Le Reti Wireless

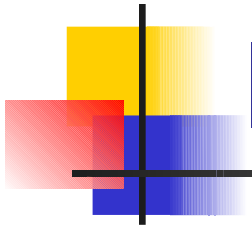
Analisi degli standard, delle componenti e delle modalità operative di una rete senza fili

Introduzione alle trasmissioni senza fili

Vantaggi, svantaggi e problematiche tipiche delle reti wireless

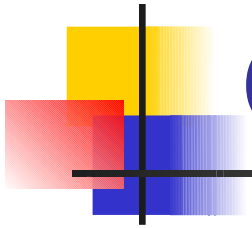
Cosa è una rete wireless?

- **Wireless** vuol dire letteralmente “senza fili” (in contrapposizione a *wired*)
- Una Rete Wireless è quindi un sistema di telecomunicazione (insieme di dispositivi, apparati, mezzi e protocolli per la trasmissione di informazione) che utilizza il mezzo radio e tecnologie a radiofrequenza al posto di connessioni cablate



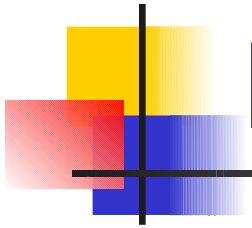
I vantaggi

- Mobilità dei terminali
- Costi di cablaggio ridotti
- Flessibilità in caso di modifiche strutt.
- Facilità di installazione e accesso
- Scalabilità
- Copertura anche in caso di ostacoli
- Robustezza



Gli svantaggi / I problemi

- Scarsa capacità / disponibilità di banda
- Sicurezza più complessa
- Bassa qualità della comunicazione
- Inquinamento elettromagnetico
- Consumo di energia
- Rischi per la salute (?)

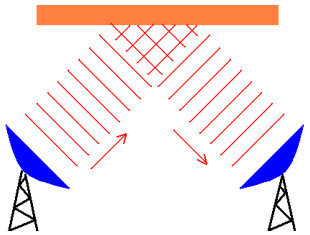


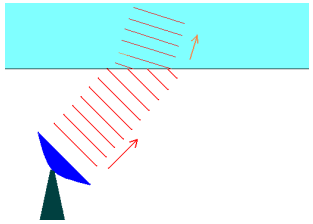
Problematiche specifiche

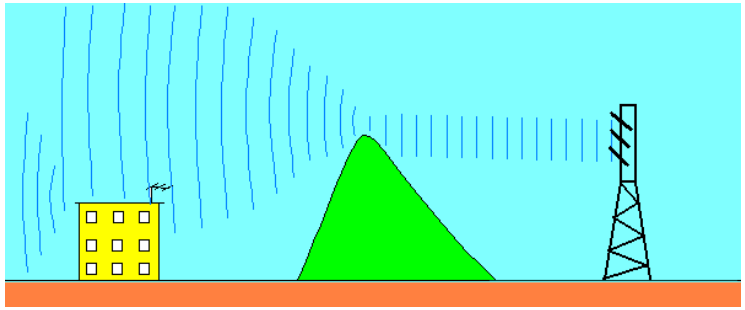
- Poiché il mezzo radio è unico, dispersivo e accessibile a chiunque, alcune problematiche sono specifiche o, comunque, diventano più critiche nel caso wireless:
  - Attenuazione del segnale
  - Interferenza tra le sorgenti
  - Intercettazione dei dati trasmessi

Problematiche della trasmissione radio (1)

- Un’onda elettromagnetica trasmessa nello spazio libero è soggetta e diversi fenomeni, che dipendono dalle caratteristiche fisiche dell’ambiente e dalla frequenza utilizzata
  - Riflessione
  - Rifrazione
  - Diffrazione
  - Diffusione
  - Irraggiamento

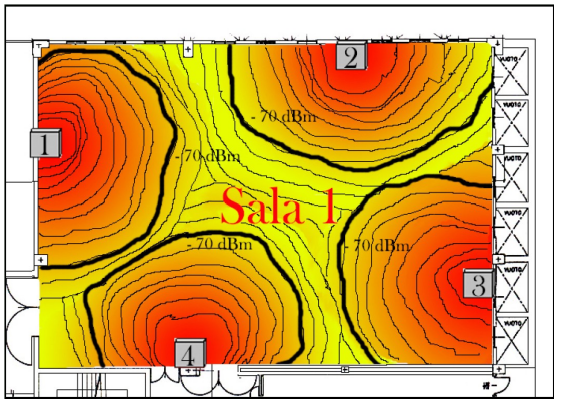






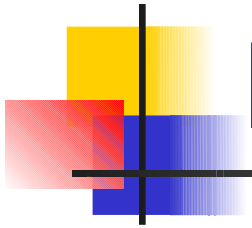
Problematiche della trasmissione radio (2)

- Il segnale trasportato da un'onda è soggetto a:
  - Attenuazione – la potenza del segnale si riduce
  - Interferenza – il segnale subisce modifiche
  - Cammini multipli – repliche dello stesso segnale seguono percorsi diversi e arrivano sfasate al ricevitore



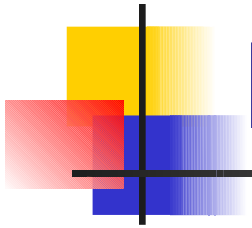
L’accesso al canale (1)

- Poiché il mezzo radio è unico, deve essere condiviso tra i diversi sistemi di trasmissione che ne fanno uso
- Servizi diversi possono usare regioni diverse delle spettro
  - Molto utilizzata è la banda ISM – Industrial, Scientific & Medical (Forni a microonde, CB, Palmari, WiFi, Bluetooth, Dect…)



L’accesso al canale (2)

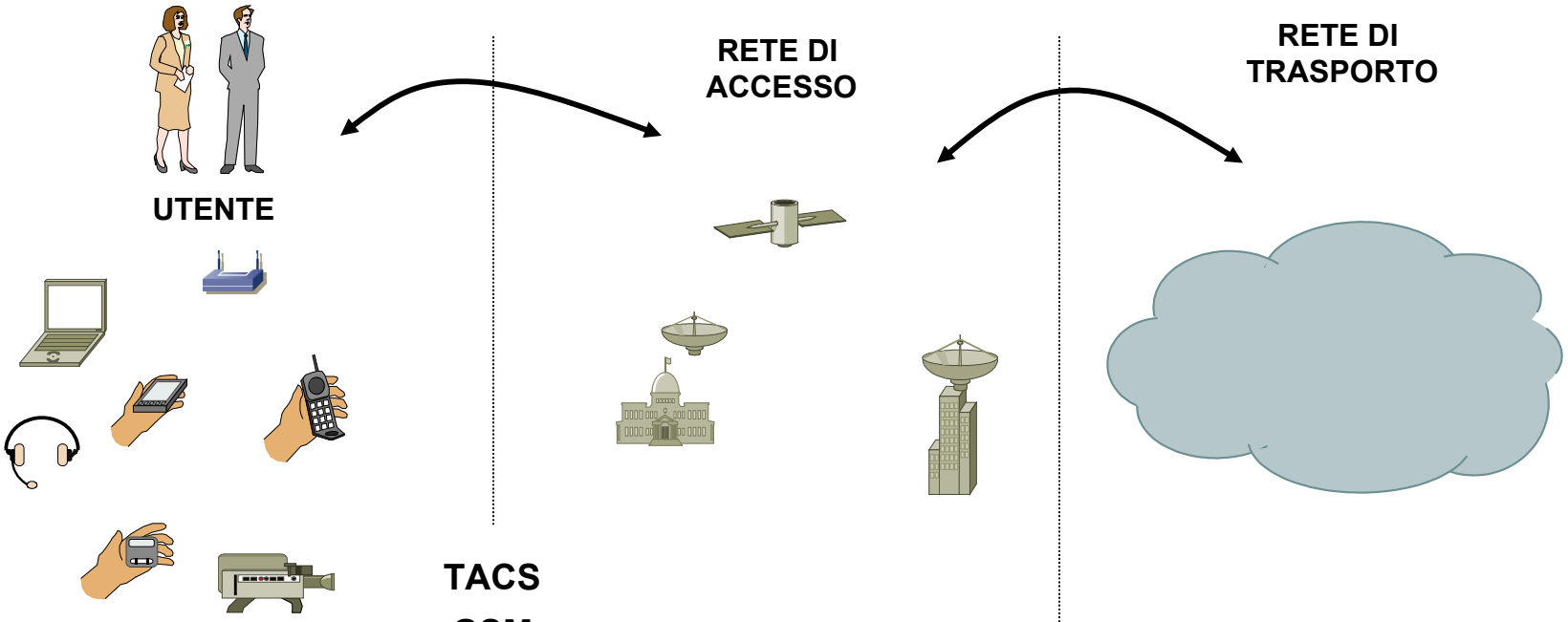
- Utenti dello stesso servizio possono riutilizzare il mezzo trasmissivo mediante tecniche di accesso multiplo
  - a divisione di frequenza (FDMA)
  - a divisione di tempo (TDMA)
  - a divisione di codice (CDMA)



Modulazione

- I segnali inviati via radio (o lungo un cavo o un mezzo magnetico) devono essere modulati con una tecnica, in modo da evitare che il segnale si degradi prima di essere ricevuto
- Un entità che trasmette ed una che riceve devono utilizzare la stessa modulazione per poter comunicare
  - Digitali (PSK, ASK, OFDM...)
  - Spread Spectrum (DSSS, FHSS...)

