

Wireless LAN (WLAN) Security

Iarno Pagliani

Cisco Certified CCNA, CCSP, NAC Specialist

HP Procurve Certified ASP, AIS, ASE, Master ASE Networking Security Specialist

iarno.pagliani@homeworks.it

Site: www.homeworks.it

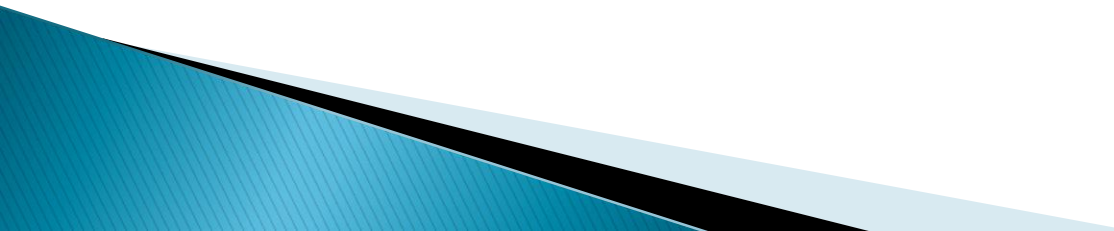
Agenda

Wireless LAN Concepts

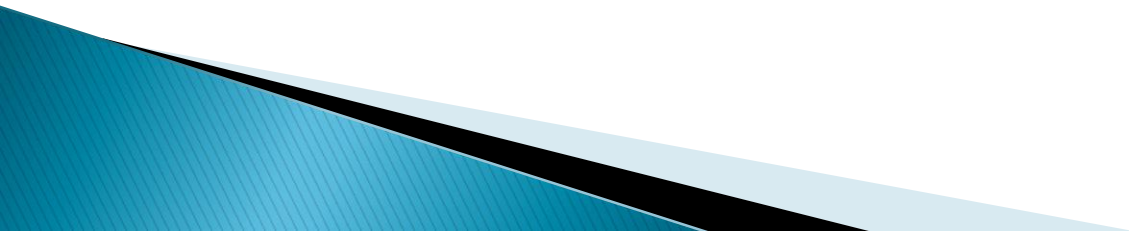
Wireless LAN Security

Wireless Design

Lab

A decorative graphic element in the bottom-left corner of the slide, consisting of overlapping blue and black geometric shapes.

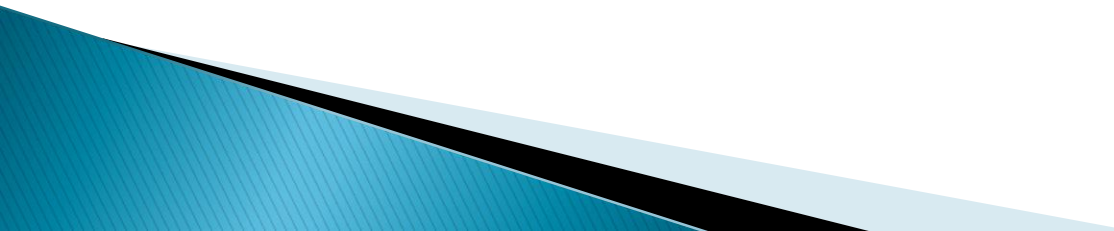
Wireless LAN Concepts



Wireless LAN (WLAN)

- ▶ WLAN è un tipo di LAN che usa le onde radio per comunicare, fornendo mobilità agli utenti di rete come se fossero utenti wired.
- ▶ IEEE fornisce gli standard di security per le reti wireless divisi in due principali componenti:
 - encryption
 - authentication

Radio Waves

- ▶ Access points (AP).
 - ▶ WLAN usa “spread-spectrum” basata su onde radio per far comunicare devices a distanza limitata BSS (basic service set).
 - ▶ Onde Radio non richiedono un allineamento del segnale fra sender e receiver
 - ▶ La trasmissione può essere propagata anche a destinatari non desiderati
- 

WLAN Components

- ▶ **Wireless Access Point**
- ▶ **Wireless Network Card (NIC)**
- ▶ **Wireless bridge**
- ▶ **Antenna**
 - **Wireless Controller**
 - **Management Station**
 - **Wireless IDS/IPS**



WLAN Components

- ▶ Ad hoc (Device-to-Device).
- ▶ Infrastructure (Device-to-AP).
 - Ogni Frame è mandata al solo AP
 - service set: Basic Service Set
 - service set: Extended Service Set ESS
 - più access point
 - più celle
 - maggior funzionalità (roaming)

IEEE Protocol Standards

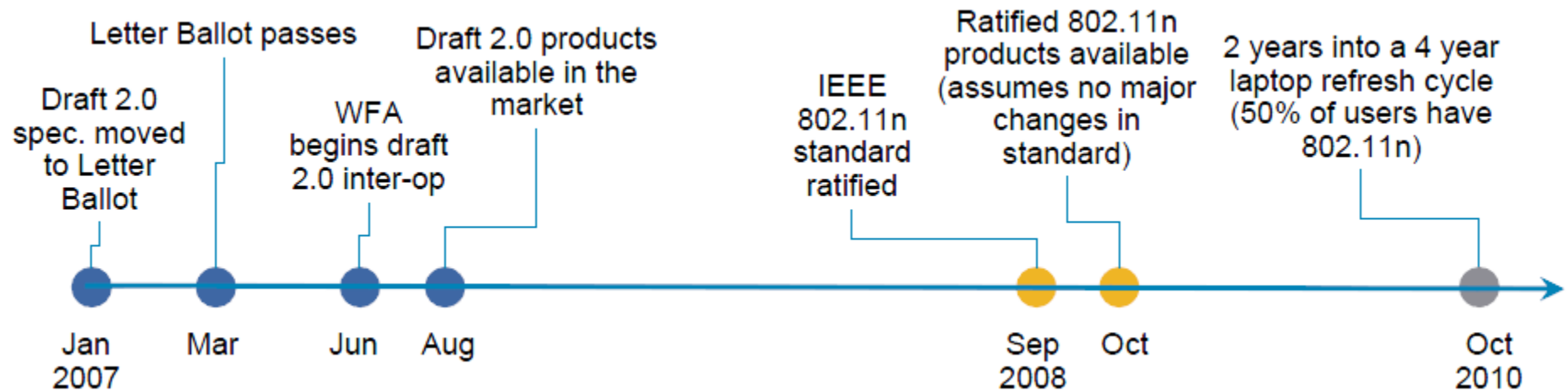
- ▶ IEEE 802.11 (Definito nel 1997)
- ▶ IEEE 802.11a (Definito nel 1999)
- ▶ IEEE 802.11b (Definito nel 1999)
- ▶ IEEE 802.11g (Definito nel 2003)
- ▶ IEEE 802.11n (Definito nel 2010)
- ▶ L'802.11a utilizza la banda ISM dei 5,4 GHz.
 - Tuttavia non risponde alla normativa europea ETSI EN 301 893[1] che prevede DFS (Dynamic Frequency Selection), TPC (Transmit Power Control) e radar meteorologici; tale normativa di armonizzazione europea è valida in Italia su indicazione del Ministero delle Comunicazioni con il decreto ministeriale del 10 gennaio 2005.
 - Per ovviare al problema in Europa è stato introdotto il protocollo 802.11h



Radio Frequency (RF)

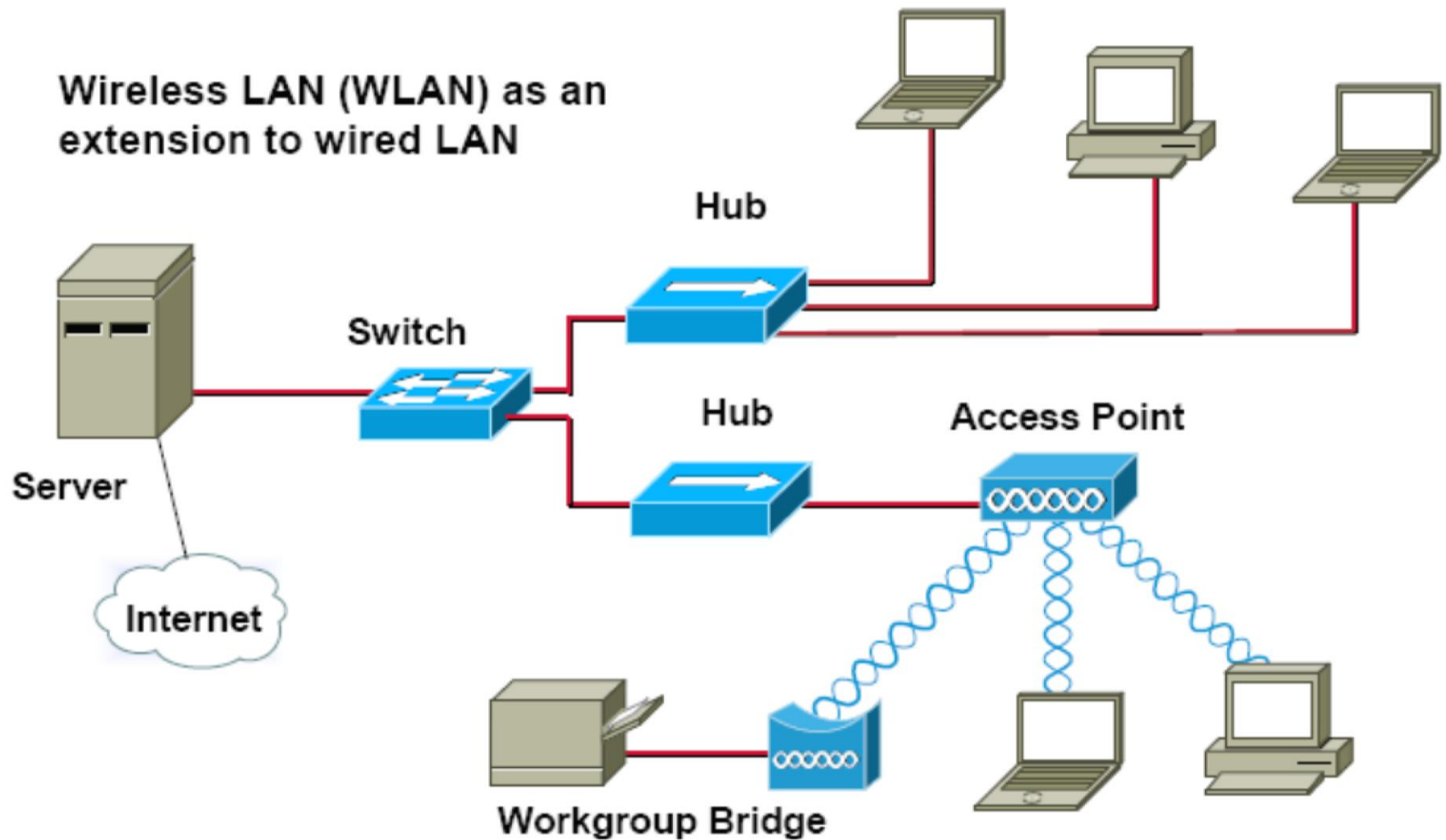
- ▶ Lo standard 802.11 utilizza le seguenti bande RF:
 - 2.4-GHz, 802.11 e 802.11b networks, (data rates da 1 a 2 Mbps e 11Mbps)
 - 2.4-GHz, 802.11g data rates fino a 54 Mbps
 - 5.4-GHz 802.11a data rates da 5 Mbps, 11 Mbps, e fino 54 Mbps.
 - 802.11n standard usa 2.4-GHz o 5.4-GHz data rates fino a 540 Mbps

