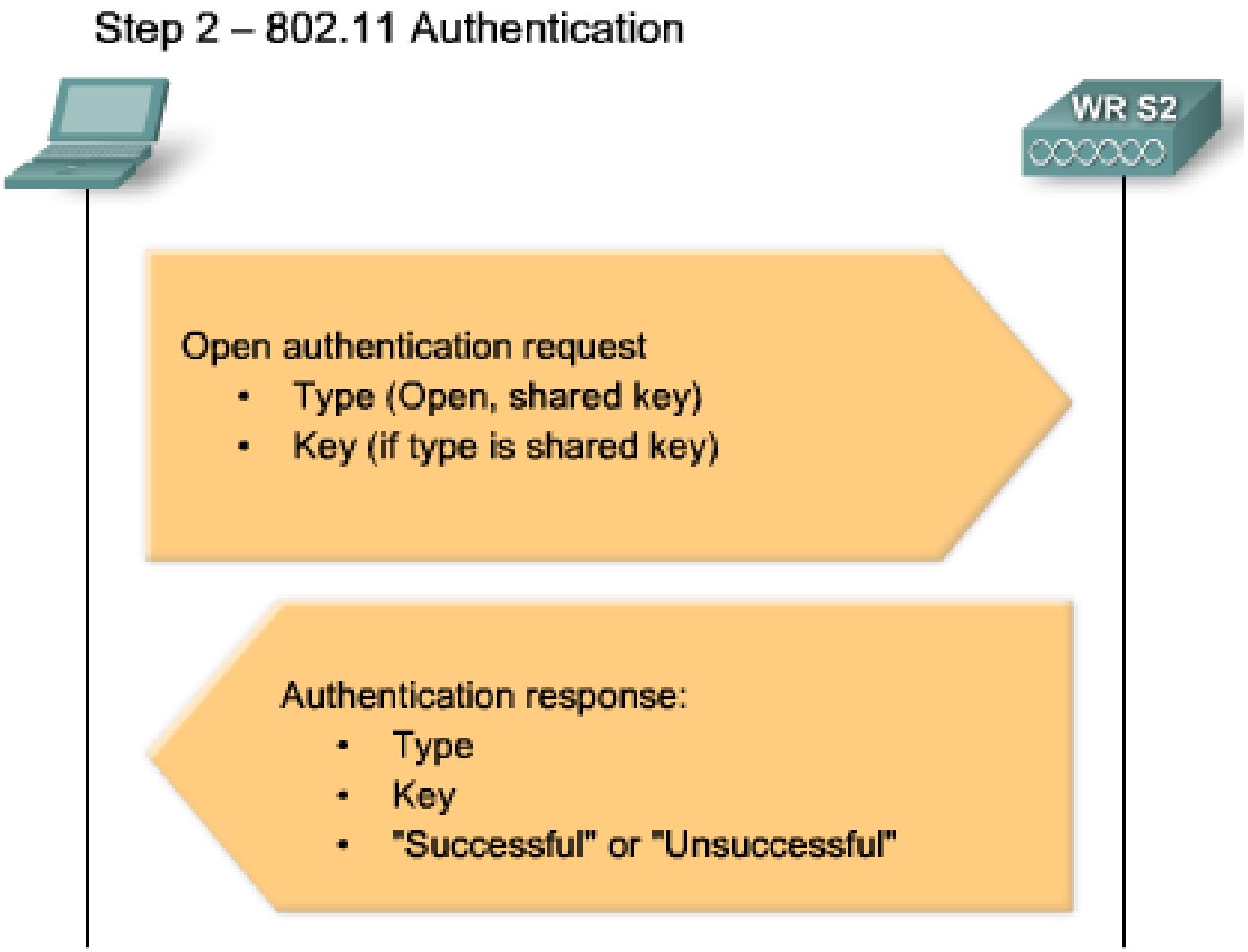
Les beacons trames



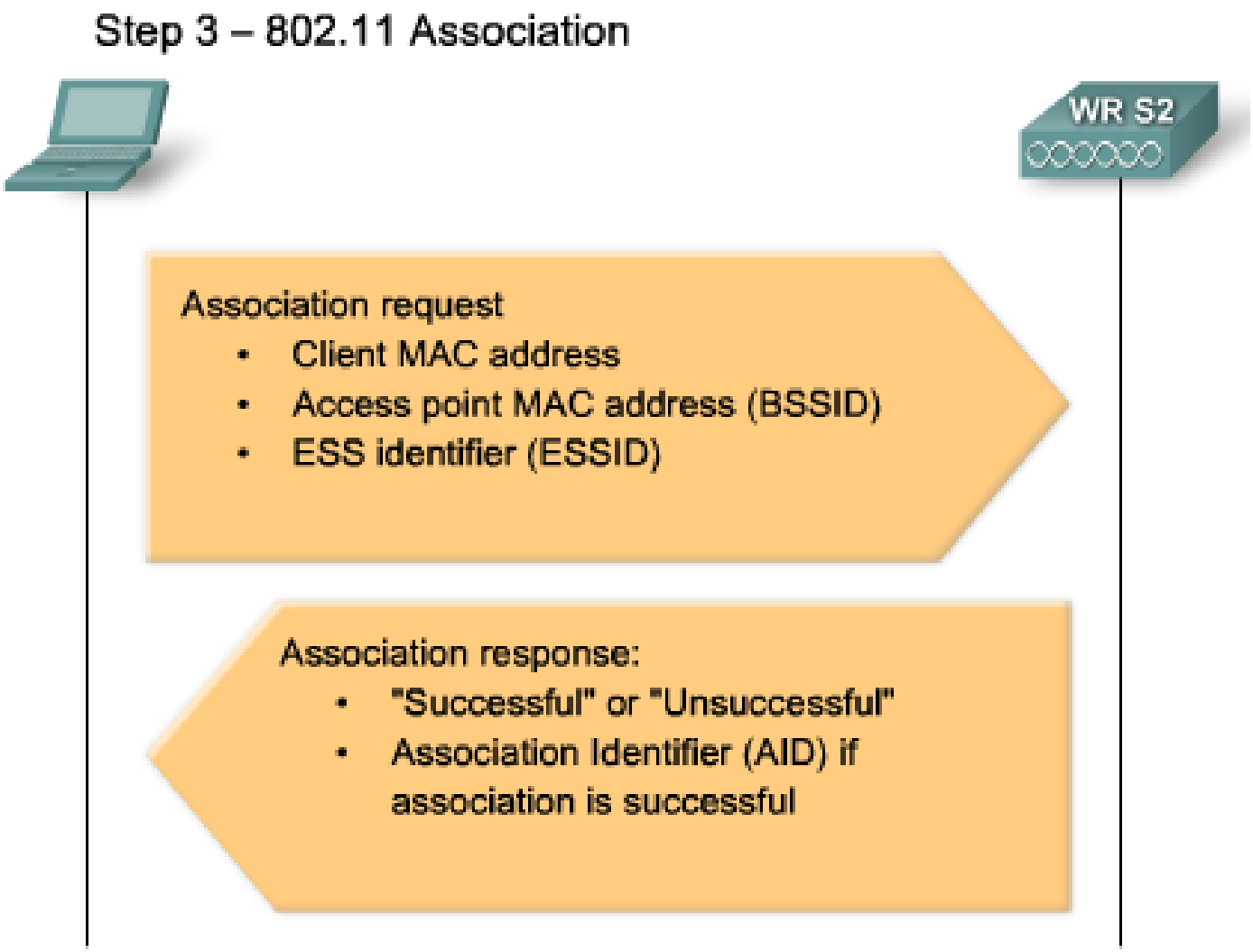
L'association Etape 1/3



L'association Etape 2/3



L'association Etape 3/3



Quiz

Phrase	Answer
The _____ enables a client station capable of sending and receiving RF signals.	
An _____ connects wireless clients to the wired LAN.	
Wireless clients that are at the maximum range and opposite sides of an access point will not be able to reach each other or detect each other's transmissions. This is known as the _____ problem.	
_____ was developed to solve the hidden node problem. When enabled, the access point will allocate the medium to a requesting station for as long as is required to complete the transmission.	
Desktops located in an existing, non-wired facility can have a wireless _____ installed.	
A _____ like the WRT300N performs the role of access point, Ethernet switch and router.	
In the 1990s, wireless NICs for laptops were cards that slipped into the _____ slot.	