Le tipologie di reti wireless (1)

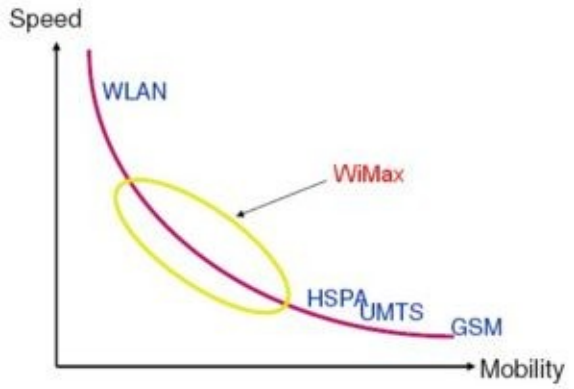


Le tipologie di reti wireless (2)

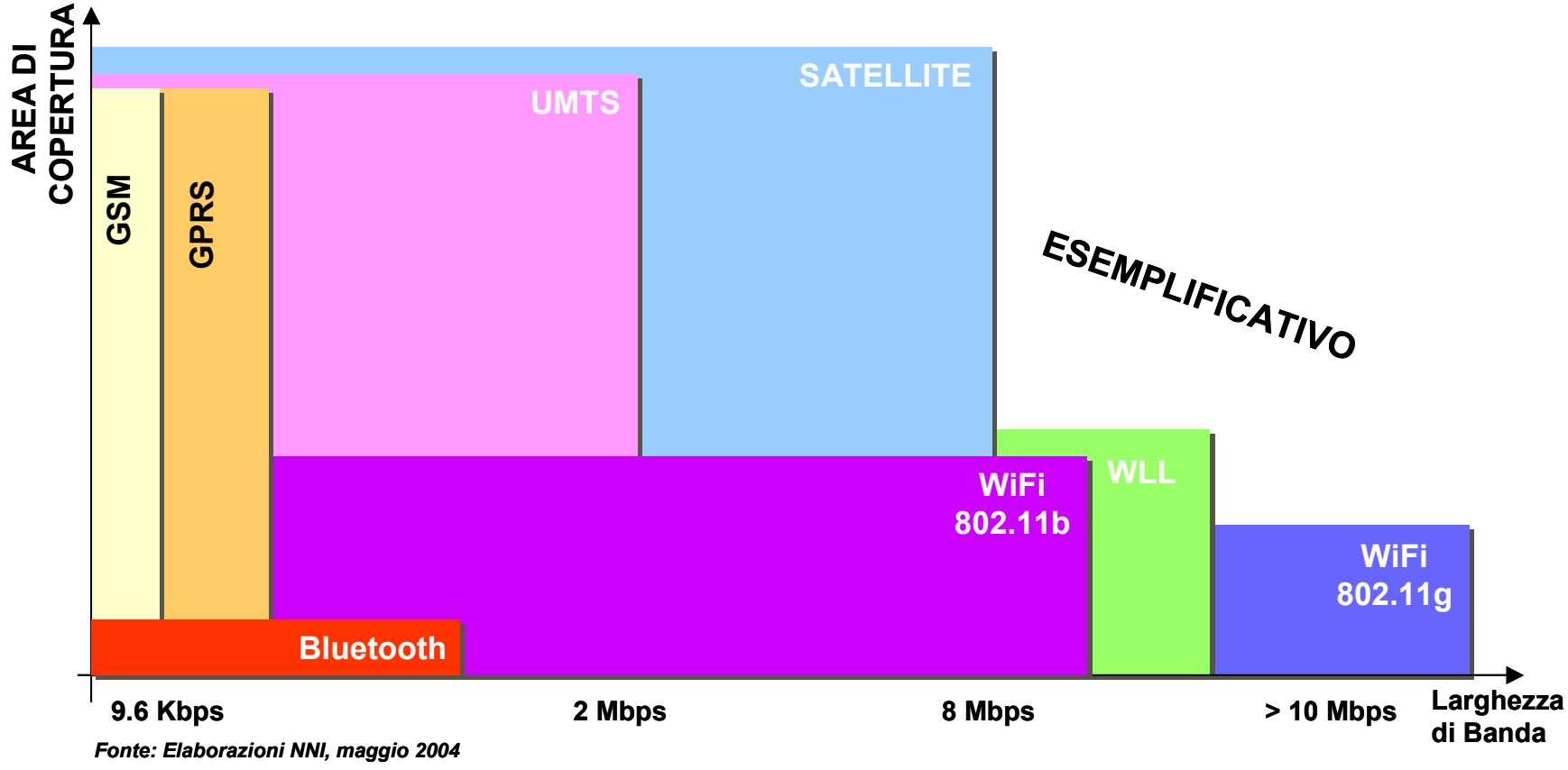
- WPAN – W. Personal Area Network
  - Comunicazione all'interno di un "sistema"
  - ~ 10 m
  - IEEE 802.15 (Bluetooth, UWB, Zigbee…)
- WLAN – W. Local Area Network
  - Comunicazione in un'area locale delimitata
  - ~ 100 m
  - IEEE 802.11 (a, b, g, n)

Le tipologie di reti wireless (3)

- WMAN – Metropolitan Area Network
  - Comunicazione su aree residenziali estese
  - ~ 10 Km
  - IEEE 802.16 (WiMax, WiBro)

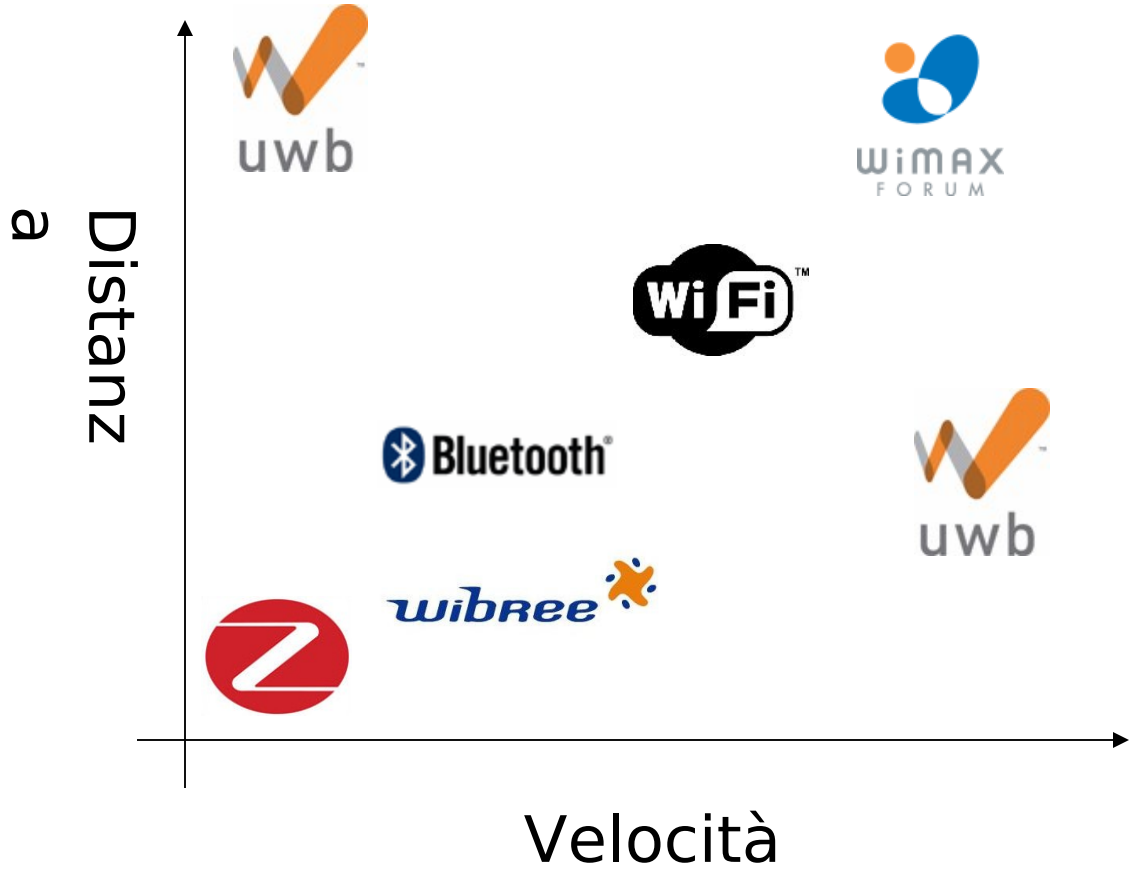


Le tipologie di reti wireless (4)

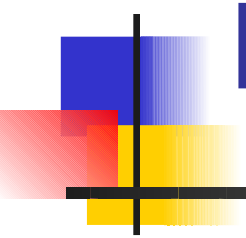


Fonte: Elaborazioni NNI, maggio 2004

Le tipologie di reti wireless (5)

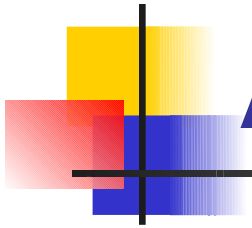


Le tipologie di reti wireless (6)



Wireless Local Area Network

Architetture e Standard di rete

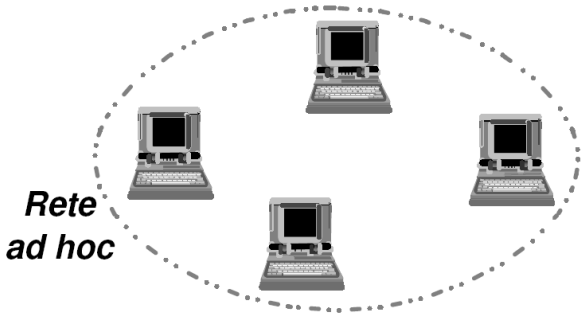


Architetture di rete

- Basic Service Set (BSS)
  - Tutte le stazioni appartengono ad 1 sola cella
  - Strutture ammesse
    - Ad hoc
    - Infrastructure
- Extended Service Set (ESS)
  - Le stazioni wireless appartengono a più celle interconnesse tra le quali è permesso il roaming
  - Unica struttura ammessa: Infrastructure
  - Per ogni cella è richiesta la presenza di un access point (AP) / stazione base, il quale è collegato agli AP delle altre celle (con link wired o wireless)

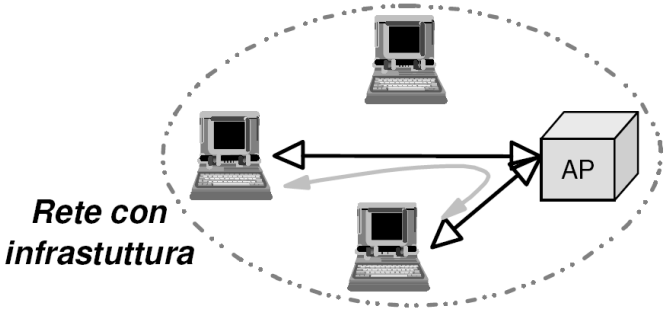
Rete ad-hoc

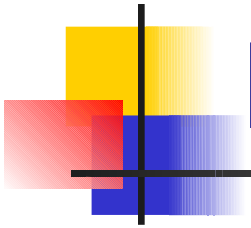
- Modalità Basic Service Set *ad-hoc*, anche detta Indipendent BSS
  - Tutte le stazioni stazioni della cella sono alla pari e nessuna controlla l'ingresso nella cella
  - Le stazioni parlano direttamente tra loro



BSS Infrastructure

- Esiste un nodo chiamato AP (Access Point), il quale controlla l'accesso della stazione alla cella ed esegue la commutazione delle frame scambiate tra le stazioni
  - La stazione ricerca l'AP tramite passive scanning (attesa del beacon frame dall'AP) o active scanning (invio di probe request frame e attesa della ricezione del probe response frame)
  - Processo di autenticazione della stazione sull'AP

