Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Reti Locali Wireless (WLAN)

Wireless Network: Ciclo di Seminari

Ing. Stefano Paris

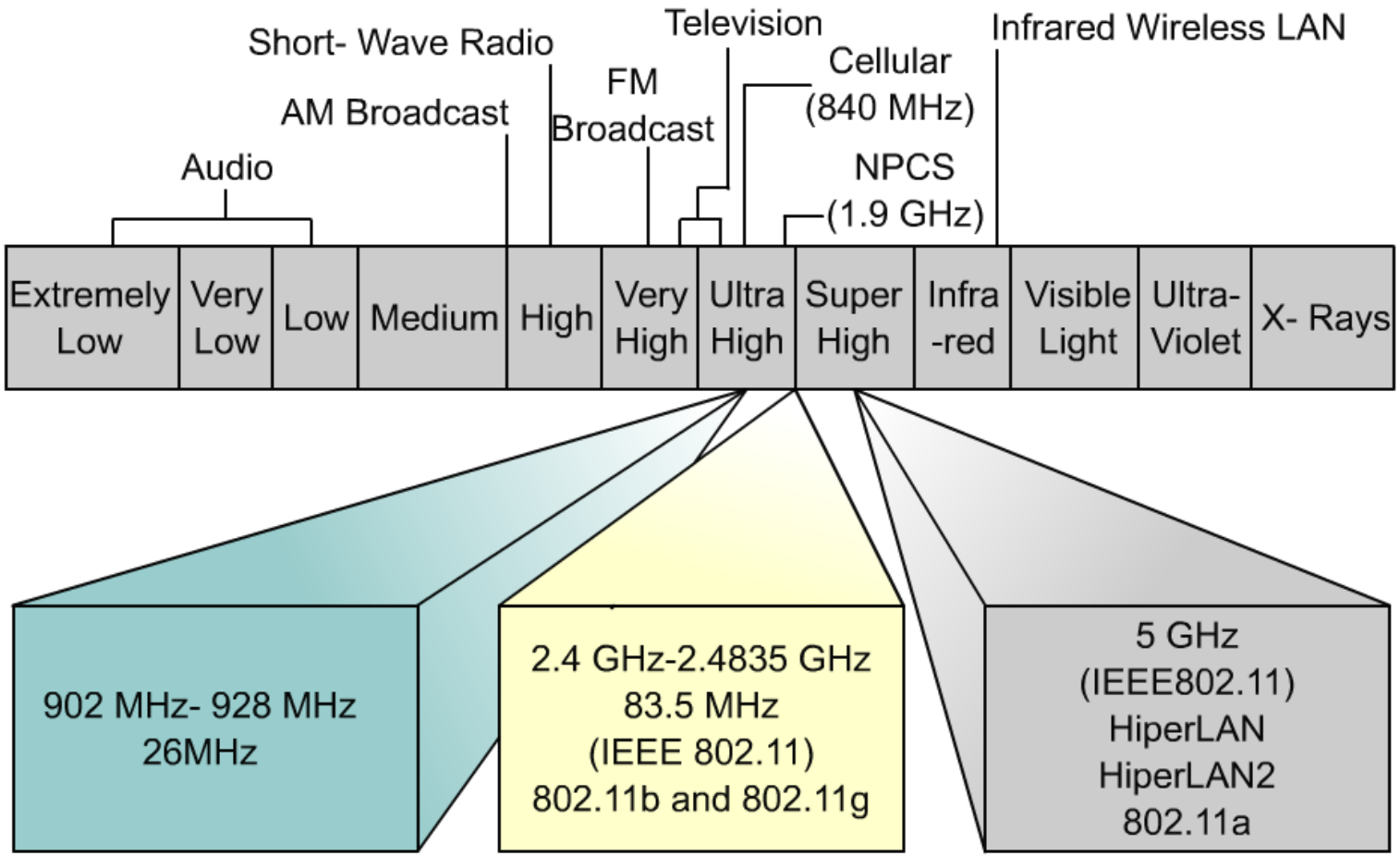
Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Regolamentazione della banda

Allocazione di banda

- Lo spettro è una risorsa scarsa,
  - Necessità di regolamentazione
  - Priorità ad applicazioni "delicate" (militari, mediche ecc..)
  - Molte bande sono licenziate (tassa sull'utilizzo)
- L'uso dello spettro di frequenze radio è regolato da:
  - *Federal Communications Commission* (FCC) in Nord America
  - *European Telecommunications Standard Institute* (ETSI) in Europa

Bande non licenziate



Bande *Industrial Scientific and Medical (ISM)*

- Bande non licenziate allocate attorno ai 900 MHz e ai 2.4 GHz (80 MHz di banda a 2.40÷2.48 GHz) per le comunicazioni di utenti individuali
  - La banda a 2.4 GHz è disponibile "*worldwide*"
  - FCC alloca sia la banda a 900 MHz che quella a 2.4 GHz
  - ETSI alloca solo la banda a 2.4 GHz (la banda a 900 MHz in Europa è usata per il GSM)
- Basso costo
- Alta interferenza

Regole d'utilizzo della banda ISM

- Uso della tecnica di ***Spread Spectrum*** (non più)
- Limiti sulla massima potenza trasmessa in banda
  - Nord America: 1* W sia a 900 MHz che a 2.4 GHz
  - Europa (*ERC/DEC/(01)07*): 100* mW a 2.4 GHz
- Limiti sulle emissioni fuori banda

* limite sull'EIRP

Bande attorno ai 5GHz

- In Europa *ERC/DEC/(99)/23*:
  - banda a 5.2 (5.15-5.35) GHz per il sistema *HiperLan*
  - banda a 5.4 (5.47-5.725) GHz per *HiperLan II*
- In Nord America
  - Banda UNII (*Unlicensed National Information Infrastructure*) 300 MHz tra 5.2 e 5.8 GHz con regole abbastanza libere
- Limiti solo sull'uso della potenza

Vantaggi/Svantaggi bande a 5 GHz

- Pochi sistemi utilizzano la banda a 5 GHz
  - Minore interferenza
  - Maggiore disponibilità
  - Maggiore velocità nominale di trasmissione
- Frequenza portante più elevata
  - Maggiore attenuazione in spazio libero del segnale
  - Maggiore potenza in trasmissione
  - Ostacoli più opachi
  - A pari potenza trasmessa il raggio d'azione è inferiore rispetto ai sistemi a 2.4 GHz
  - Necessità di installare più AP (fattore 1.5)

Banda *UNII*

- 300 MHz divisi in tre sottobande da 100 MHz ciascuna
  - *"Low"* 5.15-5.25 GHz, Potenza max 50* mW
  - *"Middle"* 5.25 - 5.35 GHz , Potenza max 250* mW
  - *"High"* 5.725 – 5.825 GHz, Potenza max 1* W
- Utilizzo delle tre sottobande:
  - *Low/Middle*: sistemi *indoor*
  - *High*: sistemi *outdoor*

* limite sull'EIRP

I 5 GHz in Europa – *Decision ECC/DEC/(04)08*

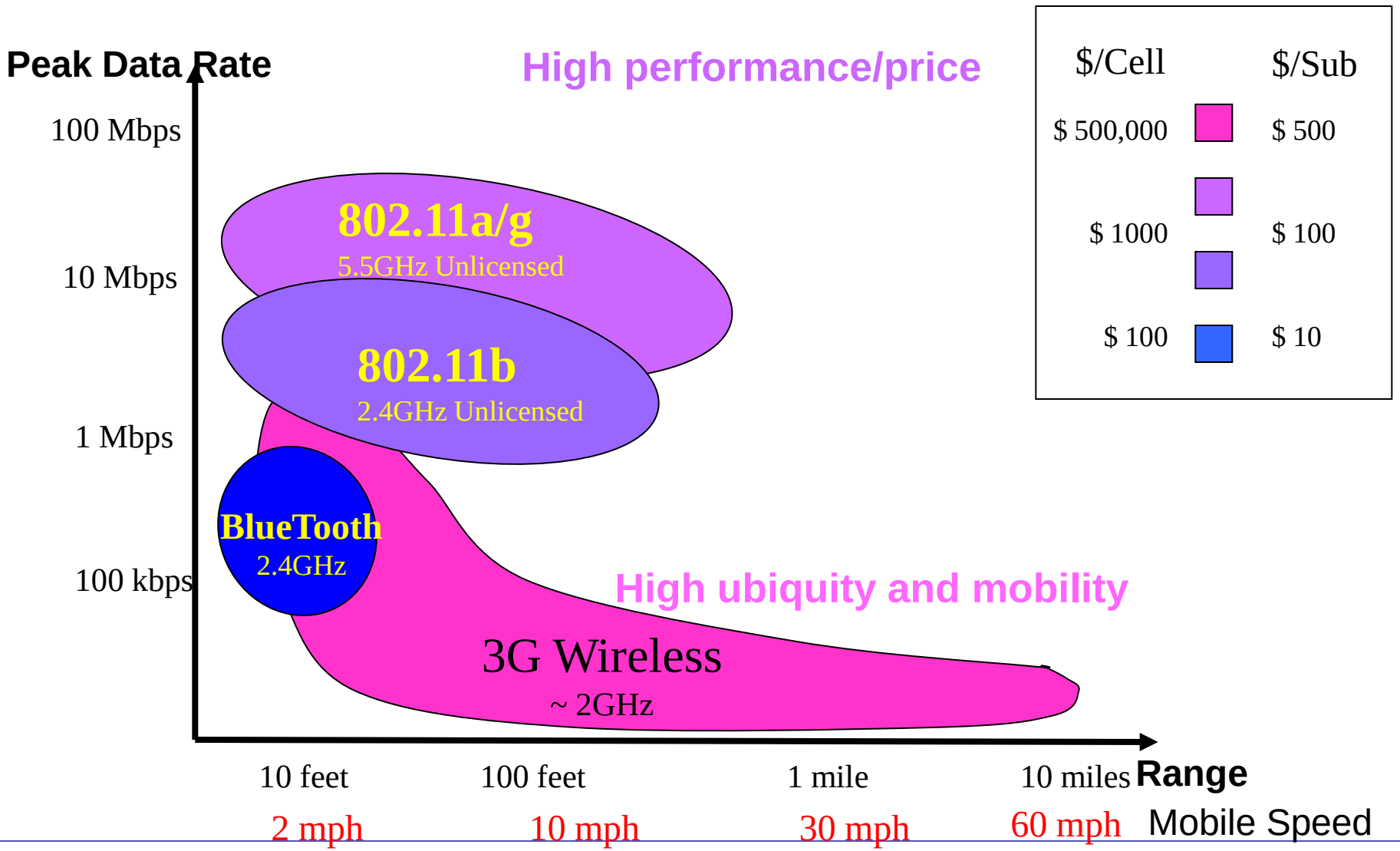
- L' 802.11a base è "fuori legge" in Europa
- E' invece consentito l'utilizzo della variante 802.11h con funzionalità di:
  - *Transmission Power Control (TPC)*
  - *Dynamic Frequency Selection (DFS)*
- In dettaglio:
  - 5.15 – 5.35 GHz: uso indoor con Potenza massima 200* mW
  - *5.47 – 5.725 GHz: uso indoor/outdoor on Potenza massima 1* W*

* limite sull'EIRP

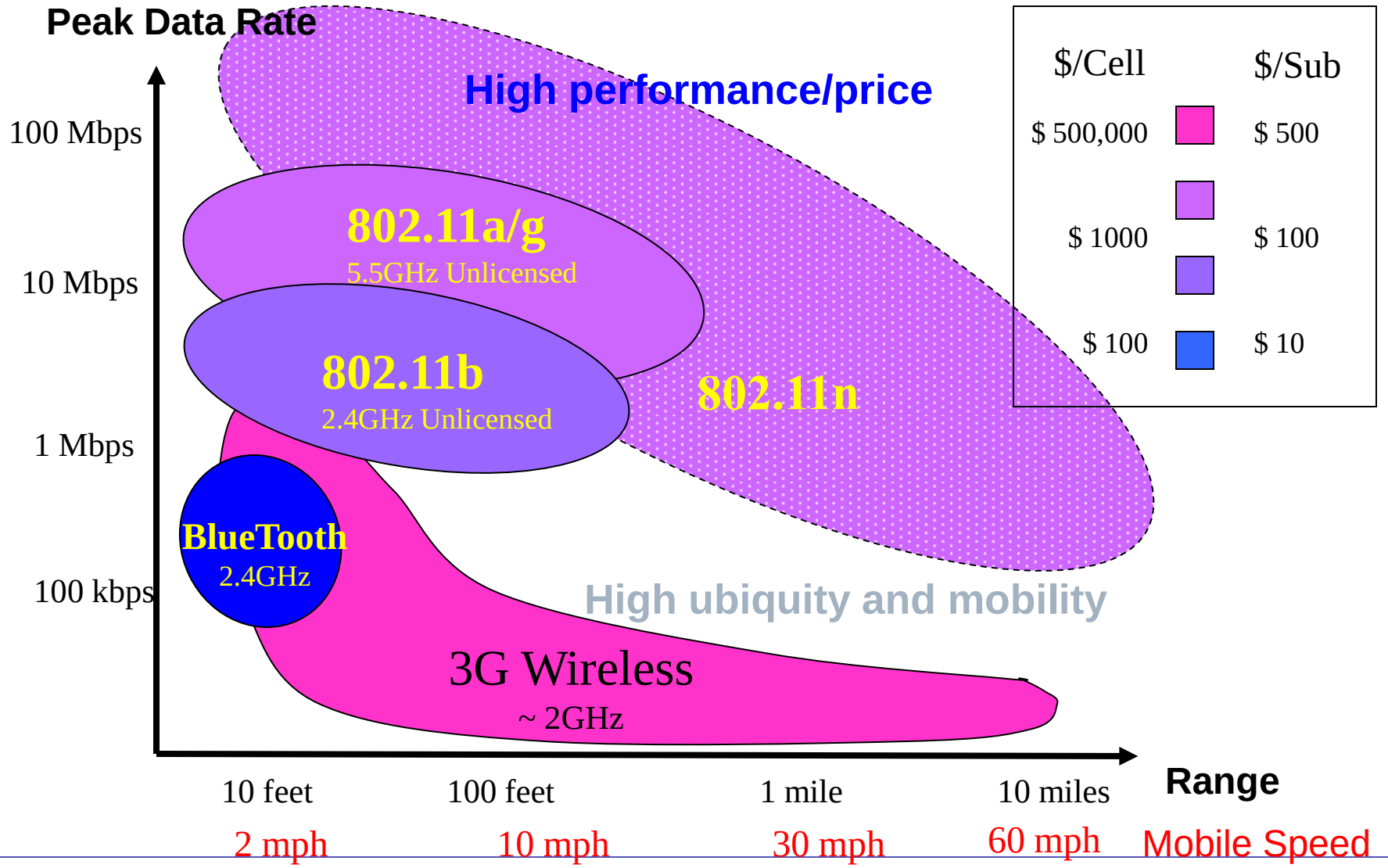
Normativa italiana - Decreto Gasparri del 28/05/03

- Si applica a reti locali wireless sia in banda 2.4GHz ahe in banda 5 GHz
- Limiti di potenza stabiliti da Decisione Europea (DE)
- Su suolo pubblico o in locali ad accesso pubblico (aeroporti, stazioni, grandi magazzini, ecc..):
  - Obbligo di registrazione al Ministero
  - Obbligo di autenticazione degli utenti
  - Obbligo di accounting
  - Obbligo di conservazione dei *log*
- Su suolo privato:
  - Nessuna restrizione (tranne quelle sulla potenza)

Panoramica Sistemi Wireless



L'evoluzione



Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

L'evoluzione delle WLAN

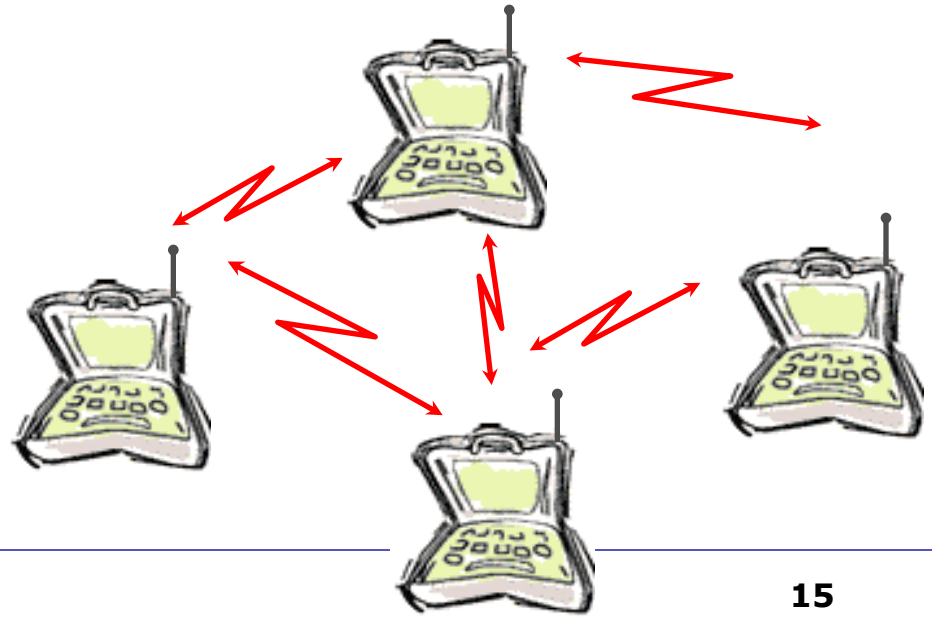
Motivazione e storia

Organizzazione della standardizzazione

Programmi di certificazione *WiFi™*

Lo standard 802.11 - Storia

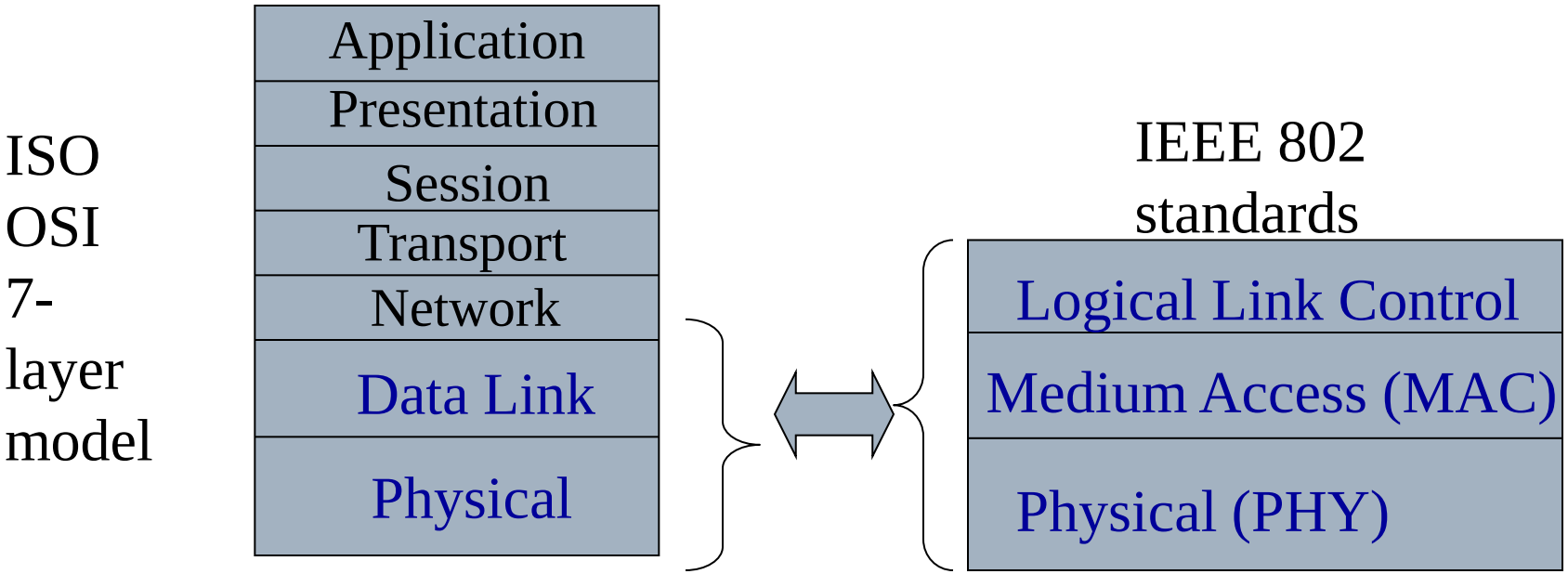
- La maggior parte delle reti locali cablate (LAN) si basano sulla tecnologia Ethernet (standardizzata da IEEE in 802.3)
- L'accesso al canale è broadcast su un mezzo a bus
- IDEA: replicare in uno scenario wireless gli stessi principi



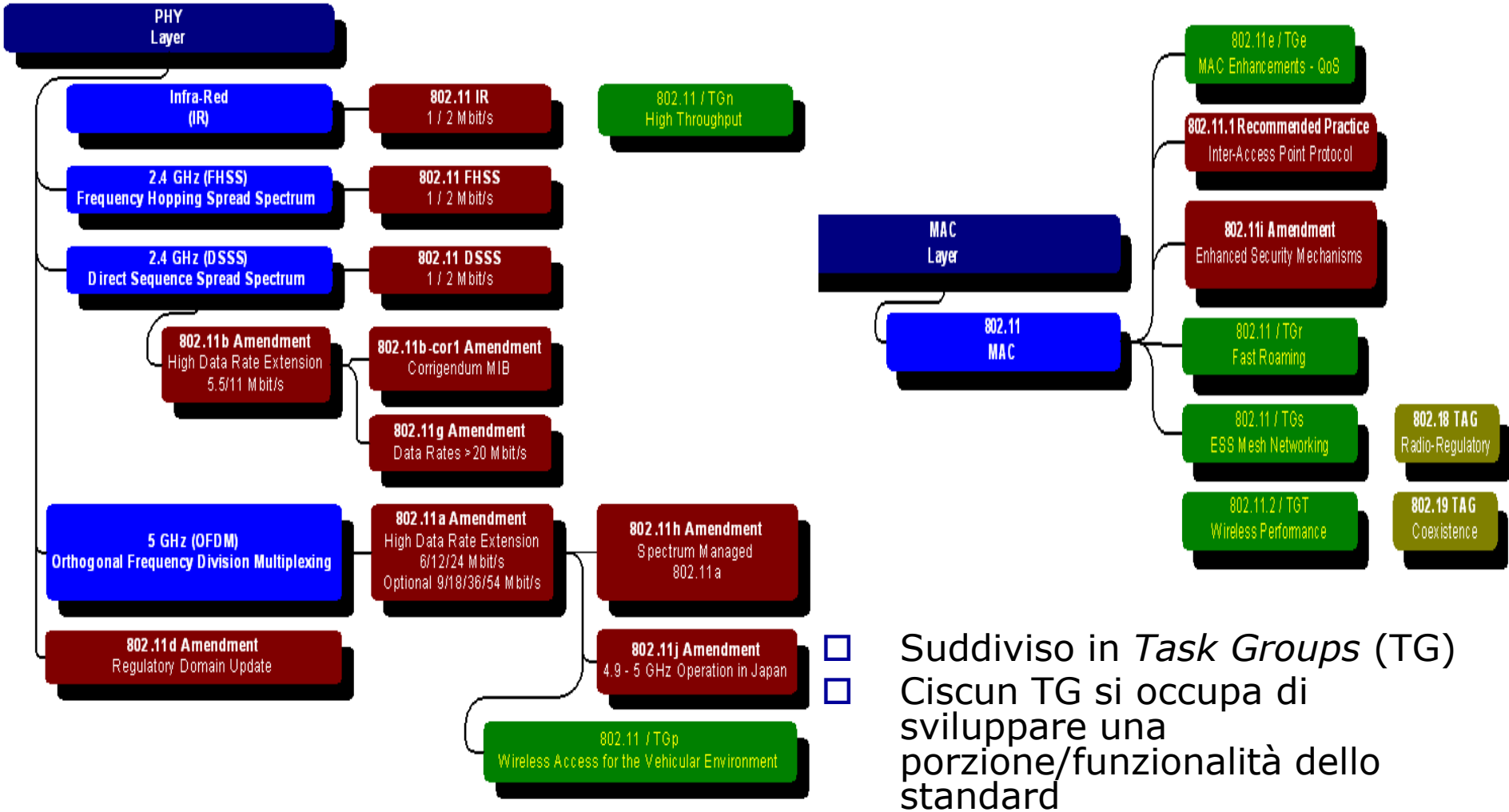
La standardizzazione

- Gli standard WLAN sono governati da IEEE sotto la guida del 802 LAN/MAN *standards committee*
- Il gruppo che si occupa delle WLAN è 802.11

  http://grouper.ieee.org/groups/802/11/



Organizzazione del gruppo 802.11



- Suddiviso in *Task Groups* (TG)
- Ciscun TG si occupa di sviluppare una porzione/funzionalità dello standard

Lo standard 802.11- *Milestones*

- Seconda metà anni ’80
  - Tecnologie propritarie per l’interconnessione LAN senza fili (prevalentemente in Nord America).
  - Operano in banda 900 MHz
- 1991: IEEE inizia la fase di standardizzazione
  - Spinta dei costruttori (*Aironet*)
- 1997: ratifica standard 802.11
  - 802.3 LAN *emulation*
  - Sono specificati 3 livelli fisici a 1 o 2 Mb/s
    - FHSS – *Frequency Hopping Spread Spectrum*
    - DSSS – *Direct Sequence Spread Spectrum*
    - Infrarosso

Lo standard 802.11 - *Milestones*

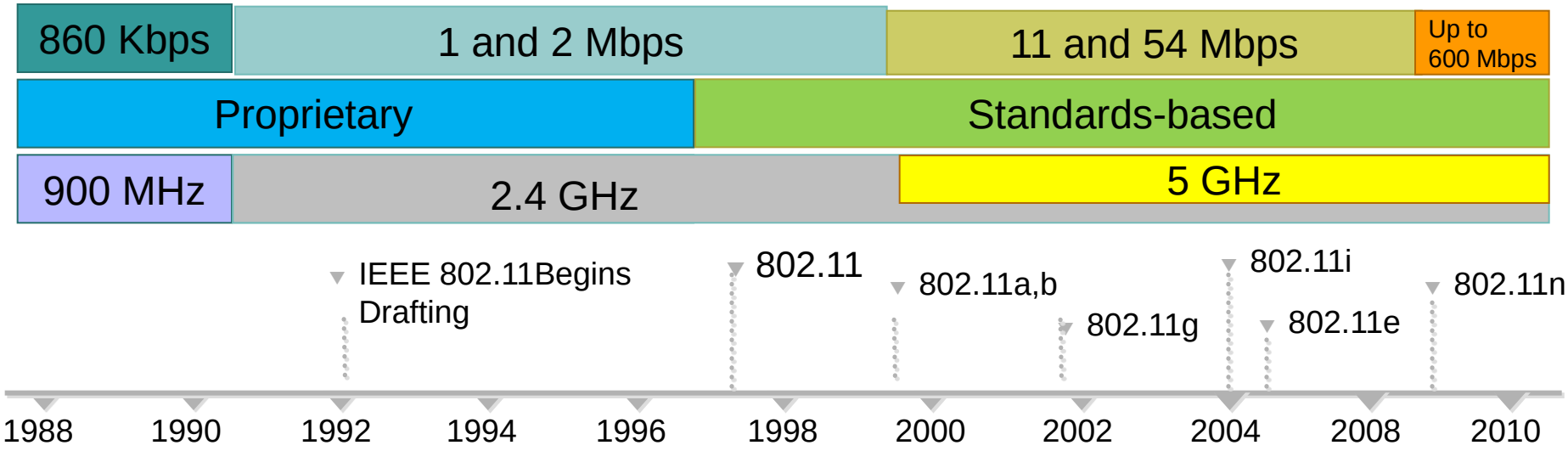
- 1999: ratifica di due nuovi livelli fisici
  - 802.11a da 6 a 54 Mb/s nella banda a 5GHz
  - 802.11b da 5.5 e 11Mb/s nella banda a 2.4GHz
- 2003:
  - Ratifica 802.11g (OFDM a 2.4GHz)
  - Ratifica 802.11F (*Inter Access Point Protocol*)
  - Ratifica 802.11h (gestione risorse radio, *channel selection* e *power control*)
- 2004:
  - Ratifica 802.11i (Sicurezza di rete)
- 2005:
  - Ratifica 802.11e (QoS)
- 2009:
  - Ratifica 802.11n (High Rate)

Task Groups Attivi

- 802.11p: estensione alle comunicazioni inter veicolari (MAC/fisico)
- 802.11s: supporto per soluzioni di rete *mesh (*Routing*)*

802.11 History

- WLAN Timeline



Wireless Ethernet Compatibility Alliance (WECA)

