Reti di Calcolatori

Protocolli datalink layer per reti WAN

Protocolli datalink layer per WLAN

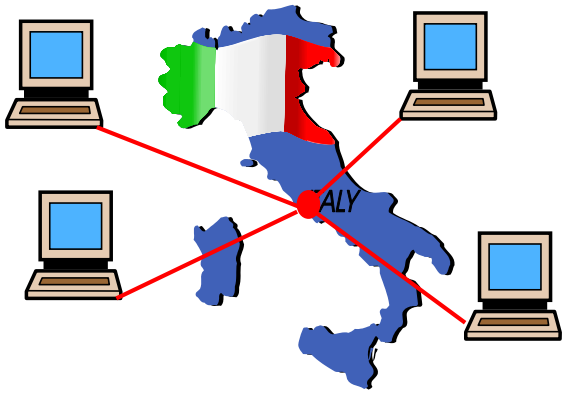
TIPI di RETI

LAN (Local Area Network)

E' limitata ad un singolo edificio, o + edifici vicini, e disposta in modo che i cavi non attraversino il suolo pubblico.

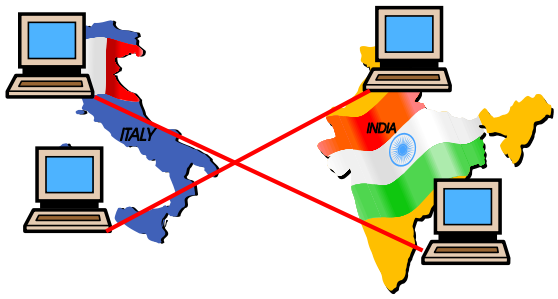
MAN (Metropolitan Area Network)

Collegamenti all'interno di una provincia.



WAN (Wide Area Network)