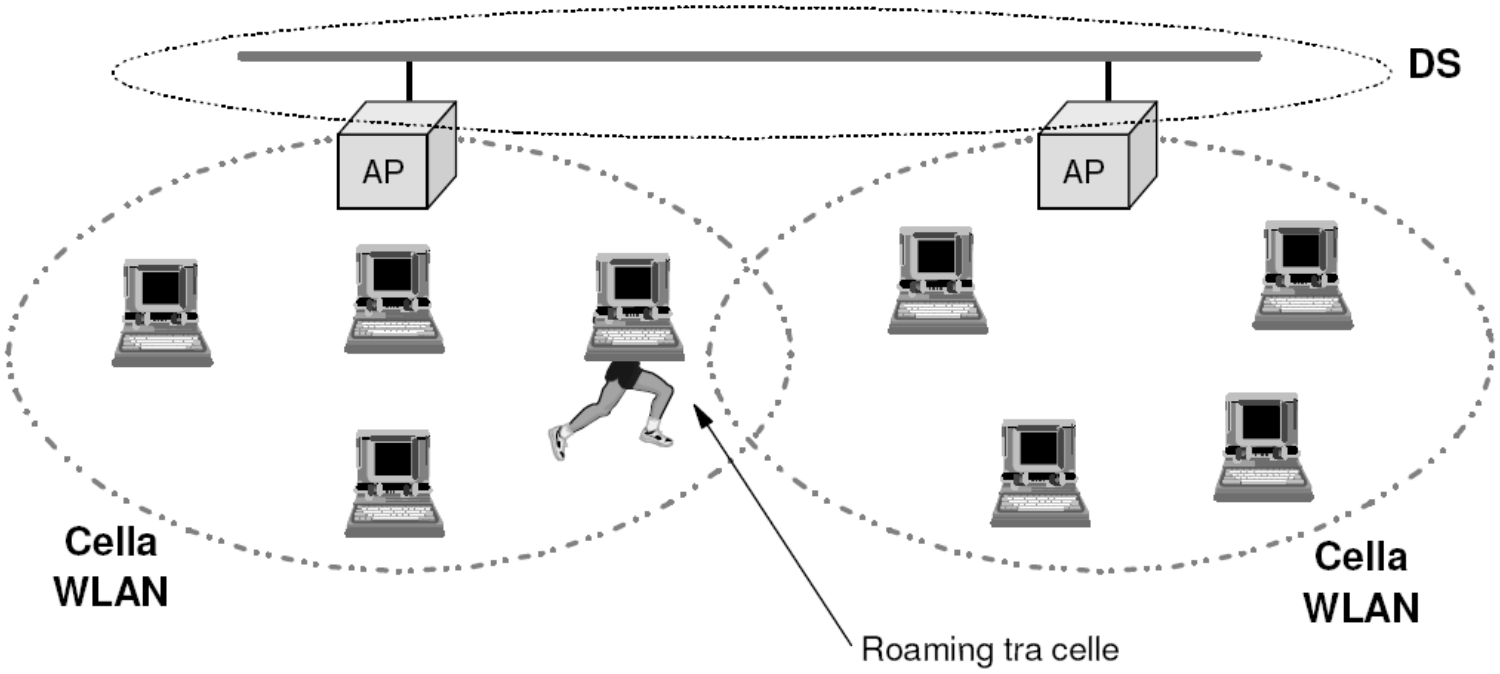




Extended Service Set (1)

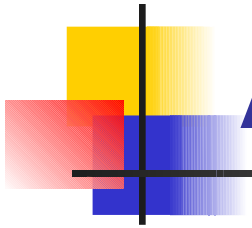
- Sistema articolato composto da 2 o più celle (BSS infrastructure), aventi ciascuna un AP, collegate attraverso un sistema di interconnessione (es. LAN Ethernet) chiamato DS (Distribution System)
- Gli AP, oltre alla commutazione delle frame, devono anche supportare il roaming tra le celle, mascherando la mobilità ai livelli superiori al MAC (ai quali il tutto appare come un'unica LAN)

Extended Service Set (2)



Modalità di funzionamento

- Un AP può, in generale funzionare, in più modalità
  - Access Point
    - I client wireless possono connettersi al dispositivo, che effettuerà il routing dei pacchetti tra tra le interfacce wireless e wired.
  - AP Client
  - Wireless Repeater
  - Wireless Bridge
    - La Base Station funge da dispositivo bridge wireless tra due (point-to-point) o più (point-to-multipoint) AP
    - Evoluzione: Wireless Distribution System



AP Client

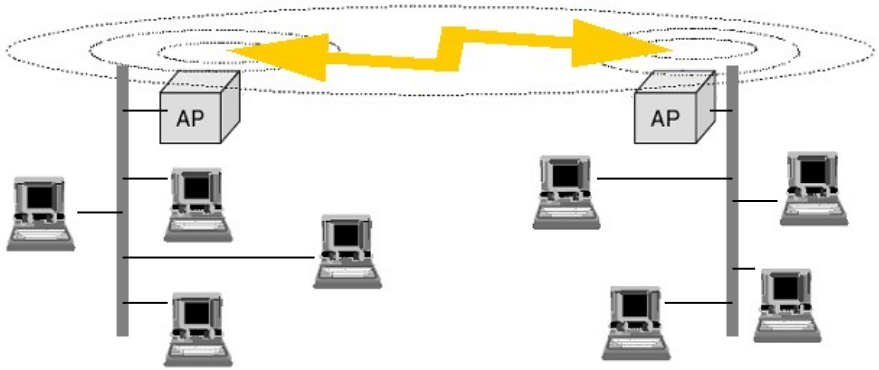
- Il dispositivo funge da client wireless (come se fosse una scheda di rete)
- E’ possibile indicare il MAC address dell’AP a cui ci si vuole connettere o effettuare una scansione delle reti disponibili
  - Solitamente l’AP deve essere simile
- Modalità raramente utilizzata

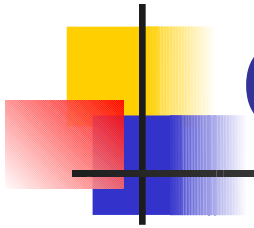
Wireless Repeater

- Il dispositivo diventa un ripetitore del segnale wireless di un altro AP
- In fase di configurazione è necessario indicare di quale AP (MAC address) è necessario “rilanciare” il segnale
  - Solitamente l’AP deve essere simile

Wireless Bridge

- Due o più AP creano una rete “virtuale” tra loro, funzionando come se fossero dei comuni bridge
  - I client wireless non saranno più in grado di connettersi agli AP



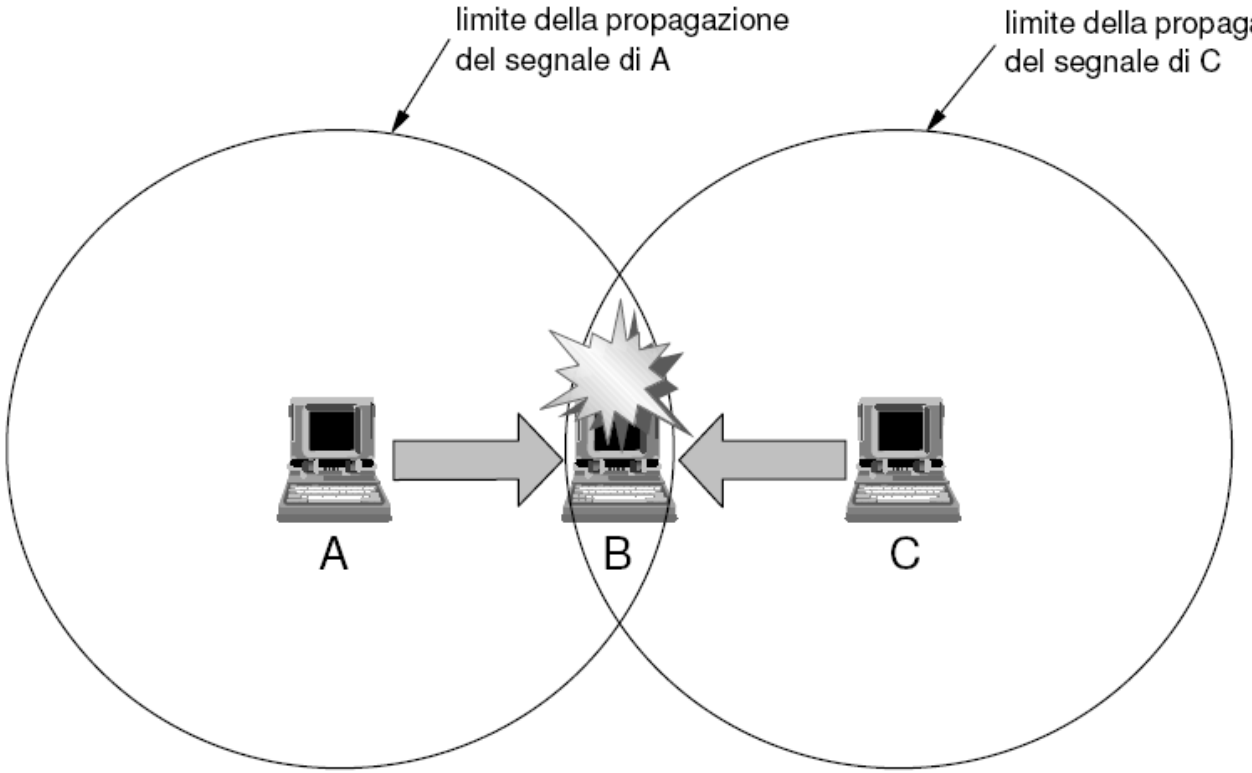


CSMA/CD nelle Wireless

- Una rete WLAN utilizza un canale condiviso ad accesso multiplo simile ad un bus (lo spazio circostante) e quindi potrebbe essere interessante esplorare la possibilità di utilizzare il protocollo d'accesso a contesa CSMA/CD utilizzato per le Ethernet
- Purtroppo la cosa permette di ottenere solo modesti risultati in quanto, a causa della caratteristica del canale wireless, si possono avere alcune condizioni anomale

Hidden Terminal

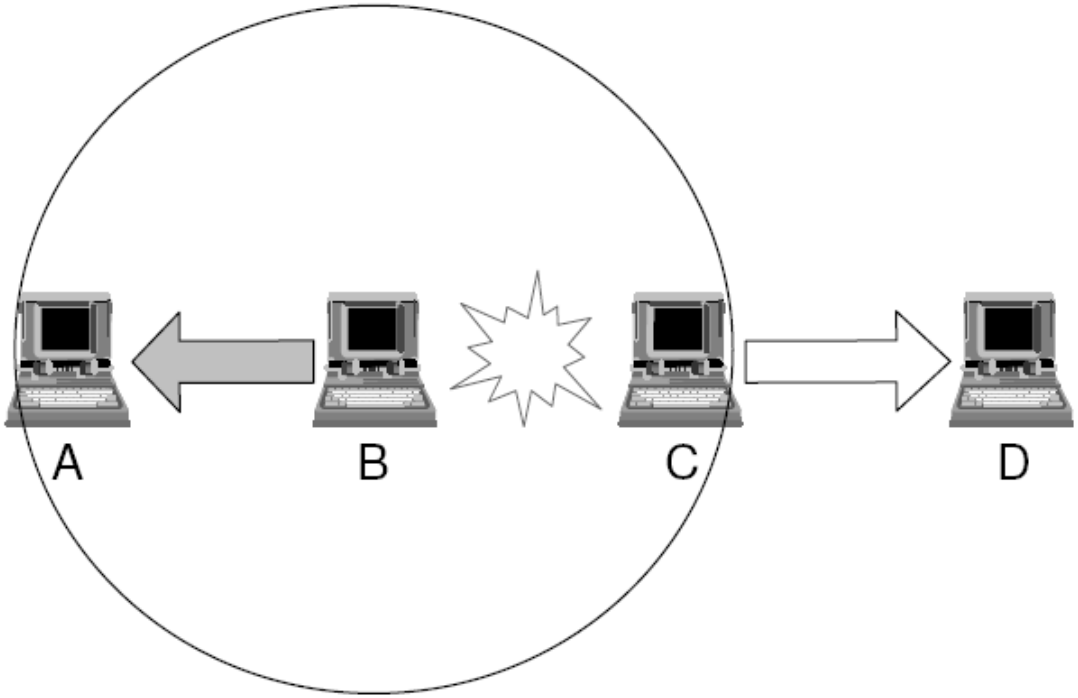
- Stazioni mittenti in collisione non sono in grado di rilevare tale condizione, ma credono che la trasmissione stia avvenendo con successo