access points | hidden node | wireless router | PCI NIC
RTS/CTS | wireless NIC | PCMCIA

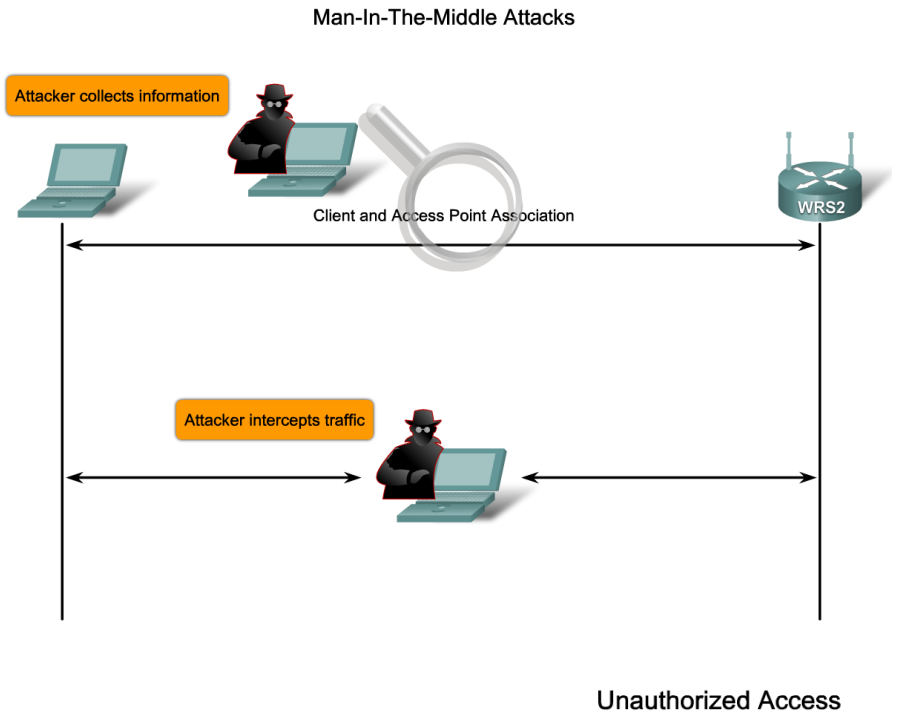
Les réponses ;-)

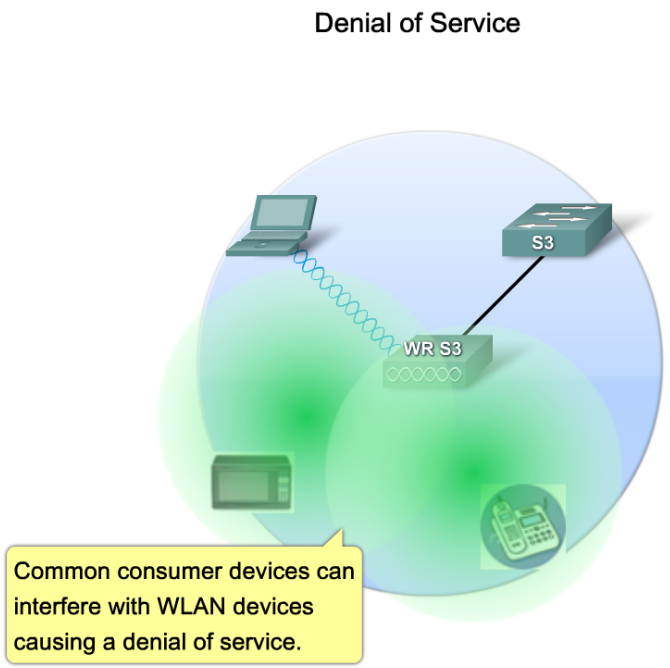
Phrase	Answer
The _____ enables a client station capable of sending and receiving RF signals.	✓ wireless NIC
An _____ connects wireless clients to the wired LAN.	✓ access points
Wireless clients that are at the maximum range and opposite sides of an access point will not be able to reach each other or detect each other's transmissions. This is known as the _____ problem.	✓ hidden node
_____ was developed to solve the hidden node problem. When enabled, the access point will allocate the medium to a requesting station for as long as is required to complete the transmission.	✓ RTS/CTS
Desktops located in an existing, non-wired facility can have a wireless _____ installed.	✓ PCI NIC
A _____ like the WRT300N performs the role of access point, Ethernet switch and router.	✓ wireless router
In the 1990s, wireless NICs for laptops were cards that slipped into the _____ slot.	✓ PCMCIA

Les réseaux sans-fil : IEEE 802.11

La sécurité

La sécurité ?