Computers collegati a grandi distanze, anche mondiale

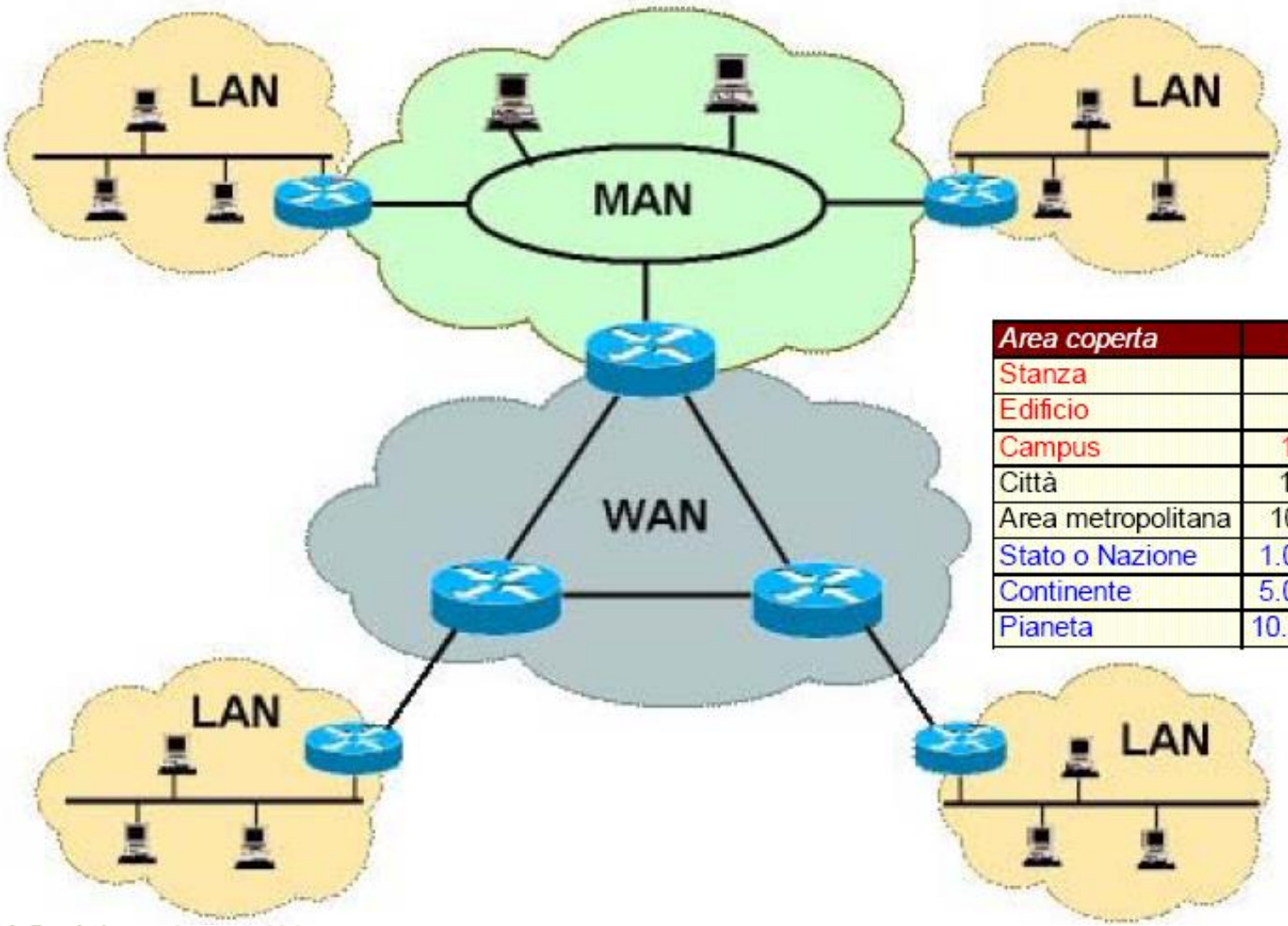


MAN

Le reti **MAN** hanno caratteristiche simili alle LAN ma su area più vasta, tipicamente una grande città o una provincia. Possono essere reti private o pubbliche e fornire servizi di vario tipo in ambito urbano (telefonia, TV via cavo, interconnessione di computer).

WAN

La rete **WAN** è costituita da un numero elevatissimo di nodi connessi tra loro su un territorio molto vasto come una nazione o addirittura diverse nazioni.
Sono anche dette **reti geografiche**. Le connessioni avvengono sia utilizzando la rete telefonica sia linee dedicate.

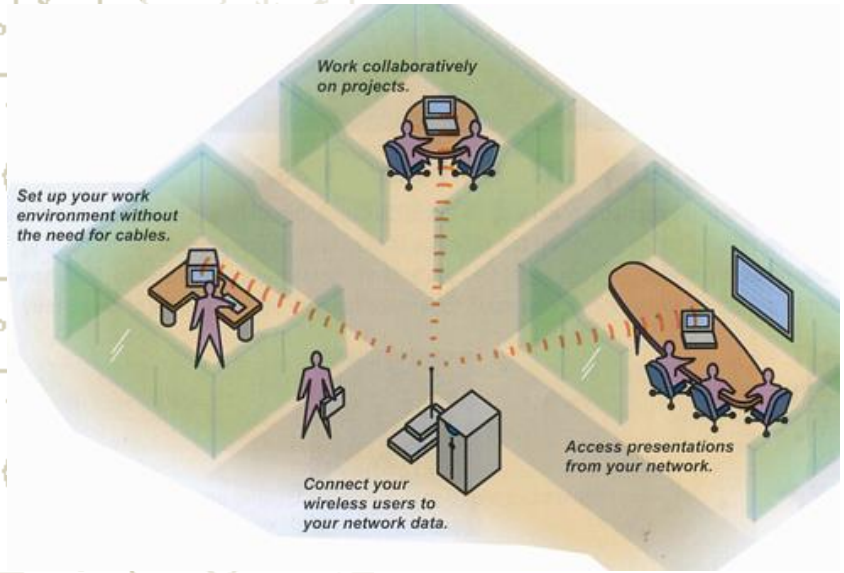


Area coperta	Distanza	Tipo di rete
Stanza	10 metri	LAN
Edificio	100 metri	LAN
Campus	1 kilometro	LAN
Città	10 kilometri	MAN
Area metropolitana	100 kilometri	MAN
Stato o Nazione	1.000 kilometri	WAN
Continente	5.000 kilometri	WAN
Pianeta	10.000 kilometri	WAN

WLAN

RETI LAN sono solitamente
le reti aziendali, scolastiche, universitarie,…

Nelle reti LAN i computer (o nodi) sono connessi mediante **schede di rete** e appositi **cavi** senza ausilio di rete telefonica.