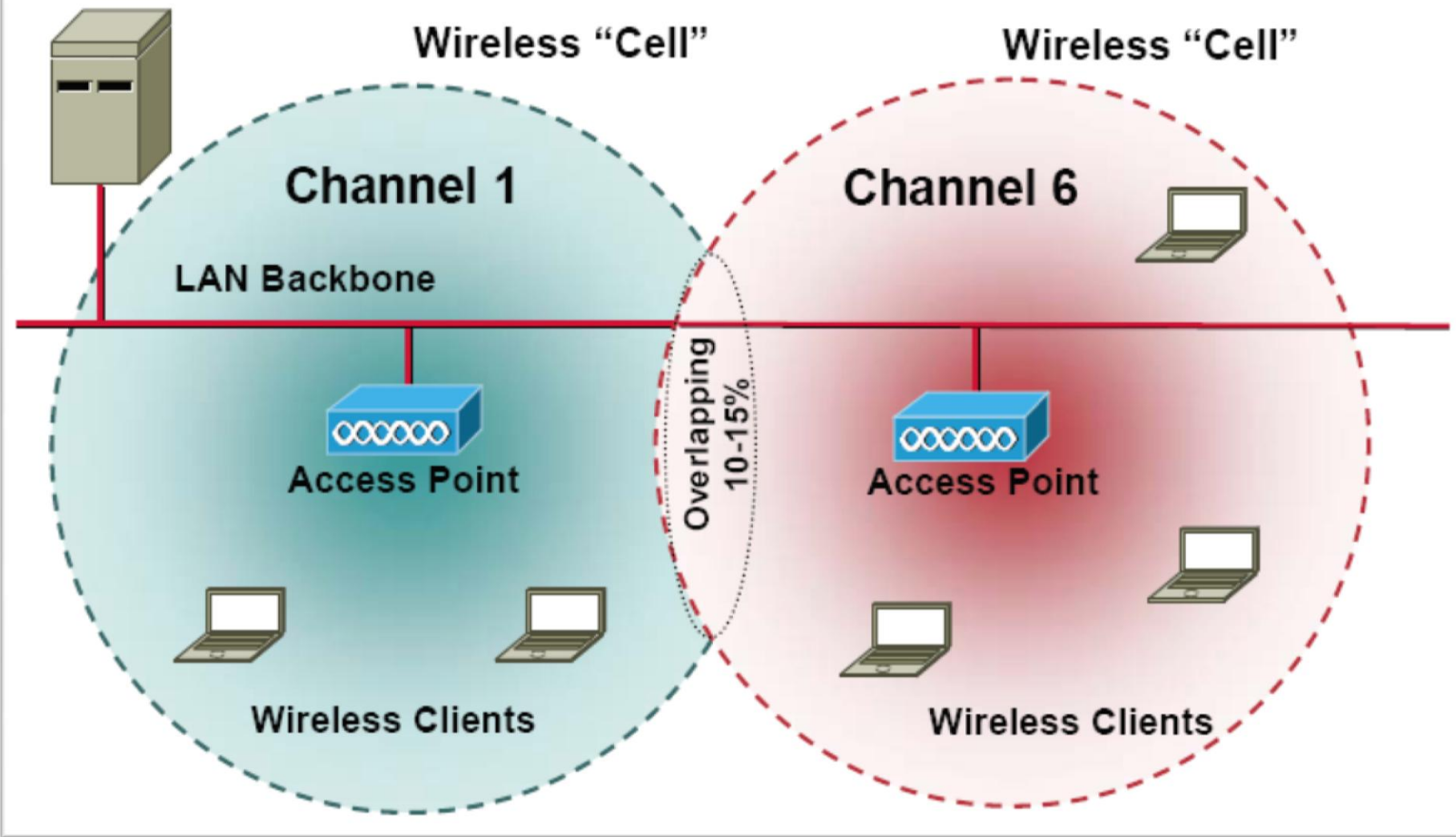
802.11n Next Generation Wireless



La versione definitiva dello standard è stata approvata l'11 settembre 2009 e la pubblicazione è prevista per l'inizio del 2010.

Wireless LAN (WLAN) as an extension to wired LAN





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

- ▶ 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

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)

- ▶ 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

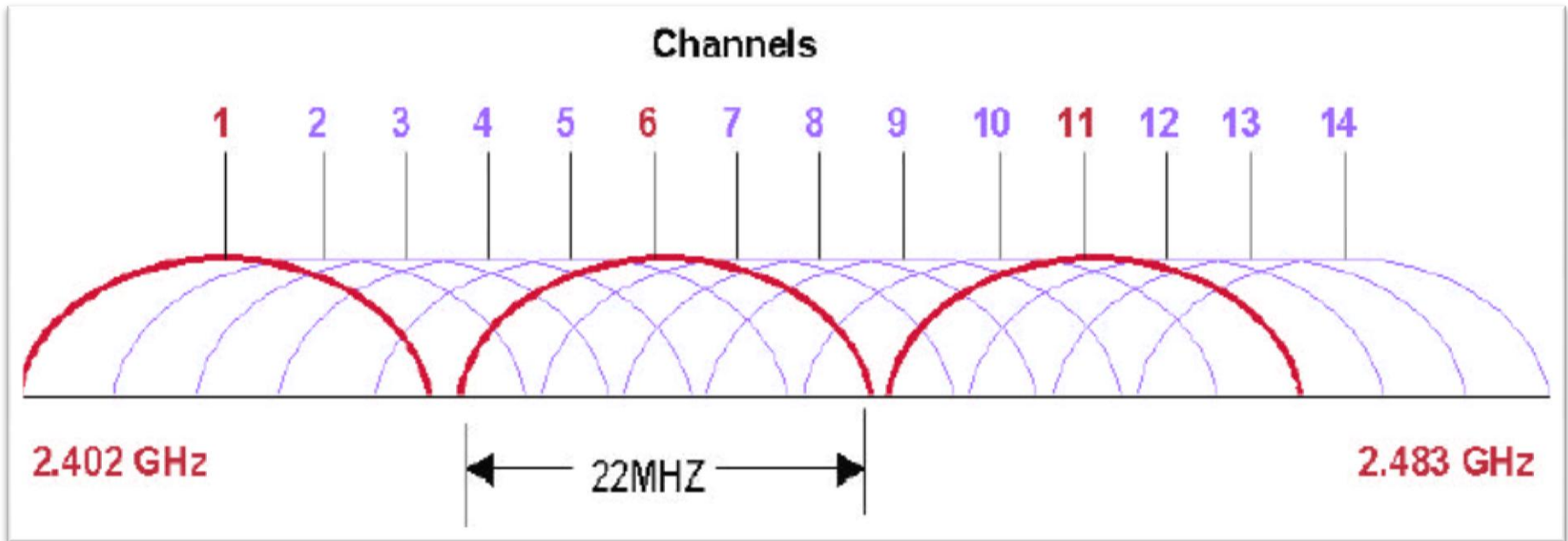
Wireless Trasmission (Layer1)

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

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 Transmission (Layer1)



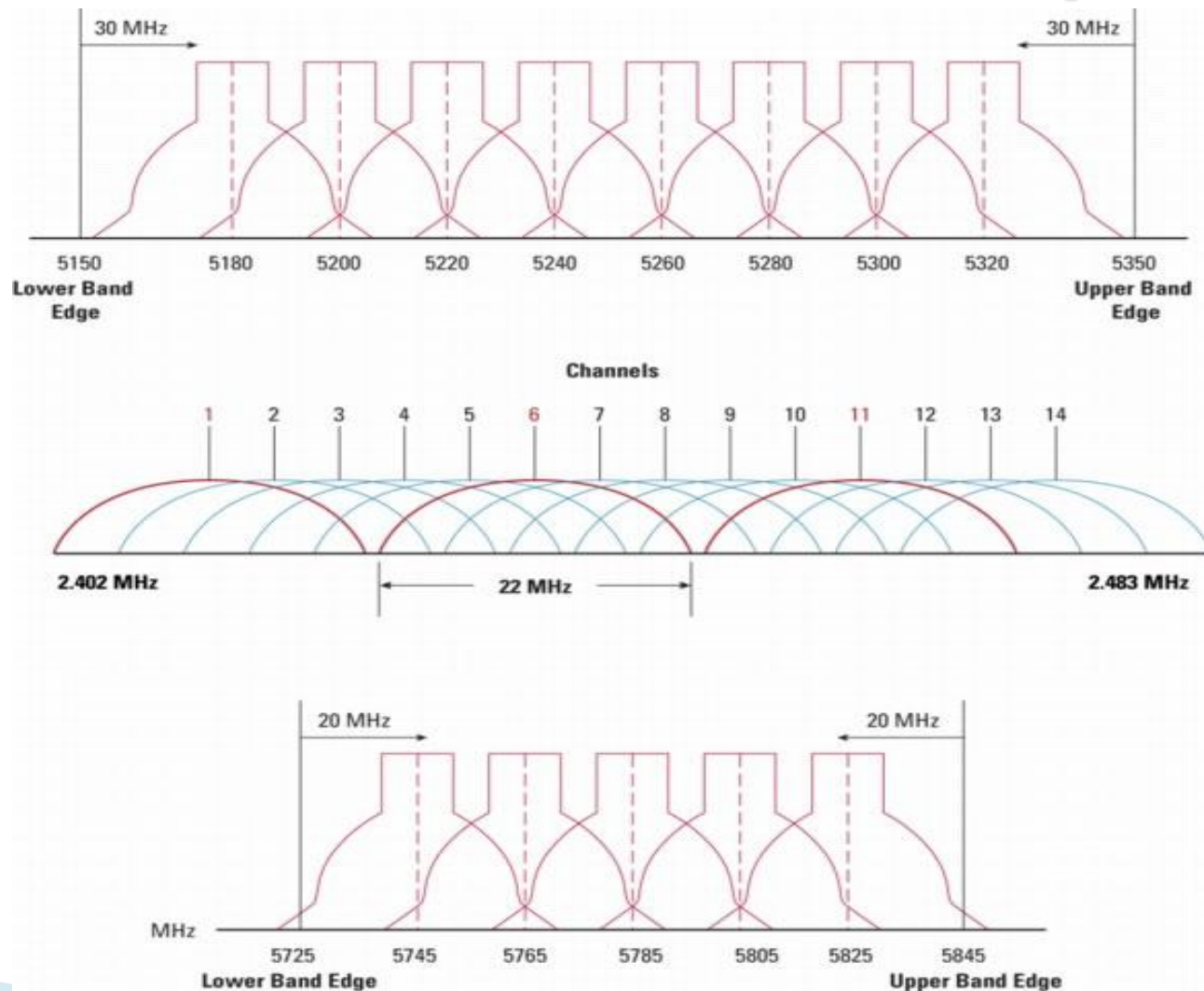
North American

- 11 channels – each channel 22 MHz wide
- Three nonoverlapping channels

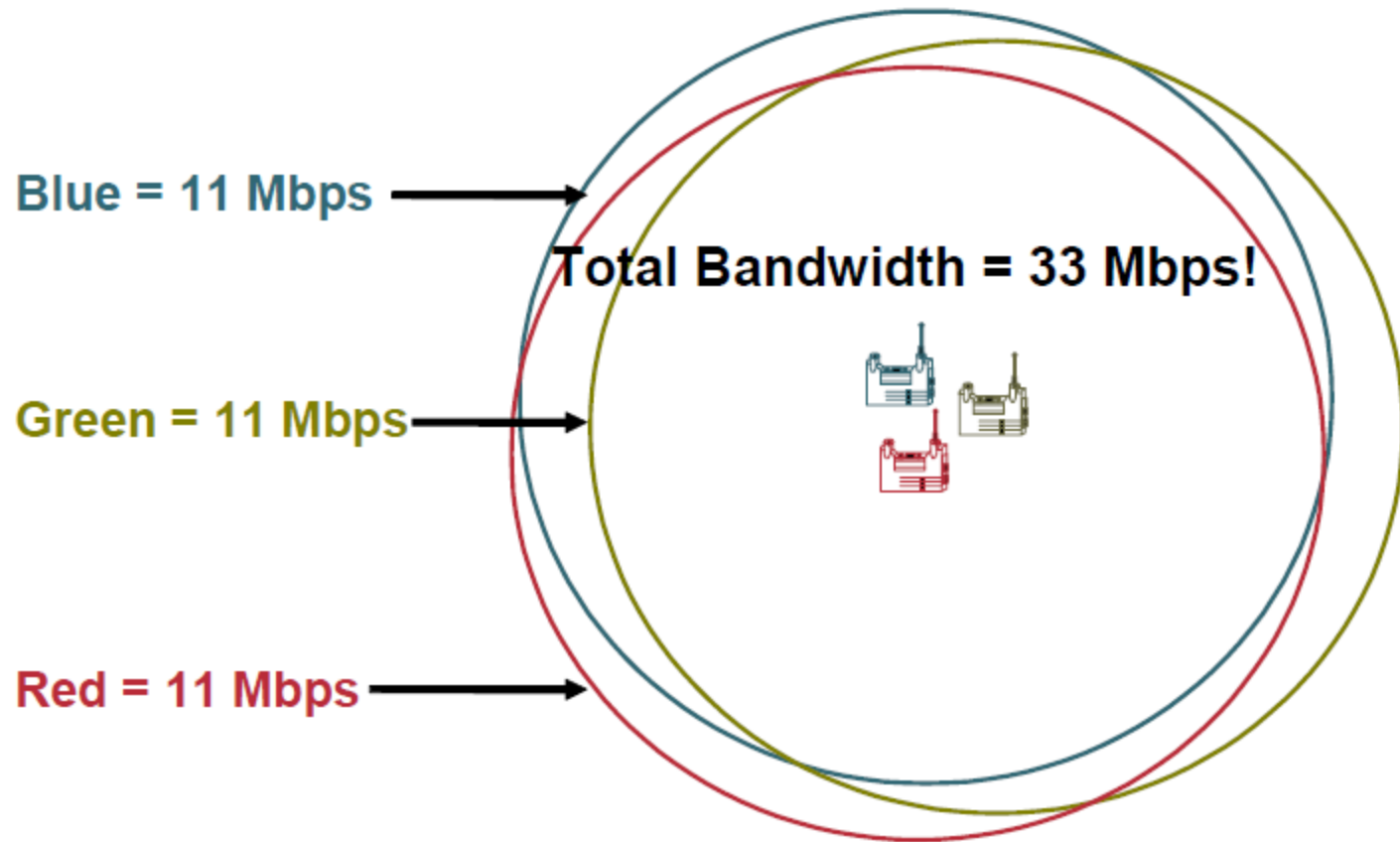
ETSI

- 13 channels – each channel 22 MHz wide
- Still only three nonoverlapping channels
- Three access points can occupy same area