"War Drivers"	Hackers	Employees
Find "Open" networks; use them to gain free Internet access	Exploit weak privacy measures to view sensitive WLAN information and even break into WLANs	Plug consumer-grade APIs/gateways into company Ethernet ports to create their own WLANs

La sécurité ?

- Transmission sans fil
  - Tout le monde peut donc intercepter les informations
- Interception suivant 2 techniques
  - Ecoute passive
  - Installation d'une borne « pirate »
    - Capture sur celle-ci des adresses MAC des clients et/ou paramètres de sécurité
- Denial of service
  - Par appareil parasitant le signal
  - En diffusant
    - des trames CTS, ainsi chaque station émet des trames et donc entre en collision
    - des trames de déassociation faisant ainsi générer une réassociation des stations, ...

Les protocoles pour la sécurité

Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i

Authentification classique

- Authentification ouverte
  - Aucune authentification n'est requise. L'association est suffisante pour communiquer avec le réseau
- Authentification par clé partagée
  - Utilisation de clés cryptographiques, basées sur le protocole WEP (*Wired Equivalent Privacy)*
  - Le client et le point d'accès partage une même information : la clé
  - Authentification fonctionne sur la technique du challenge, envoyé par le point d'accès
  - WEP : authentification sécurisée et cryptage des données par clé partagée

WEP : codage des données

- Séquence de clair (notée *M*) concaténée avec une valeur de checksum sans clé *ICV(M)* de 32 bits (CRC-32 : *Cyclical Redundancy Check*) (*M* || *ICV(M)*)
- Utilisation de l'algorithme de chiffrement RC4 (algorithme symétrique) pour générer une suite pseudo-aléatoire (initialisé avec une clé (appelée graine))
  - Clé 64 ou 128 bits en export USA
  - sinon, jusque 2048 bits
- Pour fabriquer cette clé, le WEP utilise
  - un vecteur d'initialisation (notée *IV*) de 24 bits généré pour chaque nouvelle séquence WEP
    - soit nombre aléatoire, soit issu de la simple incrémentation d'un compteur !!
  - et une clé secrète (notée *K*) de 40 ou 104 bits partagée par tous les équipements du réseau mobile
- La graine de RC4 est alors (*IV* || *K*)
- Les données cryptées C : (*M* || *ICV(M)*) XOR RC4(*IV* || *K*)
- Envoie sur le réseau : *IV* || *C*