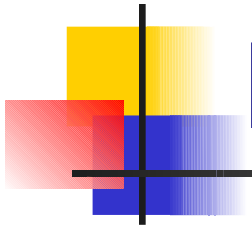
- A sta trasmettendo a B
- C deve trasmettere a B
  - C ascolta il canale e lo sente libero (in quanto non riceve la trasmissione di A)
  - C inizia la trasmissione
  - Su B si verifica una collisione ma A e C non se ne accorgono

Exposed Terminal

- Una stazione mittente non inizia una trasmissione, anche se quest'ultima potrebbe avvenire con successo



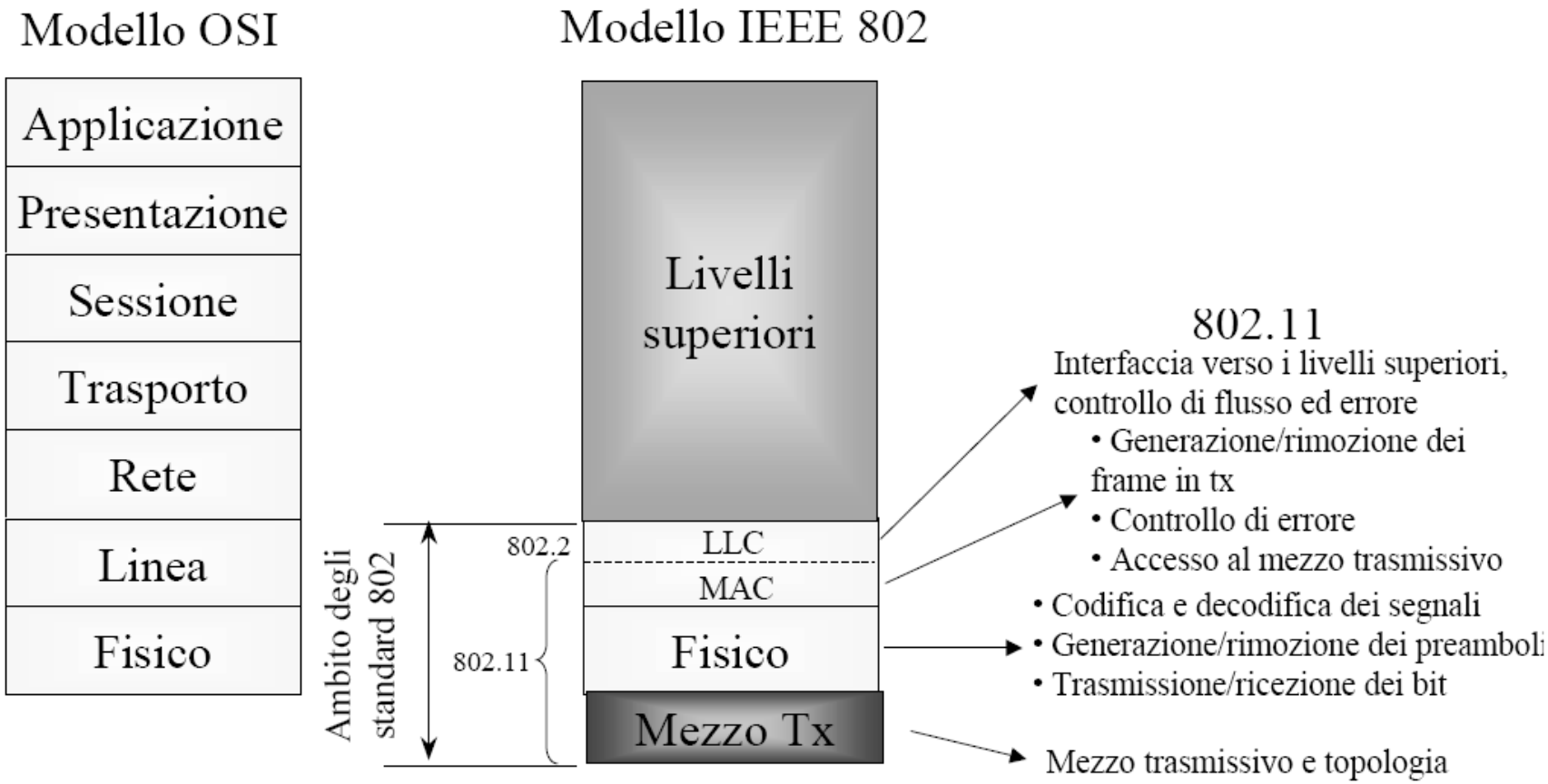
- B sta trasmettendo ad A
- C deve trasmettere a D
  - C ascolta il canale e lo sente occupato, quindi aspetta
  - In realtà C potrebbe comunque iniziare a trasmettere in quanto si verificherebbe una collisione solo nella zona tra B e C e non tra A e B né tra C e D



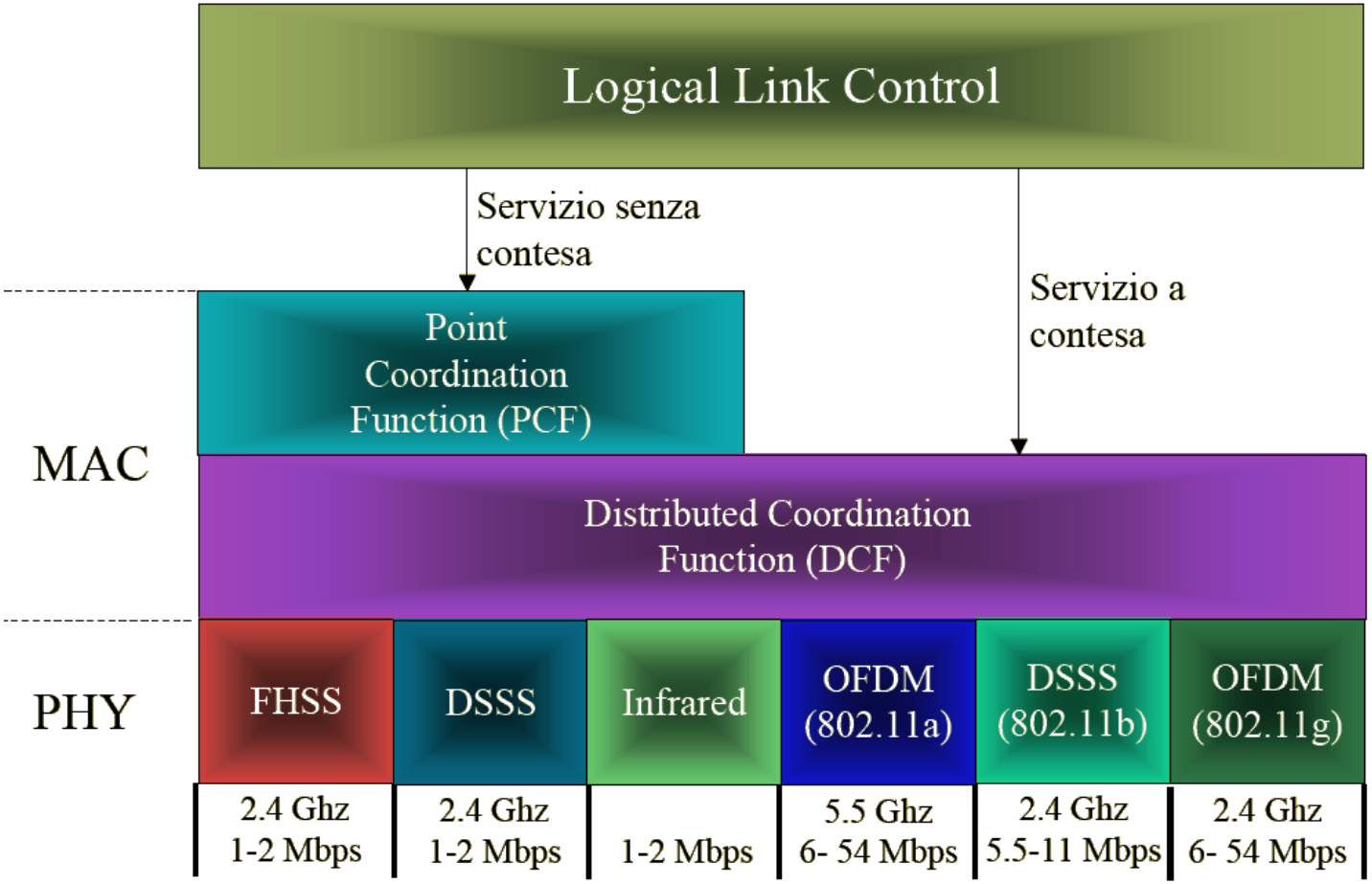
Da CSMA/CD a CSMA/CA

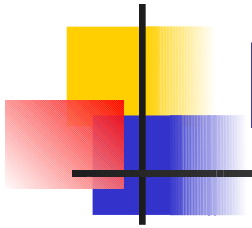
- Perchè in presenza di un canale wireless CSMA/CD genera il problema dei terminali nascosti?
  - Ciò che trasmette una stazione non è detto che venga sentito da tutte le altre
  - CSMA/CD permette di sentire solo se vi sono trasmissioni "vicino" alla stazione che sta ascoltando il canale
- Soluzione al problema:
  - Una stazione, prima di iniziare la trasmissione, dovrebbe verificare se vi sono delle trasmissioni nell'intorno della stazione destinataria
    - Protocollo d'accesso CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) con Physical or Virtual Carrier Sensing (v. DCF)

ISO/OSI e IEEE 802



Lo standard IEEE 802.11



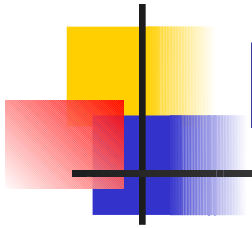


LLC

- Lo standard IEEE 802.2 definisce il livello Logical Link Control (LLC), che è lo strato superiore della porzione *data link layer* per le reti locali
- Il sottolivello LLC presenta al livello Network (o gli utilizzati comunque dei servizi data link) un’interfaccia uniforme
  - E’ quindi il sottolivello successivo, il Media Access Control (MAC), che varia in funzione del particolare mezzo utilizzato (Ethernet, token ring, FDDI, 802.11, etc.)