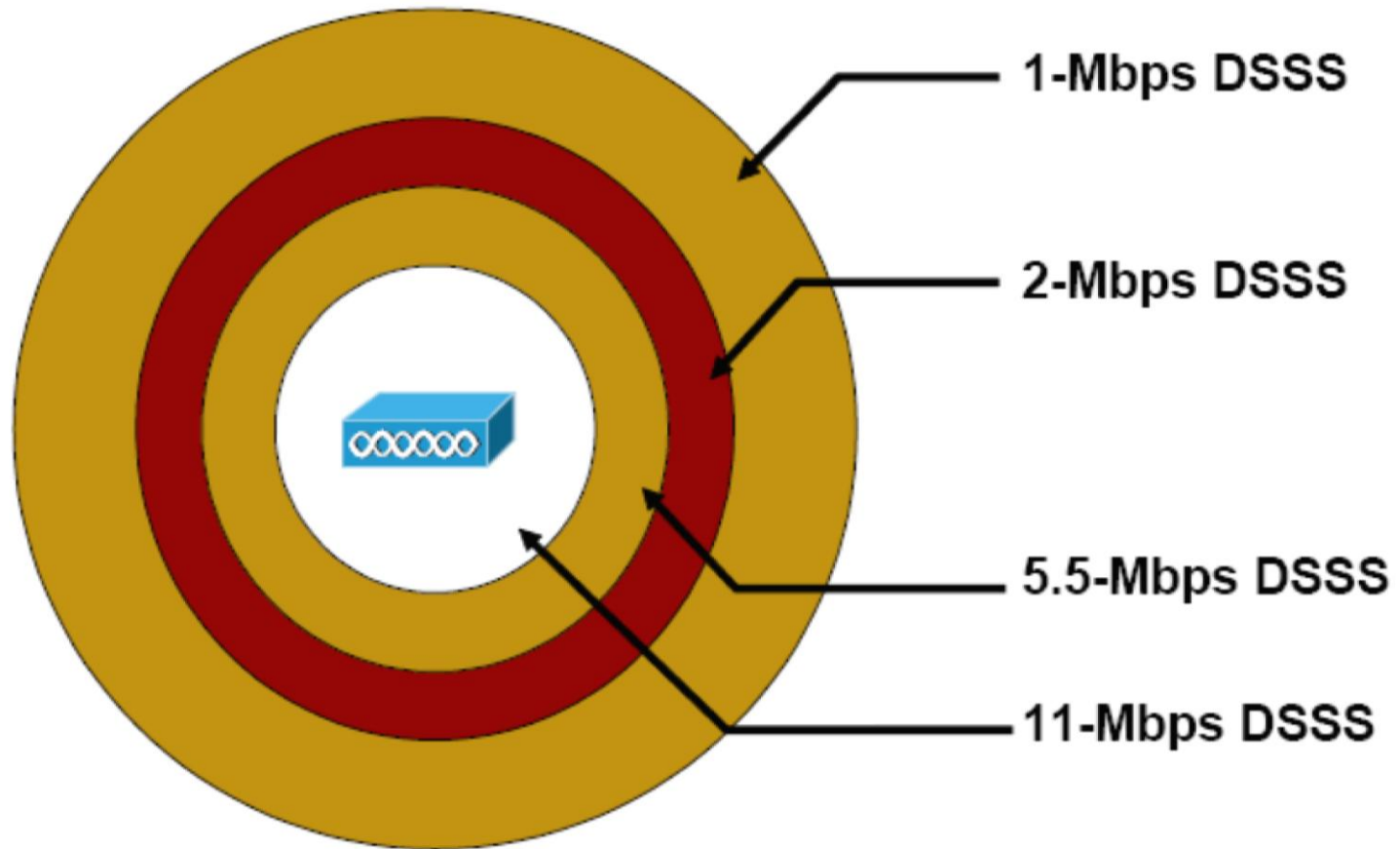
Wireless Transmission (Layer1)



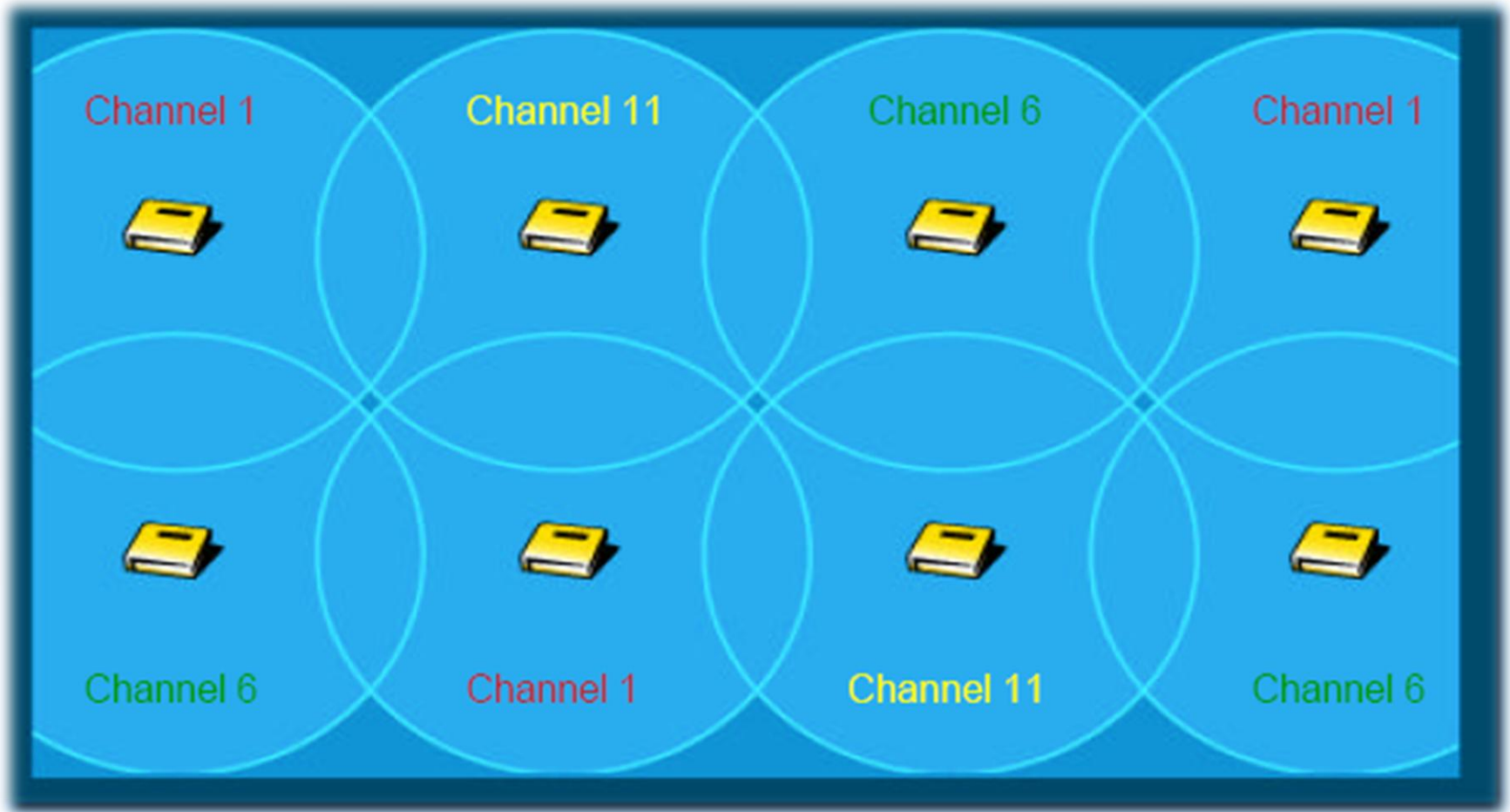
Wireless Transmission (Layer1)



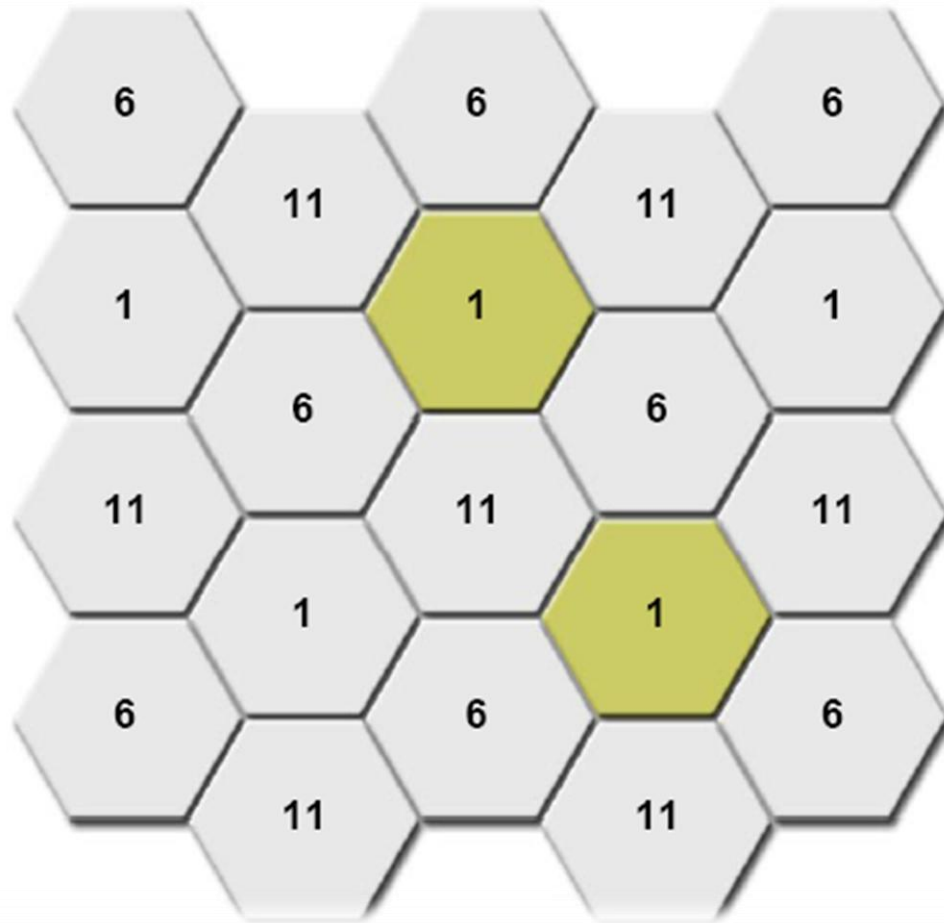
Wireless Transmission (Layer1)



Wireless Transmission (Layer1)



Wireless Transmission (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

Proprietary-
900MHz/2.4GHz

802.11 Standard
2.4GHz 2Mb DSSS

IEEE 802.11
Ratified

IEEE 802.11a/b
Ratified

802.11b Standard
2.4 GHz – DSSS
11Mbps

802.11a Standard
5 GHz – OFDM
54Mbps

802.11g
2.4 GHz – OFDM
54Mbps

1997

1999

2000

2001

2002

2003

Wireless Transmission (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.