- Membri: Cisco, Avaya, Intel, Symbol, Proxim, IBM, 3Com, IBM, Nokia, Compaq, Dell…
- Missione:
  - Garantire l'interoperabilità tra prodotti basati su tecnologia 802.11
  - Il marchio Wi-Fi™ (*Wireless Fidelity*) certifica l'hardware 802.11
    http://www.wi-fi.org
  - Con l'obiettivo di promuovere Wi-Fi™ come standard globale
  - Supportare il *roaming*
    http://www.wifizone.org

Programmi di certificazione

- Certficazione interfacce radio:
  - 802.11a (2000)
  - 802.11b (2000)
  - 802.11g (2003)
- Certficazione architetture per la sicurezza:
  - *WiFi Protected Access* (WPA), 2003
  - *WiFi Protected Access* 2 (WPA2), 2004
- Certificazione architetture per la QoS:
  - *WiFi MultiMedia* (WMM), 2004

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Lo standard 802.11 (1997)

Requisiti ed Architettura

Il livello fisico

Il livello MAC

Obiettivi dello standard 802.11

- Scenari target:
  - Connettività indoor (uffici, negozi, centri commerciali, ospedali, aziende)
  - Connettività outdoor (parcheggi, campus universitari)
- Servizi target:
  - *Connectionless* (1-2Mb/s)
  - *Packetized*

IEEE 802.11 Overview

- Requisiti
  - Un singolo MAC che supportasse diversi livelli fisici
  - Robusto all'interferenza (interna ed esterna)
  - Robusto al problema del *terminale nascosto*
- Definisce
  - *MAC sublayer*
  - *MAC management protocols and services*
  - *Physical (PHY) layers*
    - IR
    - FHSS
    - DSSS

Componenti

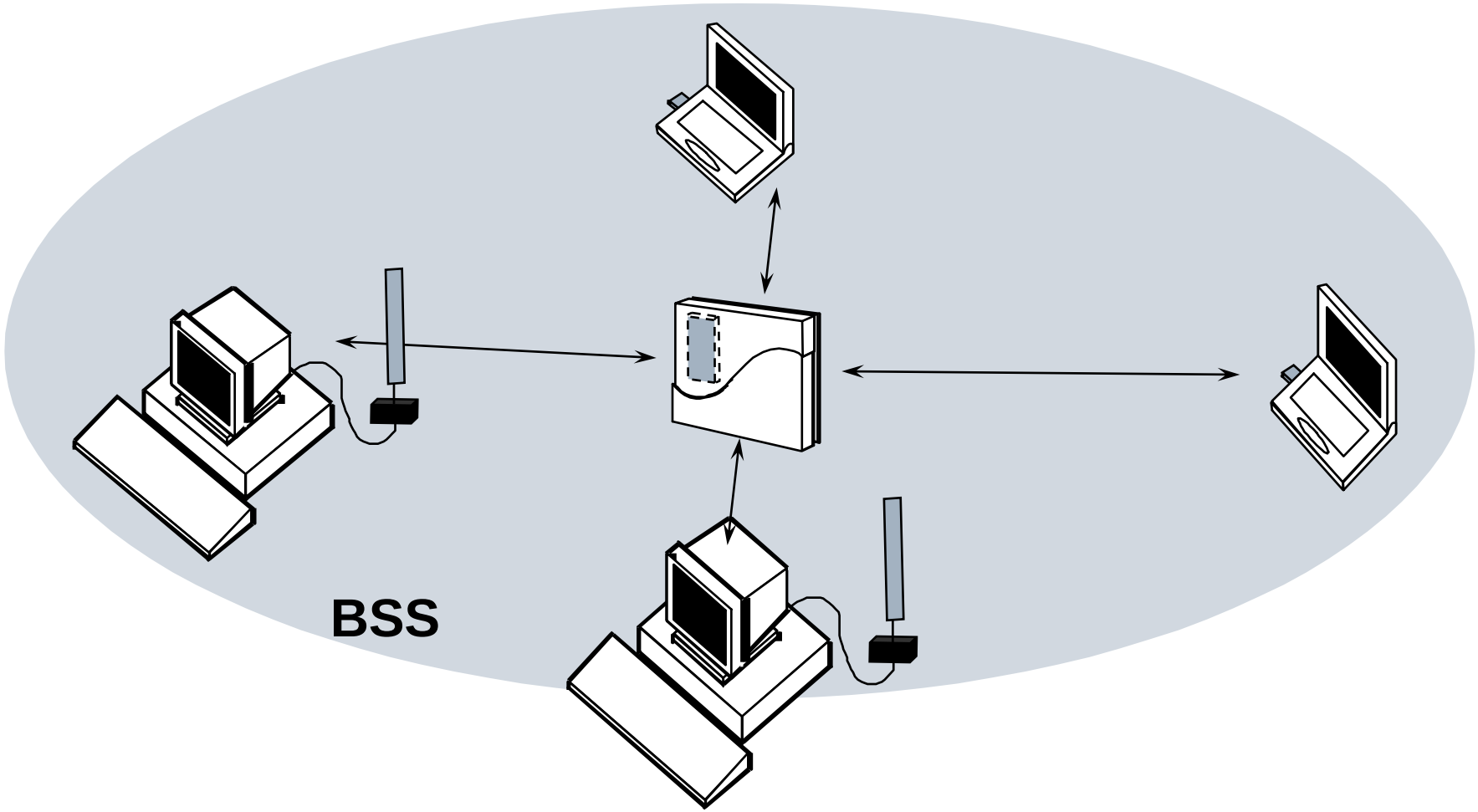
- Stazione (STA)
- *Access Point* (AP)
  - Funzionalità di *bridging wired/wireless*
- BSS - *Basic Service Set*
  - *Independent* BSS (IBSS): architettura *ad hoc*
  - *Infrastructure* BSS: architettura infrastrutturata
- ESS - *Extended Service Set*
  - Insieme di *Infrastructure* BSS.
  - Diversi *access points* collegati da:
- DS – *Distribution System* (non esplicitamente definito dallo standard)
  - Wired
  - Wireless (WDS)

Basic Service Set (BSS)

- Insieme di stazioni controllate dalla stessa "*Coordination Function*" (funzione logica che gestisce l'accesso al canale condiviso)
- Simile al concetto di cella nel mondo radiomobile
- Esistono due tipi di BSS:
  - *Infrastructure* BSS
  - *Independent* BSS (IBSS)

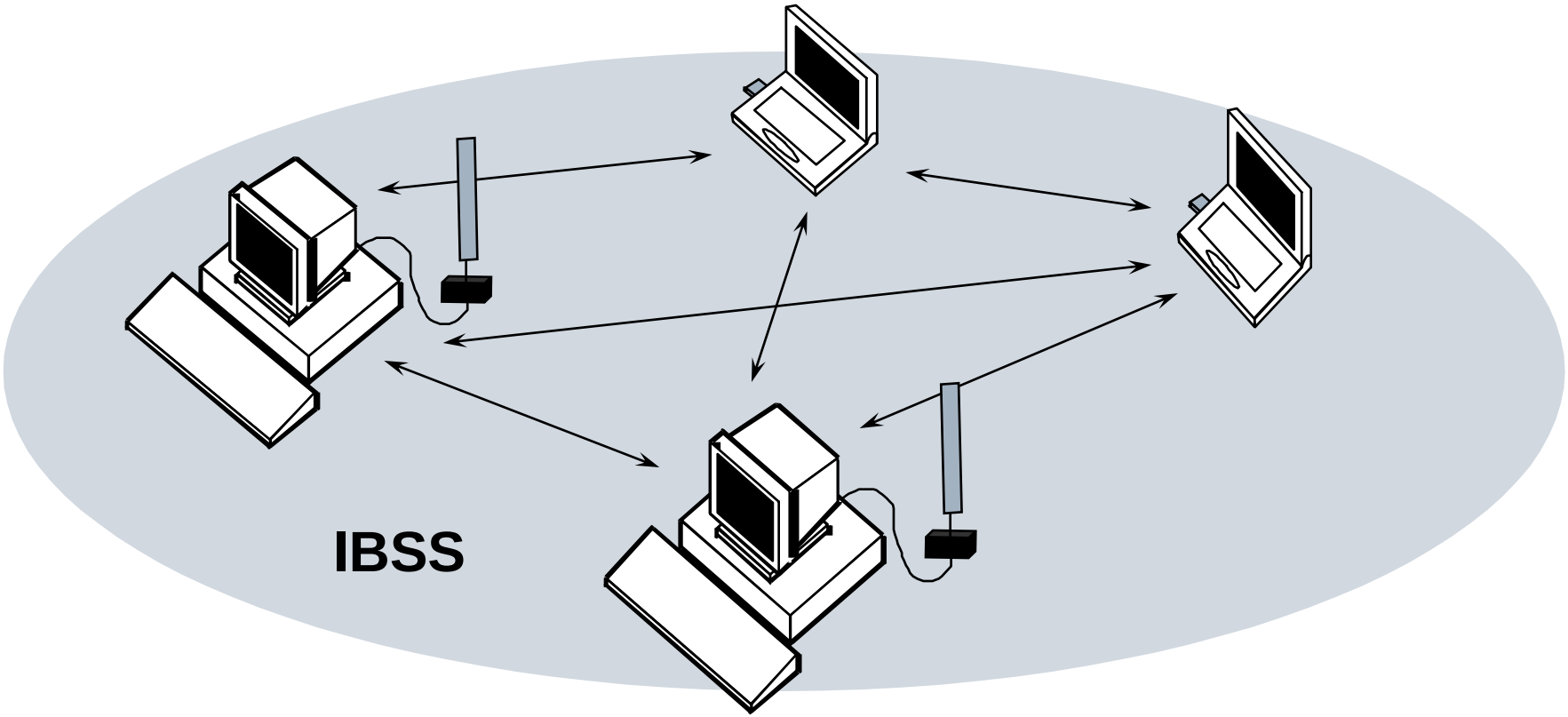
Infrastructure BSS

Modalità di interconnessione centralizzata

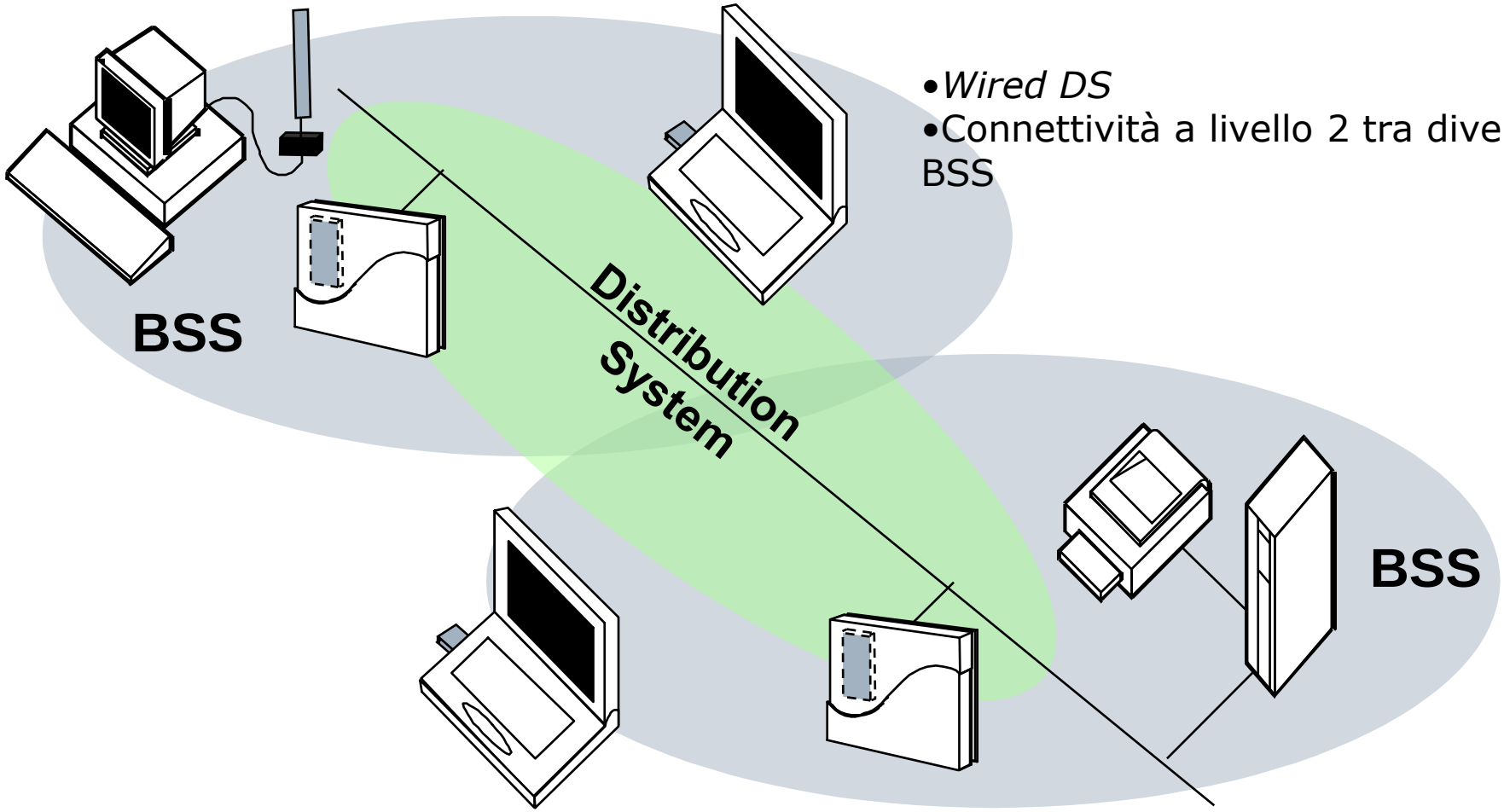


Independent Basic Service Set (IBSS)

Modalità di interconnessione ad hoc

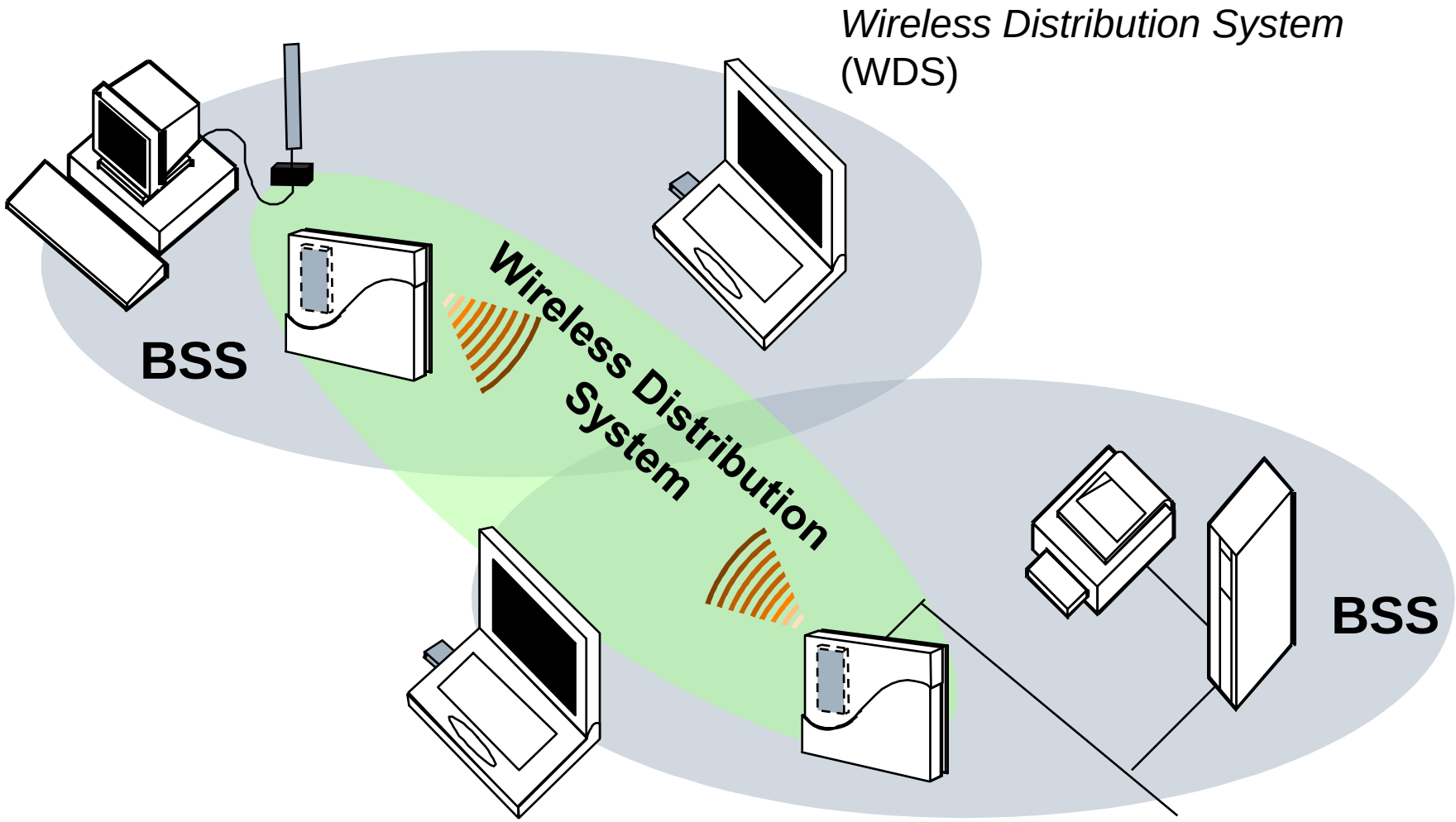


Extended Service Set (ESS)



- *Wired DS*
- Connettività a livello 2 tra diversi BSS

Extended Service Set (ESS)

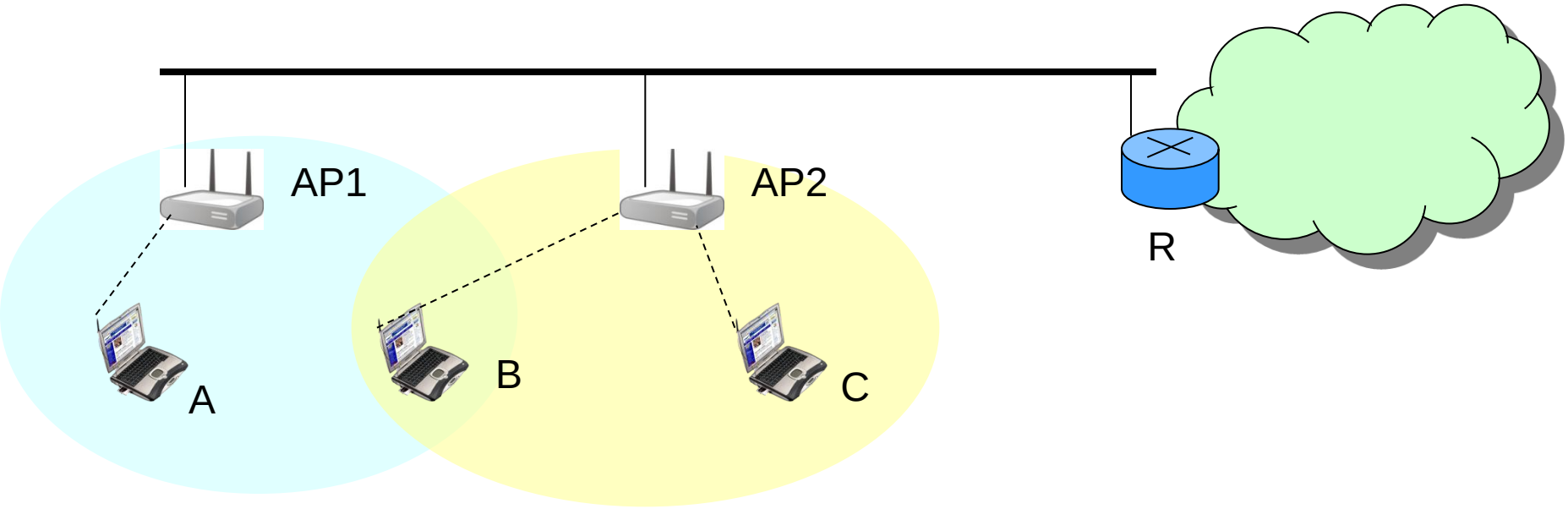


I Servizi di rete

- Si distinguono in:
  - Servizi di stazione (*Station Services*) specifici all'interfaccia wireless
  - Servizi di distribuzione (*Distribution Services*) specifici del sistema di distribuzione

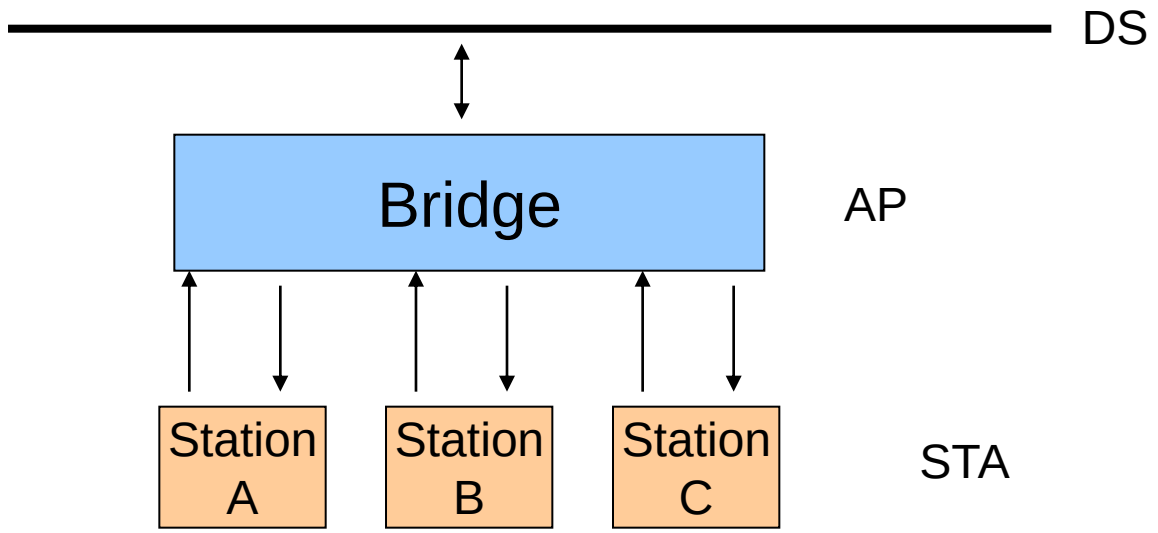
Servizio	Tipo
Distribution	DS
Integration	DS
Association	DS
Reassociation	DS
Disassociation	DS
Authentication	ST
Deauthentication	ST
Privacy	ST
MSDU delivery	ST

Distribution System



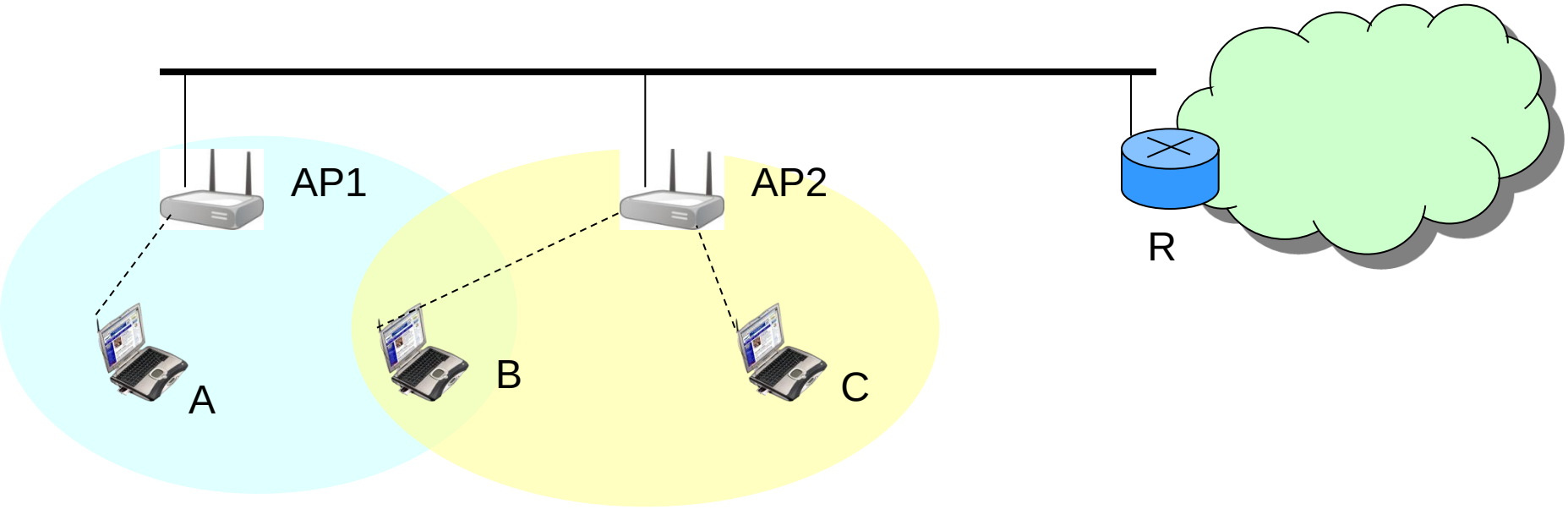
- Procedura di associazione equivante ad “attaccare il cavetto dentro la presa ethernet”
- Una STA è associata ad un solo AP
- Un ESS è una rete di livello 2, e dunque una sottorete IP con il suo spazio di indirizzamento

Distribution System



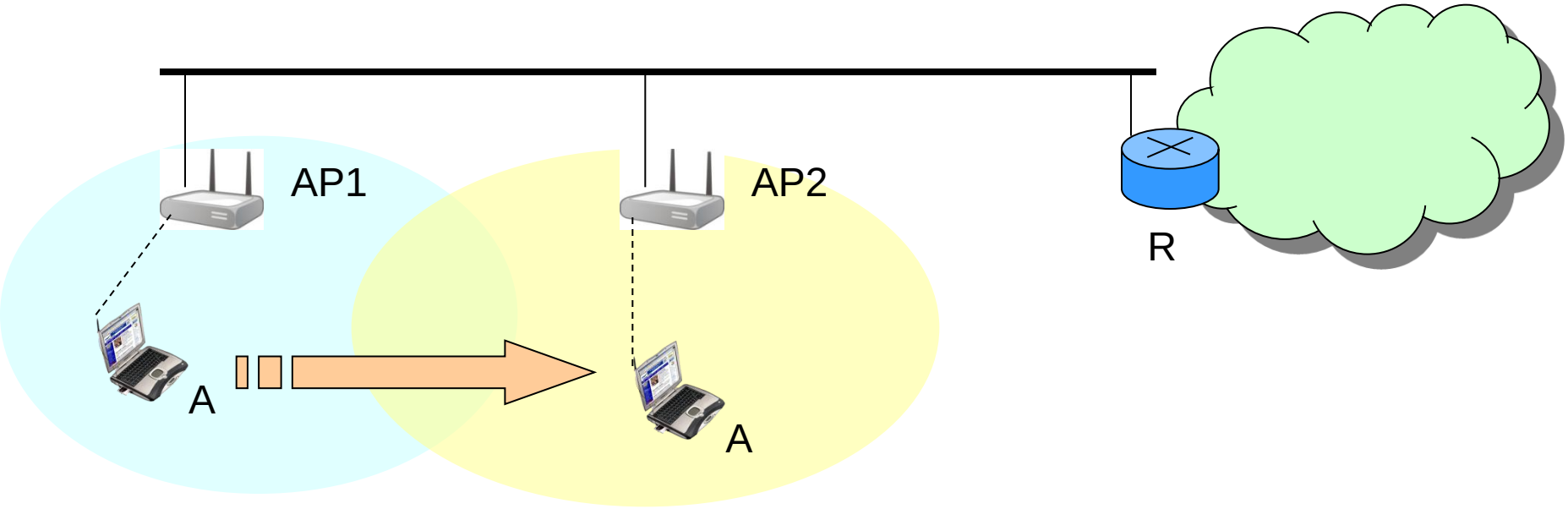
- L'access point si comporta come un bridge (layer-2 switch)
- Mantiene le tabelle di associazioni che usa per il processo di bridging
- Ad esempio le trame ricevute dal DS che contengono come destinazione un indirizzo di una STA associata vengono inoltrate sull'interfaccia radio una volta trasformate in trame 802.11

Distribution System



- Come fa un pacchetto IP ad andare dal router R alla stazione di destinazione?

Distribution System



- Come succede quando una stazione si sposta?