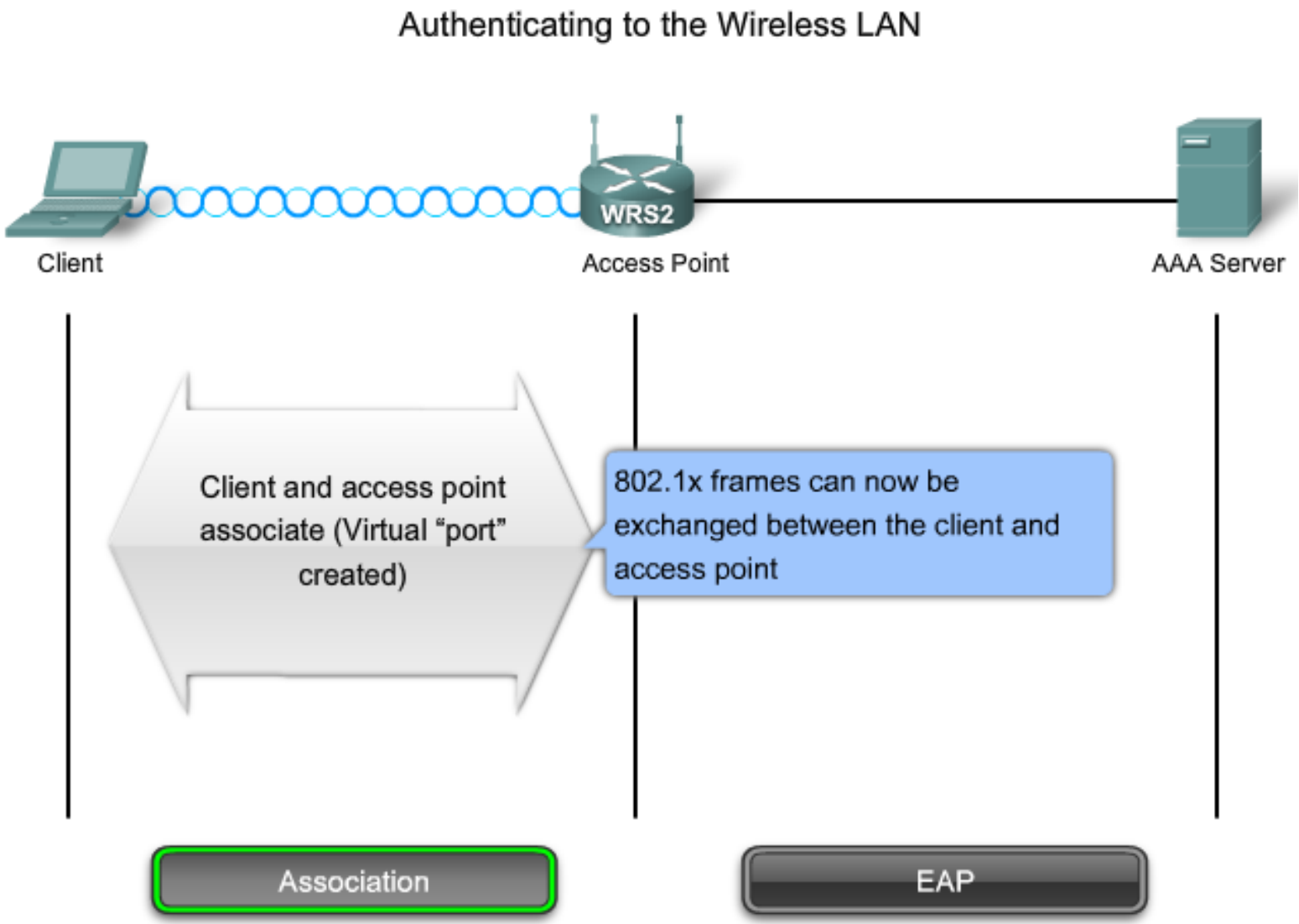
Décrypter le WEP ?

- Données M cryptées : C = (*M* || *ICV(M)*) XOR RC4(*IV* || *K*)
- Pour décrypter
  - Extraire le vecteur d'initialisation *IV* || *K*
  - Générer la même suite pseudo-aléatoire RC4(*IV* || *K*)
  - Faire le XOR entre C et RC4(*IV* || *K*)