MIMO Technology (Multiple Input Multiple 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 Technology

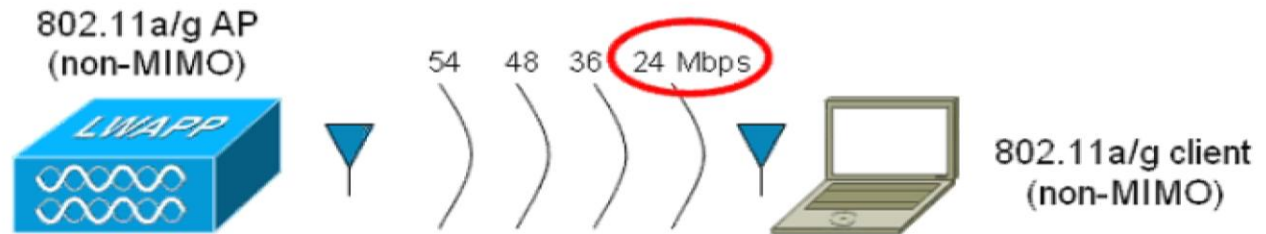
- SPATIAL MULTIPLEXING (SM)
 - Funziona solo per apparati 802.11n (AP e MIMO client)
 - Trasmetto 3x3 con la stessa modulazione e lo stesso canale.
 - 65Mbps x 3
 - Aumento SNR
- TRANSMIT BEAM FORMING (TBF)
 - AP è 802.11n ma i client no
 - Ottengo ugualmente dei vantaggi trasmettendo sulle 3 antenne, ho maggior potenza e migliora la copertura.
 - Diminuiscono ritrasmissioni

MIMO Technology

- 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 Technology

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



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



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



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 prestazioni ma permetterà la migrazione)
- Green Field
 - no a,b,g



802.11n PHYSICAL LAYER

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

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

SPECTRAL EFFICIENCY

- Rapporto Mbps/Hz è indice di efficienza per la trasmissione di dati (bit riesco a trasmettere per Hz)
- 802.11b 11Mbps/22Mhz $\rightarrow$ 1/2 bits per Herz
- 802.11n 54Mbps/20Mhz $\rightarrow$ 2.7 bits per Herz
- 802.11n migliora l'efficienza spettrale

CHANNEL-BONDING

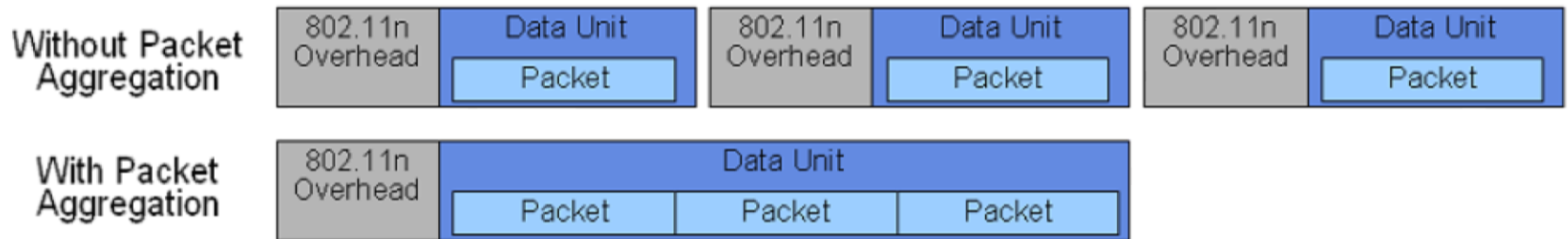
- Combino 2 canali adiacenti 2x20Mhz e miglioro l'utilizzo diminuendo lo scarto di interferenza
- Sulla banda a 5Ghz posso aggregare più canali
- fino a 12; nella banda a 2.4Ghz massimo 3 (poco consigliata e non sempre supportata: Intel 4965AGN)

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"

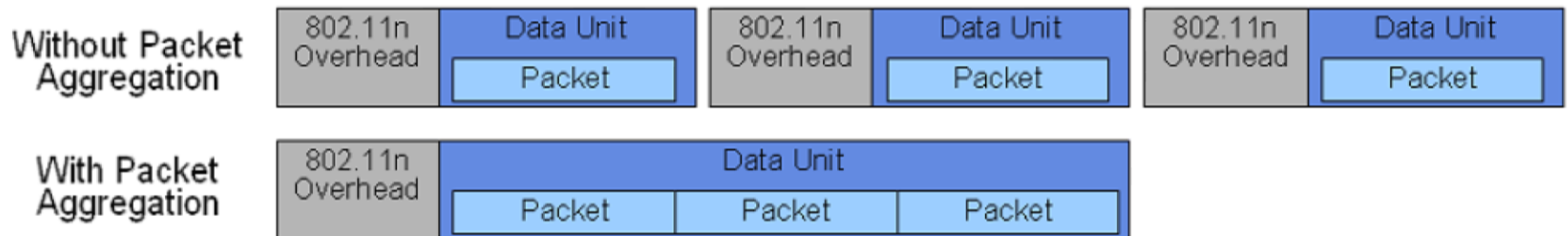
802.11n MAC LAYER

- 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



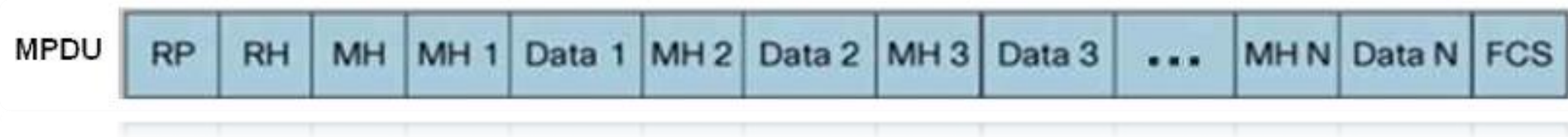
802.11n MAC LAYER

- 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



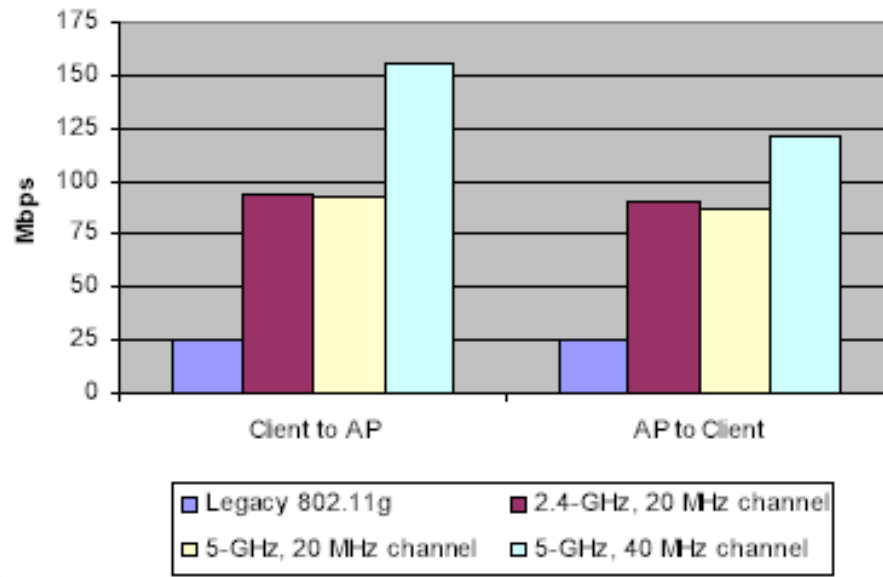
802.11n MAC LAYER

- 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

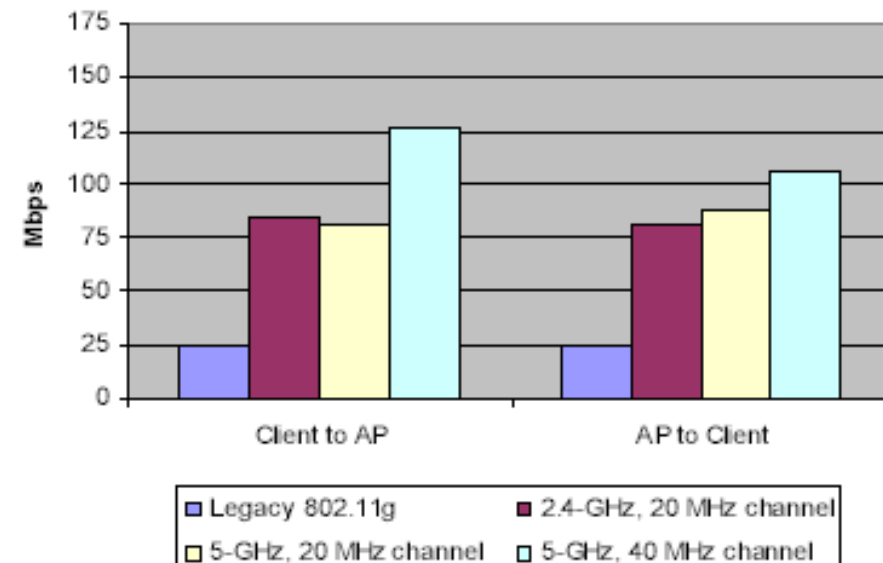


Throughput 802.11n

UDP Throughput



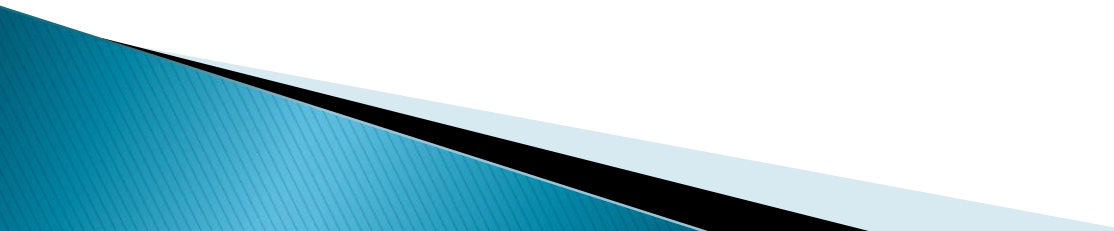
TCP Throughput



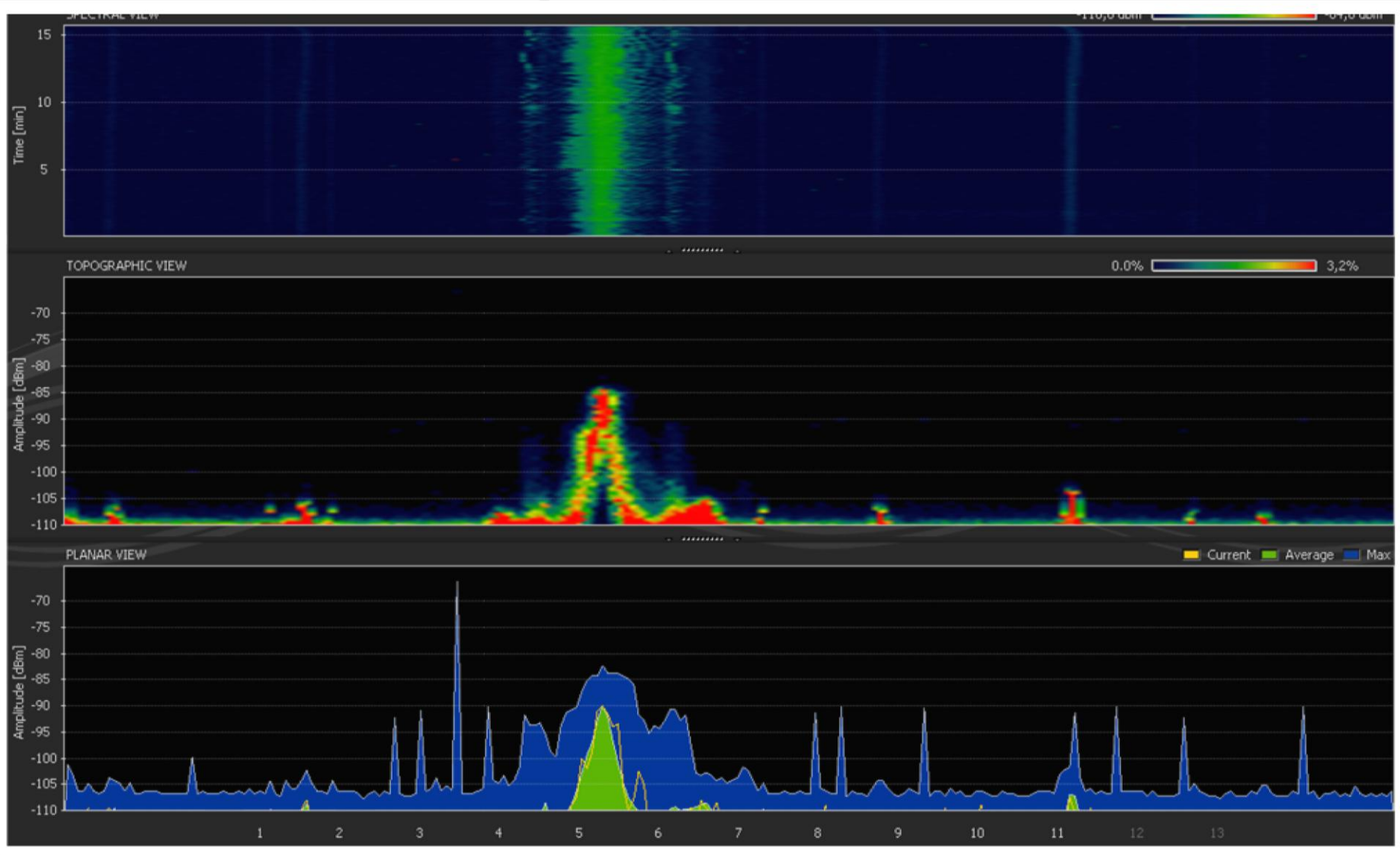
Wireless Trasmission (Layer1)

- ▶ 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.