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Il livello MAC

Accesso al canale

Recupero di errori

Indirizzamento

Funzionalità e Servizi MAC

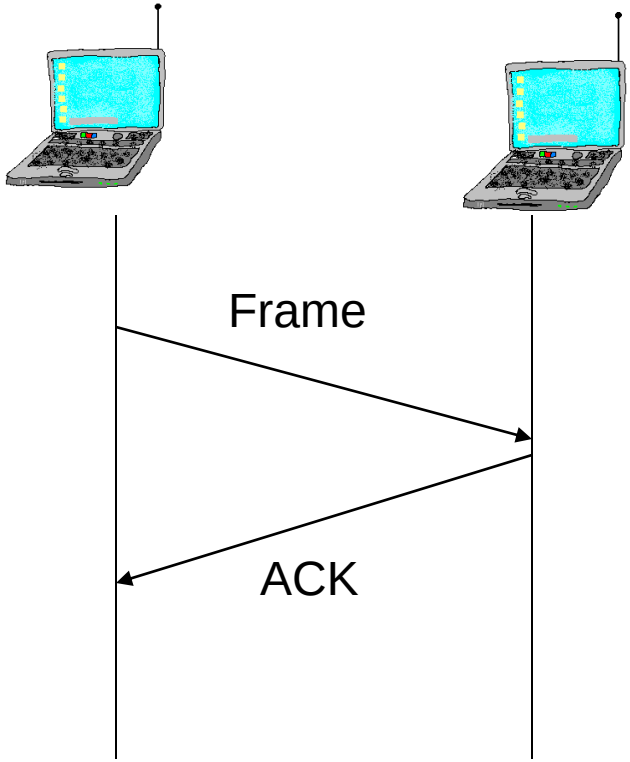
- Accesso al canale
- Recupero di errori
- Frammentazione e ricostruzione
- Risparmio energetico
- Indirizzamento e *Framing*

Accesso al mezzo fisico

- L'accesso al mezzo fisico è regolato tramite funzioni logiche di coordinamento (*coordination functions*)
- Sono definite due modalità di accesso
  - *Distributed Coordination Function* (DCF)
    - Ripresa da Ethernet
    - Si basa su accesso CSMA con *backoff*
  - *Point Coodination Function* (PCF)
    - Fornisce accesso "*collision free*"
    - Si basa su un paradigma "*poll-response*"

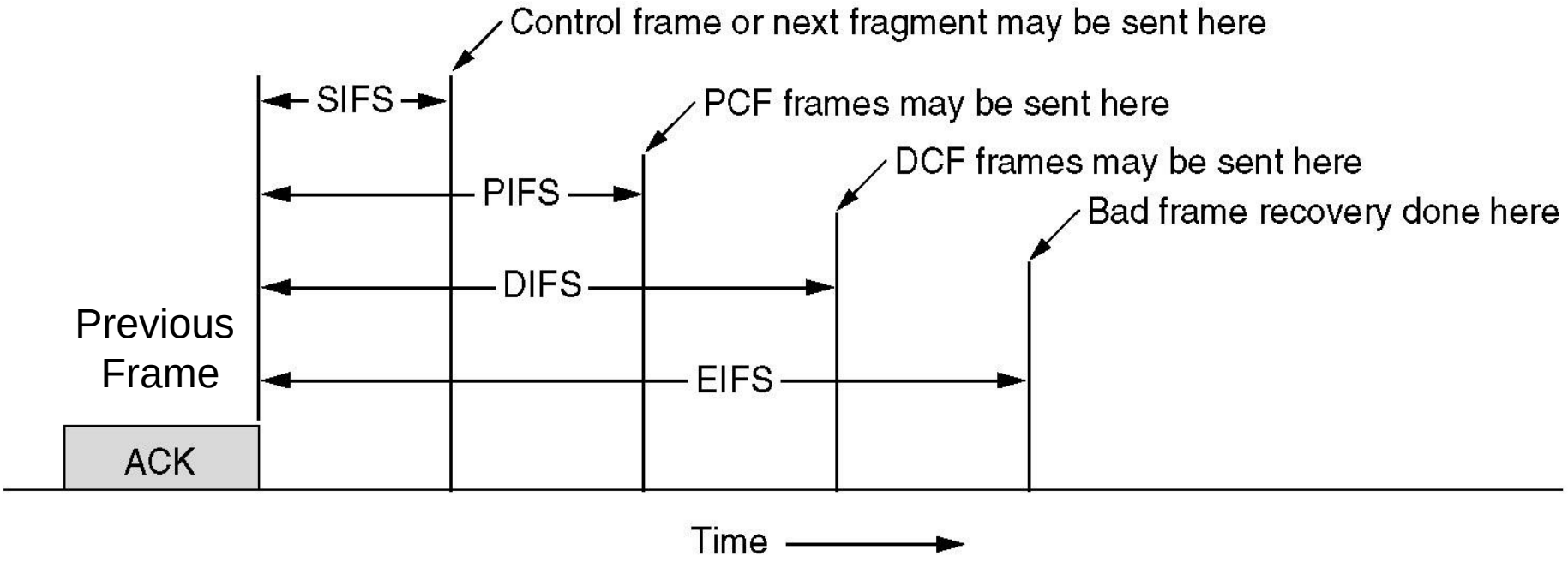
Recupero di errori

- Indispensabile in un mezzo "rumoroso"
- Definito solo per trasmissioni *unicast* (il broadcast è inaffidabile)
- Si basa sull'utilizzo di un riscontro positivo di ogni trasmissione (paradigma di tipo "*stop 'n wait*")
- Richiede l'uso di timer



C'è l'ACK in Ethernet? Perché?

Interframe spacing



- Lo standard definisce una serie di intervalli temporali che regolano l'accesso al canale
- Il meccanismo base di accesso si basa sul *carrier sensing*

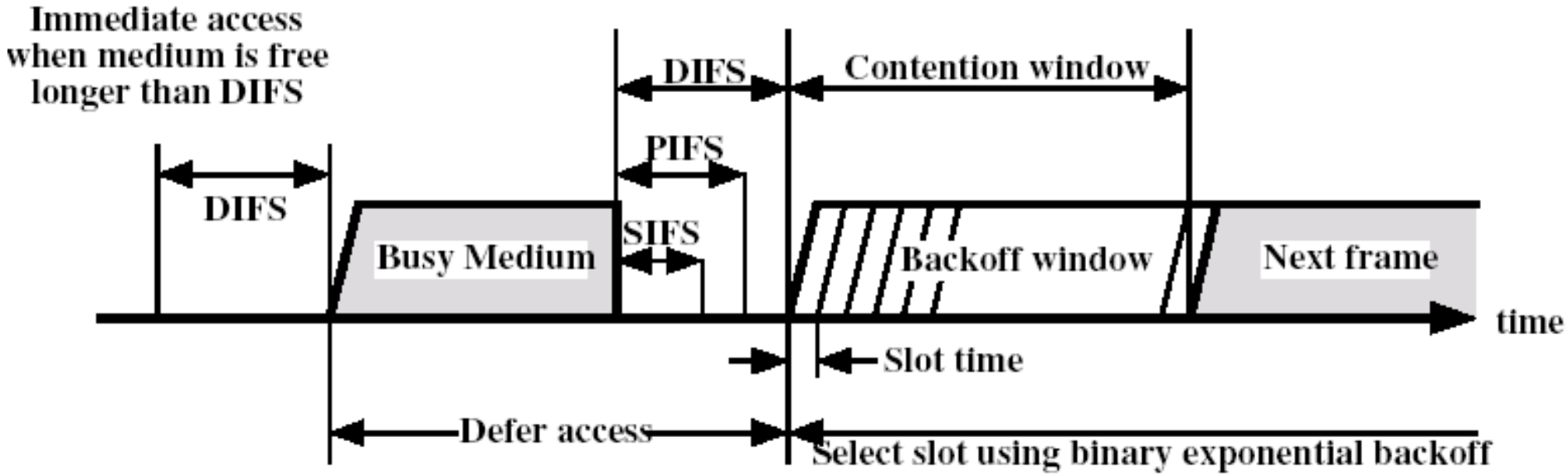
Interframe spacing

- *Short Inter Frame Spacing* (SIFS):
  - le trasmissioni ad alta priorità possono iniziare dopo la scadenza di un SIFS dalla trasmissione precedente
- *PCF Inter Frame Spacing* (PIFS):
  - Tempo medio di canale libero prima di poter accedere al canale in modalità PCF
- *DCF Inter Frame Spacing* (DIFS):
  - Tempo medio di canale libero prima di poter accedere al canale in modalità DCF
- *Extended Inter Frame Spacing (EIFS)*:
  - Usato nel caso di trasmissioni collise

L'accesso DCF

- Consente la coordinazione nell'accesso tra stazioni diverse senza bisogno di un'entità centrale
- Può essere usato sia in un IBSS che in un *infrastructure* BSS
- Si basa sul paradigma *Carrier Sense Multiple Access* con *Collision Avoidance* (CSMA/CA)
  - Prima di iniziare una trasmissione una stazione "ascolta" il canale:
    - Canale libero: la stazione trasmette
    - Canale occupato: la stazione attende ed entra in *backoff*

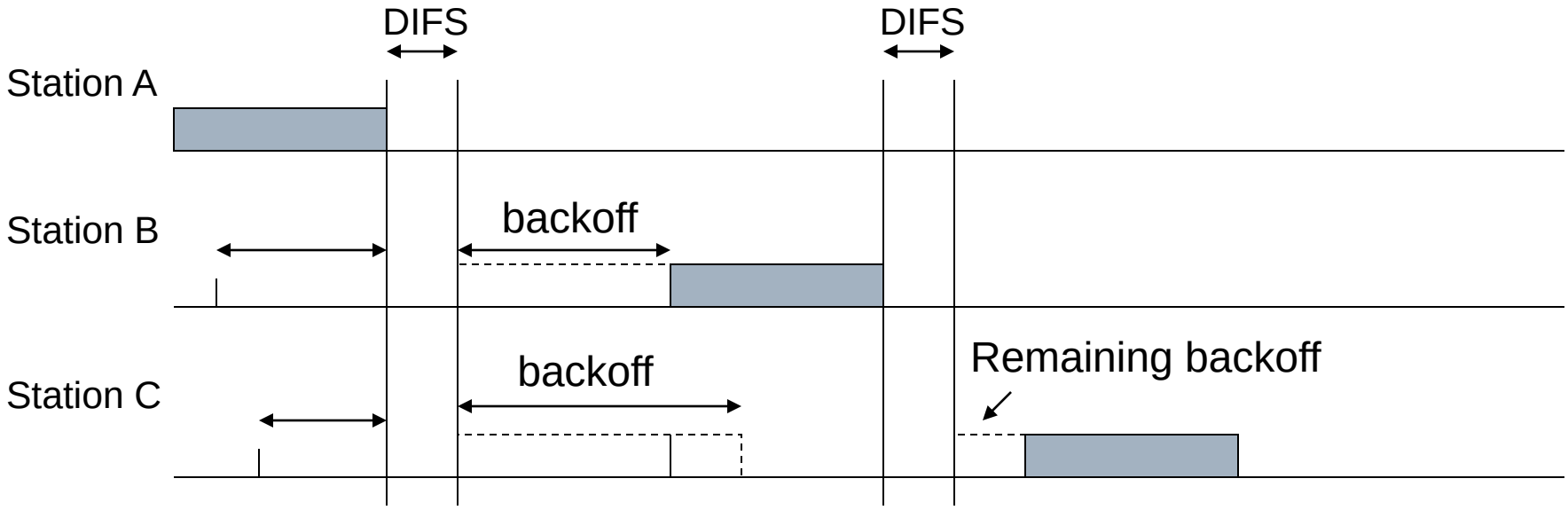
L'accesso DCF



- Se il mezzo è libero per più di DIFS trasmetti
- Se il mezzo è occupato aspetta, entra nella procedura di backoff

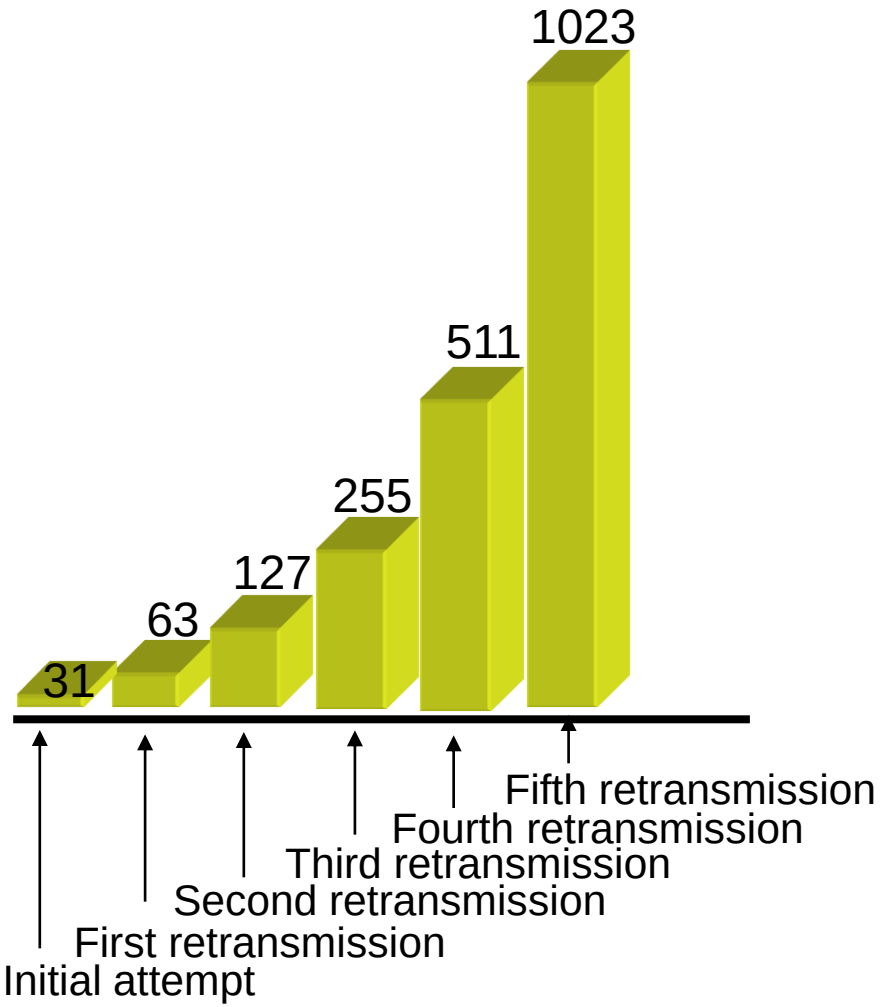
Collision Avoidance tramite *Backoff*

- Se il mezzo è occupato ogni stazione, prima di trasmettere, aspetta un numero di slot pari a DIFS + un numero casuale estratto tra 1 e CW (*Congestion Window*)
- Se durante il backoff il canale diventa occupato il conteggio si interrompe e viene ripreso quando torna libero
- Se più pacchetti consecutivi devono essere trasmessi si usa il backoff anche se il canale è libero



Il meccanismo di Backoff – il paramero CW

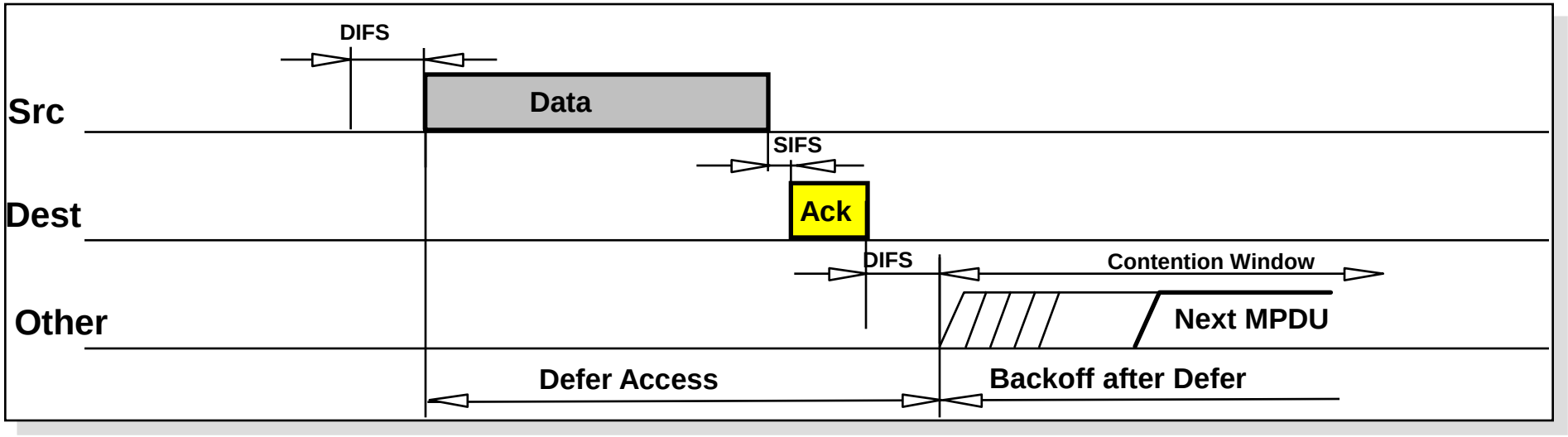
- Il numero di slot di *backoff* è scelto casulamente nell'intervallo [0, CW]
- Il valore di CW è determinato secondo le seguenti regole:
  - In seguito ad una trasmissione corrotta si pone CW = 2 (CW+1) – 1 (fino a CWmax=1023 slot)
  - In seguito ad una trasmissione corretta si pone CW=CWmin=31



Il recupero degli errori in DCF

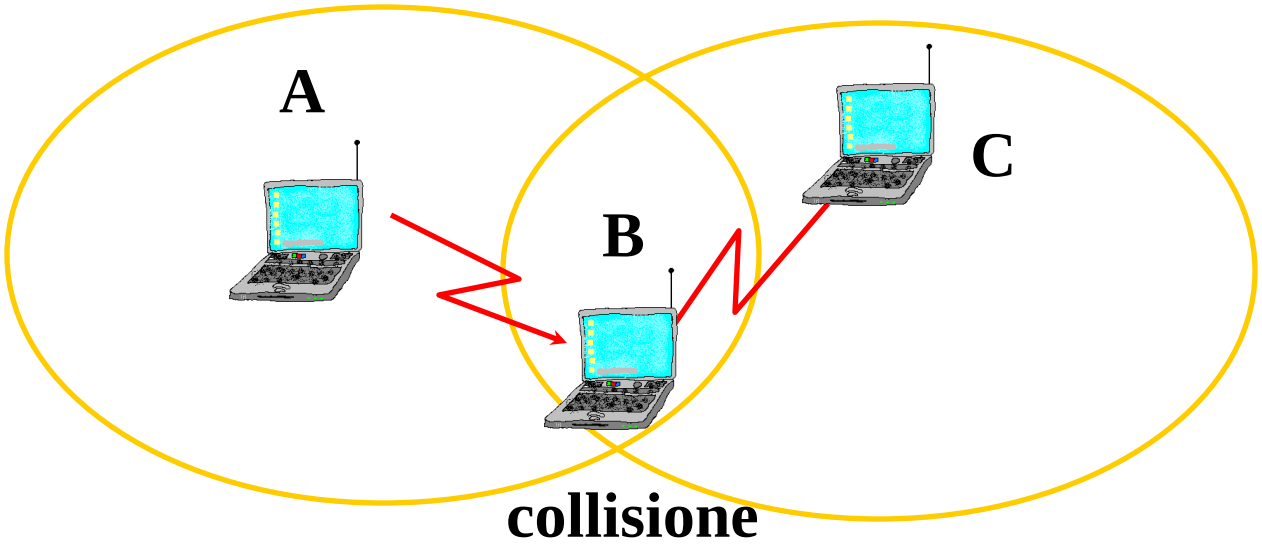
- E’ la stazione trasmittente a recuperare gli errori tramite ritrasmissione
- L’individuazione degli errori avviene tramite un meccanismo basato sul “*positive acknowledgement*”
  - Ogni trama *unicast* deve essere riscontrata
  - Se non viene riscontrata è dichiarata persa e viene ritrasmessa
  - Esiste un limite massimo sul numero di ritrsmissioni per trama
- Contatori di ritrasmissione (*Retry Counters*)
  - *Short Retry counter (per trame corte)*
  - *Long Retry counter (per trame lunghe)*

Esempio sequenza di trasmissione



- SIFS < DIFS, gli ACK hanno priorità d'accesso rispetto al traffico dati

L' *Hidden Terminal*

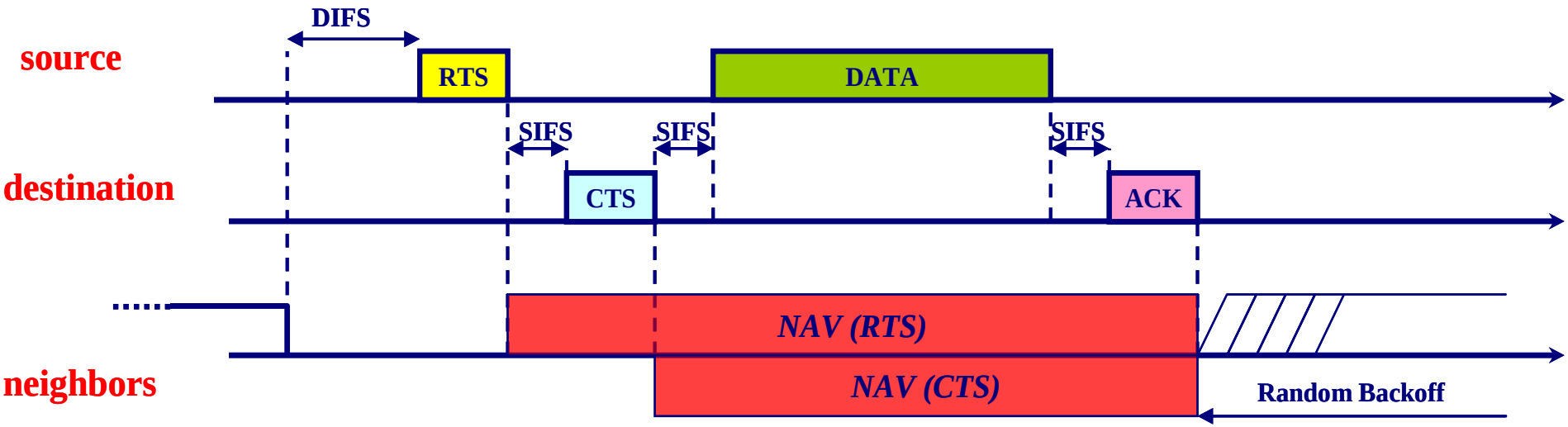


- La stazione A è nascosta alla stazione C
- Problema di collisione ad un ricevitore in comune

Soluzione all'*Hidden Terminal*

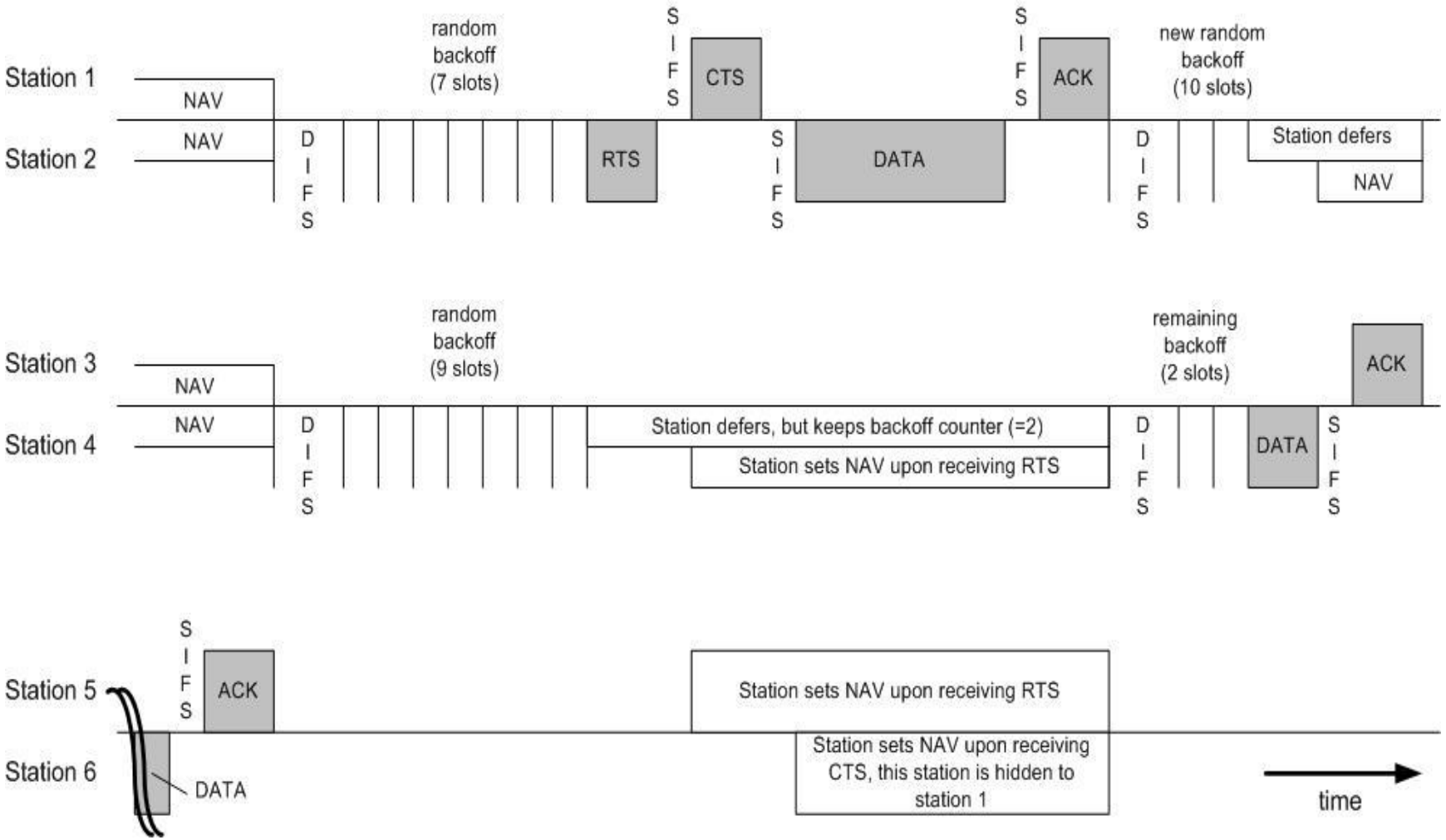
- Lo standard aggiunge una procedura di *carrier sensing* logico a quello fisico
- Utilizzo di trame di controllo in cui viene codificato il *Network Allocation Vector* (NAV)
- Il NAV riporta la durata della comunicazione in atto
- Le stazioni che ricevono le trame di una comunicazione in atto non accedono al canale per il tempo codificato nel NAV delle trame corrispondenti

Il *Carrier Sense* Virtuale

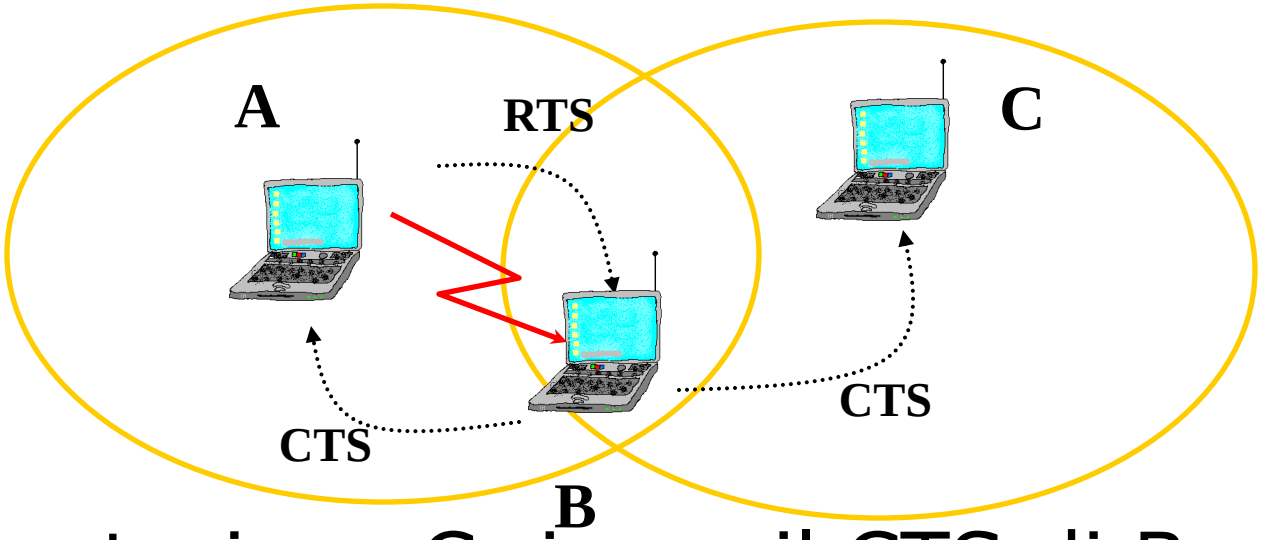


- Ingredienti
  - Trame di controllo (*Request To Send, Clear To Send*)
  - NAV

Esempio trasmissione con con Carrier Sense virtuale



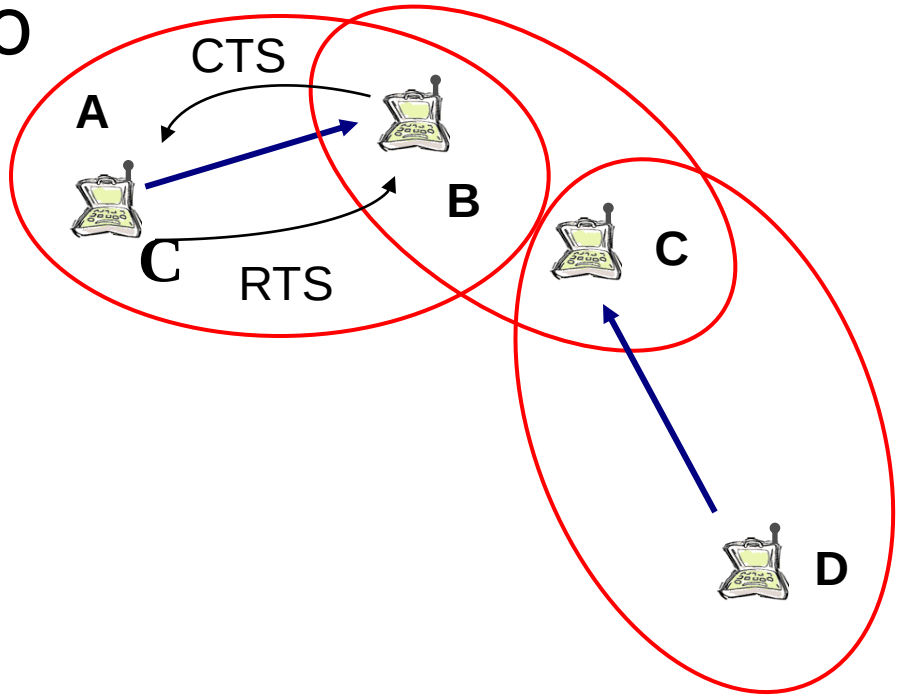
Vantaggi della procedura d'accesso con NAV