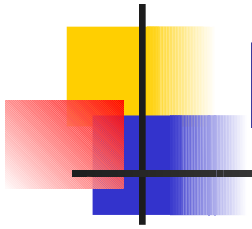
Servizi del MAC 802.11

- Lo standard 802.11 fornisce, tramite opportune trame MAC di gestione, una serie di servizi che il livello LLC richiede
  - Station Services (IBSS e ESS)
    - Authentication, Deautentication, MSDU Delivery, Privacy
  - Distribution System Services (solo ESS)
    - Association, Disassociation, Distribution, Integration, Reassociation



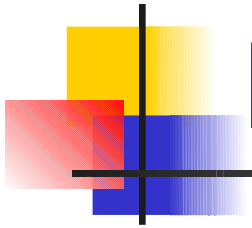
DCF e PCF

- MAC IEEE 802.11 prevede 2 modalità operative (tipi di protocollo d'accesso)
  - DCF (Distributed Coordination Function)
    - Possibile sia con la modalità ad hoc che con la modalità infrastructure
    - Il controllo dell'accesso al canale è distribuito sulle stazioni
    - Tutte le implementazioni WLAN devono supportare questa modalità
  - PCF (Point Coordination Function)
    - Possibile solo con la modalità infrastructure
    - Il controllo dell'accesso al canale è centralizzato sull'AP
    - Nelle implementazioni la modalità PCF è opzionale



DCF (1)

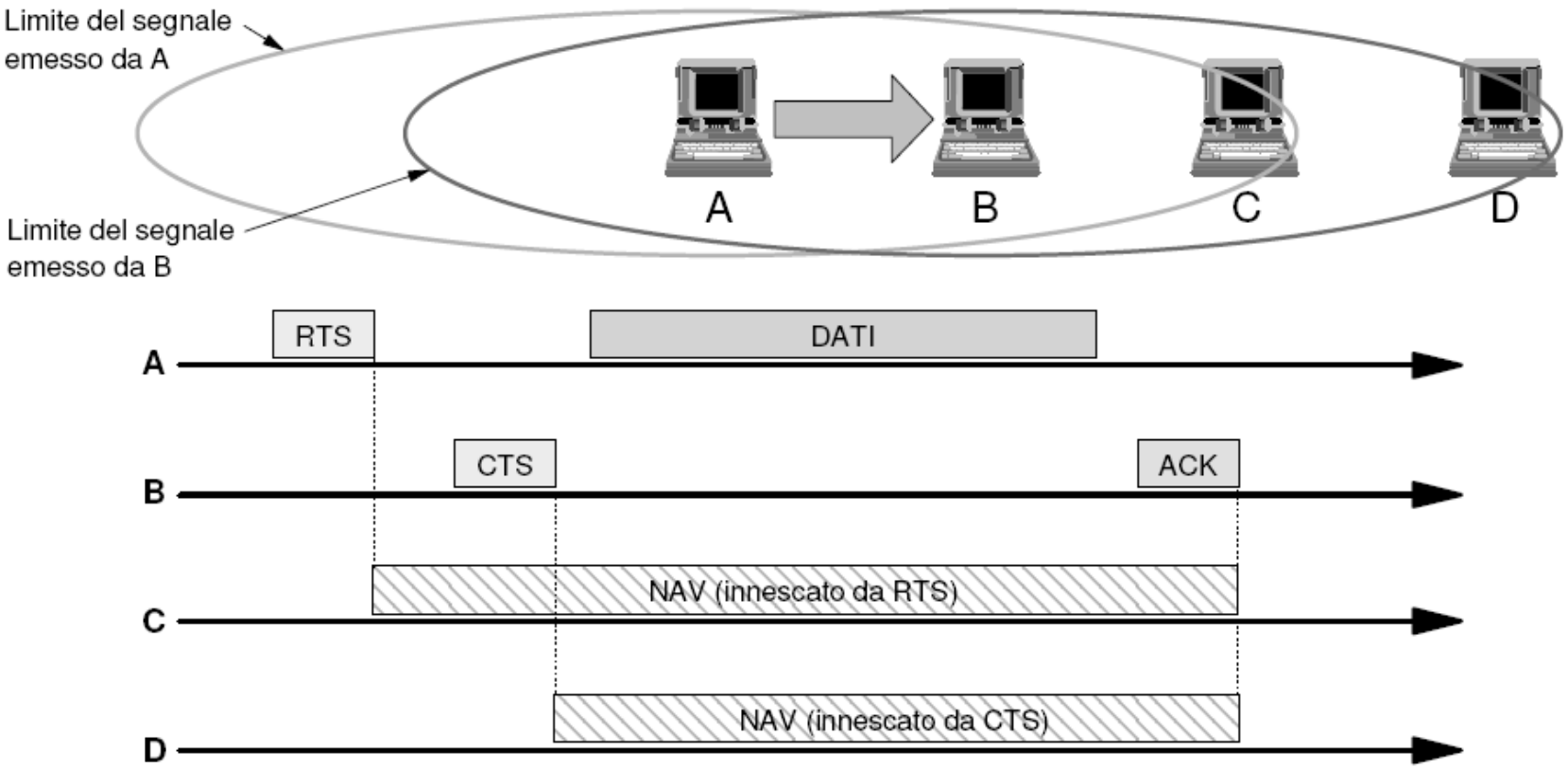
- DCF prevede l'utilizzo del protocollo d'accesso CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) e può funzionare in 2 modalità operative
  - Physical carrier sense
    - Una stazione trasmette solo se il canale è libero, altrimenti rimanda l'operazione
    - Modalità utilizzata per l'invio di frame broadcast, multicast e unicast (se sotto una certa dimensione)
  - Virtual carrier sense
    - Ha l'obiettivo di risolvere il problema degli hidden terminal
    - Modalità utilizzata per l'invio di frame unicast (di dimensione superiore ad un valore impostabile)

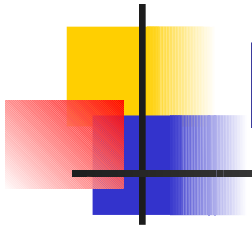


DCF (2)

- Virtual carrier sense
  - **Una stazione, prima di trasmettere una frame, ascolta se vi sono trasmissioni sul canale**
    - Se occupato aspetta
    - Se libero lo "prenota" per il tempo necessario alla trasmissione della frame (questo tuttavia non elimina completamente il rischio di una collisione)
    - Il mittente invia una (breve) frame RTS (Request To Send) di servizio verso il destinatario contenente la durata prevista della futura trasmissione
    - Il destinatario autorizza la trasmissione restituendo una (breve) frame CTS (Clear To Send) di servizio verso il mittente
    - Tutte le altre stazioni che sentono RTS e/o CTS aspettano per la durata indicata (impostazione dell'indicatore di NAV)
    - Il mittente invia la frame dati e aspetta per un time-out la PDU-ACK del MAC

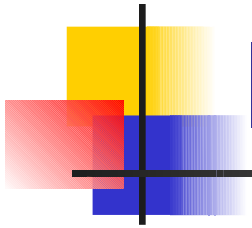
DCF (3)


Limite del segnale
emesso da A
Limite del segnale
emesso da B
A
B
C
D
RTS
DATI
CTS
ACK
NAV (innescato da RTS)
NAV (innescato da CTS)



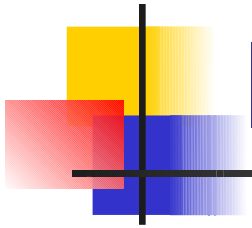
PCF

- Metodo di contesa alternativo, costruito sopra la struttura DCF
- Fondamentalmente si tratta un polling gestito da una stazione specializzata, denominata Point Coordinator (PC)
- In sostanza viene creata una struttura temporale, detta Superframe, divisa in due parti:
  - Contention Free Period (polling)
  - Contention Period (DCF)



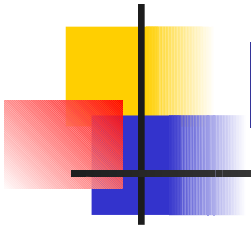
Il livello Fisico

- Lo strato fisico si occupa della trasmissione vera e propria delle trame secondo le specifiche stabilite
- Interagisce con il livello MAC per segnalare l’attività del canale (protocollo di acceso)
- Sostanzialmente tutte le evoluzioni dello standard IEEE 802.11 nell’ultimo decennio hanno riguardato questo livello
- Viene utilizzata la banda ISM
  - Limiti sulla potenza ma non occorrono licenze



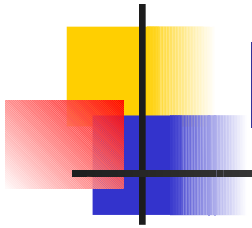
IEEE 802.11

- Prima versione (1997)
- Velocità: 1 Mb/s e 2 Mb/s
- Trasmissione a radiofrequenza
  - Tecnica spread spectrum FHSS o DHSS
  - ISM a 2.4 GHz (2.40 – 2.4835 GHz)
- Trasmissione ad infrarosso diffuso
  - Poco utilizzata (non devono esserci ostacoli tra Tx e Rx)



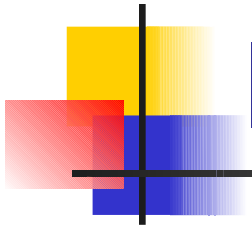
IEEE 802.11a

- Molto diffuso negli USA (1999)
- Incompatibile con le evoluzioni b e g
- Velocità massima: 54 Mb/s
  - Codifiche e modulazioni diverse in base alla distanza da coprire
- Utilizza la banda ISM a 5 GHz
  - Meno “trafficata”, con limiti solo sulla potenza massima e maggior larghezza di banda disponibile
- Tecnica OFDM
  - 52 sottoportanti (48 per dati e 4 per la sincronizzazione)



IEEE 802.11b

- Emesso nel 1999
- Velocità massima: 11 Mb/s
- Utilizza la banda ISM a 2.4 GHz
- Tecnica High-Rate DSSS
- Bit rate variabile in funzione delle condizioni del canale
  - Dynamic Rate Shifting



IEEE 802.11g

- Emesso nel 2003
- Velocità massima: 54 Mb/s
- Utilizza la banda ISM a 2.4 GHz
- Tecnica OFDM (ma può utilizzare anche High-Rate DSSS)
- Retro-compatibile con 802.11b (possono coesistere nella stessa rete)
- Espande il livello fisico
  - Ad esempio, in alternativa allo schema RTS/CTS, prevede anche il più semplice CTS-to-self