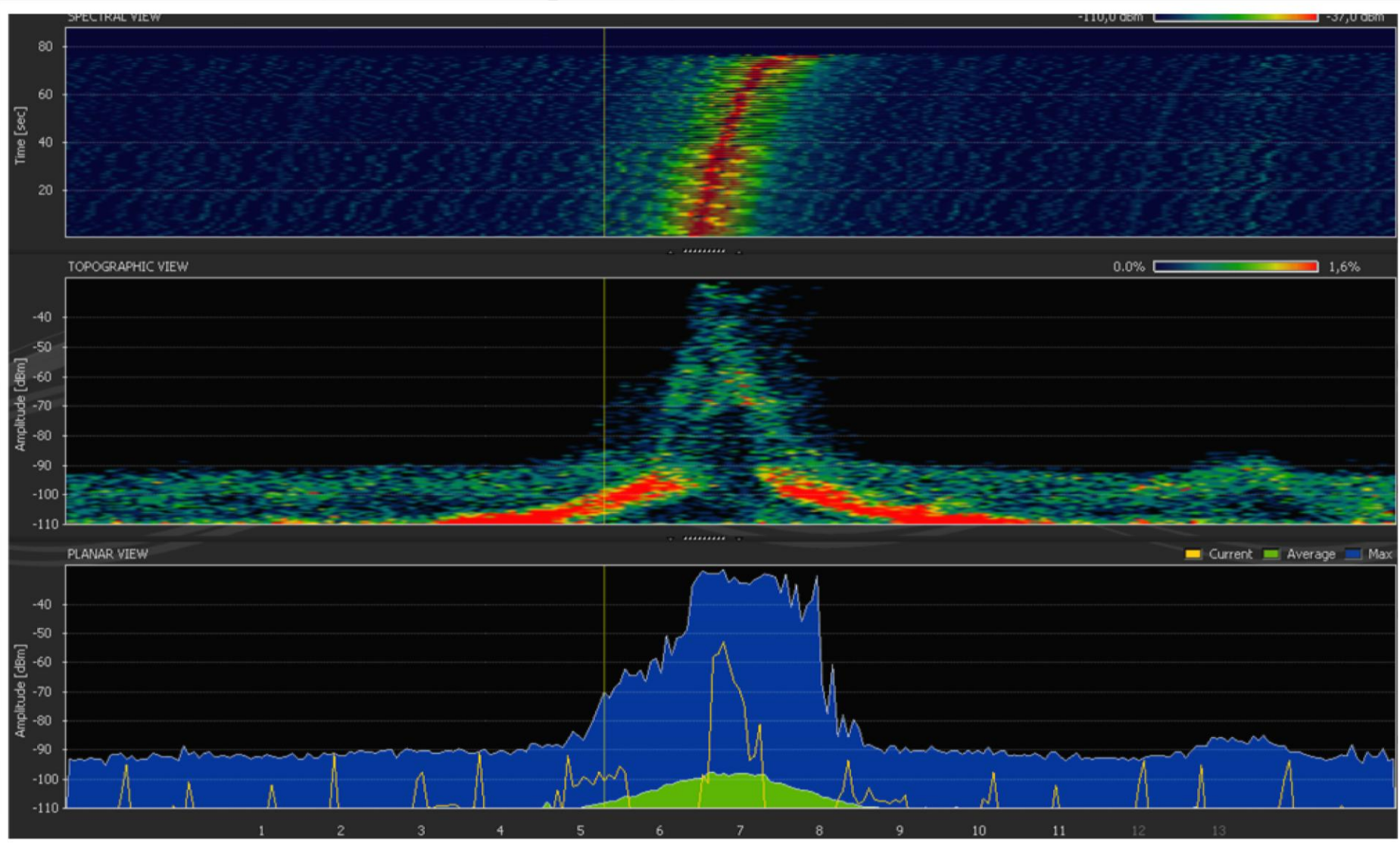
Site Survey

- ▶ Il primo passo per il deployment di una rete wireless
 - ▶ Capire eventuali problemi di comportamento o copertura delle RF
 - ▶ Tools (es. analizzatore di spettro)
- 

Tool (esempio) WI.SPY



Tool (esempio) WI.SPY

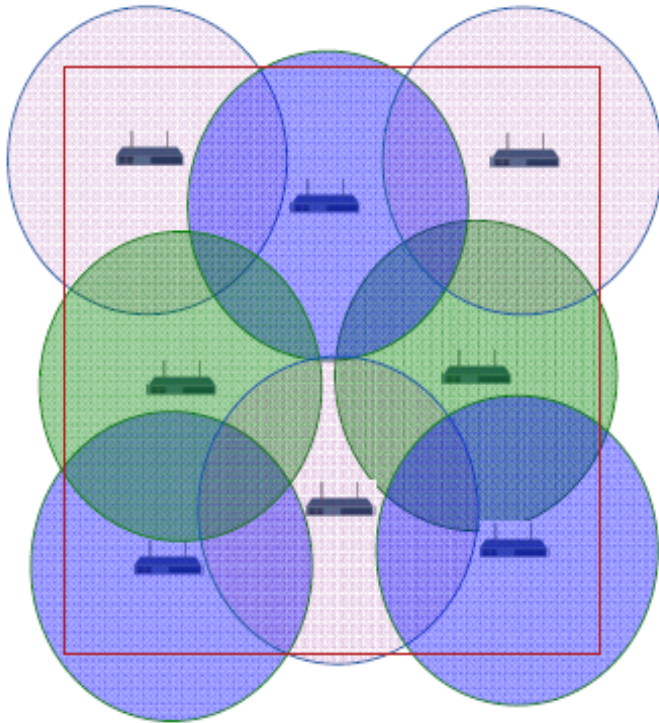


Wireless Transmission (Layer1)

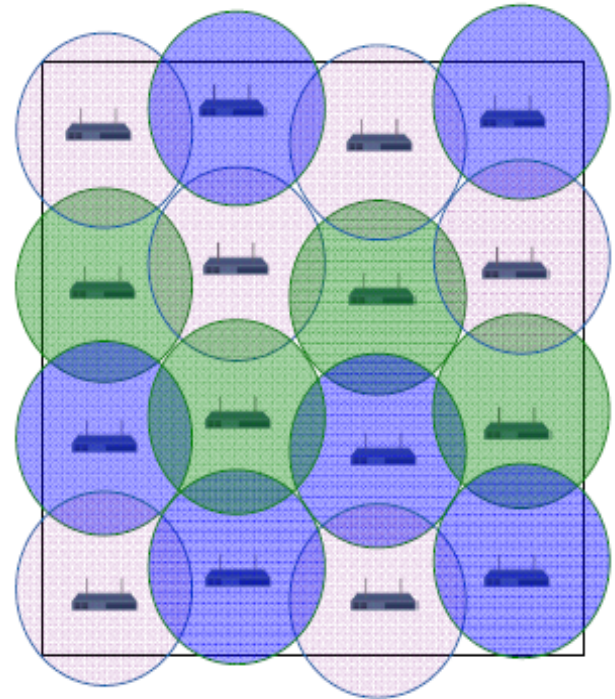
Data Rate (Mbps)	Data Cell		WIPT Cell	
	Minimum Cell Edge Signal Strength	Minimum SNR	Minimum Cell Edge Signal Strength	Minimum SNR
54	-71	25	—	—
36	-73	18	—	—
24	-77	12	—	—
12 or 11	-82	10	-67	25
6 or 5.5	-89	8	-74	23
2	-91	6	-76	21
1	-94	4	-79	19

WIPT-> per Wireless IP telephony

Wireless Transmission (Layer1)



Coverage Model



Voice Model

Wireless Trasmission (Layer1)

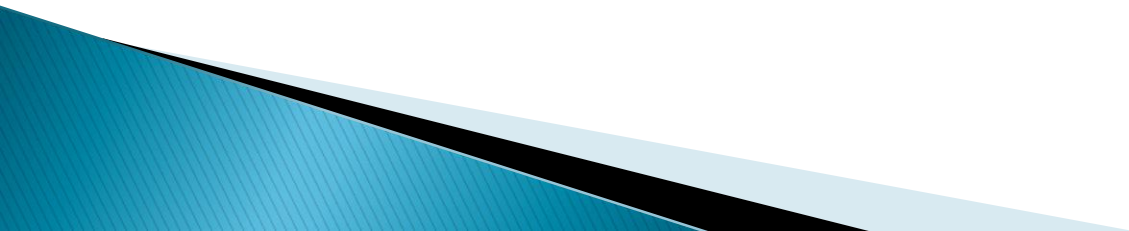
► Copertura, Velocità e Capacità

◦ Trasmissione 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:
 - $-3\text{dBm} = 1/2$ potenza
 - $+3\text{dBm} = *1/2$ potenza
 - $-10\text{dBm} = 1/10$ potenza
 - $+10\text{dBm} = *10$ potenza

- ## ► In generale frequenza maggiore = maggiore invio dei dati ma < copertura -> + AP

Network Stumbler

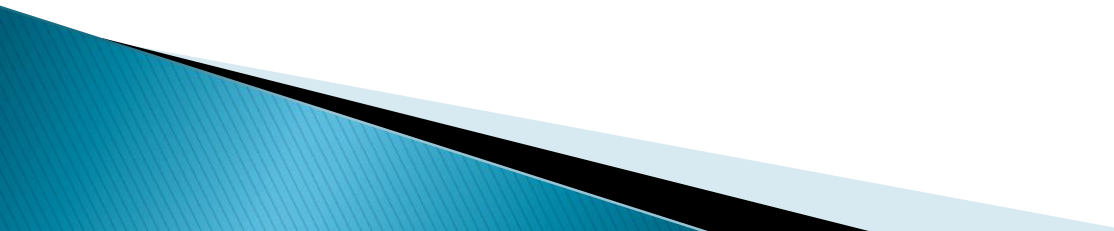


WLAN Security

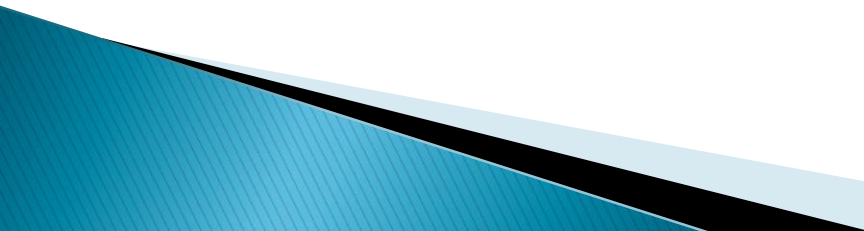
WLAN Security

- ▶ Security nelle reti WLAN significa:
 - **Authentication:** Meccanismi di “Strong authentication” imponendo una politica di controllo di accesso per consentire agli utenti autorizzati di connettersi rete wireless
 - **Encryption:** Data encryption, aiuta a garantire che solo i destinatari autorizzati siano in grado di capire i dati trasmessi fra due componenti principali