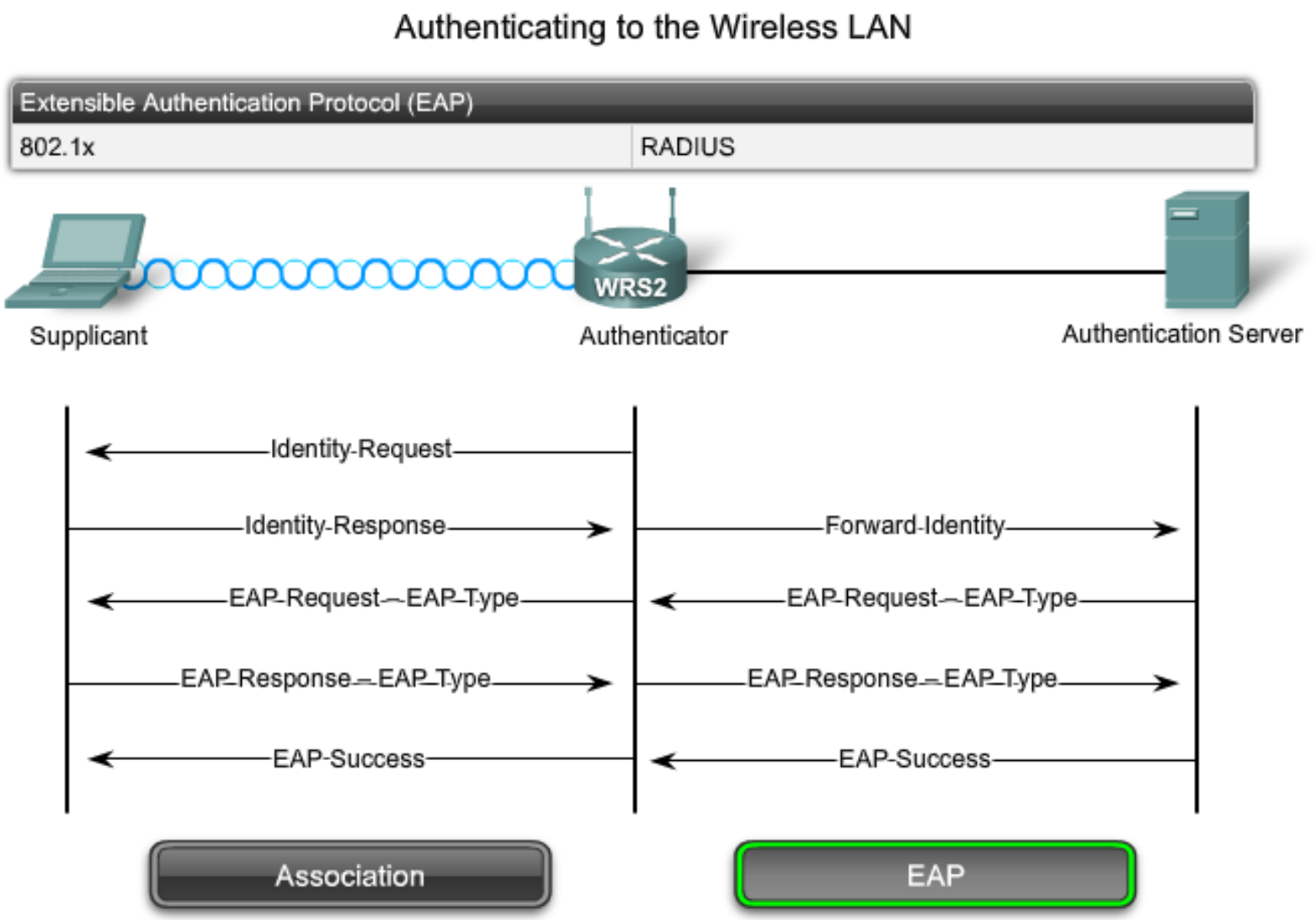
Le WEP est-il sûr ?

1. Fiabilité de la clé
   - Clé de 40 bits (soit 5 caractères)
     - nombre de combinaison peu important
   - Clé de 104 bits
     - La force brute n'est plus envisageable !
   - Mais ...
2. Le vecteur d'initialisation est envoyé en clair sur le réseau
3. Et entre 2 paquets codant 2 messages identiques
   - Seul le vecteur d'initialisation change
4. Or quand une collision survient, il faut ré-emettre le même message
5. Attendre les collisions permet d'avoir des informations sur la clé secrète

