Académie Cisco
Reims
Champagne-Ardenne

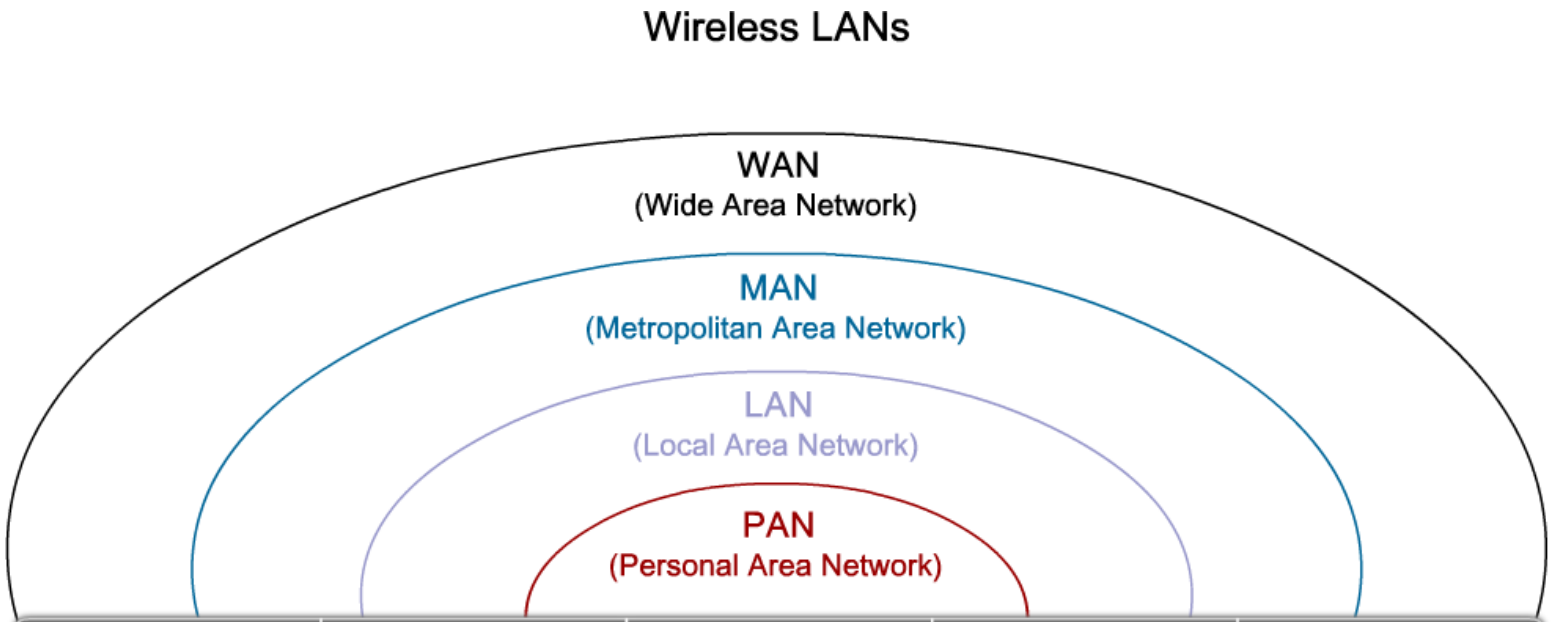
UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

Le Wireless

Le Wireless

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

Les normes

	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		Unconfirmed Possibly 2.4 and 5 GHz bands
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 248 Mbps for two MIMO streams
Pros	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Cons	October 1999	October 1999	June 2003		Expected in 2008
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		

- Pour le 802.11n, incompatibilité avec le 802.11b/g, version draft 3.0 en cours et certain annonce un finalisation pour 2009 !

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

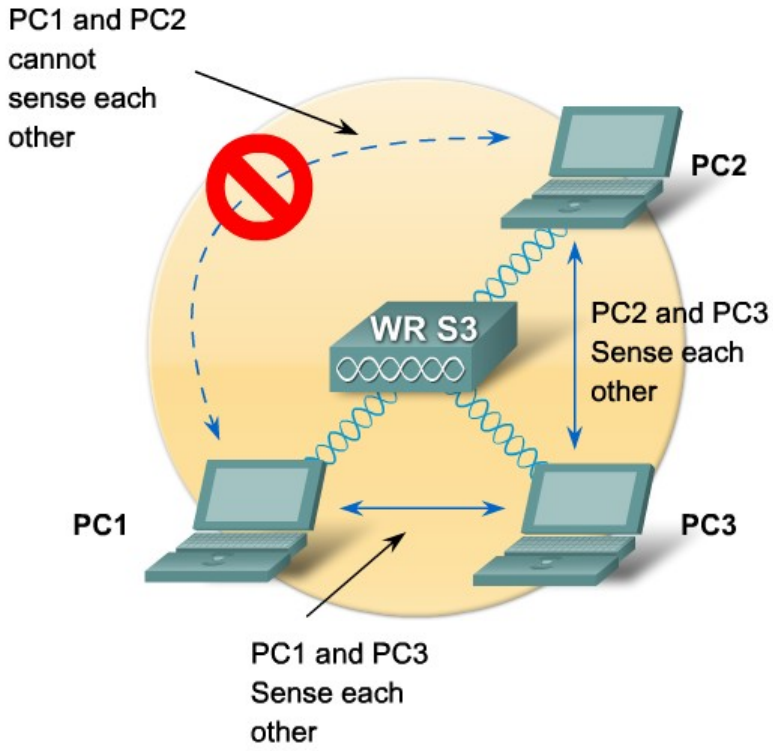
CSMA/CA ?

- 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.



La connexion ?

- En Wifi, 3 étapes
  - La recherche du point d'accès
  - L'authentification
    - En clair
    - Avec clé partagé
  - L'association

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

La cryptographie dans WPA et 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

- 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 de WPA ou WPA2, il est possible de rencontrer 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