Features and technologies are available to secure WLAN networks

- ▶ Service Set Identifiers (SSID)
 - ▶ MAC authentication
 - ▶ Client Authentication (Open e Shared Key)
 - ▶ Static WEP
 - ▶ WPA, WPA2, and 802.11i (WEP enhancements)
 - ▶ 802.1x and EAP
 - ▶ WLAN NAC
 - ▶ WLAN IPS
 - ▶ VPN IPsec
- 

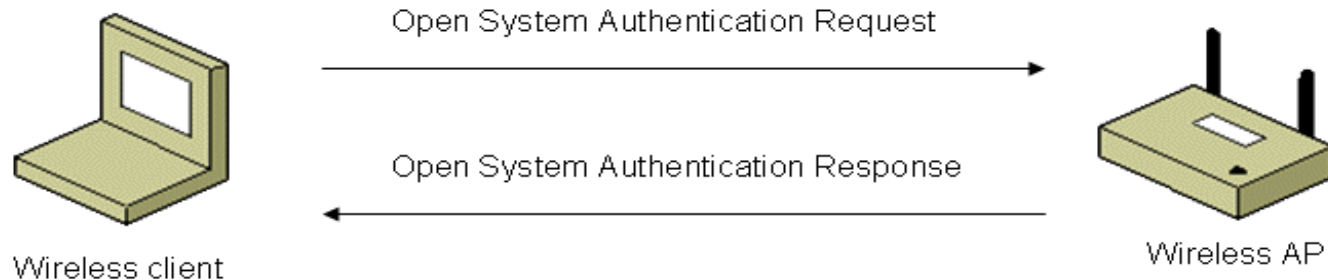
Service Set Identifiers (SSID)

- ▶ SSID è un ID arbitrario che identifica il nome di una rete wireless.
 - ▶ SSID fornisce l'accesso di base ai meccanismi di controllo.
 - ▶ SSID, anche se non è progettato per essere usato come un meccanismo di sicurezza, può impedire l'accesso non autorizzato ai clienti.
 - ▶ Per default, un AP invia un SSID in broadcast in plain text, la disattivazione della trasmissione di un SSID, può impedire la connessione alla rete inavvertitamente.
- 

MAC authentication

- ▶ Un'altra caratteristica comune è l'uso di indirizzi MAC per l'autenticazione.
 - L' AP verifica l'indirizzo MAC del client verificando un elenco di indirizzi a configurato localmente o centralizzato in un server di autenticazione esterno
 - E' molto semplice da configurare ma altrettanto vulnerabile (MAC spoofing)

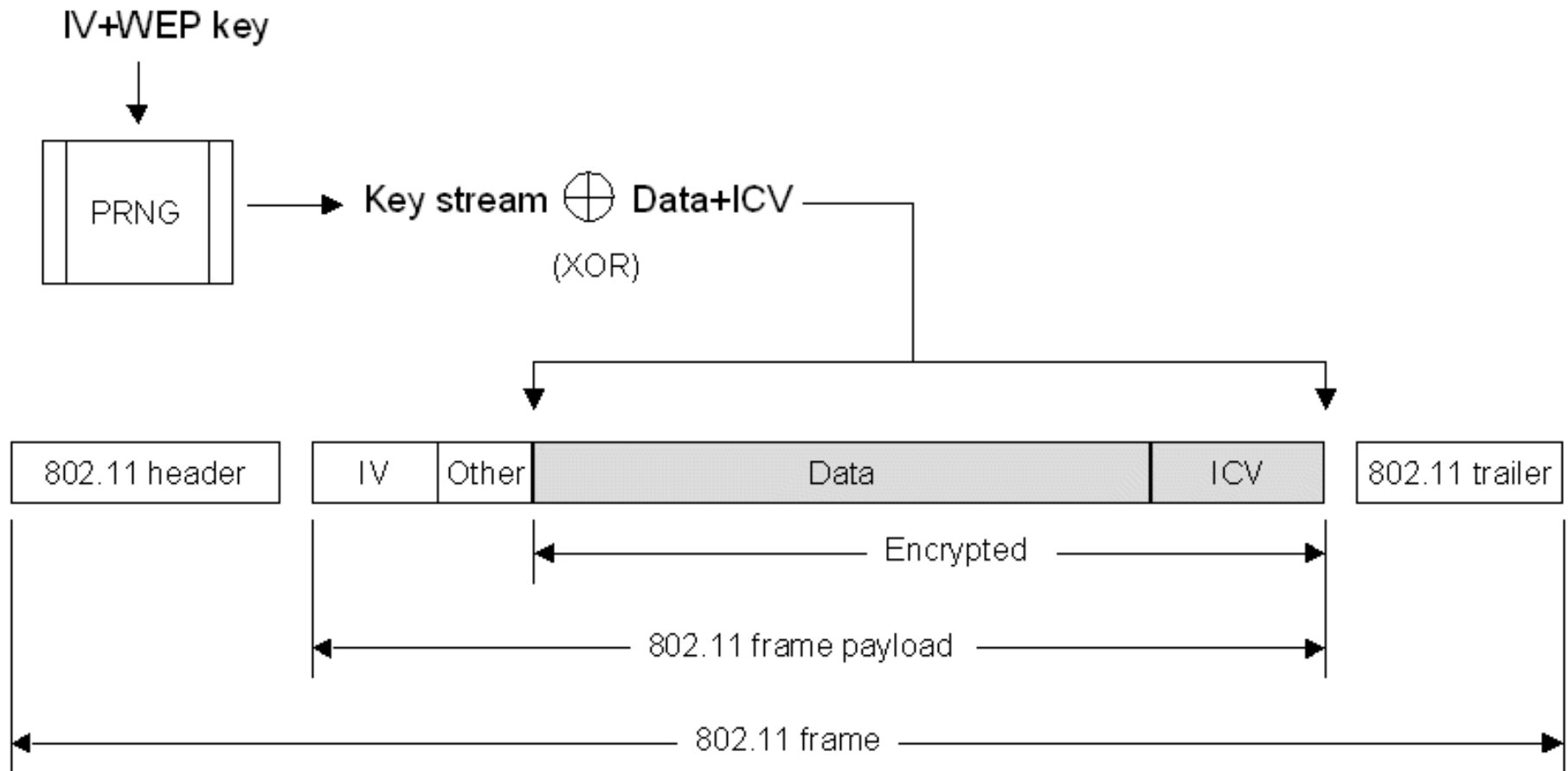
Client Authentication (Open e Shared Key)



Static Wired Equivalent Privacy (WEP)

- ▶ Una WEP key statica è composta da 40 o 128 bits.
- ▶ Non è molto scalabile
- ▶ Algoritmo violato !!!!

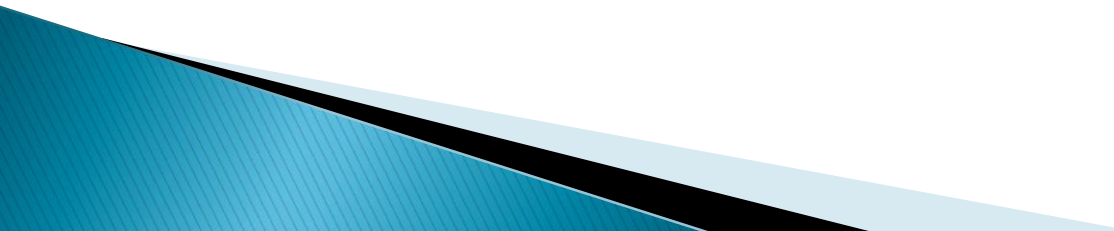
Static Wired Equivalent Privacy (WEP)



802.11i (WEP enhancements)

- ▶ Per ovviare ai problemi WEP fu introdotto 802.11i:
 - Temporal Key Integrity Protocol (TKIP)
 - Advanced Encryption Standard (AES-CCMP)

WPA e WPA2



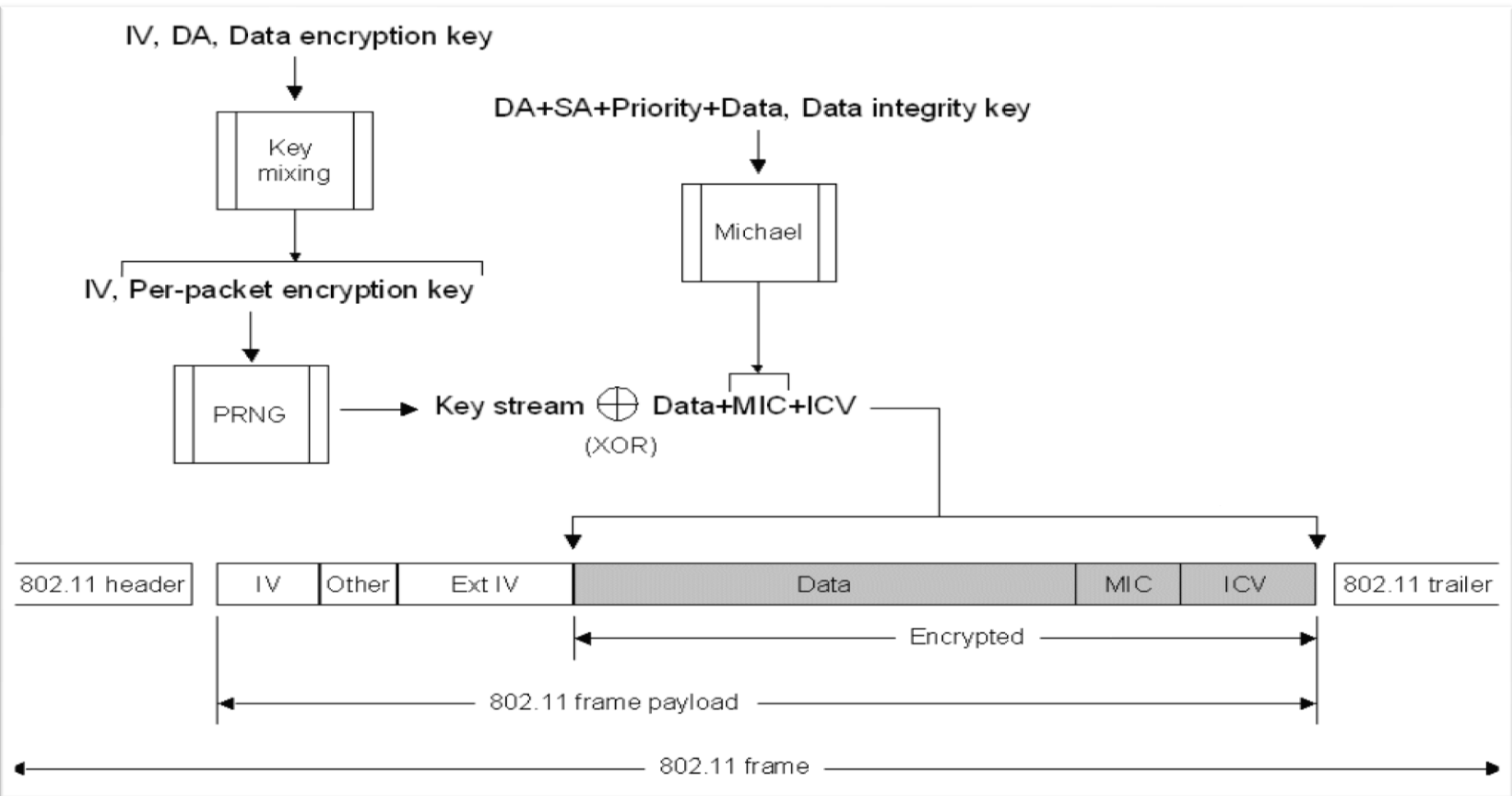
802.11i (WEP enhancements)

- ▶ WPA e WPA2 hanno due modi per operare
 - Personal Mode
 - Preshared key configurata manualmente
 - Destinata per ambienti Small Office Home Office (SOHO)
 - Enterprise Mode
 - Utilizza IEEE 802.1x/EAP
 - Un server radius AAA
 - La gestione dell' autenticazione, delle chiavi e delle credenziali è centralizzata

802.11i (WEP enhancements)

- ▶ Personal Mode (Recommended for SOHO, Home/Personal)
 - ▶ Authentication: PSK Encryption: TKIP/MIC
 - ▶ Authentication: PSK Encryption: AES-CCMP
- ▶ Enterprise Mode (Recommended for Business, Government, Education)
 - ▶ Authentication: IEEE 802.1x/EAP Encryption: TKIP/MIC
 - ▶ Authentication: IEEE 802.1x/EAP Encryption: AES-CCMP