- La stazione C riceve il CTS di B e non accede al canale per tutta la durata della trasmissione A-B
- Risoluzione del problema del terminale nascosto

Svantaggi della procedura d'accesso con NAV (1)

- Insorgere del problema del "terminale esposto"
- Riduzione del riuso
- Soluzioni
  - Scheduling "intelligente" delle connessioni
  - Pianificazione in frequenza



Svantaggi della procedura d'accesso con NAV (2)

- Riduzione della capacità del sistema (*Overhead* introdotto dallo scambio dei pacchetti di controllo)
- L'efficienza del NAV dipende da:
  - Caratteristiche del canale
  - Dimensione delle trame in trasmissione
- Lo standard definisce una soglia (*RTSThreshold*) sulla dimensione (D) delle trame in trasmissione
  - Se D < *RTSThreshold* il NAV non è usato (si preferisce ritrasmettere)
  - Se D > *RTSThreshold* il NAV è usato (si preferisce proteggere la trasmissione)

Point Coordination Function (opzionale)

Meccanismo di accesso "*contention free*"

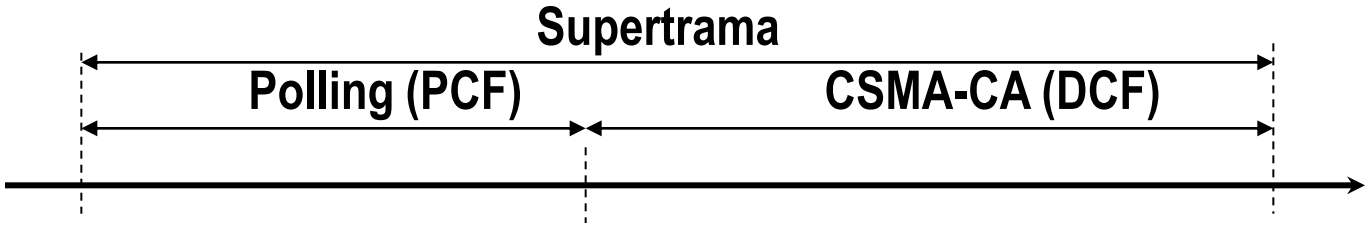
Supporto di traffico *real-time*

PCF – Generalità (1)

- L'accesso al mezzo è gestito da un "*point coordinator*" implementato nell'AP
- PCF funziona solo in un'architettura di rete centralizzata (*infrastructure* BSS)
- Le stazioni associate possono trasmettere dati solo dopo esplicita segnalazione del "*point coordinator*"
- Simile ai sistemi d'accesso "*token based*"

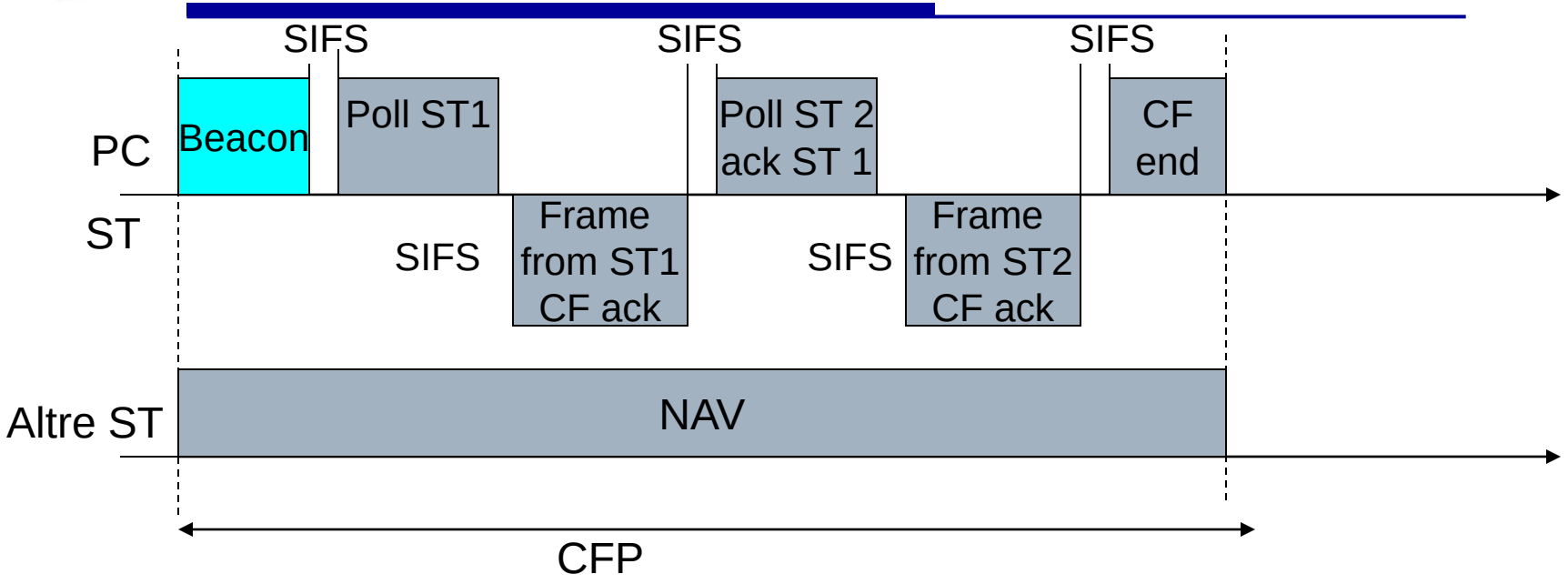
PCF – Generalità (2)

- La vita della rete è divisa in periodi governati dalla DCF (*contention based*) e periodi governati dalla PCF (*contention free*) che si alternano



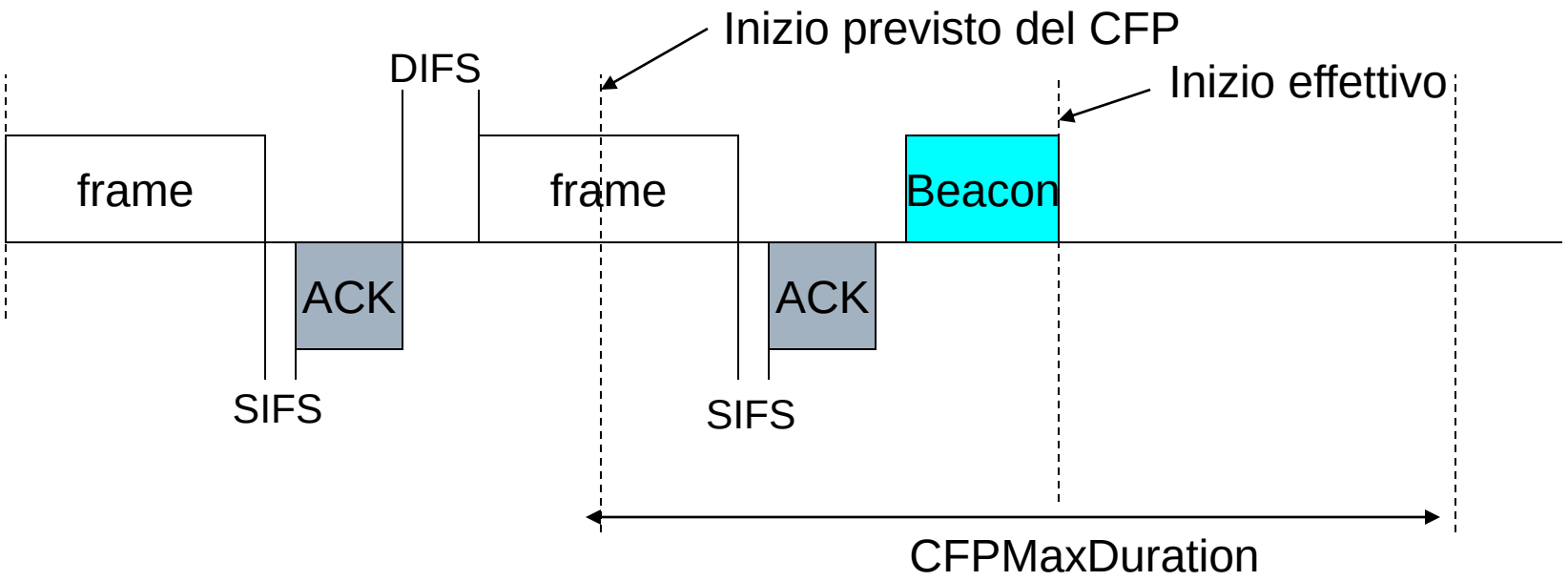
- La temporizzazione della supertrama è fornita da trame di *beacon* trasmesse dall'AP

Dinamica dell'accesso PCF



- All'inizio di un C*ontention Free Period* (CFP) l'AP invia una trama di *beacon* con l'indicazione della durata massima del CFP (*CFPMaxDuration*)
- Tutte le stazioni che ricevono la trama di beacon settano il NAV per *CFPMaxDuration* (DCF inibita)
- In un CFP le trasmissioni seguono un paradigma POLL/RESPONSE (con *piggybacking*)

Durata del CFP



- Nel caso in cui la fase contention si protragga, l'inizio del CFP viene ritardato e la sua durata ridotta del ritardo
- L'AP può interrompere il CFP (*CF-End Frame*)

Commenti

- PCF scarsamente diffusa per motivi di complessità della gestione
  - Nessuna limitazione sulla durata delle trasmissioni
  - Ritardi nella trasmissione dei *beacon*
- Di fatto non esiste nessuno strumento a livello MAC per la gestione della QoS
- Necessità di evoluzioni dello standard (802.11e)

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Sintassi del MAC 802.11

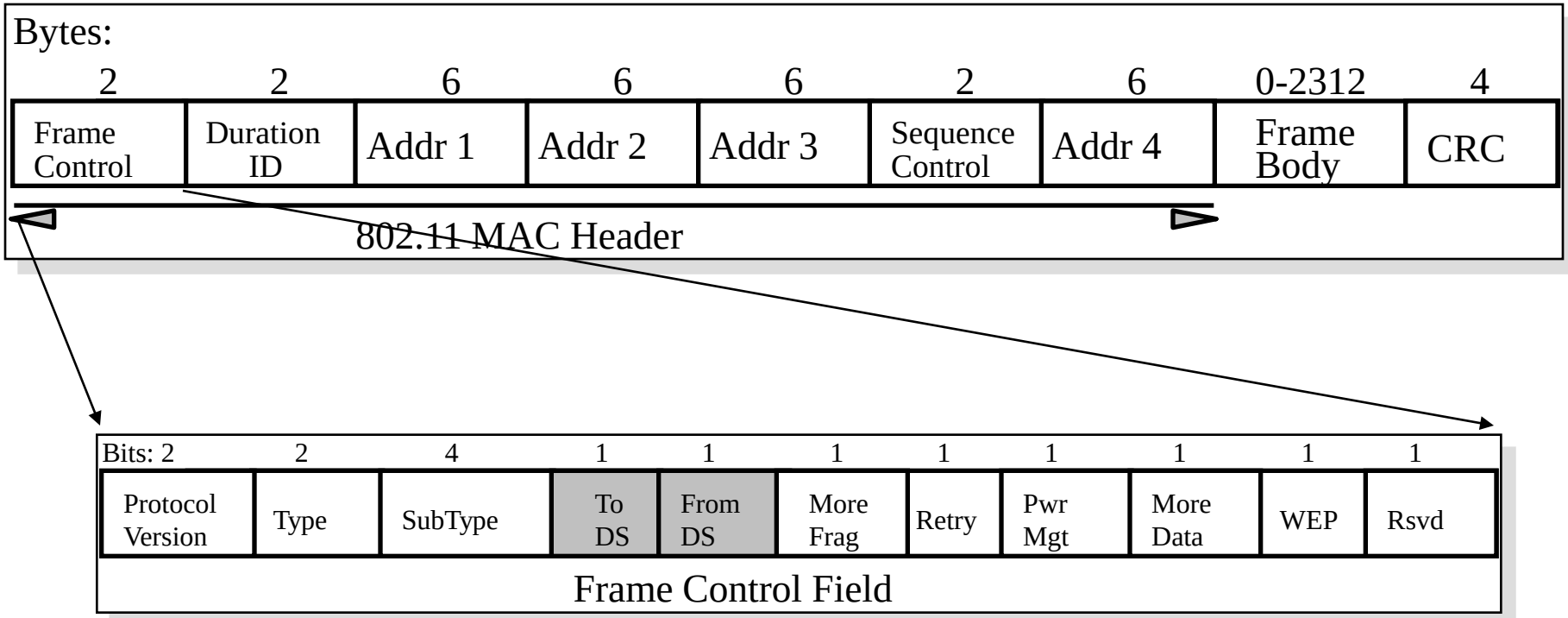
Formato delle trame

Indirizzamento

Warning

- L'approccio dello standard è quello di definire un unico MAC che supporti diversi livelli fisici
- Con l'obiettivo di replicare funzionalità e servizi dell'ethernet
- Il MAC 802.11 è complesso dal punto di vista sintattico
  - Elevato numero di trame
  - Complessità nell'interpretazione

Il formato generale delle trame: il *Frame Control Field*



- *Protocol Version*: indica il tipo di MAC implementato (attualmente 1 solo MAC definito)

Type e Subtype

- La combinazione di questi due campi identifica il tipo di trama
  - Dati (type=10)
  - Controllo (type=01)
  - Management (type=00)

management

Subtype bit	**Tipo di trama**
0000	Association request
1000	Beacon
1011	Authentiction

controllo

Subtype bit	**Tipo di trama**
1011	RTS
1100	CTS
1101	ACK

dati

Subtype bit	**Tipo di trama**
0000	DATA
0001	DATA+CF ack
0010	Data+CF poll

L'indirizzamento

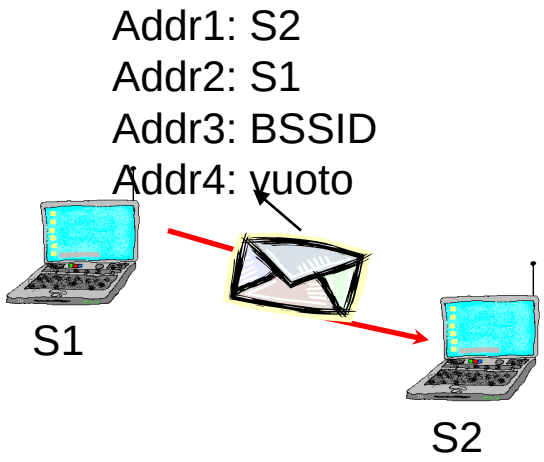
- *Destination Address (DA):* indirizzo della destinazione finale
- *Source Address (SA):* sorgente della trama in trasmissione
- *Receiver Address (RA):* indirizzo dell'interfaccia che deve processare la trama in trasmissione
- *Transmitter Address (TA):* indirizzo dell'interfaccia che trasmette la trama sul DS wireless (usato solo in caso di WDS)
- *Basic Service Set ID (BSSID):* indirizzo che identifica un BSS
  - *Infrastructure* BSS: indirizzo MAC dell'nterfaccia wireless dell'AP
  - IBSS: numero pseudocasuale

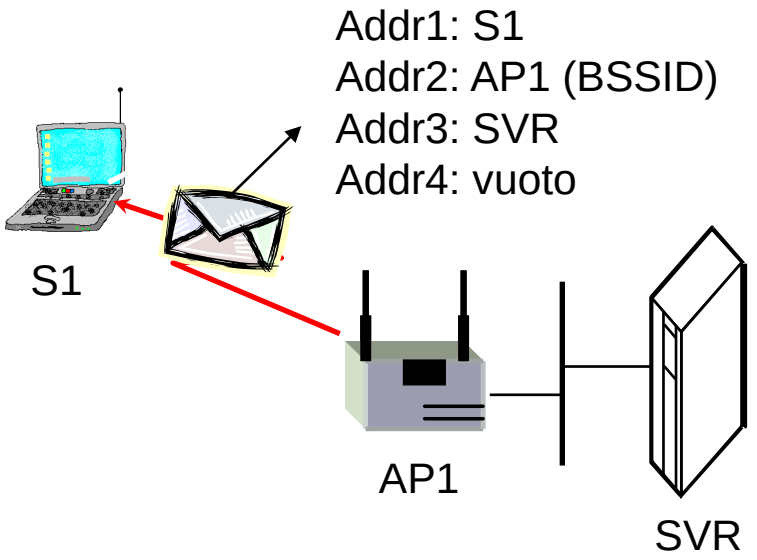
Gestione degli indirizzi

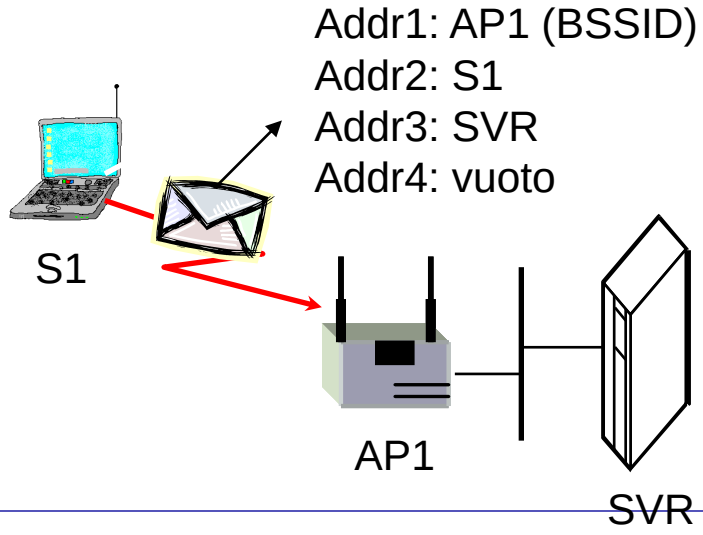
Tipo di TX	ToDS	FromDS	Address 1	Address 2	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Non usato
TO AP Infra.	1	0	BSSID	SA	DA	Non usato
FROM AP Infra.	0	1	DA	BSSID	SA	Non usato
WDS	1	1	RA	TA	DA	SA

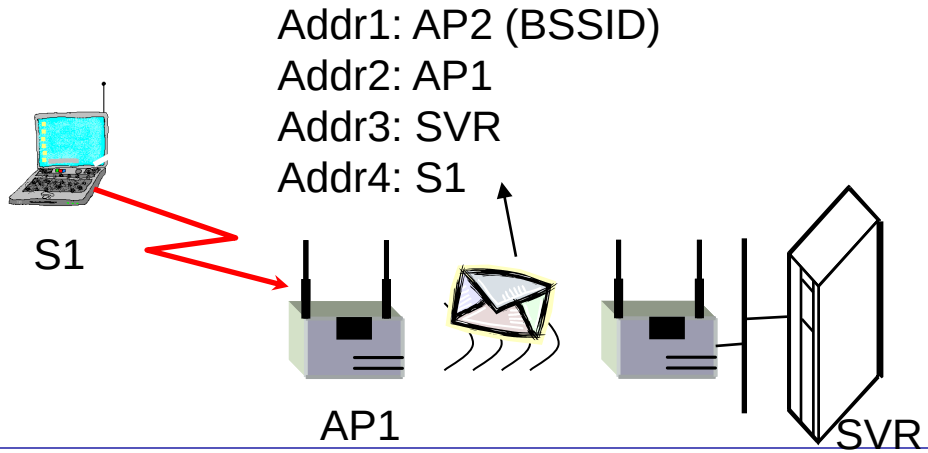
- DA: *Destination Address*
- SA: *Source Address*
- TA: *Transmitter Address*
- RA: *Receiver Address*

Gestione indirizzi









Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Network Management

Scanning

Autenticazione

Associazione

Power Management

Sincronizzazione

Procedure di *Management*

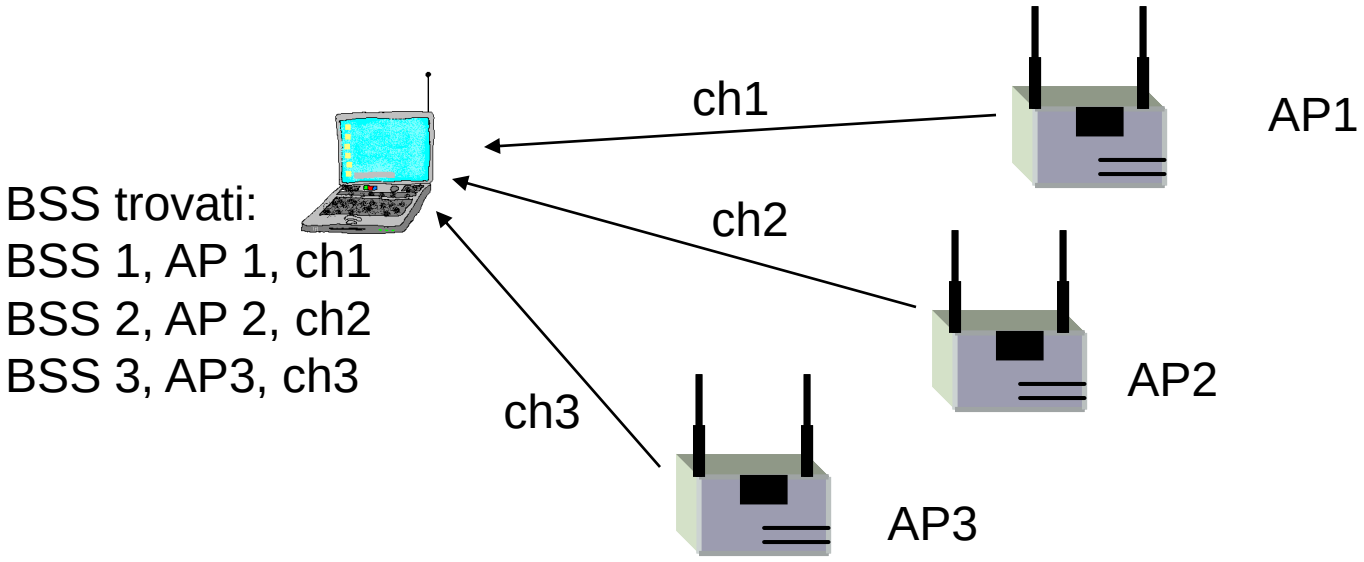
- *Scanning*: individua BSS disponibili
- *Autenticazione*: autentica la stazione all'interno del BSS scelto
- *Associazione*: crea l'associazione STA/BSS
- *Power Management*: gestisce il risparmio di potenza
- *Sincronizzazione*: procedure per il corretto funzionamento del livello fisico

Scanning

- L'obiettivo è di individuare un BSS a cui collegarsi
- Non esiste nelle reti cablate (basta trovare un *jack* di rete)
- L'operazione di *scanning* è effettuata dalla stazione
- Sono definite due modalità (generalmente configurabili)
  - Modalità passiva
  - Modalità attiva

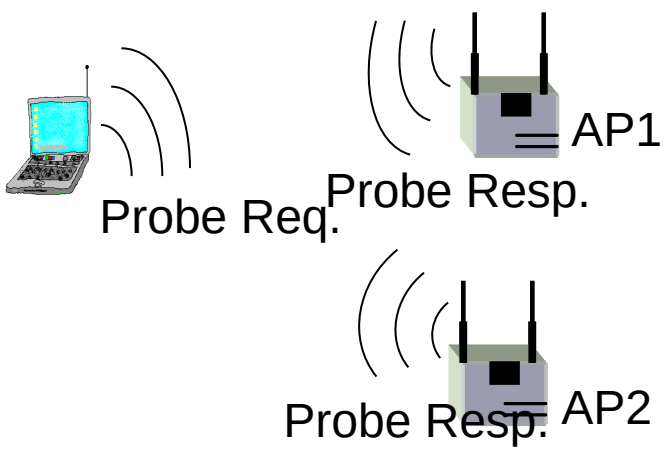
Passive Scanning

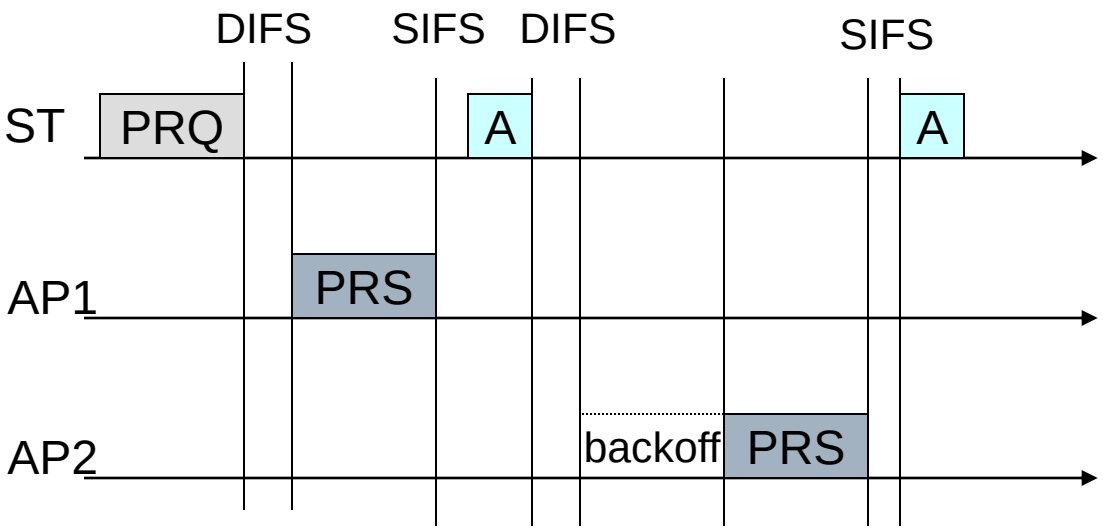
- La stazione ascolta in sequenza tutti i canali disponibili
- e memorizza tutte le trame di *beacon* che riceve



Active Scanning

- Per ogni canale disponibile, la stazione utilizza delle trame di *Probe Request* per sollecitare l'invio di una trama di *beacon*
- Le trame di *Probe Request* possono essere sia unicast che broadcast



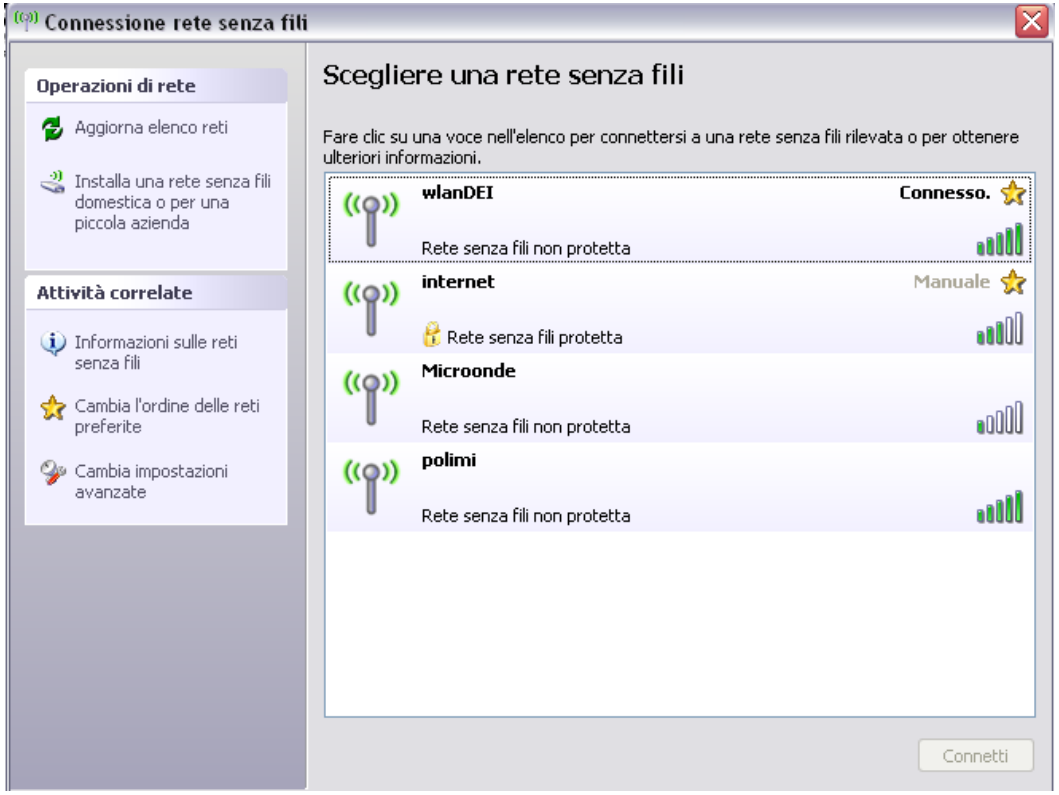


Scanning Report

- Alla fine della fase di scanning la stazione si costruisce un data base con una *entry* per ogni BSS individuato
- Per ciascuna entry sono registrati
  - BSSID, SSID, BSSType
  - Frequenza dei *beacon*
  - Info di sincronizzazione
  - Info sul livello fisico
  - Frequenza trame DTIM (gestione potenza)

Come scegliere il BSS?