Tra le reti LAN vi sono le **WLAN** (**Wireless LAN** o 'rete locale senza fili') impiegate dove risulta difficoltoso l'uso di cavi.
Vista la diminuzione dei costi trova impiego nell' uso domestico per la connessione a Internet in famiglia e in aziende o scuole.

Cos'è una Wireless LAN

- Una Wireless Local Area Network (W-LAN) è una rete locale i cui nodi comunicano tra loro attraverso il canale radio

- Nota: wireless significa "senza cavo"
  - Per le reti, si può trattare di radio od infrarossi
  - Noi faremo generalmente riferimento alla tecnologia radio

Motivazioni e Vantaggi delle WLAN

- Motivazioni:
  - Una WLAN è un sistema di comunicazione dati molto flessibile e può essere utilizzato come estensione o anche alternativa alle normali LAN su cavo
  - principalmente la diffusione di computer portatili, per offrire mobilità senza perdita di connessione
  - un altro fattore è l'estensibilità della rete senza necessità di cablaggio
- Vantaggi:
  - *Mobilità*: Gli utenti possono accedere alle risorse di rete da qualsiasi posizione senza doversi collegare ad una presa
  - *Velocità e semplicità di installazione*: È possibile installare una WLAN senza dover stendere cavi attraverso muri o sotto i pavimenti
  - *Flessibilità di installazione*: La tecnologia radio fa sì che la copertura sia garantita anche dove non è possibile cablare

Motivazioni e Vantaggi delle WLAN

- Vantaggi:
  - *Costi*:
    - Le spese di installazione ed i costi di esercizio e manutenzione per una WLAN sono molto inferiori rispetto ad una LAN cablata.
    - I benefici di costo a lungo termine sono maggiori soprattutto in ambienti dinamici dove ci sono cambiamenti frequenti
  - *Scalabilità*:
    - Le WLAN possono essere configurate in diverse topologie in modo da soddisfare le diverse esigenze di particolari applicazioni
    - Reti peer-to-peer adatte per un numero piccolo di utenti
    - Infrastrutture di rete per il supporto di migliaia di stazioni in mobilità su un'area molto estesa
    - La configurazione può essere modificata facilmente

Bande trasmissive delle WLAN

- Lo strato fisico è realizzato con la trasmissione omnidirezionale in modulazione digitale di una portante
- Esistono bande di frequenza dedicate all'utilizzo senza necessità di registrazione ed allocazione
  - queste bande si chiamano **ISM** (Industrial, Scientific, Medical)
  - la legislazione specifica determinate caratteristiche obbligatorie per utilizzare queste bande, come ad esempio la potenza massima di trasmissione e l'utilizzo di tecniche trasmissive spread spectrum
- le bande utilizzate nelle trasmissioni wireless sono a 2.4 GHz ed a 5 GHz
  - in questa regione le trasmissioni competono con apparati radiocomandati, telefoni cordless, forni a microonde, …