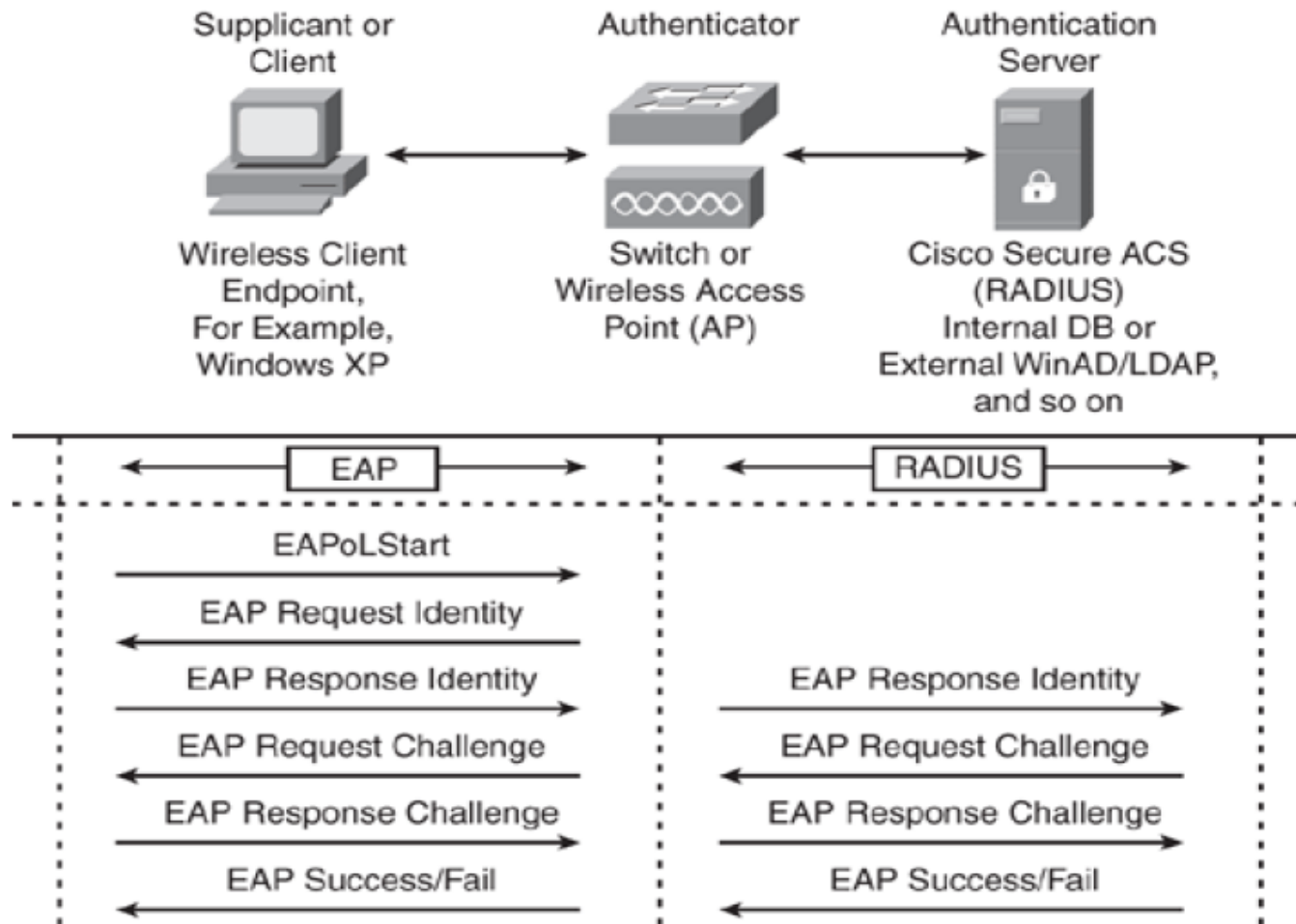
WPA



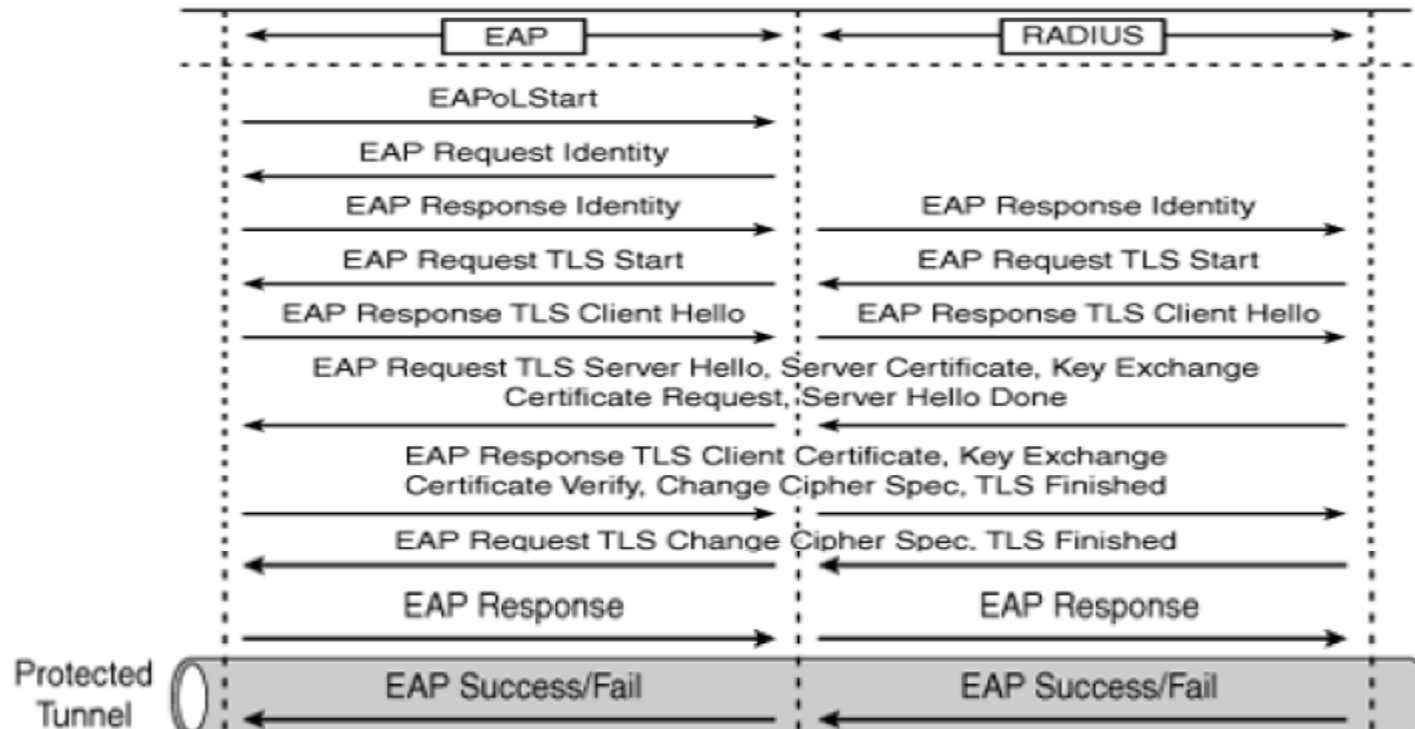
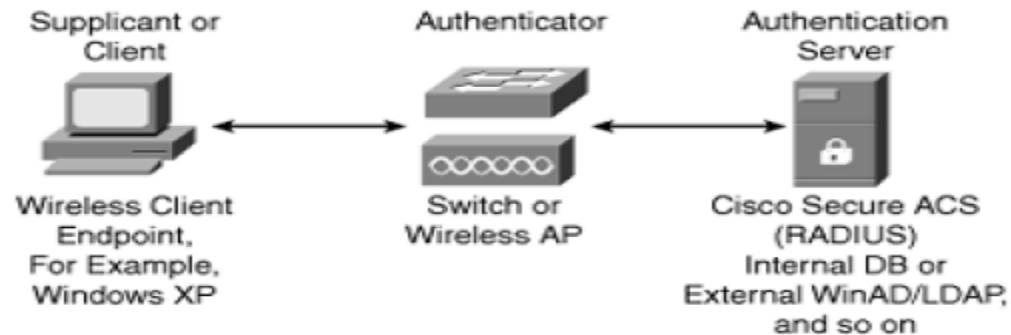
802.1x and EAP

- ▶ 802.1x viene usato come metodo di accesso alle rete via autenticazione (identity-based network access)
- ▶ EAP è un framework che gestisce diversi metodi per autenticare (estensione PAP/CHAP). Esistono quindi diverse varianti. Un esempio:
 - ▶ EAP Message Digest 5 (EAP-MD5)
 - ▶ EAP Transport Level Security (EAP-TLS)
 - ▶ EAP Tunneled Transport Level Security (EAP-TTLS)
 - ▶ EAP Flexible Authentication via Secure Tunneling (EAP-FAST)
 - ▶ Protected EAP (PEAP)
 - ▶ Cisco Lightweight Extensible Authentication Protocol (Cisco-LEAP)

EAP-MD5 Message Exchange



EAP Transport Layer Security (EAP-TLS)

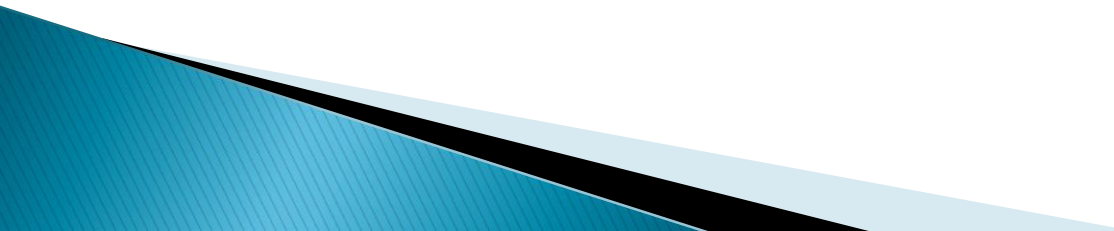


WLAN NAC

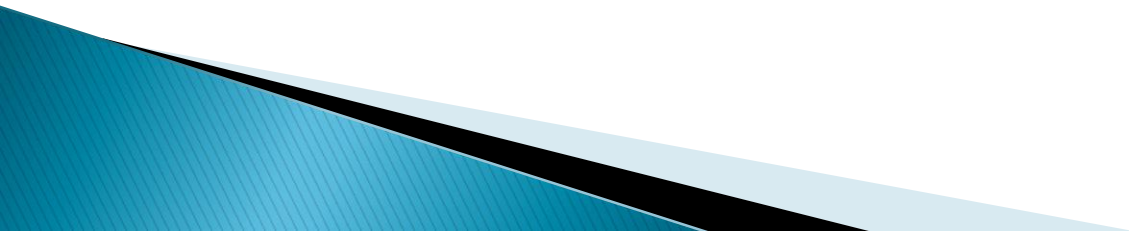
- ▶ Network Admission Control (NAC) per le reti WLAN è un insieme di tecnologie e soluzioni utilizzate per applicare le policy di dispositivi di sicurezza usando criteri che i client devono soddisfare:
 - Aggiornamenti SW
 - Programmi attivi
 - Etc.

E' possibile limitare i danni da emergenti minacce alla sicurezza.