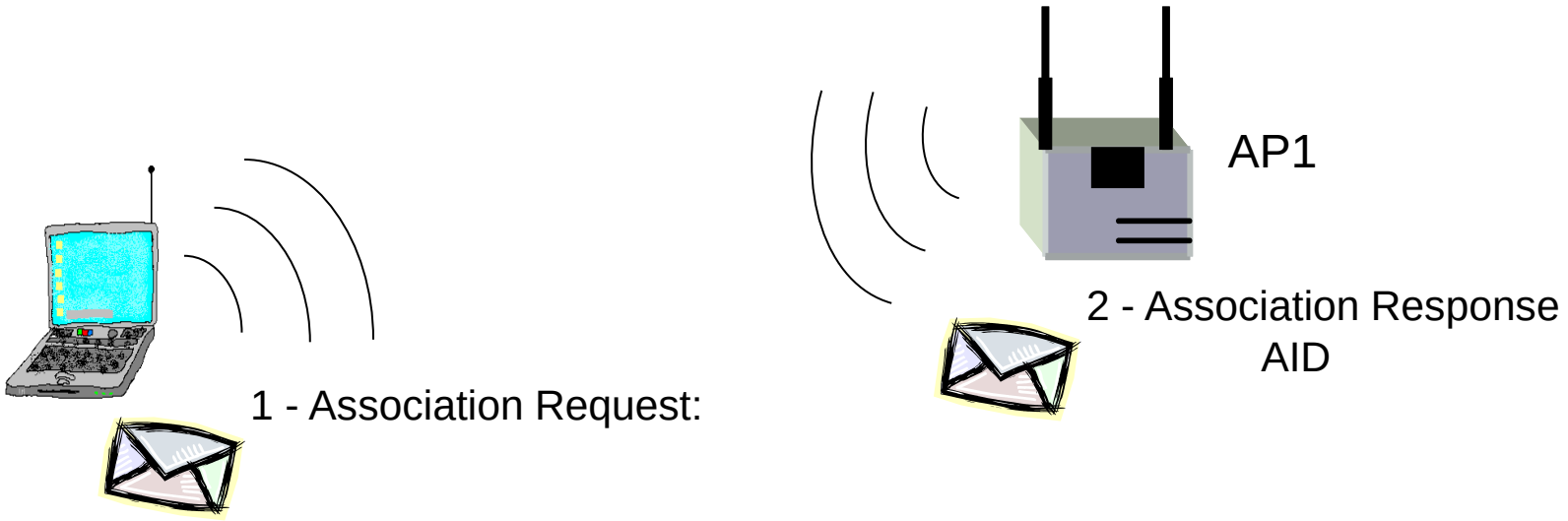
- La scelta è fuori standard
- Dipende generalmente dall'implementazione
- La maggior parte dei dispositivi sul mercato consente una scelta manuale



Associazione

- Di fatto equivale a connettere il cavo di rete alla presa di rete
- A valle della procedura di associazione
  - L'AP registra la stazione nel *data base* di associazione
  - la STA può usare i servizi del *Distribution System*
- Lo standard proibisce associazioni multiple

Associazione (2)



- Procedura iniziata dalla STA
- Scambio di trame di *management unicast*
- L'AP assegna alla STA un *Association ID* (AID) che la identifica univocamente

Power Saving

- *Infrastructure* BSS:
  - Funzionalità di *buffering* nell'AP
  - Le stazioni alternano periodi di *sleep* e di *activity*
  - L'AP segnala alle stazioni di attivarsi tramite informazione contenuta nelle trame di beacon
- *Independent* BSS:
  - Non efficiente come nel caso infrastrutturato
  - Necessità di algoritmi distribuiti
  - Generalmente non usato

Sincronizzazione

- *Infrastructure* BSS:
  - La sincronizzazione è gestita dall'AP
  - Inserisce il valore del proprio clock locale all'interno delle trame di *beacon e di Probe Response*
- *Independent BSS:*
  - Le STA si sincronizzano sul *clock* del primo che trasmette la trama di beacon

Autenticazione

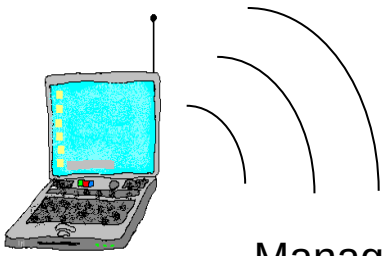
- Nell'ambiente wireless il mezzo trasmissivo è condiviso
- Potenzialmente ogni stazione dotata di un apparato rice/trasmittente *standard compliant* può accedere alla rete
- Necessità di verificare l'identità delle stazioni accedenti
- Necessità di controllare l'accesso

Autenticazione

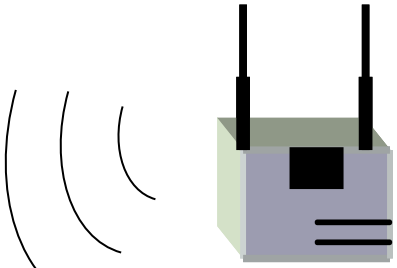
- Due tipi di approcci all'autenticazione
  - *Open System Authentication* (obbligatoria): vincoli blandi sull'accesso
  - *Shared Key Authentication* (opzionale): autenticazione basata sullo scambio di una chiave condivisa

Open System Authentication (obbligatoria)

- L'AP autentica qualunque STA che ne faccia richiesta



Management Frame:
From STA1
Authentication Algorithm: 0
(Open System)
Sequence Number: 1

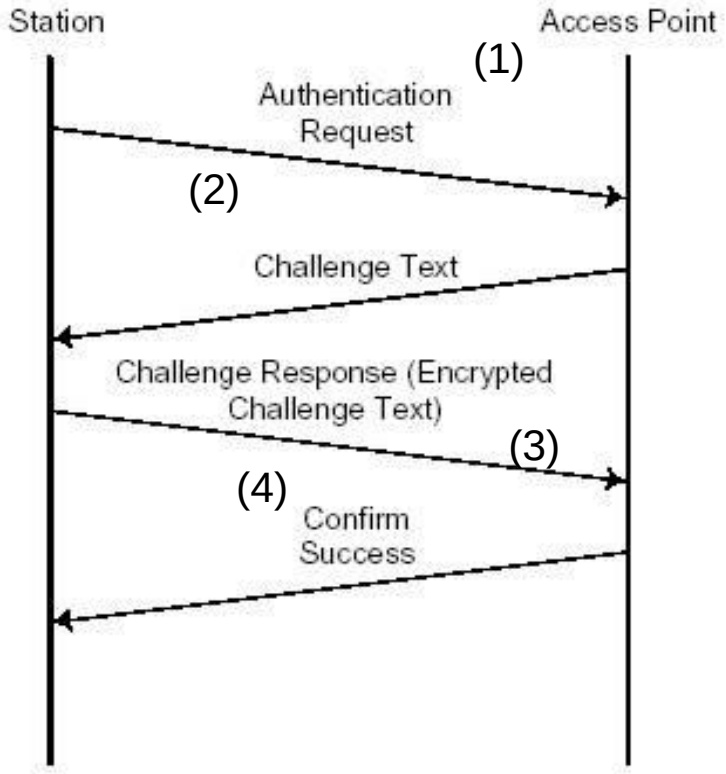


Management Frame:
From AP1
Authentication Algorithm: 0
(Open System)
Sequence Number: 2
Status Code

- Soluzione poco sicura
- Possibilità di applicare *MAC Address Filtering*

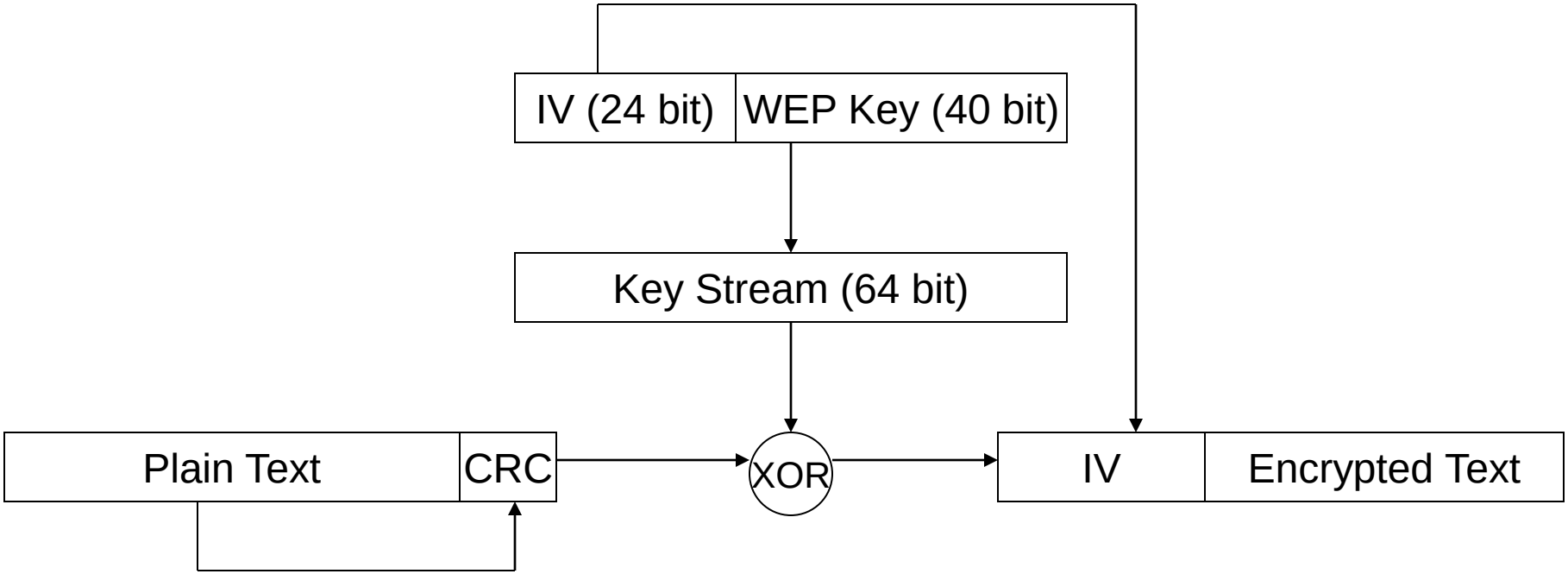
Shared Key Authentication (Opzionale)

- Due componenti:
  - Meccanismo di *challenge/response*
  - Algoritmo di crittografia a chiave privata (basato su WEP)



(1)From STA,
Authentication: 1 (SKA)
Sequence Number: 1
(2)Authentication: 2
Sequence Number: 2
Status Code: 0
Challenge
(3)Authentication: 2
Sequence Number: 3
Challenge
(4)Authentication: 2
Sequence Number: 4
Status code

Cifratura con WEP



- Algoritmo di cifratura di tipo *keystream* basato su RC4
- *Keystream* a 64 bit

Debolezze di WEP

- Riusa la stessa WEP Key per diversi pacchetti cambiando solo l'IV
  - Un AP molto "trafficato" con pacchetti di 1500 byte a 11 Mb/s esaurisce lo spazio degli IV dopo 5 ore
  - Un hacker riesce ad ottenere in 5 ore due spezzoni di messaggi codificati con la stessa chiave e lo stesso IV
  - Possibilità di attacchi statistici passivi ed attivi
- Vulnerabile dal punto di vista dell'integrità (CRC debole)
  - Un attaccante può facilmente cambiare dei bit nel pacchetto criptato e cambiare i bit corrispondenti nel CRC
  - Il pacchetto risultante è valido per il ricevente ma non ha alcun senso

Problemi di Sicurezza

- Problemi di autenticazione
  - Solo le stazioni devono autenticarsi, non gli AP
  - L'approccio è vulnerabile ad attacchi di tipo *man-in-the-middle* (un AP fittizio può intercettare il traffico di autenticazione)
- Problematiche di *privacy*
  - E' stato dimostrato che il WEP può essere violato in tempi ragionevoli (*Airsnort, WepCrack*, ecc..)
- Necessità di:
  - Paradigmi di autenticazioni robusti
  - Algoritmi di crittografia avanzati

} 802.11i

Il Working Group 802.11i

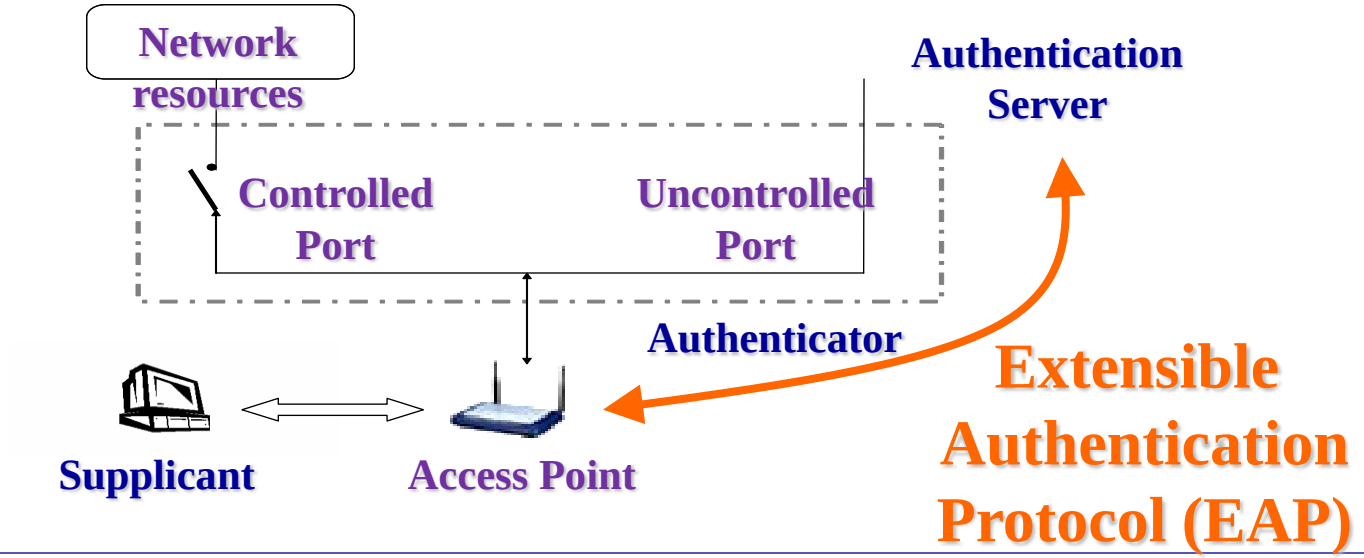
- Ha concluso i lavori nel Giugno 2004
- Caratteristiche dello standard:
  - Autenticazione demandata ai livelli superiori (non più a livello di *link*)
  - Introduzione di protocolli/infrastrutture per l'autenticazione
  - Miglioramento delle procedure di privacy ed integrità
- *Wireless Protected Access (WPA1 e WPA2)*

IEEE 802.11i

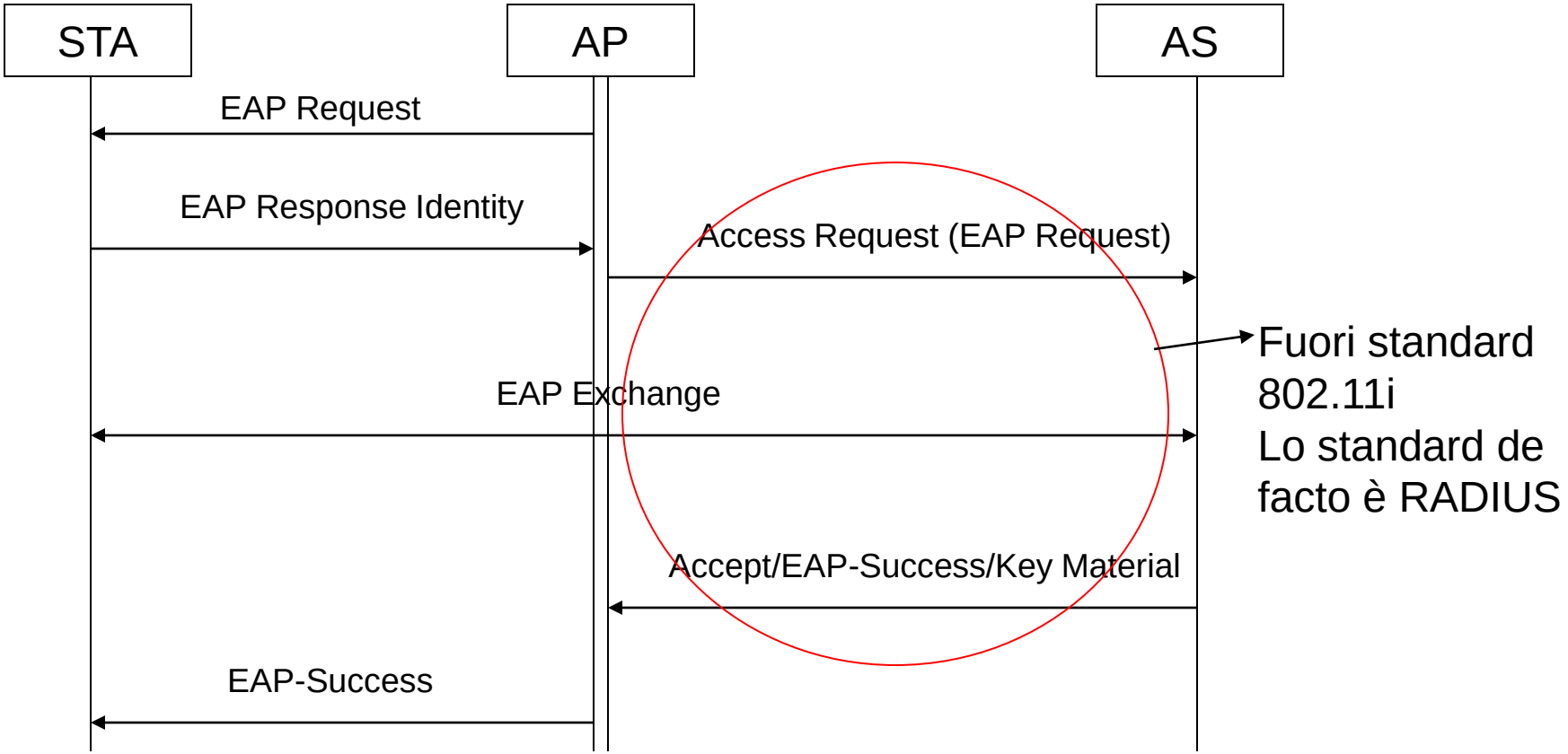
- Autenticazione
  - Protocollo 802.1X
- Privacy
  - Temporary Key Integrity Protocol (TKIP)
    - Basato su tecnologia RC4
    - Integrity check robusta con *Message Integrity Check (MIC)*
    - Cambio di chiave per ogni pacchetto
  - Counter Mode/CBC MAC Protocol (CCMP)
    - Basato su tecnologia AES
    - Più robusto e performante di TKIP

Autenticazione 802.1X

- Basata *sull'Extensible Authentication Protocol (EAP)*
- Entità del processo di autenticazione
  - *Supplicant*
  - *Authenticator*
  - *Authentication Server*



Extensible Authentication Protocol (EAP)



- E' possibile l'autenticazione "two-ways"
- Contiene funzionalità per lo scambio delle chiavi

Procedura di scambio delle chiavi

STA 

AP

AS 

Step 1: Use RADIUS to push PMK from AS to AP

Step 2: Use PMK and 4-Way Handshake to derive, bind, and verify PTK

Step 3: Use Group Key Handshake to send GTK from AP to STA

PMK: Pairwise Master Key
PTK: Pairwise Transient Key

I programmi di certificazione WPA

	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

- La certificazione WPA supporta diversi tipi di protocolli EAP
  - *LightWeigth EAP (LEAP): proprietario CISCO,* basato su password
  - EAP *Transport Layer Security* (EAP-TLS): basato su certificati
  - EAP *Tunneled TLS* (EAP-TTLS)
  - Protected EAP (PEAP)

} Soluzioni ibride basate su Password + certficati

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

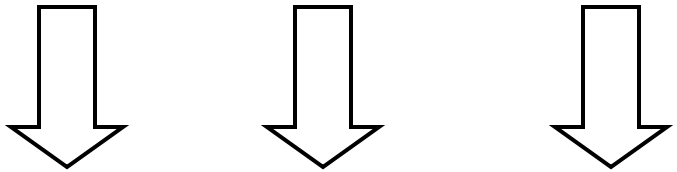
Il livello fisico

Frequency Hopping Spread Spectrum (FHSS)

Direct Sequence Spread Spectrum (DSSS)

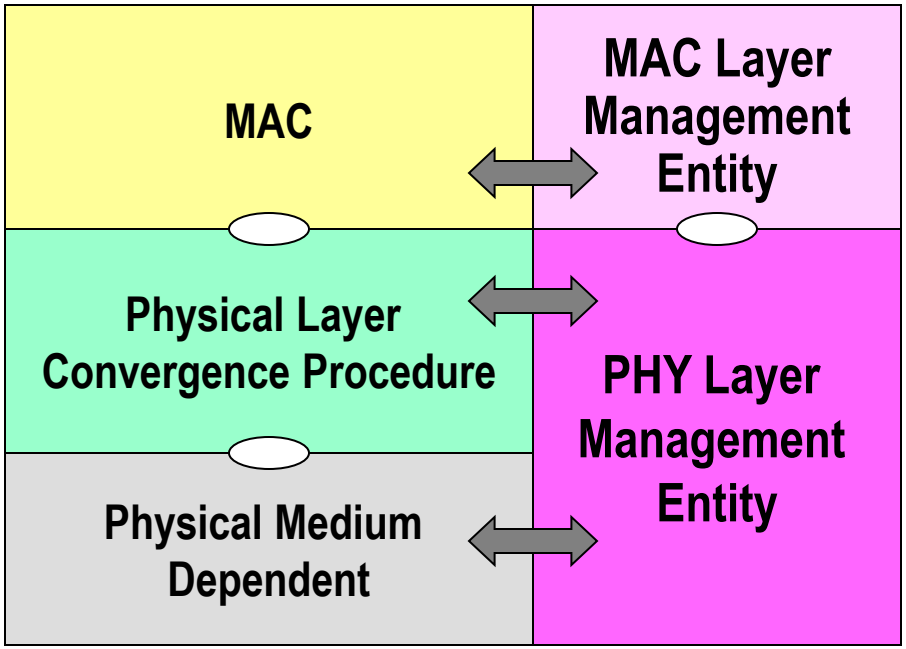
Progetto del livello fisico

- Mezzo radio condiviso
- Deve operare in una banda non licenziata
- Interferenza altamente variabile



- Necessità di progettare un livello fisico robusto all'interferenza

Struttura protocollare



- *Physical Layer Convergence Procedure (PLCP):* livello che adatta le trame MAC per la trasmissione sul mezzo
- *Physical Medium Dependent (PMD):* livello che gestisce la trasmissione dei bit (modulazione)

Le Interfacce radio standardizzate

- Approccio con livelli fisici multipli (motivazioni storico/politiche)
- Vengono definite tre modalità di trasmissione dell'informazione:
  - Infrarosso (IR, ormai obsoleta)
  - Frequency Hopping Spread Spectrum 1-2Mb/s (FHSS, usata in scenari particolari)
  - Direct Sequence Spread Spectrum 1-2 Mb/s (DSSS, Wifi)

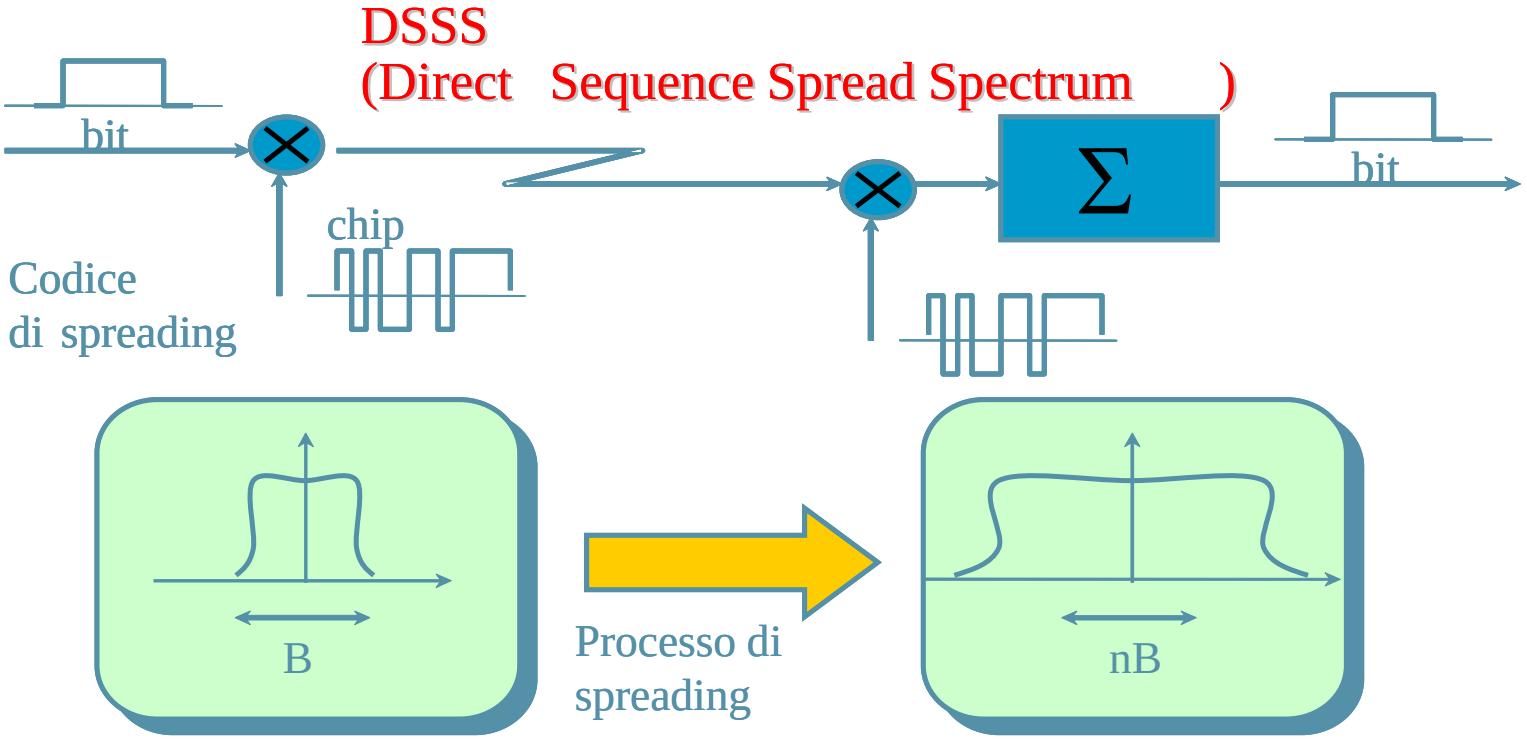
DSSS vs FHSS

- Sia DSSS che FHSS si ripropongono di limitare l'impatto dell'interferenza sulle prestazioni del sistema di trasmissione