IEEE 802.11g non-standard

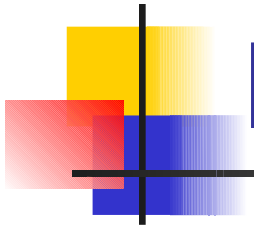
- Gli utenti richiedono maggiore velocità
  - Molti chip-maker hanno sviluppato tecnologie proprietarie per aumentare la velocità dei dispositivi wireless (*channel bonding, Packet bursting, MIMO, compressione*)
    - Atheros Super G (108 Mbps)
    - Broadcom 125 High Speed Mode
    - Airgo MIMO
    - …
  - Interferenze, problemi di retrocompatibilità, necessità di utilizzare un unico modello

IEEE 802.11n

- Estende i precedenti standard 802.11:
  - multiple-input multiple-output (MIMO)
  - 40 MHz PHY channels
  - MAC-layer frame aggregation
- Banda dei 2.4 GHz / 5 GHz
  - Legacy (solo 802.11a o b/g)
  - Mixed (sia 802.11a che b/g che n)
  - Greenfield (solo 802.11n) – max. perf.
  - N.B. Rischio interferenza con Bluetooth/Wifi nei 2.4
- Fino a 600 Mbps (4 stream su canale da 40MHz)
- Esistono in commercio già dal 2007 dispositivi pre-n WiFi Alliance-certified basati sulla *Draft 2*
- Nell'Ottobre 2009 è stato finalmente approvato lo standard IEEE 802.11n-2009

Confronto tra gli standard

Standard 802.11	*Copertura tipica (raggio in metri)*	*Portante*	*Velocità (Mbps)*	*Tecnica di modulazione*	*Note*
802.11a	15 – 25	5 GHz	54	Orthogonal Frequency Division Multiplexing (OFDM)	Incompatibile con b e g
802.11b	20 – 100	2.4 GHz	11	Direct Sequence Spread Spectrum (DSSS)	Compatibile con 802.11g; Usa tre canali condivisi anche da sistemi Bluetooth, Cordless e microndе (forni)
802.11g	20 - 80	2.4 GHz	54	Orthogonal Frequency Division Multiplexing (OFDM)	Compatibile con 802.11b
802.11n	20 - 70	2.4 GHz – 5 Ghz	600	Quadrature amplitude modulation (QAM)	MIMO & Frames aggregation; Retrocompatibile

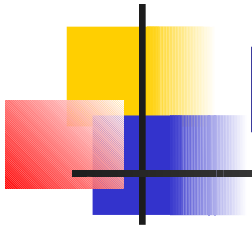


HYPERLAN

- Hyperlan/1 (1991)
  - Alternativo a IEEE 802.11
- Hyperlan/2 (2000)
  - “Fast wireless connection for many kinds of networks: UMTS backbone, ATM & IP networks”
  - Banda dei 5 GHz
  - Velocità fino a 54 Mbit/s
  - Livello fisico simile a 802.11a
    - Utilizza tuttavia Dynamic TDMA e non CSMA/CA
  - Attenzione alla qualità del servizio
  - Sicurezza con DES e 3DES
- Poco diffuso, ma alcune idee sono state riutilizzate..
  - Dynamic Frequency Selection (DFS) eTransmit Power Control - IEEE 802.11n.
  - Dynamic TDMA - IEEE 802.16 (WiMax).
- Impiegato in diverse zone per attivare connessioni WADSL

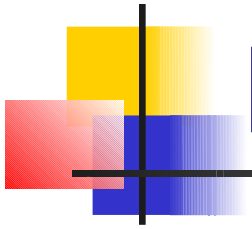
La sicurezza nelle reti Wi-Fi

Protocolli, meccanismi e pratiche per aumentare la sicurezza all’interno della propria rete



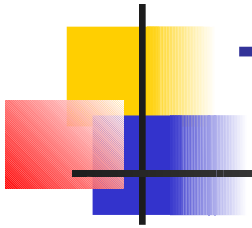
Requisiti di sicurezza (1)

- Garantire la sicurezza di un sistema informativo significa impedire a potenziali soggetti attaccanti l'accesso o l'uso non autorizzato di informazioni e risorse
- Due *golden rules*
  - La sicurezza perfetta non esiste
  - La resistenza di una catena è pari alla forza del suo anello più debole



Requisiti di sicurezza (1)

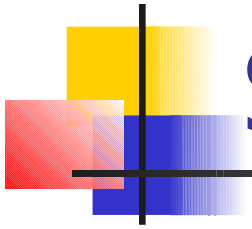
- Autenticazione (authentication)
- Autorizzazione (authorization)
- Riservatezza (privacy)
- Integrità (integrity)
- Disponibilità (availability)
- Paternità (non-repudiability)



Tipi di attacchi in rete

- Intercettazione
- Intrusione
- Furto di informazione
- Negazione del servizio

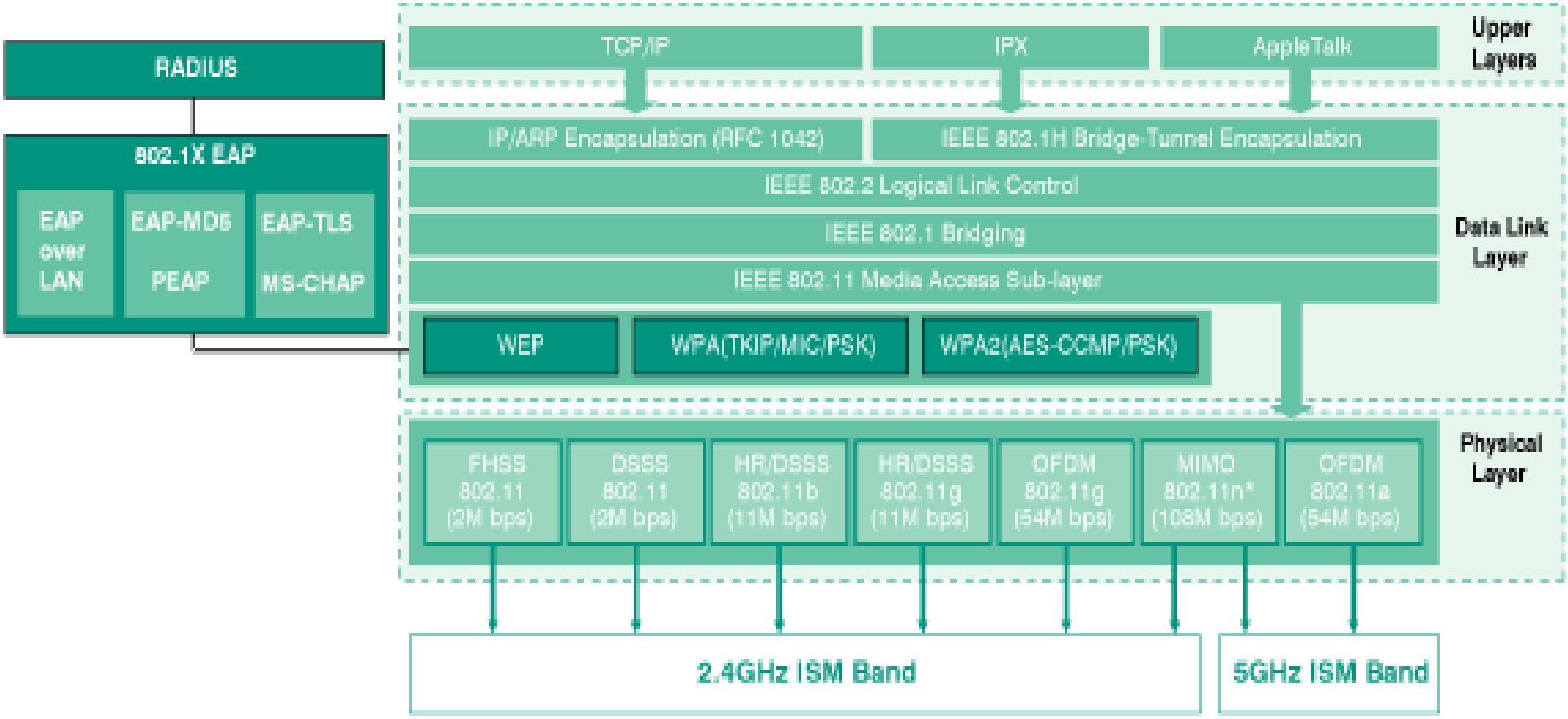
- Le reti wireless sono, da questo punto di vista, più vulnerabili di quelle wired

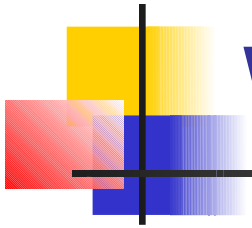


Strategie di protezione

- *Security through obscurity*
- Sicurezza a livello di rete
  - Firewall, VPN, controllo accesso…
- Sicurezza a livello di host
  - Firewall, antivirus, crittografia…
- Sicurezza a livello di applicazione
  - Crittografia, autenticazione/controllo d’accesso..

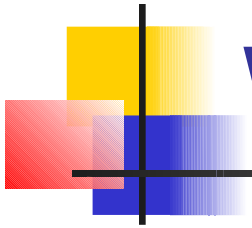
Sicurezza nelle WLAN





WEP (1)

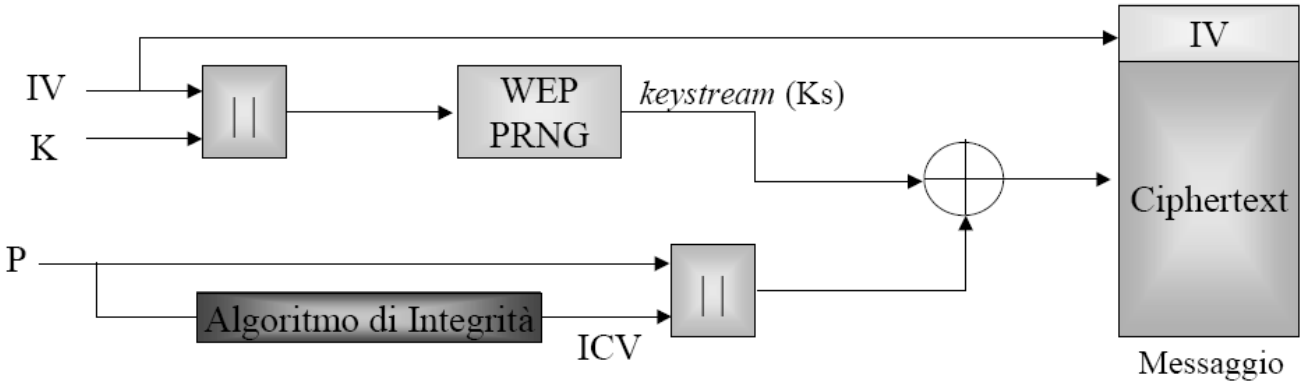
- Crittografia introdotta nelle reti Wireless per garantire un livello di sicureza paragonabile a quello delle reti cablate
- WEP (Wireless Equivalent Privacy) è un protocollo fondato su 3 principali funzionalità
  - Confidenzialità
  - Controllo di accesso
  - Sicurezza di trasmissione dei dati



WEP (2)