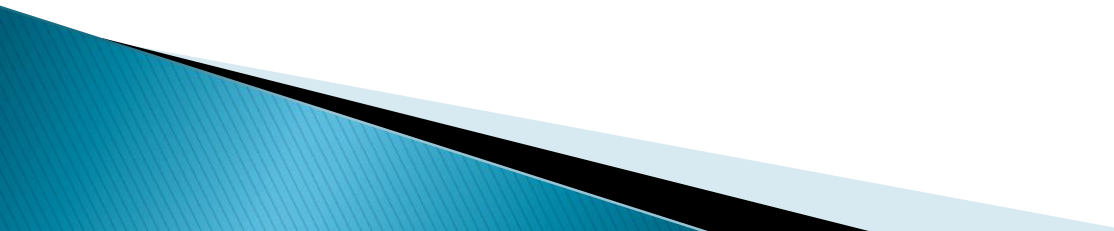
WLAN IPS

- ▶ Un Intrusion Prevention System (IPS) per le reti WLAN fornisce funzionalità di rilevamento delle intrusioni, e contemporaneamente provvede alla trasmissione di dati via etere.
 - ▶ Questo permette un punto di accesso per controllare in tempo reale i dati sulla rete wireless e la scansione per le potenziali minacce.
- 

wIPS Policy Alarm Encyclopedia



VPN IPsec

- ▶ Virtual Private Network (IP Security VPN IPsec) è un architettura di standard aperti per garantire sicurezza nelle comunicazioni su reti IP.
 - ▶ VPN IPsec offre la riservatezza, l'integrità e l'autenticità dei dati attraverso l'utilizzo di reti pubbliche.
- 

Wireless Design

WiFiTM Protected Access

All Wireless Traffic Must Be Authenticated and Encrypted Between the Client and the Access Point to Ensure Information Integrity

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

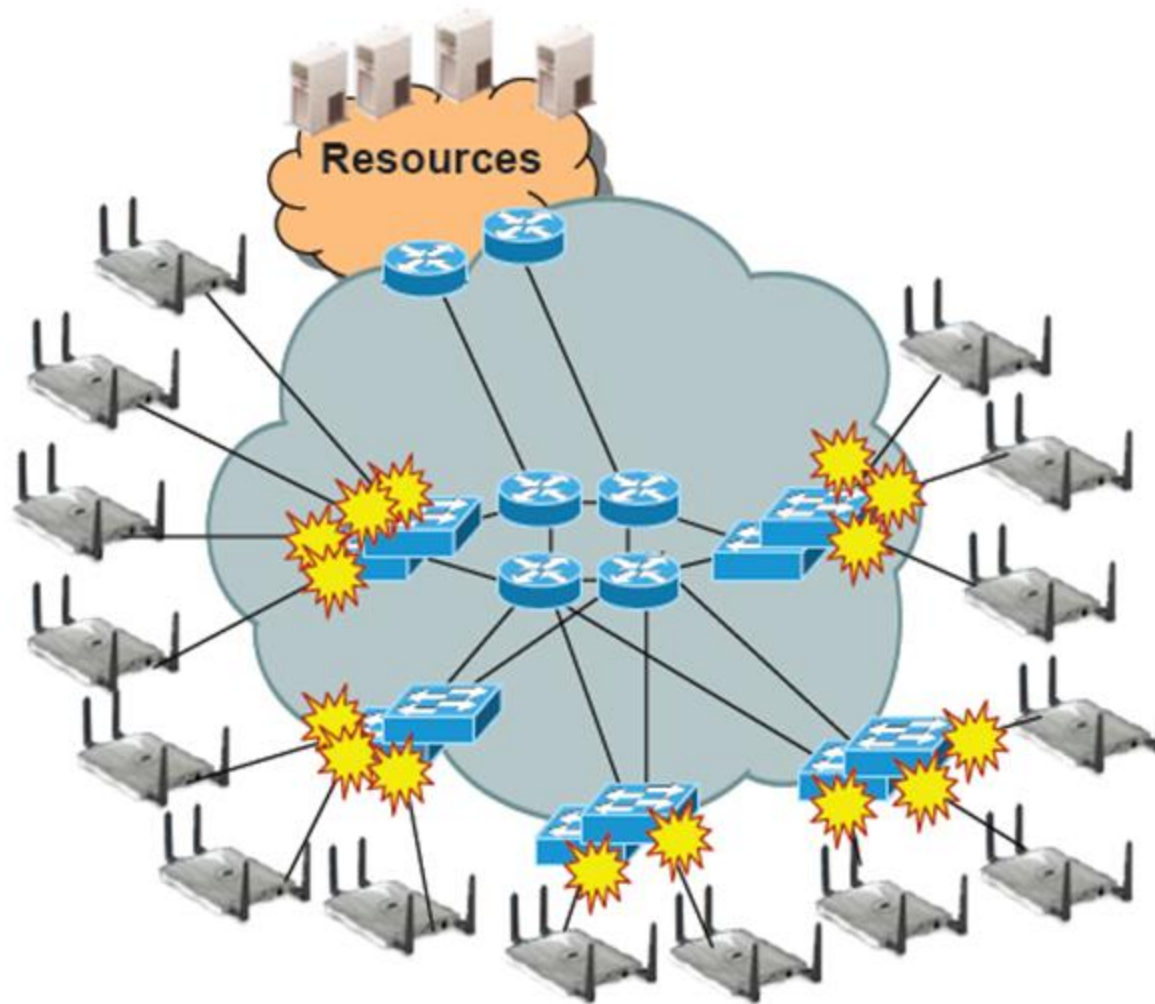
Dynamic WEP

- EAP/LEAP
- VLANs + ACLs

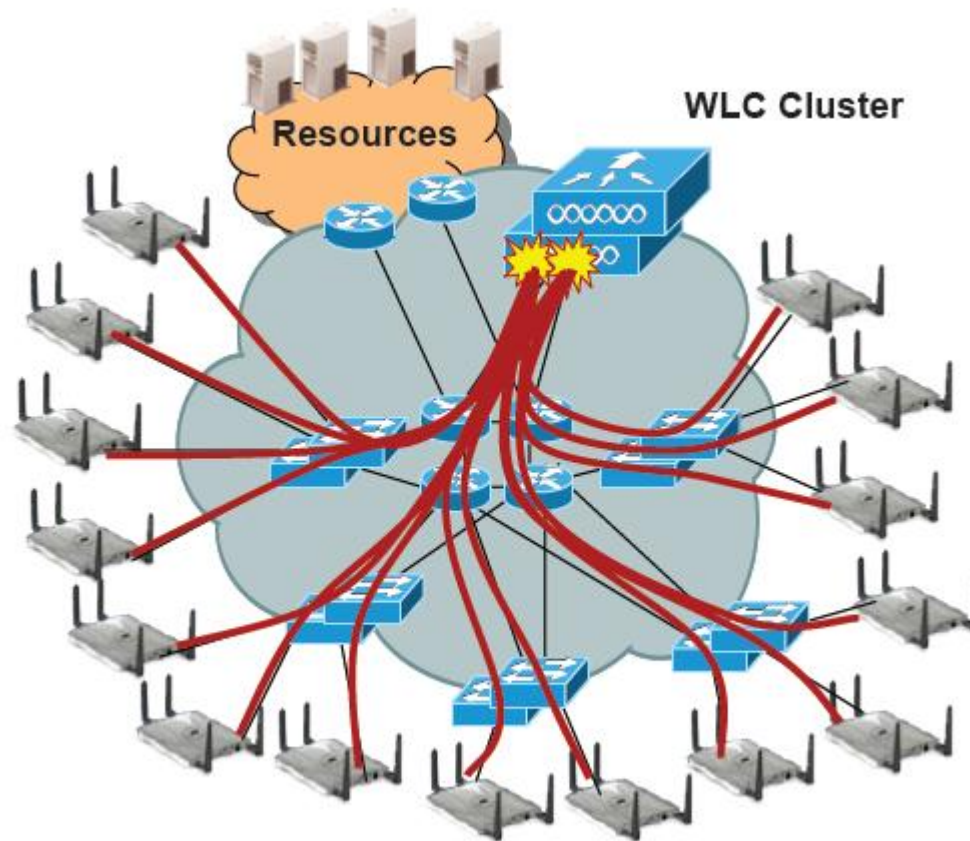
EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
Off-Line Dictionary Attacks	No	No	Yes ¹	No
Fast Secure Roaming (CCKM)	No	No	Yes	Yes
Local Authentication	No	No	Yes	Yes
WPA Support	Yes	Yes	Yes	Yes
Application Specific Device (ASD) Support	No	No	Yes	Yes
Server Certificates	Yes	Yes	No	No
Client Certificates	Yes	No	No	No
Deployment Complexity	High	Medium	Low	Low
RADIUS Server Scalability Impact	High	High	Low	Low/ Medium

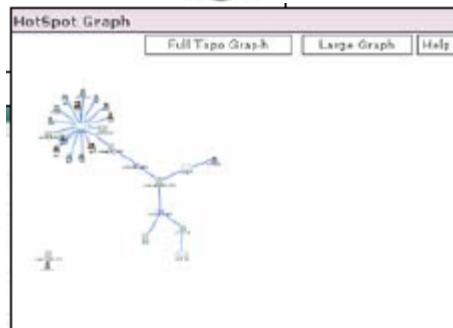
AP Standalone mode



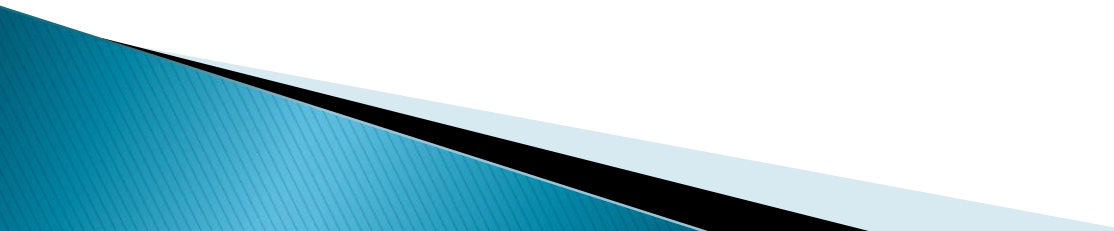
AP LWAPP / CAPWAP



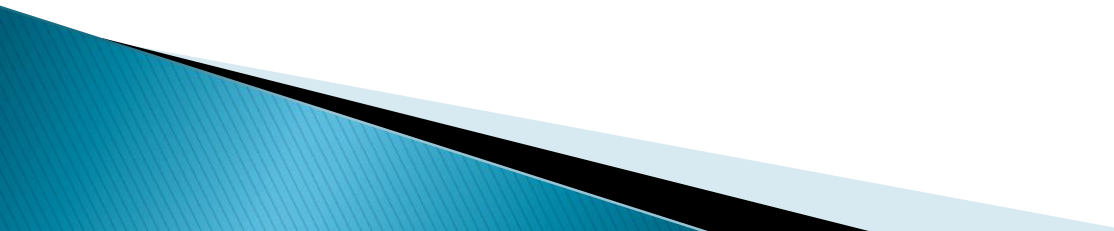
Management



BEST PRACTICE

- ▶ Posizione migliore per un AP 802.11n è a soffitto: migliore copertura
 - ▶ Usate 5Ghz con aggregazione 2x20Mhz
 - ▶ Disabilitare le velocità minori come la modalità legacy
 - ▶ Minimizzare le interferenze
- 

BEST PRACTICE

- ▶ 10/100/1000 Ethernet port
 - ▶ Modular platform
 - ▶ Flexible powering options
 - ▶ Migliori performance con WPAII e AES
- 

BEST PRACTICE

	AP1240	AP1250
Chassis	Fixed	Modular
Number of radio(s)	2	Up to 2
Enhanced 802.11a, g performance	No	Yes
Upgradeable to 802.11n	No	Yes
Maximum data uplink speed	FE	GigE
Spatial diversity	SISO	MIMO
High speed processor (MHz)	196	533
DRAM / Flash memory (MB)	32 / 16	64 / 32
Power requirement for dual radios AP-1250 can run 802.3af power when using only one radio	802.3af	802.3at (Draft) 1 radio 15.4 W 2 radios 18.5W

DOMANDE



LAB

Chipset Schede Wireless

- ▶ Aircrack
 - Chipset compatibili per l'injection
 - Prim2, PrimsGT, Atheros, Broadcom, alcune RTL...
- ▶ www.aircrack-ng.com
- ▶ 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 tools e driver proprietari. Funzionano solo con alcuni Chipset o schede. ES: Airglobe, Linkferret, Airmagnet.

▶ LINUX

- Wireless Extension
- Wlan NG
- HOST AP

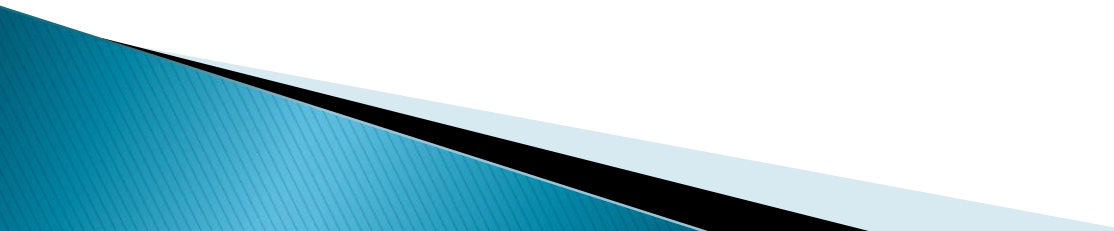
Lab 1 / 5

- 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
- # attacco basato su dizionario da utilizzare con WPA avendo 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
- 