- DSSS
  - Spalma l'energia del segnale su una banda in frequenza più larga rispetto a quella del segnale stesso
- FHSS suddivide la banda in sottocanali disgiunti da 1MHz ciascuno
  - Ogni trasmissione "salta" da un sottocanale ad un altro secondo una sequenza prestabilita
  - Le diverse sequenze di salto assegnate ad ogni stazione sono ortogonali tra di loro

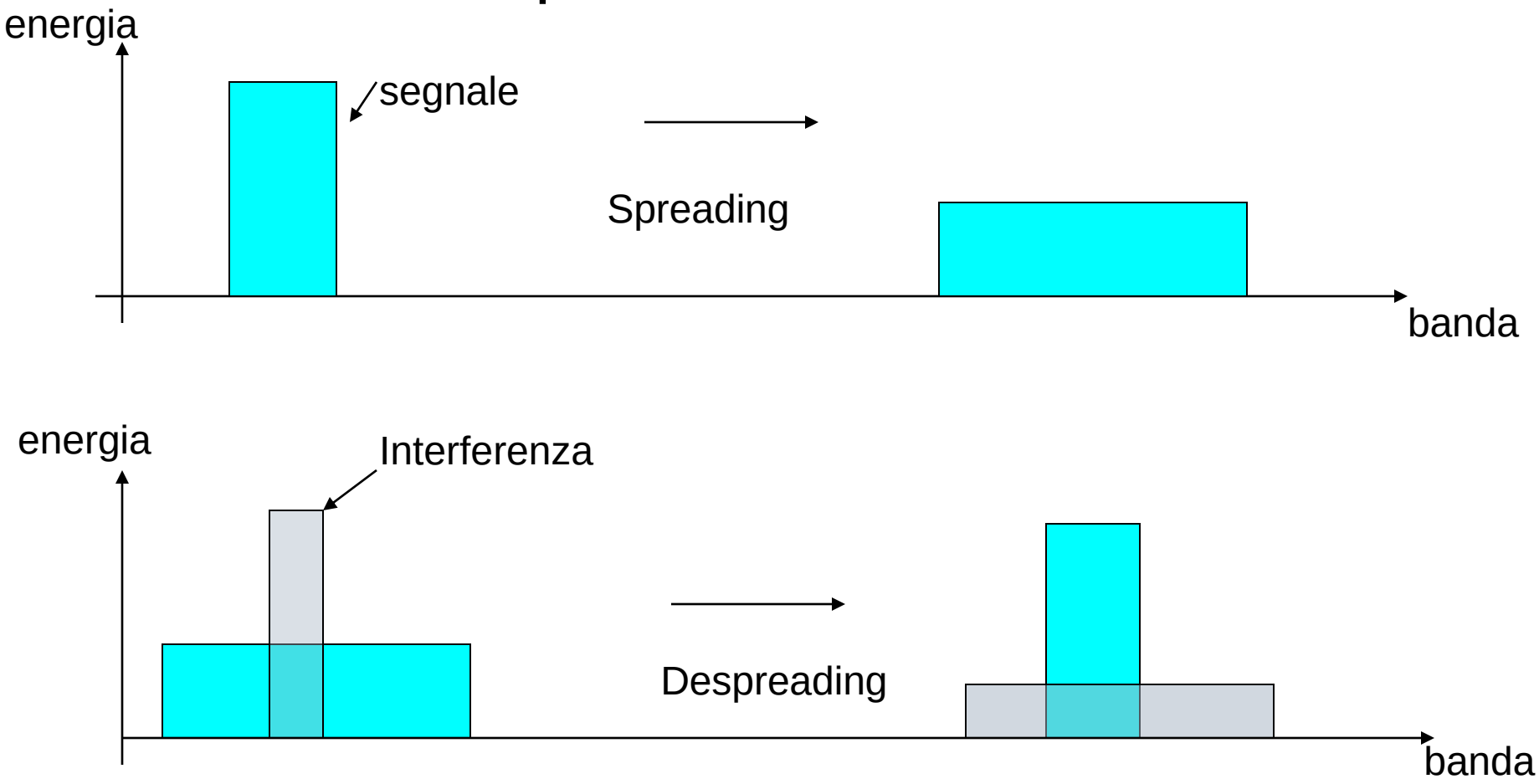
DSSS

- Viene usato un approccio a divisione di codice per allargare lo spettro del segnale (sequenza di *Barker*)



Vantaggi DSSS

- Robusto a picchi di interferenza



DSSS

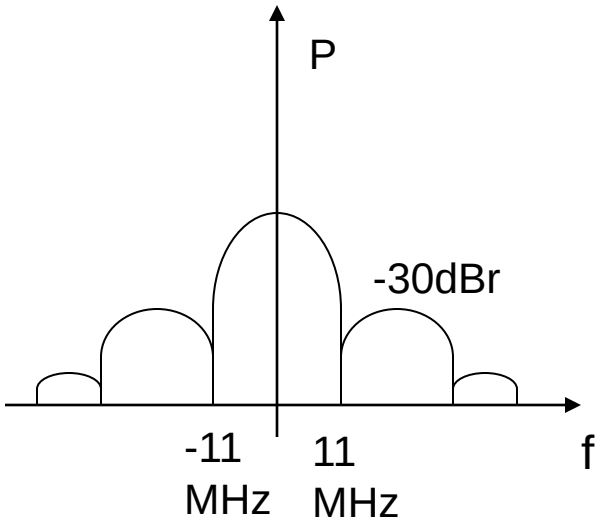
- Non è usato per multiplare più trasmissioni
- Tutte le trasmissioni usano la stessa sequenza di *Barker*

Canalizzazione (1)

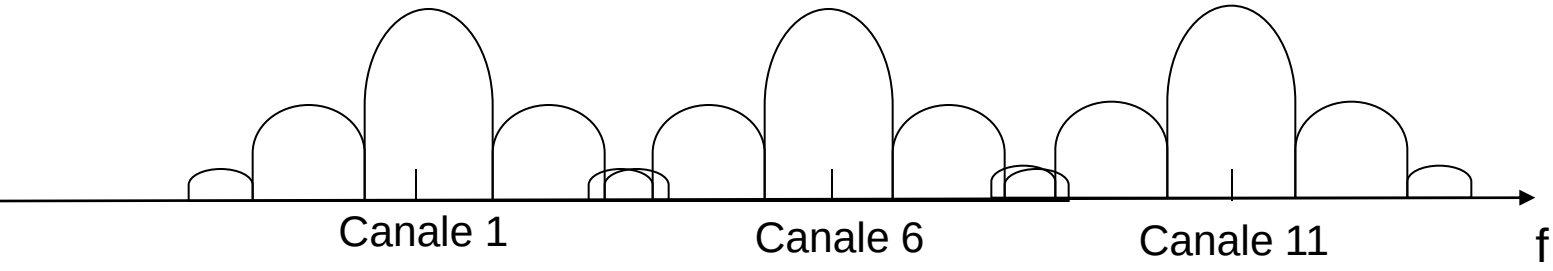
- Lo standard definisce 14 canali di 5 MHz ciascuno a partire dalla frequenza 2.412 GHz
- Non tutti i canali sono disponibili nelle varie nazioni

Nazione	**Canali disponibili**
USA	1-11 (2.412-2.462GHz)
Europa	1-11 (2.412-2.472GHz)
Spagna	10-11 (2.457-2.462 GHz)
Francia	10-13 (2.457-2.472 GHz)
Giappone	14 (2.484 GHz)

Canalizzazione (2)



- La maggior parte dell'energia del segnale è confinata in una porzione di banda di 22MHz
- Non è possibile usare canali adiacenti

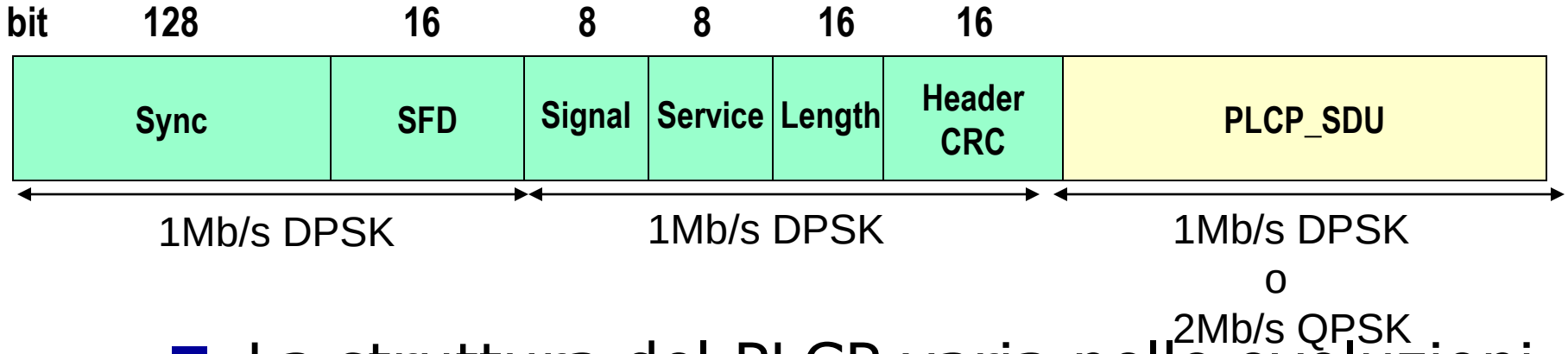


La modulazione

- Sono definiti due tipi di modulazione
  - *Differential Phase Shift Keying* (DPSK):
    - garantisce un data rate di 1 Mb/s,
    - un bit di informazione definisce un simbolo (fase)
  - *Differential Quadrature Phase Shift Keying* (DQPSK):
    - garantisce un data rate di 2 Mb/s,
    - due bit di informazione definiscono 4 simboli
- Per aumetare il data rate
  - Cambiare modulazione (HR/DSSS)
  - Cambiare livello fisico (802.11a/g)
  - Modificare dispositivi rice/trasmittenti (MIMO, 802.11n)

PLCP

- Aggiunge ulteriore protezione contro l'interferenza e correzione d'errore
  - Scrambling
  - Cyclic Redundancy Check



  - La struttura del PLCP varia nelle evoluzioni dello standard

DSSS – Caratteristiche Generali

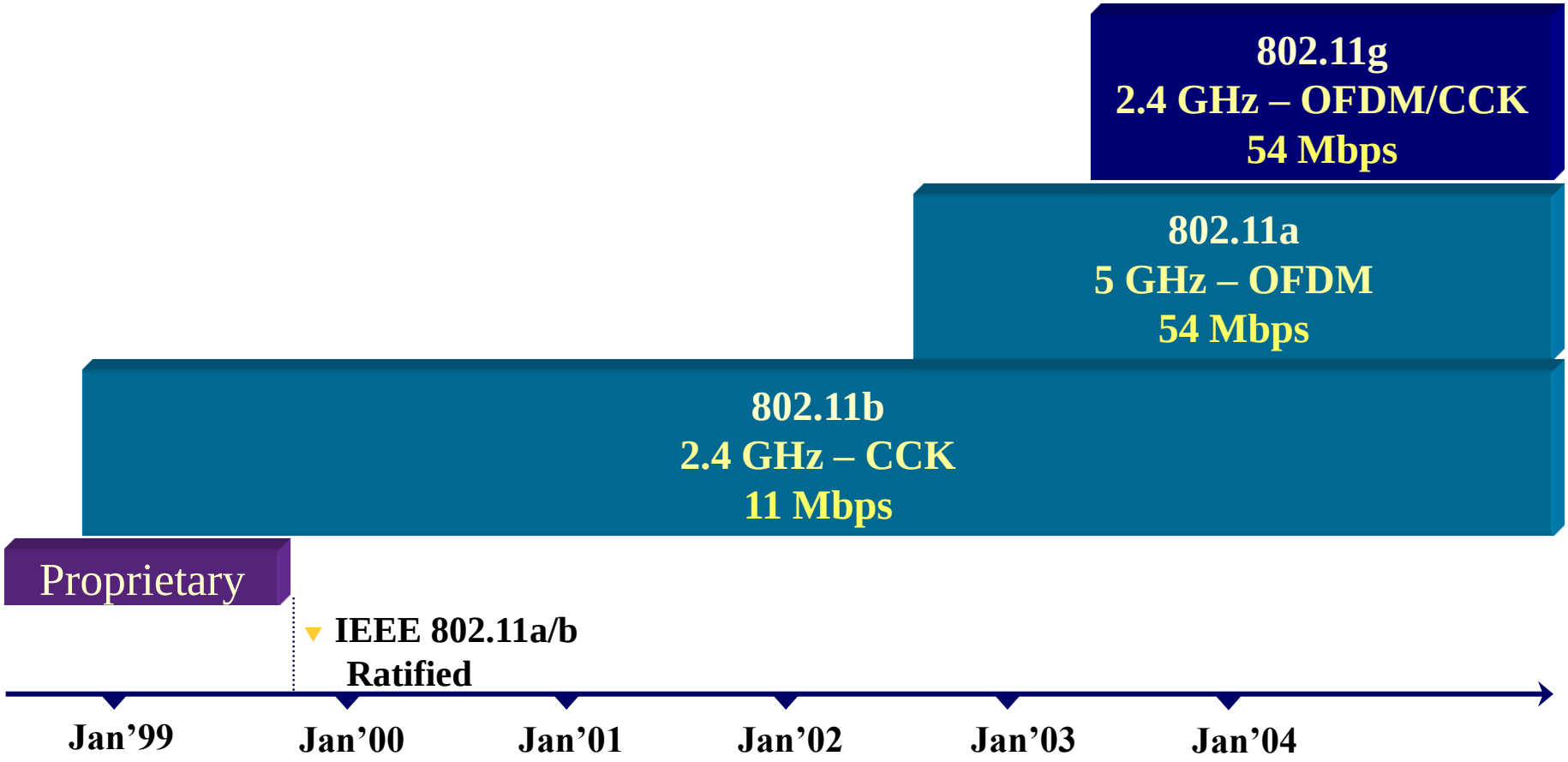
Parametro	Valore
Durata Slot	20us
Durata SIFS	10us
Dimensione CW	Da 31 a 1023 slot
Preambolo PLCP	144us
Header PLCP	48us
Trama MAC	Da 4 a 8191 byte

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Le evoluzioni del livello fisico

802.11b HR/DSSS (standard dal 1999)
802.11a (standard dal 1999)
802.11g (standard dal 2003)
802.11n (work in progress)

Le evoluzioni del fisico

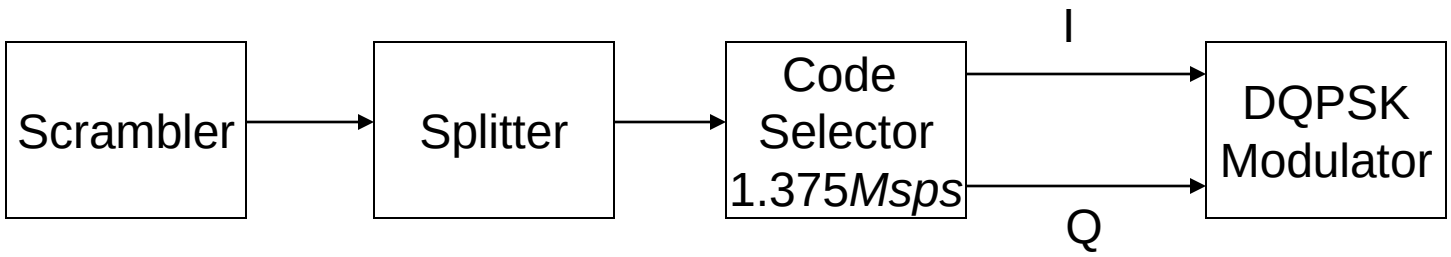


802.11b – HR/DSSS

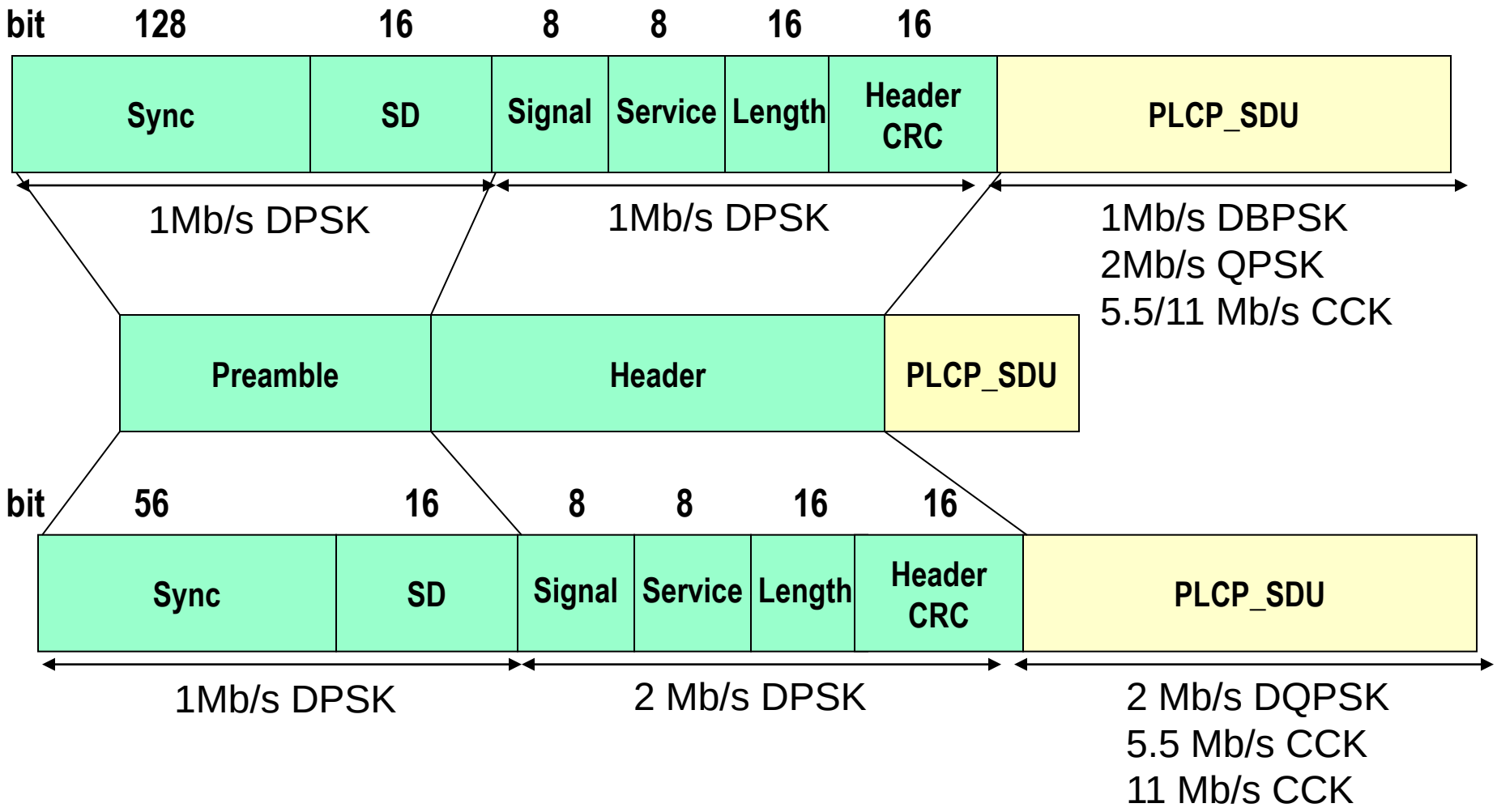
- Modifica al PMD:
  - introduzione di nuovi sistemi di modulazione per garantire bit rate più elevato (fino a 11Mb/s)
- Modifica al PLCP:
  - La struttura di *header* e preambolo PLCP cambia
- Compatibile con la versione precedente dello standard

Modifica al PMD – Modulazione CCK

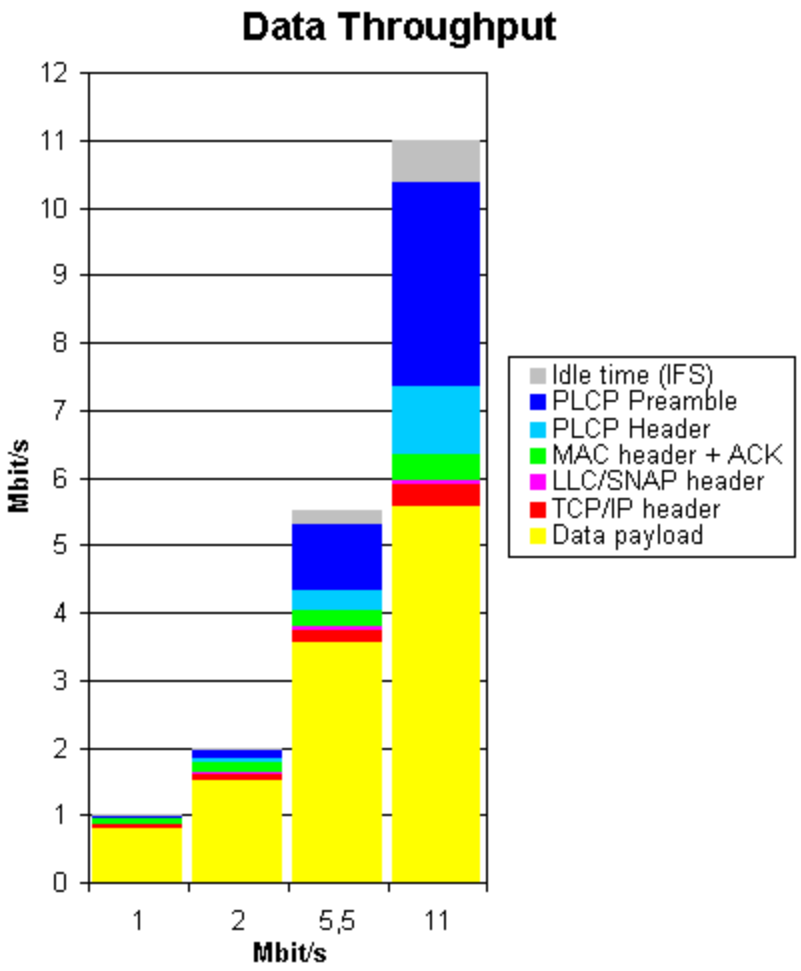
- Modulazione QPSK (*Quadrature Phase Shift Keying*) con spreading
- Rate di trasmissione = 1.375 *Msimboli/s*
- Due *data rate* definiti:
  - 5.5 Mbit/s, 4 bit per simbolo
  - 11 Mb/s, 8 bit per simbolo

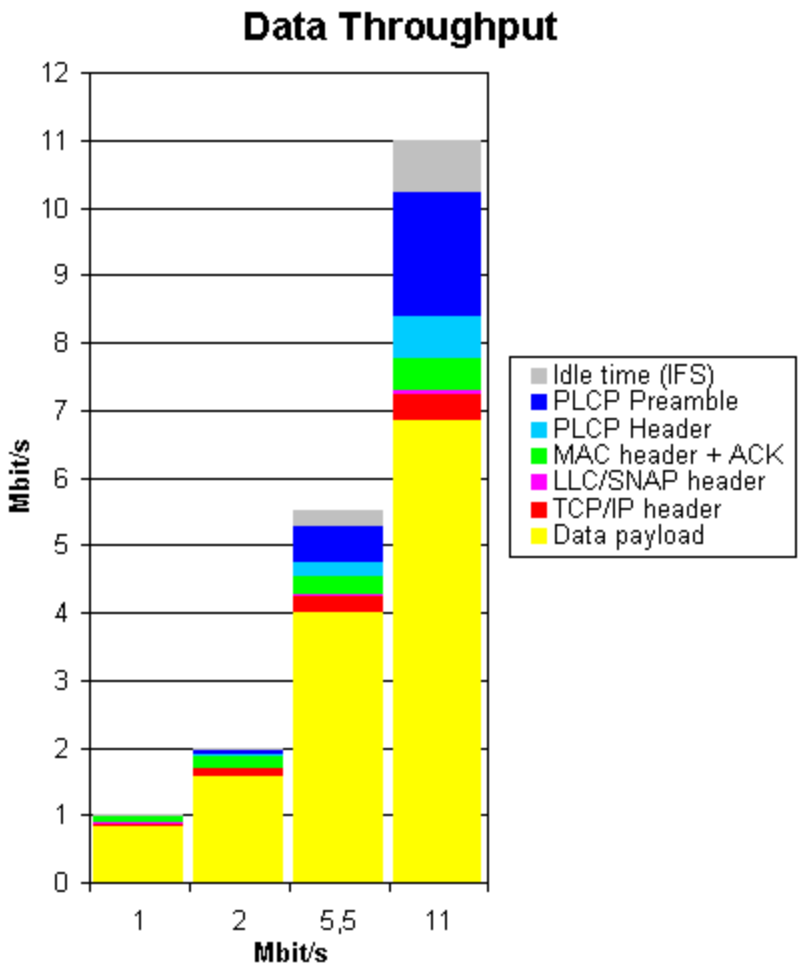


Modifiche al PLCP



802.11b - Prestazioni





Source: http://www.uninett.no/wlan/throughput.html

802.11a – La soluzione OFDM

- Motivazioni:
  - Necessità di banda, la porzione a 2.4GHz è sovraffollata
  - Necessità di data rate più elevati, gli 11 Mb/s sono ormai pochi
- Soluzioni
  - Utilizzo della banda U-NII (*Unlicensed National Information Infrastructure*) attorno ai 5 GHz
  - Utilizzo di modulazione OFDM

Vantaggi e svantaggi

- Vantaggi
  - Data rate più alti (fino a 54 Mb/s)
  - Minore interferenza in banda (banda più libera)
- Svantaggi
  - Minore copertura
  - Maggiore consumo di potenza
  - Regolamentazione in Europa
  - Maggiore costo (scheda 802.11a costa 2 volte una scheda 802.11b)
  - Minore diffusione

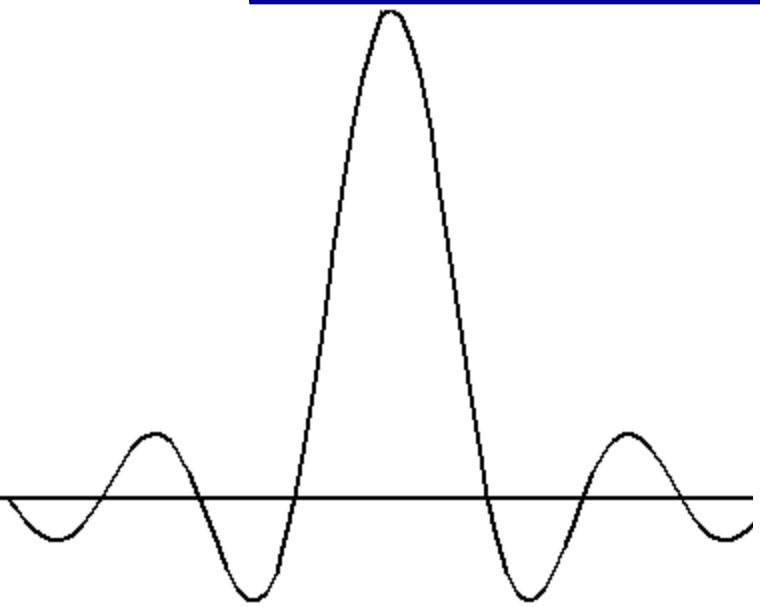
OFDM – Concetti base

- Converte un unico flusso a data rate elevato in flussi multipli a data rate inferiore
- I flussi multiplati sono trasmessi su portanti in frequenza ortogonali
- Consente tecniche efficienti per ricostruire i simboli modulati su ciascuna portante senza interferenza reciproca (FFT/IFFT)

OFDM – Concetti base (2)