L'authentification par EAP – Etape 1/2



L'authentification par EAP – Etape 2/2



Temporal Key Integrity Protocol

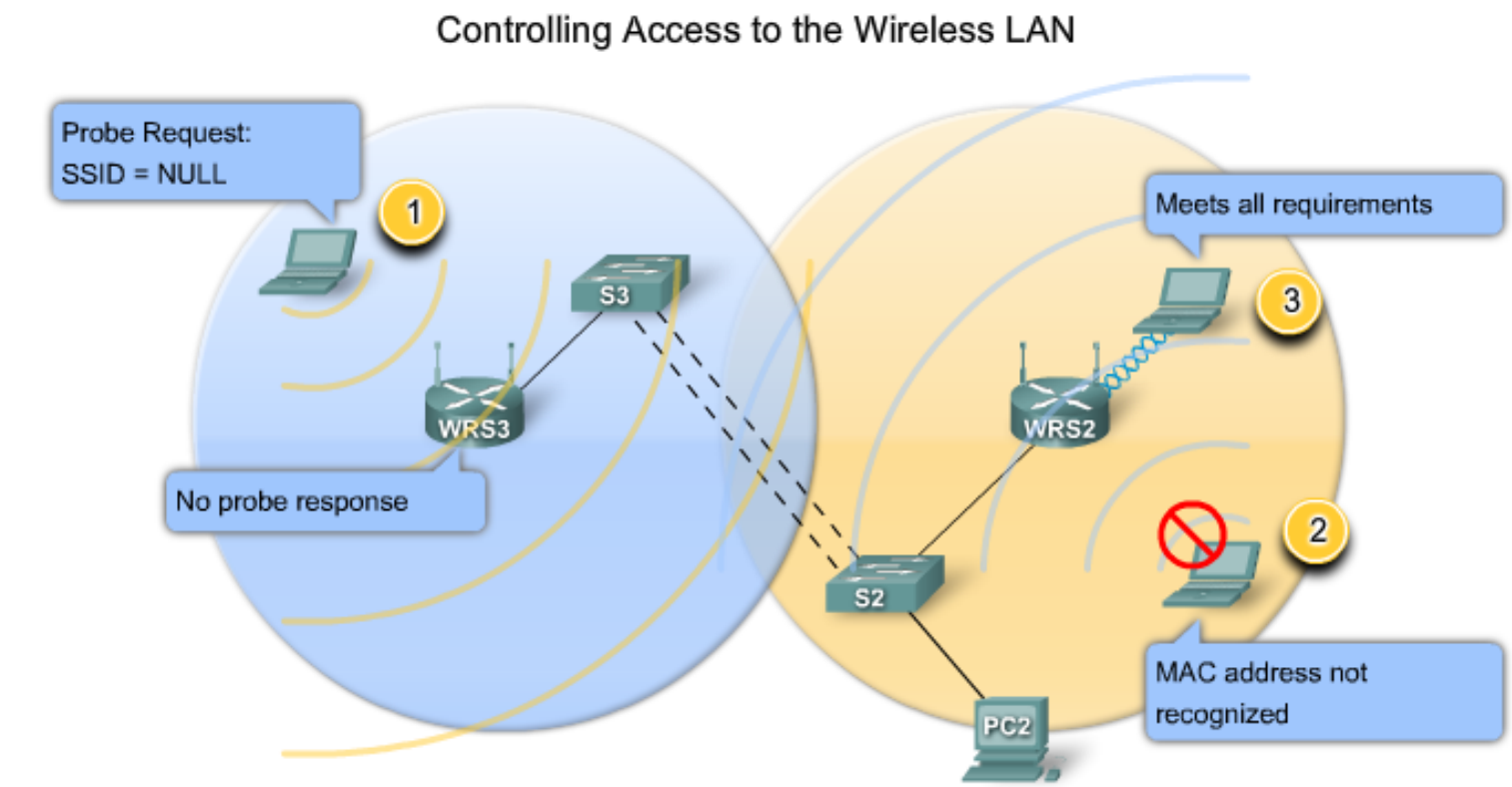
- TKIP est la première tentative de réponse aux problèmes du WEP
- Chaque station utilise la même clé, comme pour le WEP, à laquelle elle concatène leur adresse MAC
- Utilisation d'un IV de 6 octets au lieu de 4 dans le WEP
- Changement périodique de la clé, calculée à partir de la précédente

La cryptographie dans WPA et WPA2

- TKIP et AES sont des algorithmes cryptographiques recommandés dans la norme 802.11i
- TKIP est certifié pour WPA et AES pour WPA2
- A la place des termes WPA ou WPA2, il est possible de rencontrer les termes PSK ou PSK2 pour Pre-Shared Key
  - PSK ou PSK2 avec TKIP est équivalent à WPA
  - PSK ou PSK2 avec AES est équivalent à WPA2
  - PSK2, sans cryptographie est équivalent à WPA2

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Encrypts by adding increasingly complex bit coding to each packet • Based on same cipher (RC4) as WEP	• New cipher used in 802.11i • Based on TKIP with additional features that enhances the level of provided security

Que faire pour sécuriser mon WLAN ?



Methods for controlling wireless LAN access:

1. SSID broadcasts from access points are off
2. MAC Address filtering is enabled
3. WPA2 Security implemented

CAUTION: Neither items 1 or 2 are considered valid security measures