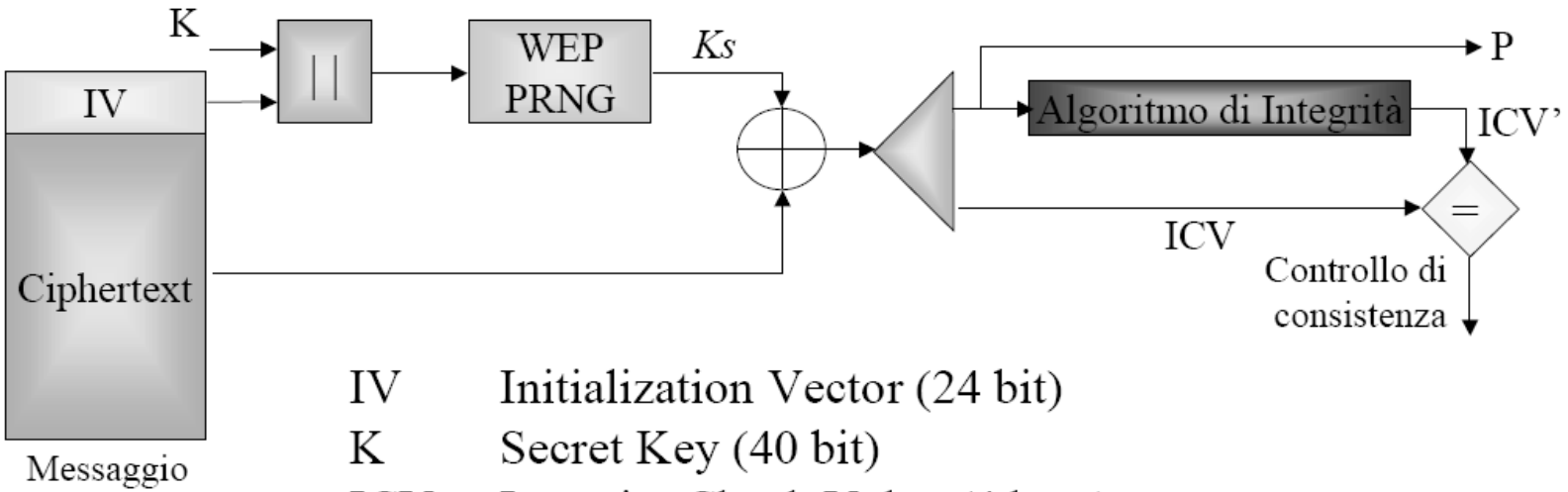
- WEP è basato su una chiave segreta (40bit) condivisa tra tutti i membri della rete autorizzati ad accedere all'AP
  - tutti possono vedere il traffico della rete, come in una rete Ethernet
- L'algoritmo utilizzato è il RC4 (Rivest, 1994)
  - al messaggio viene aggiunto un CRC;
  - il risultato viene posto in XOR con un keystream generato dall'algoritmo RC4 a partire dalla chiavesegreta e da un vettore iniziale IV;
  - il pacchetto risultante (IV + messaggio cifrato) viene inviato sul canale.

WEP - Cifratura



IV Initialization Vector (24 bit)
K Secret Key (40 bit)
ICV Integrity Check Value (4 byte)
PRNG Pseudo Random Number Generator (RC4)
P Frame MAC in chiaro

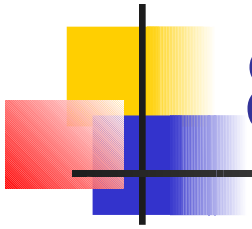
WEP - Decifratura



IV	Initialization Vector (24 bit)
K	Secret Key (40 bit)
ICV	Integrity Check Value (4 byte)
PRNG	Pseudo Random Number Generator (RC4)
P	Frame MAC in chiaro
Ks	Keystream

Attacchi al WEP

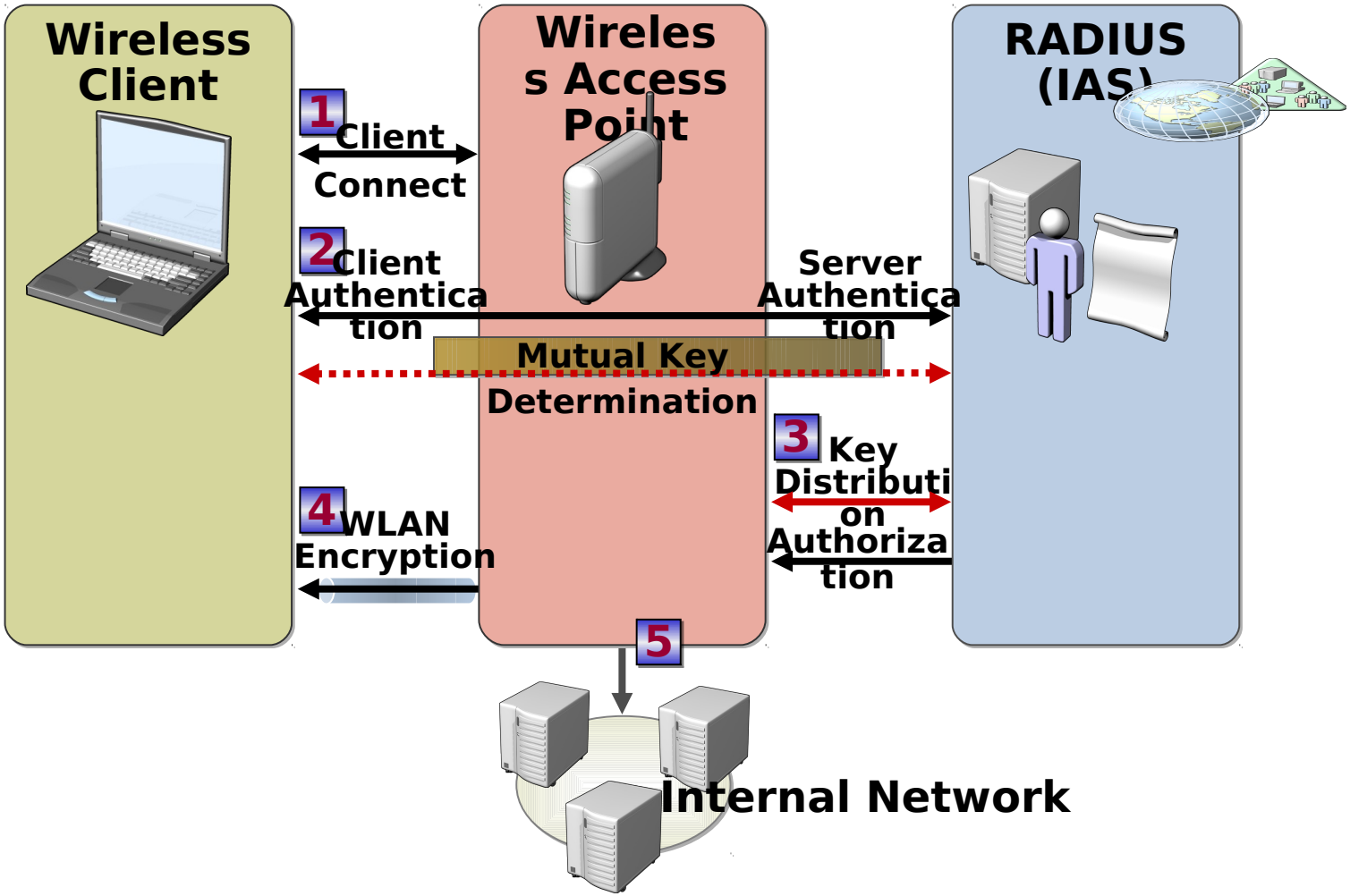
- Riutilizzo del keystream
  - Poiché IV è di 24 bit, è facile ottenere in breve tempo frame cifrate con lo stesso keystream
    - $1500*8/(11*10^6)*2^{24} = 18000$ s = 5 ore
- Decription Dictionary
- Alterazione del messaggio
  - CRC _NON_ è un algoritmo di hashing (solo rilevazione di errori casuali)
- Decodifica della chiave
  - Con 5 milioni di pacchetti catturati è possibile effettuare un attacco passivo e risalire alla chiave