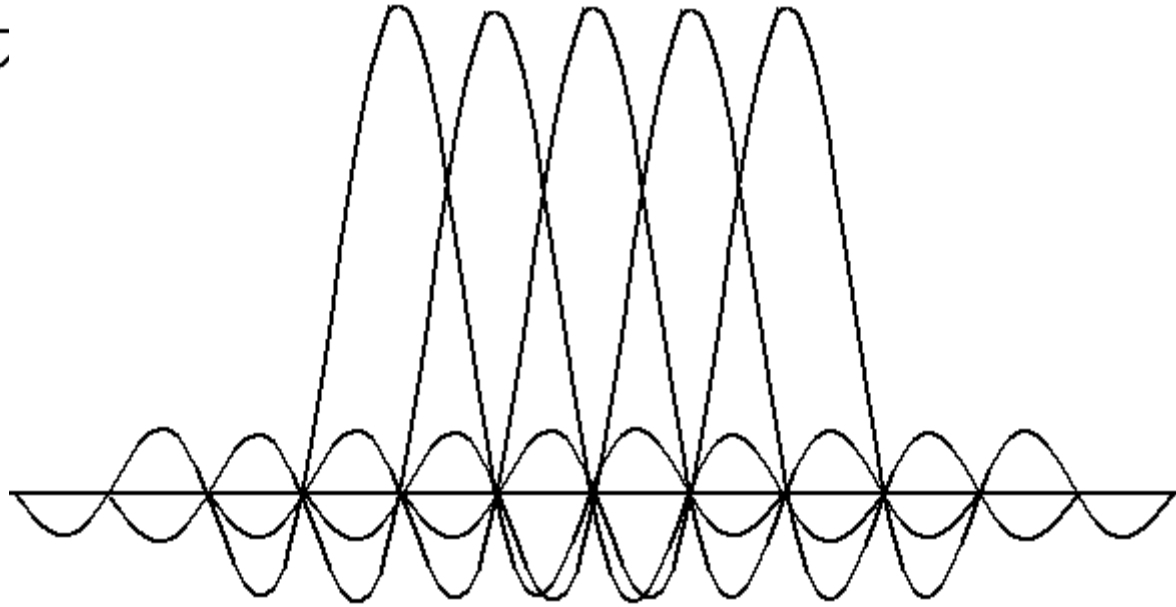
- Sistema di trasmissione a multi-portante
- Il flusso di informazione è suddiviso in blocchi di N simboli trasmessi in parallelo sulle portanti
- Interferenza nulla tra due simboli dello stesso blocco

Spettro



- Spettro di un simbolo in trasmissione

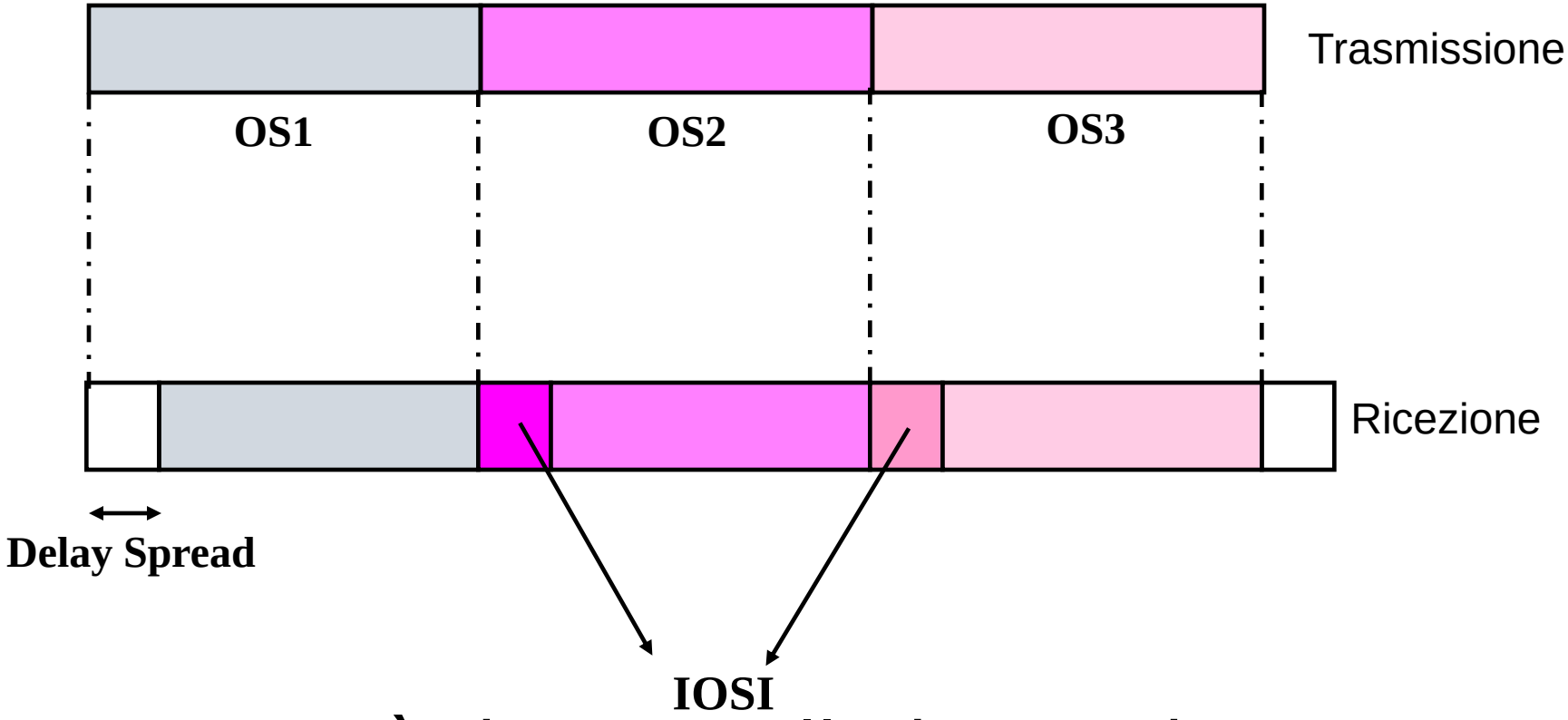
- Spettro di un bloco di simboli in trasmissione
- Rispetto all FDM canonico è consentita la sovrapposizione dei diversi canali in frequenza



Terminologia OFDM

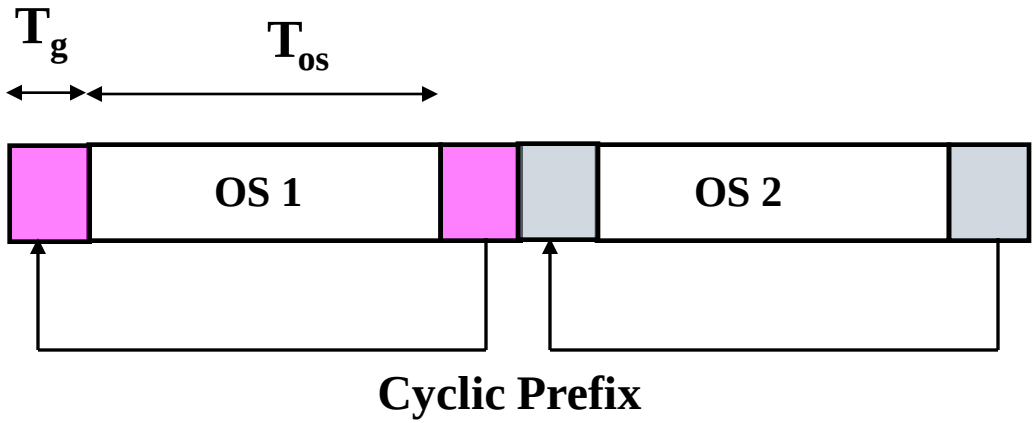
- Sottoportanti
  - Unità minima in cui viene diviso lo spettro
- Simbolo OFDM
  - Simbolo in trasmissione che viene suddiviso sulle N sottoportanti

Interferenza Inter Simbolica



- Necessità di intervalli di guardia tra simboli OFDM (realizzati con prefissi ciclici)

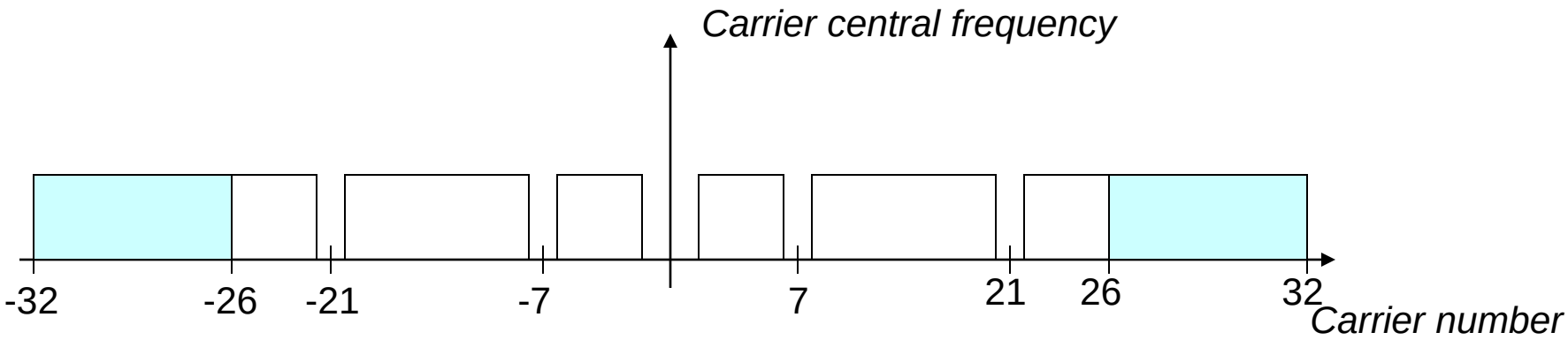
Tempo di guardia



- Il prefisso ciclico consente di
  - Manterenre l'ortogonalità tra le sottoportanti
  - Evitare ISI
- Il valore del tempo di guardia dipende da:
  - Il delay spread massimo (4 volte)

OFDM in 802.11a

- Lo spettro è organizzato in canali di 20MHz
- Ciascun canale è suddiviso in 52 sottoportanti spaziate di 0.3125MHz



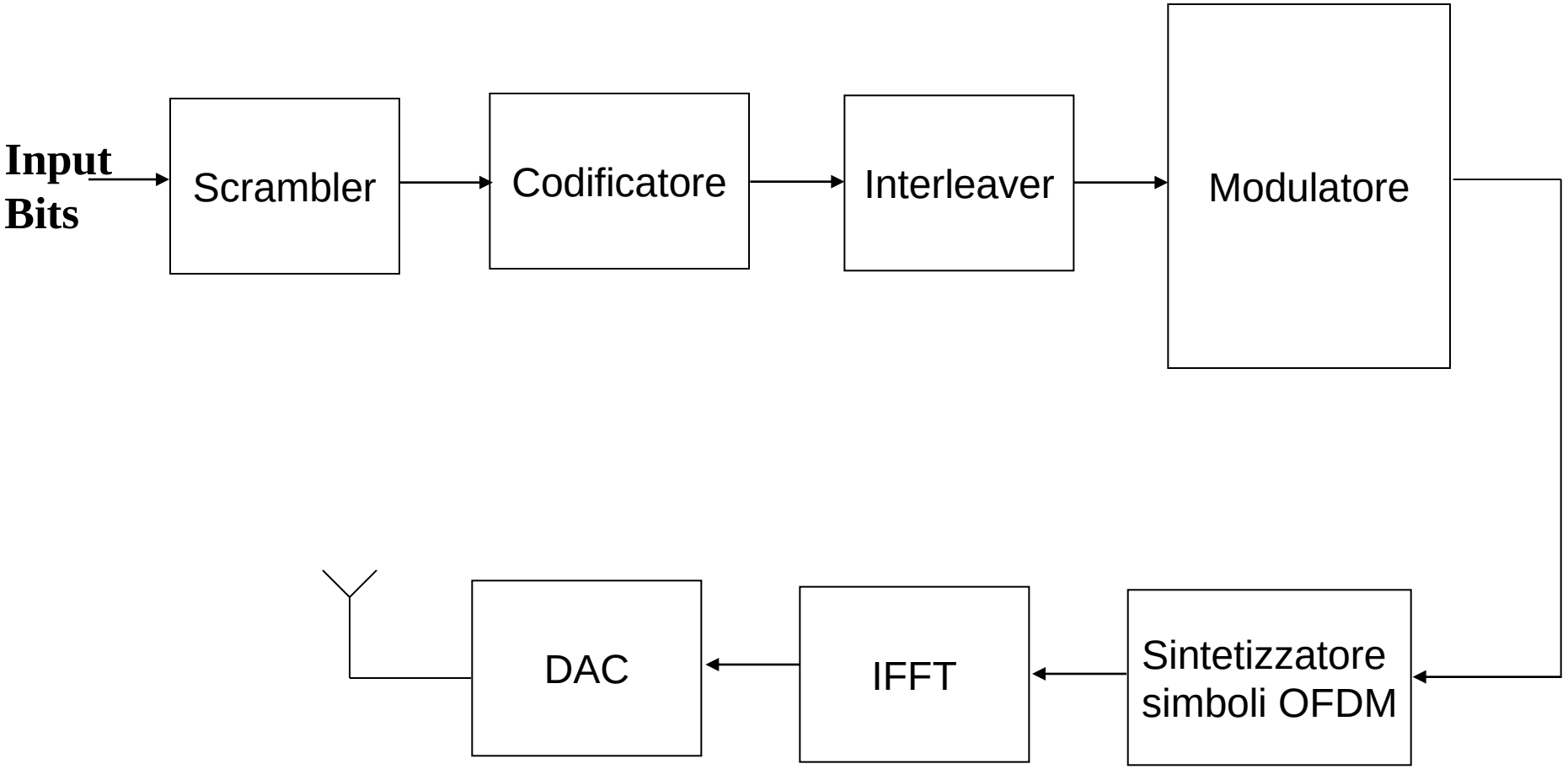
- 48 sottoportanti dati, 4 sottoportanti di controllo

Parametri di 802.11a

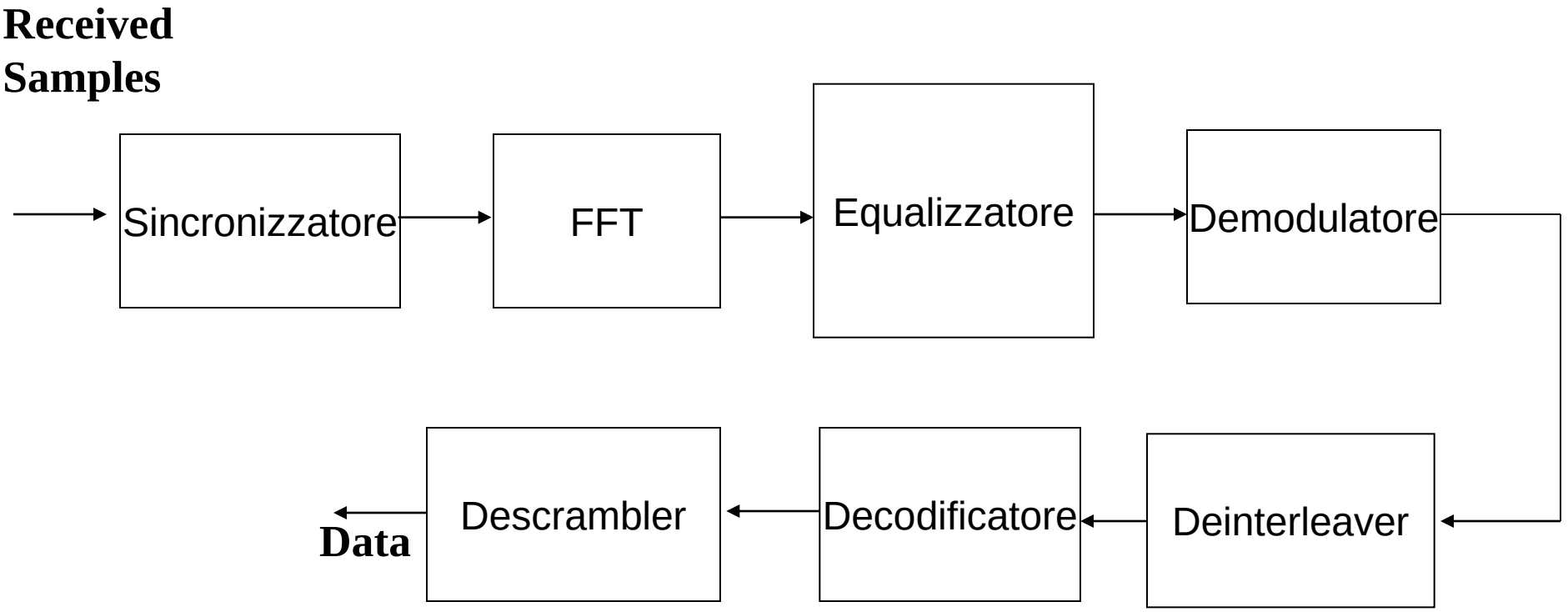
- Durata del simbolo OFDM 4μs
- Durata dell'intervallo di guardia 0.8μs
- Durata del simbolo utile 3.2μs

- Utilizza tecniche di interleaving, scrambling e codifica per proteggere l'informazione in trasmissione

Trasmettitore 802.11a



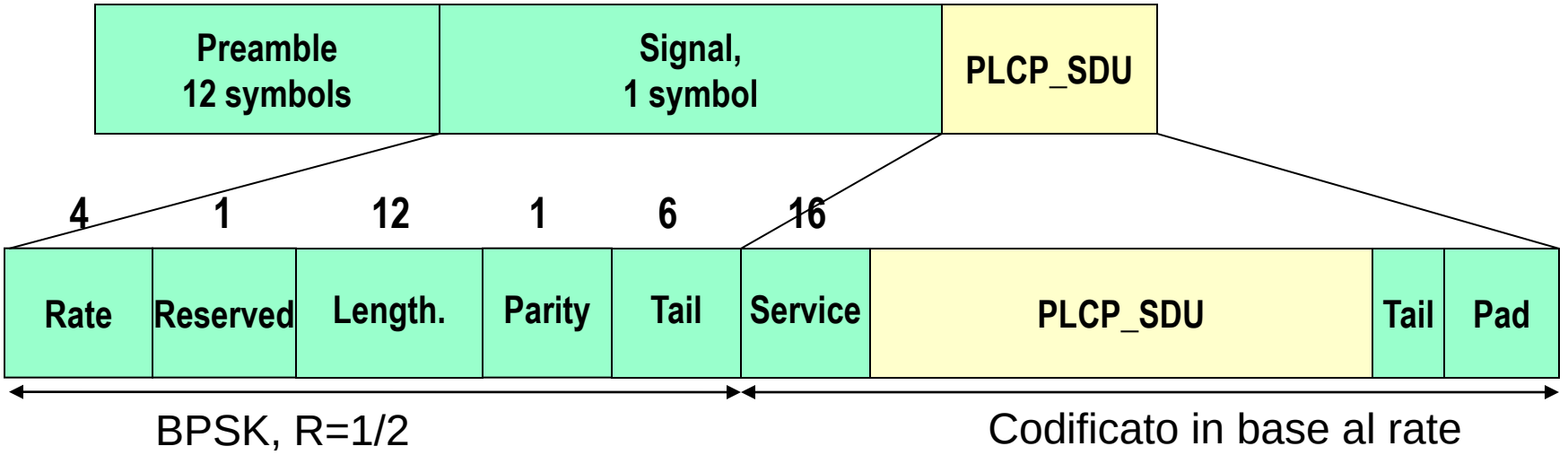
Ricevitore 802.11a



Multiple Data Rates/Modes

Mode	Data Rate (Mbps)	Coding rate	Modulation	No. of coded bits/ OFDM Symbol	No. of data bits/ OFDM symbol
1	6	½	BPSK	48	24
2	9	¾	BPSK	48	36
3	12	½	QPSK	96	48
4	18	¾	QPSK	96	72
5	24	½	16 QAM	192	96
6	36	¾	16 QAM	192	144
7	48	²/₃	64 QAM	288	192
8	54	¾	64 QAM	288	216

PLCP 802.11a



- Struttura completamente diversa rispetto al PLCP 802.11 e 802.11b

Caratteristiche 802.11a

Parametro	Valore
Durata Slot	9us
Durata SIFS	16us
Dimensione CW	Da 15 a 1023 slot
Preambolo PLCP	16us
Header PLCP	4us
Trama MAC	Da 4 a 4095 byte

802.11g, Standard dal 2003

- Motivazioni:
  - Incremento del *data rate* di 802.11b all'interno della stessa porzione di spettro
  - Compatibilità con i dispositivi 802.11b
- Background:
  - Due soluzioni tecnologiche concorrenti:
    - PBCC, sostenuta da *Texas Instruments*
    - DSSS-OFDM, sostenuta da *Intersil*
- Soluzione
  - Un livello fisico (*Extended Rate Physical* OFDM) "*mandatory*" ripreso da 802.11a
  - Due soluzioni (PBCC, DSSS-OFDM) opzionali

Caratteristiche livello fisico 802.11g

Parametro	Valore
Durata Slot	9us o 20us
Durata SIFS	10us (+6us di estensione virtuale)
Dimensione CW	Da 15 a 1023 slot
Preambolo PLCP	16us
Header PLCP	4us
Trama MAC	Da 4 a 4095 byte

Relazioni di compatibilità

- 802.11g è in grado di riconoscere i preamboli di 802.11b (short, long) e 802.11a, *carrier sensing* possibile
- 802.11g "parla" 802.11b nello scambio di pacchetti RTS/CTS
  - Stesso data rate
  - Stessa modulazione
  - Stessa durata di slot
- Dispositivi 802.11b NON sono in grado di ricevere trasmissioni 802.11g

Prestazioni dei diversi Livelli fisici

Distanza	802.11b	802.11a	802.11g solo	802.11g/b RTS/CTS	802.11g/b Self CTS
3m	5.8	24.7	24.7	11.8	14.7
15m	5.8	19.8	24.7	11.8	14.7
30m	5.8	12.4	19.8	10.6	12.7
45m	5.8	4.9	12.4	8	9.1
60m	3.7	0	4.9	4.1	4.2
75m	1.6	0	1.6	1.6	1.6
90m	0.9	0	0.9	0.9	0.9

- Throughput in Mb/s misurato al netto degli overhead dei livelli MAC e fisico
- Fonte: *Broadcom*

Quale standard scegliere?

- Parametri di confronto:
  - Data rate nominale
  - Range
  - Capacità (numero di canali disponibili)
  - Costo
  - Compatibilità

Tecnologia	Velocità di picco	Range	Compatibilità 802.11b	Capacità	Costo
802.11b	Media	Alto	Sì	Bassa	Basso
802.11a	Alta	Ridotto	No	Alta	Medio
802.11g	Alta	Alto	Sì	Media	Basso

L'802.11n – Sempre più veloce

- Standard da Settembre 2009
- Obiettivo: raggiungere data rate nominali più elevati
- Approccio della standardizzazione:
  - Modifica al livello fisico OFDM
  - Modifica al livello MAC

Come aumentare il data rate?

$$\text{Data Rate} = \underbrace{\frac{20M \text{ time samples}}{\text{second}}}_{\text{channel spacing}} \cdot \underbrace{\frac{48 \text{ freq tones}}{64 \text{ freq tones}}}_{\text{guard band overhead}} \cdot \underbrace{\frac{6 \text{ coded bits}}{\text{freq tone}}}_{\text{constellation size}} \cdot \underbrace{\frac{3 \text{ info bits}}{4 \text{ coded bits}}}_{\text{coding rate}} \cdot \underbrace{\frac{64 \text{ freq tones}}{80 \text{ times samples}}}_{\text{guard interval overhead}}$$

$$= 54M \text{ info bits/second}$$

- Modi per aumentare il data rate:
  - Multiplazione spaziale
  - Aumentare la banda del segnale
  - Aumentare la dimensione della costellazione di modulazione
  - Aumentare il rate del codice
  - Diminuire i tempi di guardia

Parametri di standardizzazione

802.11a/g	802.11n	Requirement	*Throughput Scaling Factor*
Channel BW = 20MHz Number of data subcarriers = 48	Channel BW = 20MHz Number of data subcarriers = 48	Mandatory	*1x*
	Channel BW = 40MHz Number of data subcarriers = 108	Mandatory	*2.25x*
Number of Transmit Antennas = 1	Number of Transmit Antennas = 2	Mandatory	*2x*
	Number of Transmit Antennas > 2	Optional (e.g. 3 and 4)	*3x or 4x*
Maximum Constellation Size = 64QAM	64-QAM	Mandatory	*1x*
	>64QAM (i.e. 128 or 256 QAM)	256QAM optional	*1.16x (128-QAM)* *1.33x (256-QAM)*
GI = 800ns Tsymbol = 3200ns	GI / Tsymbol = 800ns/3200ns	Mandatory	*1x*
	GI / Tsymbol = 400ns/3200ns	Mandatory	*1.11x*
Coding Rate	1/2, 2/3, 3/4	Mandatory	*1x*
	7/8	Mandatory	*1.167x*

802.11n – Il livello fisico

- Funziona nelle bande 2.4GHz, 5GHz e 4.9GHz (Giappone)

- Modifiche primarie:
  - MIMO – OFDM: multiplazione a divisione di spazio dei flussi in trasmissione
    - 2 Antenne (obbligatorio)
    - 4 Antenne (opzionale)
  - Estensione della banda di canalizzazione:
    - 20MHz (obbligatorio)
    - 40MHz (opzionale)

802.11n – Il livello fisico

- Modifiche secondarie:
  - Riduzione dei tempi di guardia tra simboli OFDM (400ns obbligatorio nei 20MHz)
  - Supporto modulazione fino a 64QAM
  - Supporto codifica convoluzionale
  - Supporto codifiche ottimizzate per il MIMO
- Data rate nominale massimo:

!! 600Mb/s !!

802.11n – Il livello fisico

MCS Index	Spatial Streams	Modulation Type	Coding Rate	Data Rate Mb/s			
				20 MHz channel		40 MHz channel	
				800ns GI	400ns GI	800ns GI	400ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
...	3	...	...	...	...	...	...
23	3	64-QAM	5/6	195.00	216.60	405.00	450.00
...	4	...	...	...	...	...	...
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

802.11n – il livello MAC

- Supporto della QoS: lo standard 802.11n ingloba il lavoro del TG 802.11e
- Funzionalità aggiuntive di aggregazione di trame MAC
- Estensione dell'entità di MAC *Management* per supportare funzionalità di r*adio resource management* avanzate

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Le evoluzioni dello strato d'accesso

802.11e

Limiti della PCF

- Nessun meccanismo per la differenziazione dei diversi flussi
  - Una sola coda presente a livello MAC
- Ritardi della temporizzazione di super trama
  - La trasmsissione del *beacon* che segnala l'inizio di un periodo CF può essere ritardata
- Nessun controllo sulle trasmissioni
  - Una stazione che ha ricevuto una trama di *poll* dal PC può trasmettere più trame o una trama di lunghezza arbitraria

La soluzione 802.11e

- Differenziazione dei flussi
  - Ogni dispositivo deve implementare 4 code per 4 tipologie di traffico
- Introduzione delle *Transmission Opportunities* (TXOP)
  - Ad ogni trasmissione viene assegnato un tempo massimo di completamento
- Possibilità di comunicazioni dirette tra stazioni anche in scenari infrastrutturati
- Utilizzo della tecnica di *Block ACK (*singolo riscontro per "treni" di trame*)*

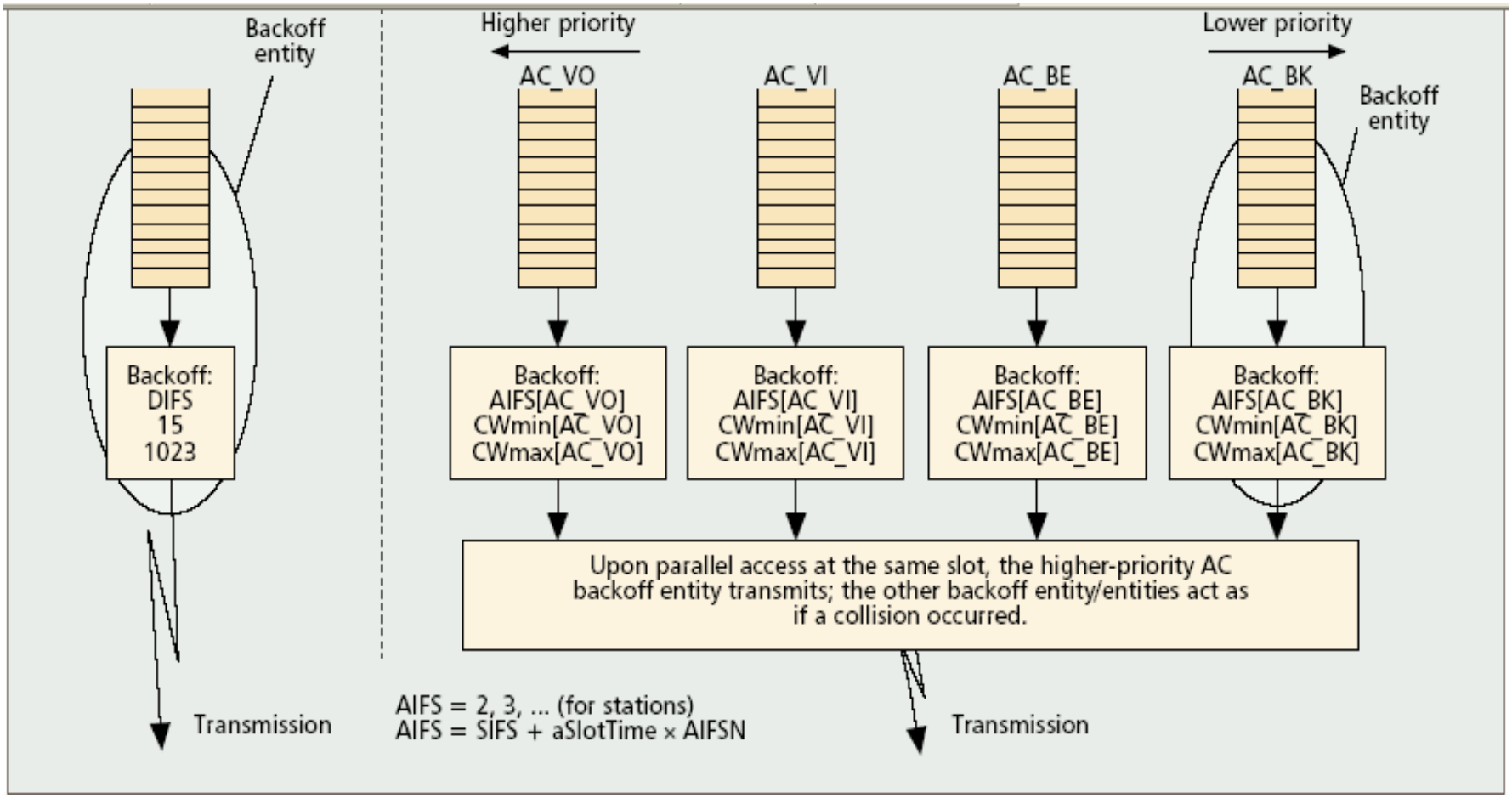
802.11e – L'accesso al canale

- Gestito dalla *Hybrid Coordination Function (HCF)*
- Due modalità
  - A contesa (EDCA, *Enhanced Distributed Channel Access*)
  - Controllato (HCCA, *HCF Controlled Channel Access*)

EDCA – Accesso a Contesa

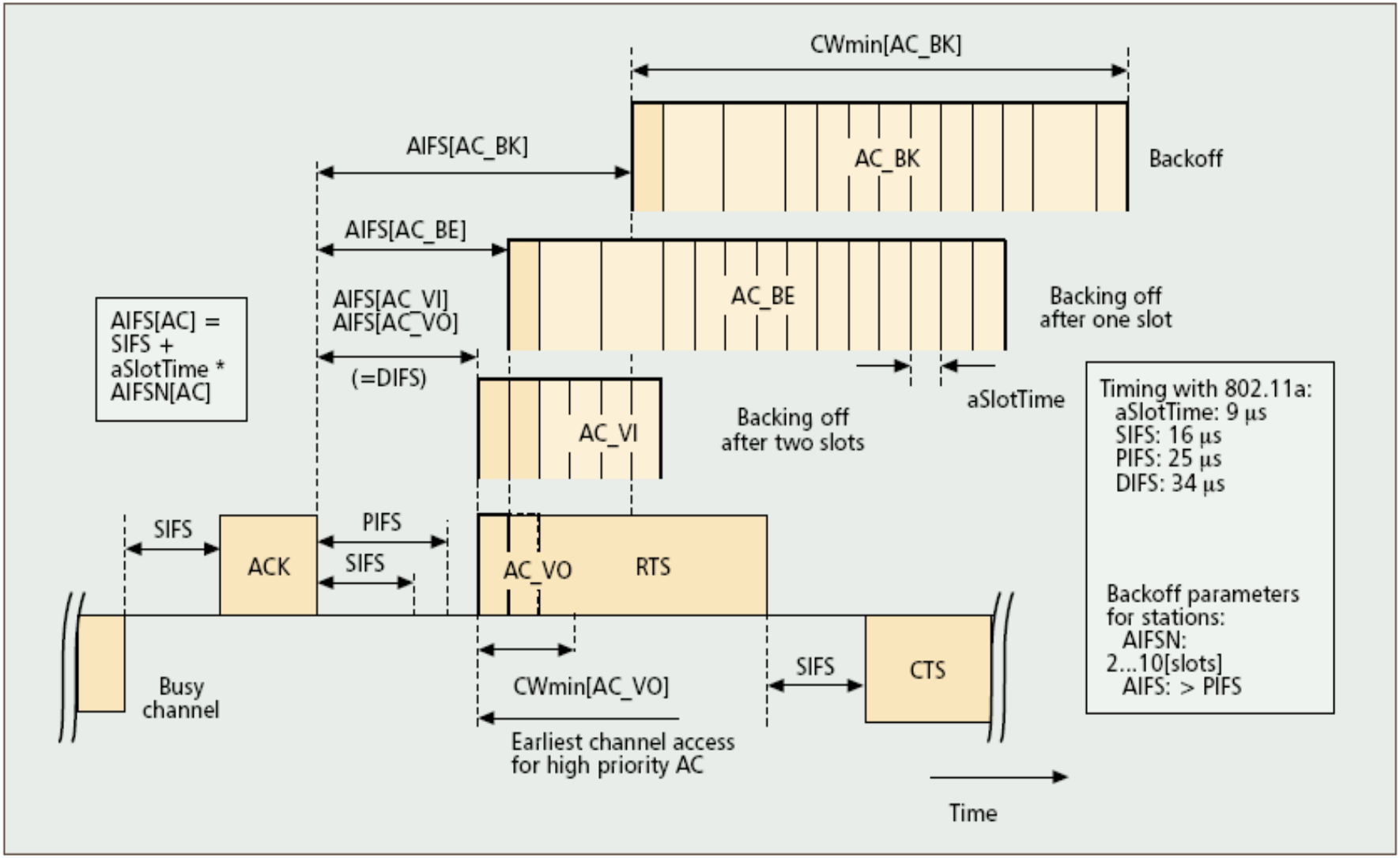
- Definisce 4 Categorie d'Accesso (AC) che individuano 4 tipologie di traffico
  - AC_VO: voce
  - AC_VI: video
  - AC_BE: best effort
  - AC_BK: background
- Ciscuna AC è caratterizzata da diversi parametri del meccanismo di *backoff*
  - *AIFS[AC]: tempo di "ascolto del canale"*
  - *CWMin[AC]: durata minima della finestra di backoff*
  - *CWMax[AC]: durata massima della finestra*
  - *TXOPlimit[AC]: durata massima della trasmissione*

Le classi di accesso



- Diverse entità di backoff all'interno della stessa stazione

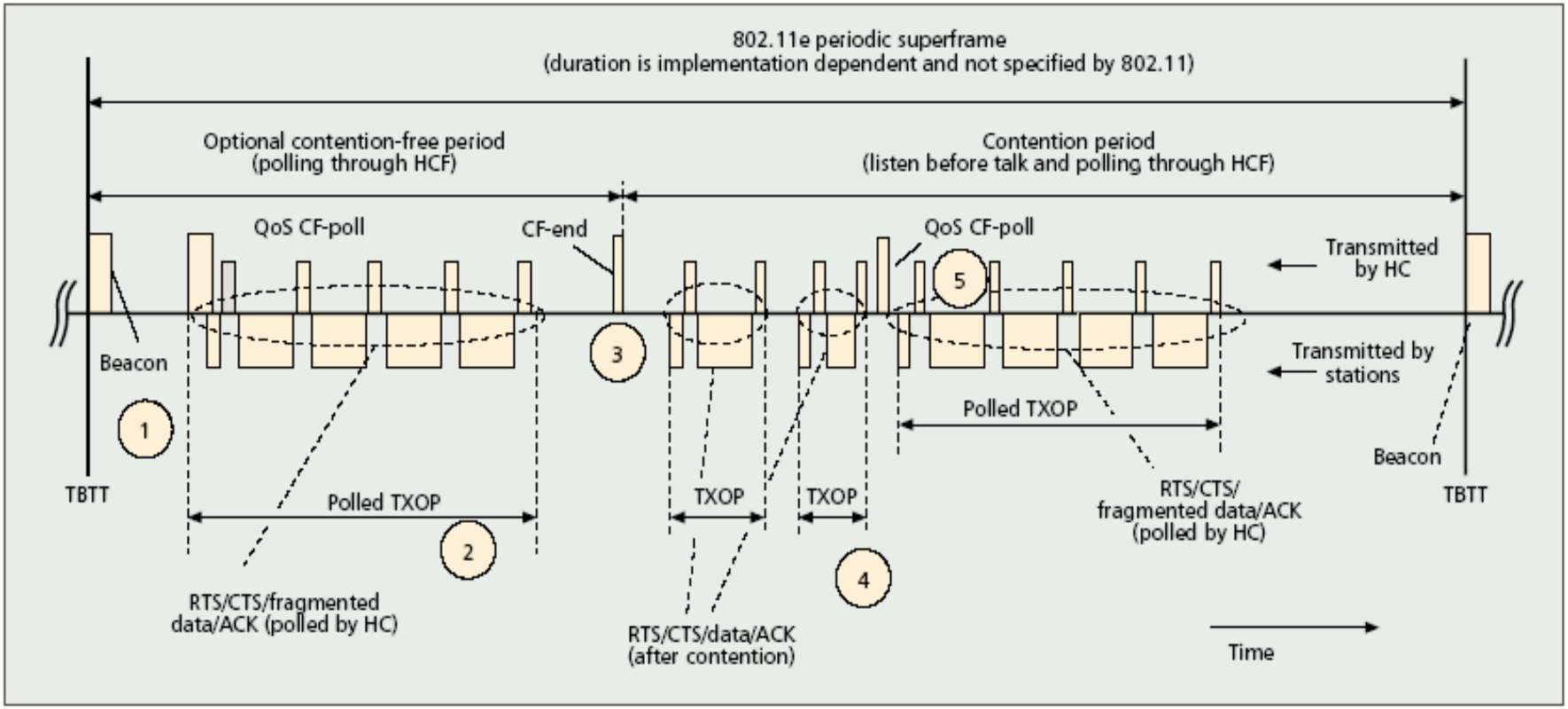
Esempio di accesso EDCA



L'accesso controllato HCCA

- Funziona sostanzialmente come la PCF
- L'HC può decidere di interrogare una stazione inviando una trama di *QoS CF-Poll* o una trama dati
- L'HC può accedere al canale dopo un PIFS, senza backoff (con priorità)
- Differenze rispetto a PCF:
  - HC specifica un *TXOPLimit* per tutte le tipologie di traffico
  - Possibilità di funzionamento ibrido (contesa/polling)

Esempio di accesso ibrido



- L'HC può decidere di interrogare una stazione anche durante la fase a contesa

Miglioramenti ulteriori

- *Block ACK*: idea di introdurre ACK cumulativi per blocchi di trame (si abbandona il paradigma “stop ‘n wait”)
  - Riduce l’overhead
  - Funziona solo con canali “buoni”
- *Direct Link Protocol* (DLP): protocollo per la comunicazione diretta tra STA in un’architettura *infrastructure*
  - Aumenta la capacità
  - Difficile realizzazione (sincronizzazione, power saving, ecc..)

Università degli Studi di Bergamo
Dipartimento di Ingegneria dell'Informazione e Metodi Matematici

Mesh Networking

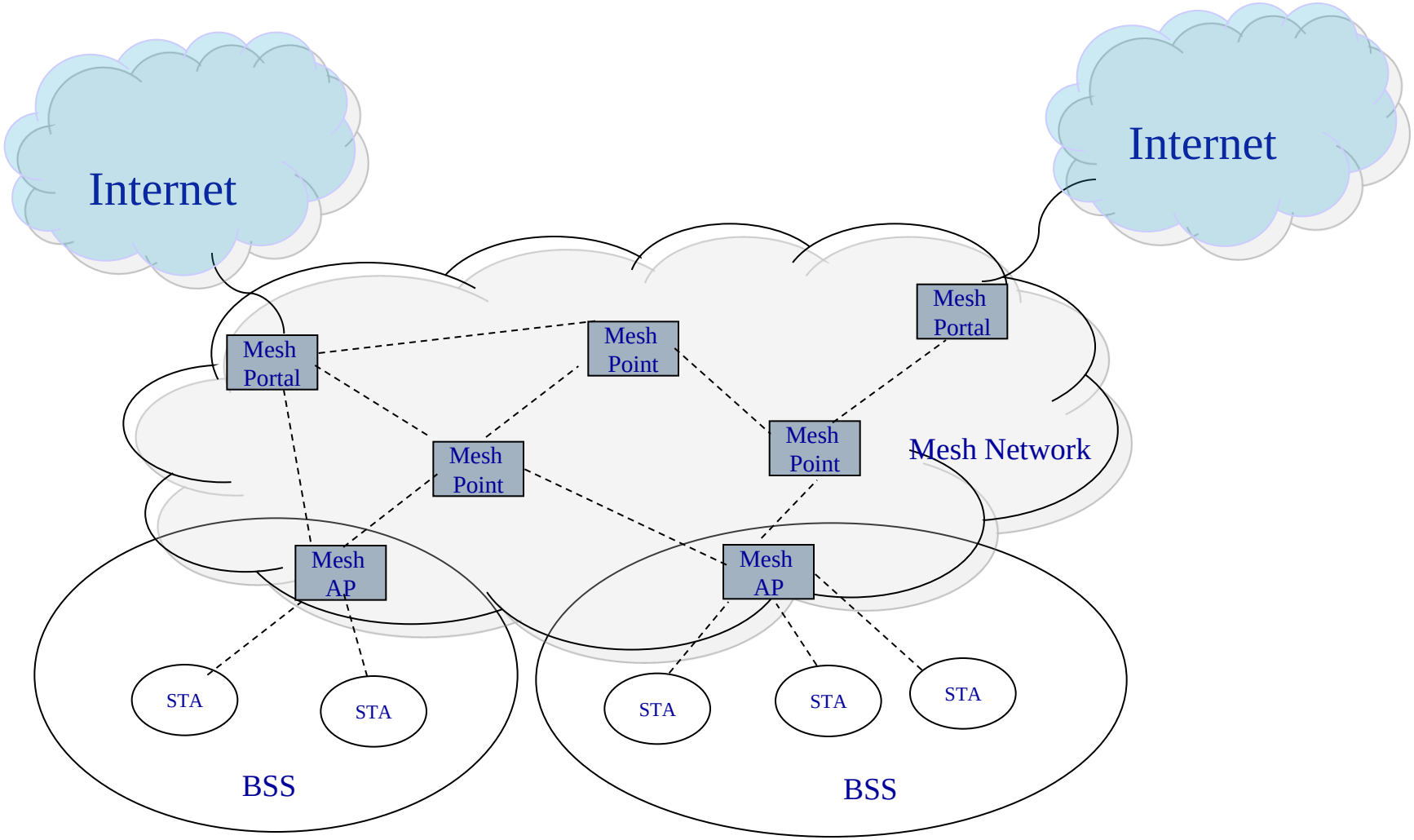
IEEE 802.11s

Soluzioni commerciali

Mesh Networking e 802.11

- Obiettivi
  - Estendere le dimensioni degli *hot spot* 802.11 tramite un'infrastruttura di tipo *mesh*
  - Ampliare gli scenari applicativi della tecnologia WLAN
- Soluzioni
  - Infrastrutture decentralizzate
  - Reti magliate di *Infrastructure BSS* con gli AP connessi tramite un sistema di distribuzione *wireless*

Esempio di rete *Mesh*



Scenari Applicativi

- Accesso residenziale (concorrenza con WiMax)
- Uffici
- Reti pubbliche di accesso ad internet
- Reti pubbliche di sicurezza
- Reti militari

Il mercato delle reti *Mesh*

- Applicazioni residenziali
  - Indoor
  - Dimensioni ridotte
  - Coesistenza con altre reti
- Applicazioni Business
  - Indoor
  - Dimensioni ridotte
  - Complessità (e quindi costo) maggiore
- Campus/Reti cittadine/Accesso pubblico
  - Connettività su ampie aree geografiche
  - Scalabilità
  - Riconfigurabilità
- Applicazioni Militari

Standardizzazione

- Il TG 802.11s ha lo scopo di definire un *Extended Service Set (ESS)* per supportare servizi b*roadcast/multicast* ed *unicast* in reti *multihop.*
- Draft 1.0 Novembre 2006
- Draft 2.0 Marzo 2008
- Draft 3.0 Marzo 2009

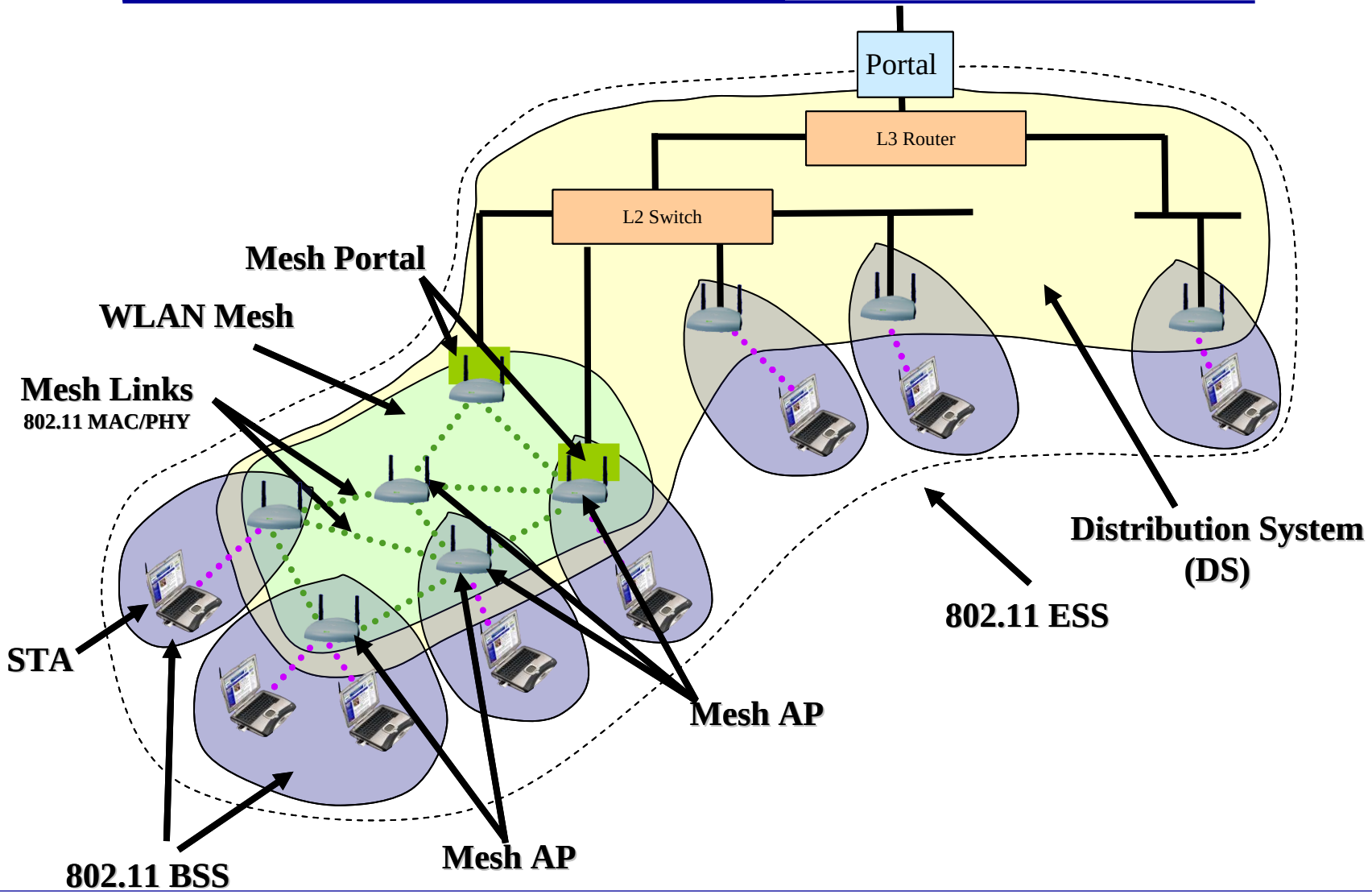
802.11s

- Routing robusto ed efficiente:
  - *Mesh Topology Learning,*
  - *Routing and Forwarding*
- Sicurezza:
  - *Compatibilità con 802.11x*
- Flessibilità del livello MAC
  - *Mesh Measurement*
  - *Mesh Discovery and Association*
  - *Mesh Medium Access Coordination*
  - *Supporto alla QoS*
- Trasparente ai livelli superiori
- Compatibile con dispositivi *legacy*

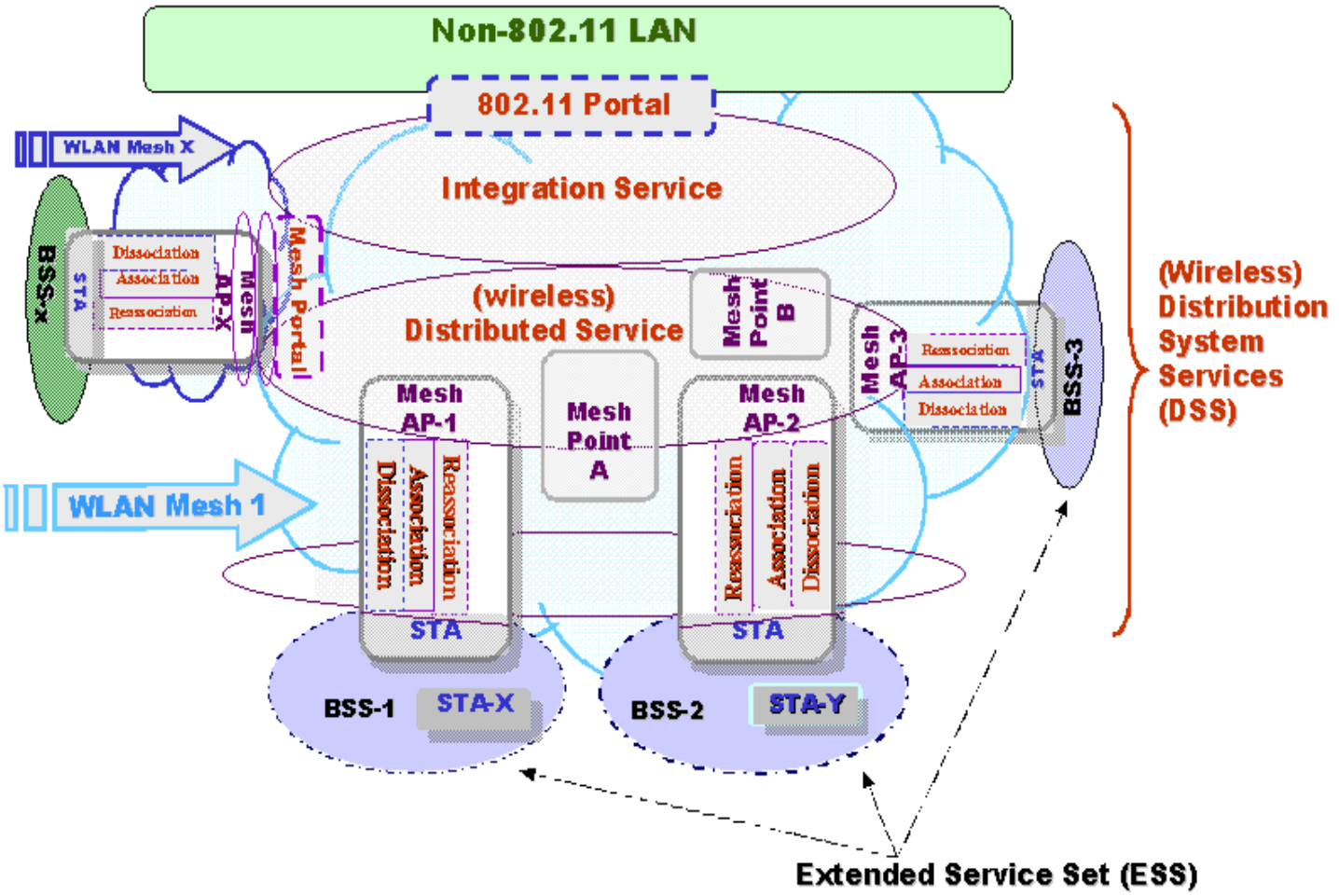
802.11s

- Routing: Hybrid Wireless Mesh Protocol (HWMP) – combinazionbe di AODV e protocollo tree-based
- Applicazioni:
  - OLPC (One Laptop Per Child)
  - Open802.11s

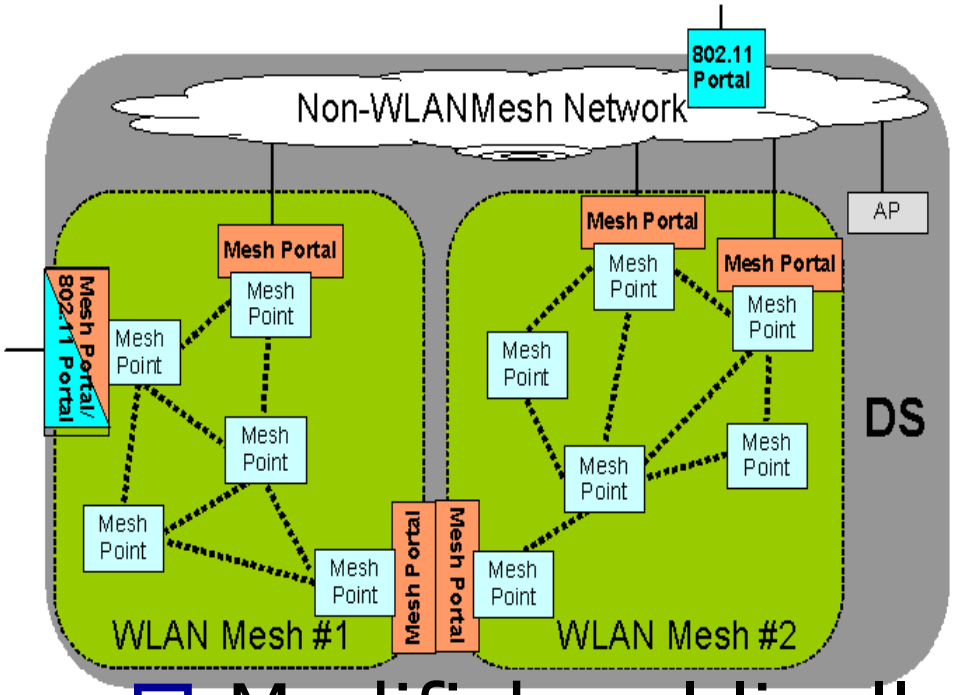
Una rete *Mesh*

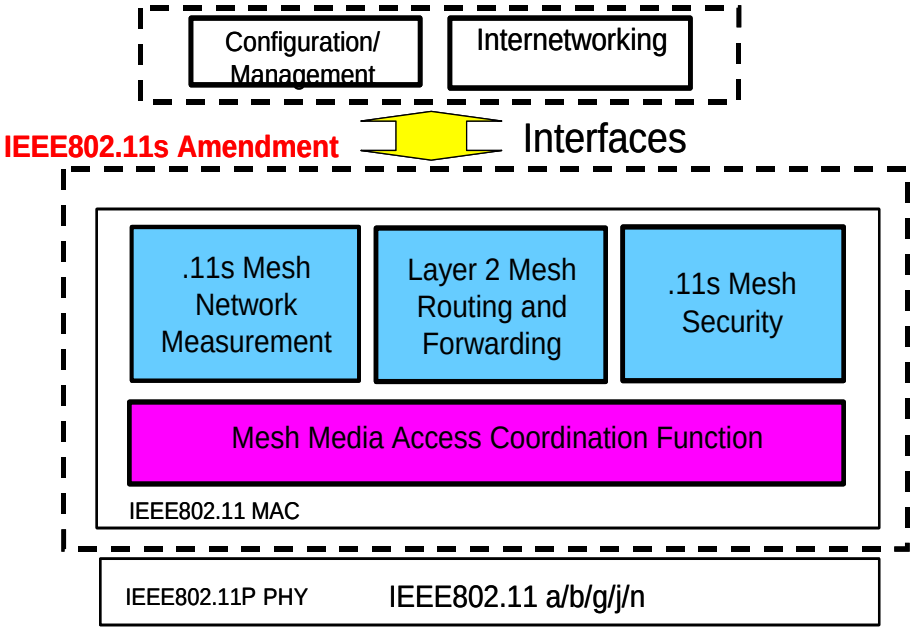


Architettura di una rete Mesh



Architettura e Protocolli





- Modifiche al livello MAC e al livello di routing
- Nessuna modifica al livello fisico

Soluzioni "Off the Shelves"

- Molte aziende producono già dispositivi per l'implementazione di reti *mesh*:
  - *Motorola* (*MeshNetworks*^{TM}): *MeshNetworks Enabled Appliances* (MEA)
  - *Tropos Networks (*802.11-*compliant)*
  - *Nortel (*802.11-*compliant)*
- Tutte le soluzioni commerciali forniscono l'hardware e il software (proprietario) per l'implementazione delle reti *Mesh*