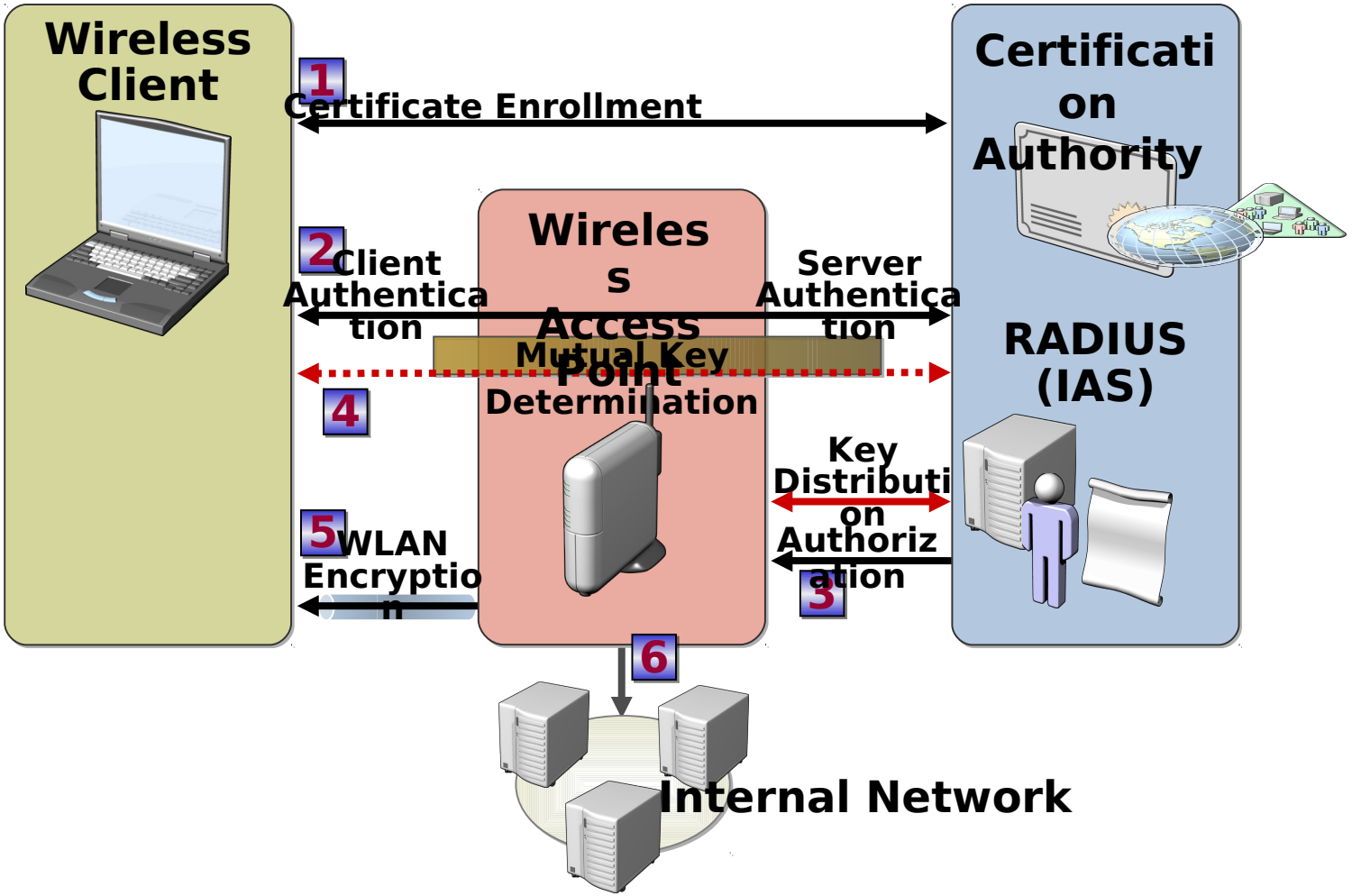
802.1x

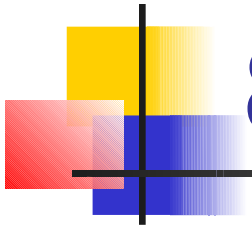
- Si basa su tecnologie esistenti:
  - Extensible Authentication Protocol (EAP)
  - Remote Authentication Dial-In User Service (RADIUS)
- Aggiunge a WEP le caratteristiche del protocollo 802.1x (meccanismi di autenticazione e autorizzazione, rotazione della chiave WEP) per mitigarne le principali debolezze e per usare un server RADIUS
  - Protected EAP (PEAP) con le password (802.1X con PEAP-MS-CHAPv2)
  - Certificate Services (802.1X con EAP-TLS)

802.1x: PEAP e Password



802.1x: EAP e TLS





802.11i

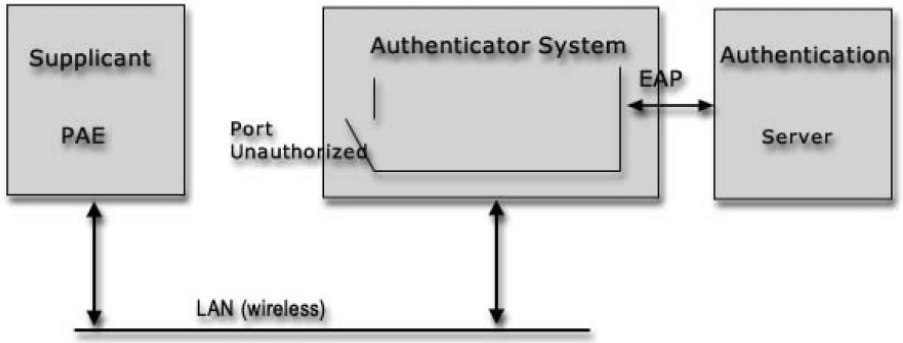
- Nuovo standard (non ancora del tutto supportato) diffuso nel giugno del 2004
- Costituito da:
  - RSN (Robust Secure Network)
  - TKIP (Temporal Key Integrity Protocol)
  - Message Integrity Check
  - WPA (Wi-Fi Protected Area)

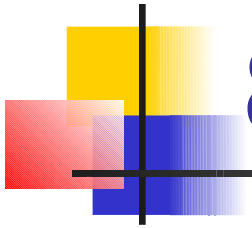
802.11i: RSN (1)

- Le funzionalità di RSN sono:
  - Autenticazione ed Integrità
  - Stabilità e flessibilità
  - Access Control
  - One-Way Authentication
- Ogni client che vuole accedere alla rete deve autenticarsi tramite l'Autenticator
  - Due porte logiche
    - Authentication PAE – canale sempre aperto per il transito delle sole trame di autenticazione
    - Service PAE – canale aperto solo se l'autenticazione va a buon fine ed è utilizzato quindi dal client per "muoversi"

802.11i: RSN (2)

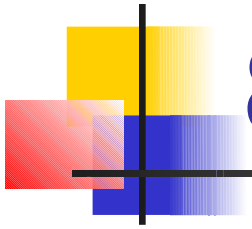
- RSN è formato da tre entità principali
  - Supplicant
    - Es: client
  - Authenticator
    - Es: l'AP
  - Authentication server
    - Es. server RADIUS





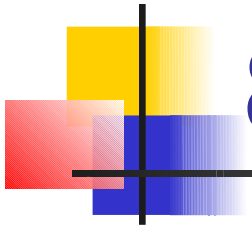
802.11i: MIC

- Formato da tre componenti principali
  - Chiave segreta k
  - Funzione di tagging
  - Predicato di Verifica
- La funzione etichettatrice prende in ingresso la chiave K ed un messaggio M, restituendo un tag T chiamato Message Integrity Code



802.11i: TKIP

- Temporal Key Integrity Protocol
  - Utilizza RC4 e lo stream cipher a 128 bit per crittare i dati
  - Di fatto è un insieme di funzionalità aggiunte allo standard WEP
  - Per evitare pacchetti replicati, viene utilizzato IV come un sequence number
  - Mixing delle chiavi
    - Per risolvere il problema delle chiavi deboli WEP
    - Vengono utilizzate chiavi temporanee diverse

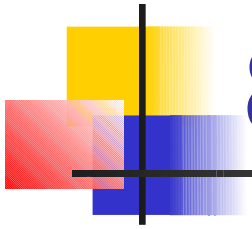


802.11i: WPA (1)

- WPA e WPA2 forniscono le seguenti caratteristiche crittografiche:
  - Crittazione dei dati, usati con gli standard di autenticazione 802.1X
  - Integrità dei dati
  - Protezione da attacchi di tipo “replay”
  - Operano a livello MAC (Media Access Control)

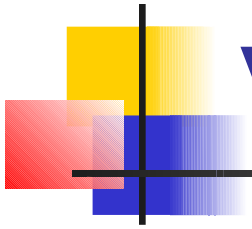
802.11i: WPA (2)

- WPA nasce per eliminare le problematiche di cifratura del WEP
- Di fatto è ancora un’estensione di WEP
  - Basata su RC4
  - Include un IV di 48 bit (anziché 24)
  - Utilizza MIC
  - Implementa funzionalità di derivazione e distribuzione delle chiavi



802.11i: WPA2

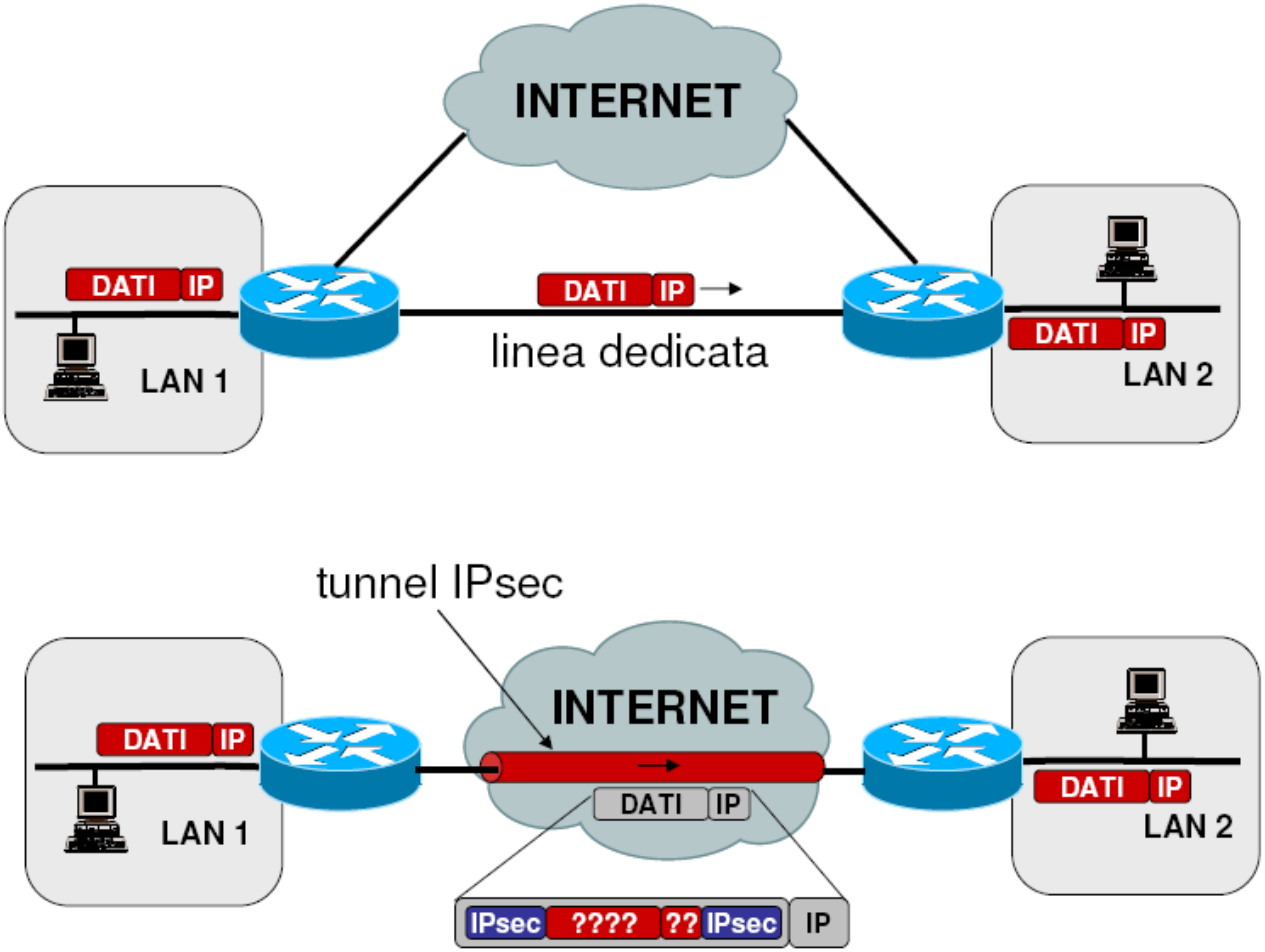
- Inserita nello standard ufficiale IEEE 802.11i
  - Commercialmente 802.11i viene chiamato proprio WPA2
- Abbraccia totalmente le funzionalità RSN
- Utilizza per la cifratura il più sicuro AES



VPN (1)

- Virtual Private Network
  - Creano un tunnel attraverso Internet
    - IPSec (estensione di IP con apposito Header)
  - Sono usate nell’accesso dial-up da remoto
  - La tecnologia VPN può utilizzare una cifratura forte e può anche fornire l’autenticazione per utenti e terminali wireless utilizzando RADIUS.

VPN (2)


INTERNET
DATI
IP
LAN 1
DATI
IP
linea dedicata
DATI
IP
LAN 2
tunnel IPsec
INTERNET
DATI
IP
LAN 1
DATI
IP
DATI
IP
LAN 2
IPsec
????
??
IPsec
IP