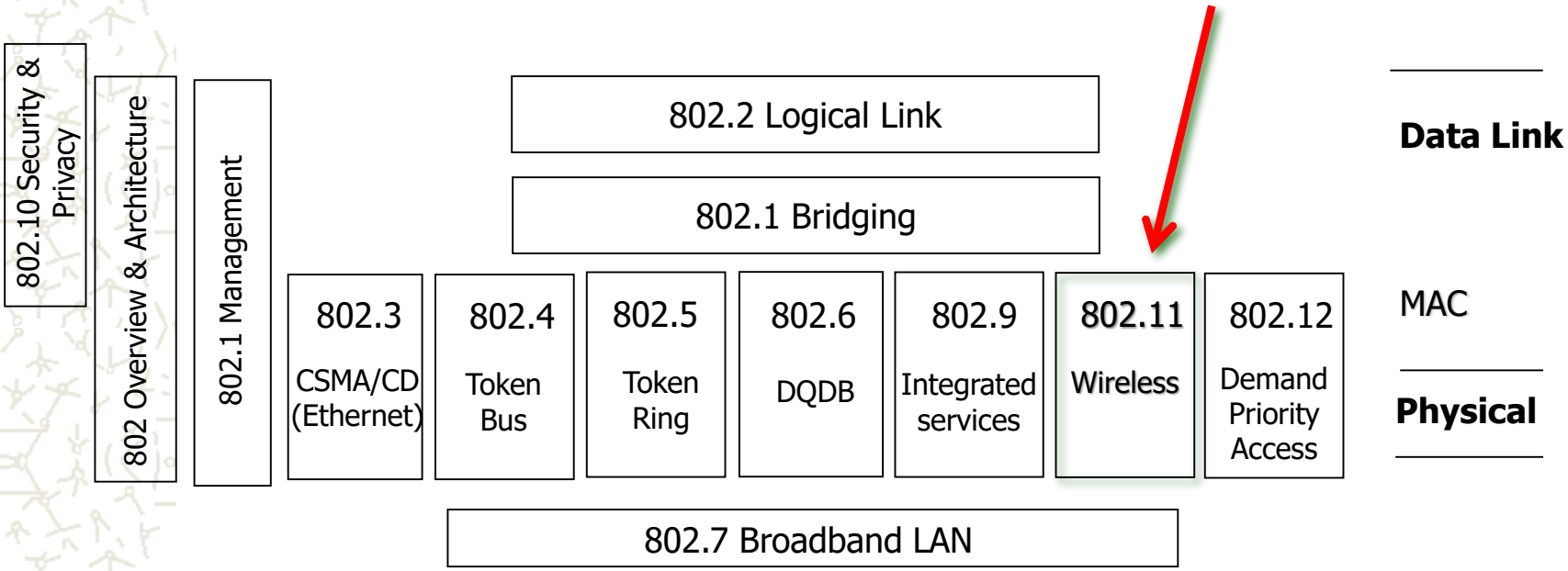
Regole per le bande ISM

- Per evitare abusi, le organizzazioni hanno comunque imposto delle regole per queste bande, e solo i prodotti conformi con queste regole possono emettere in tali bande
  - Uso della tecnica di **Spread Spectrum** (FHSS o DSSS)
  - Limiti sulla massima potenza trasmessa in banda e sulle emissioni fuori banda per limitare l'inquinamento dei sistemi adiacenti nello spettro
    - FCC (America del Nord) impone 1 W sulle bande a 900 MHz e 2.4 GHz
    - ETSI (Europa) impone 100 mW sulla banda a 2.4 GHz
  - Definizione dei canali per garantire la coesistenza tra sistemi

Standard 802.11x

- L'IEEE ha definito diversi standard nel corso del tempo per le trasmissioni wireless
- Questi standard sono:
  - IEEE 802.11 con tre differenti tecniche trasmissive (IR, FHSS, DSSS) e velocità ad 1 o 2 Mbps nella banda a 2.4 GHz
  - IEEE 802.11b a velocità 1, 2, 5.5 e 11 Mbps a 2.4 GHz via HR-DSSS
  - IEEE 802.11a con velocità fino a 54 Mbps nella banda a 5 GHz tramite OFDM
  - IEEE 802.11g fino a 54 Mbps nella banda a 2.4 GHz
  - IEEE 802.11n fino a 300 Mbps sia a 2.4 GHz che a 5 GHz, utilizza la tecnologia MIMO (multiple-input multiple-output) per utilizzare più antenne per trasmettere e più antenne per ricevere incrementando la banda disponibile utilizzando una multiplazione a divisione di spazio
  - IEEE 802.11ac fino a 1Gbps a 5 Ghz estendendo i concetti di 802.11n

I protocolli della famiglia IEEE 802.x

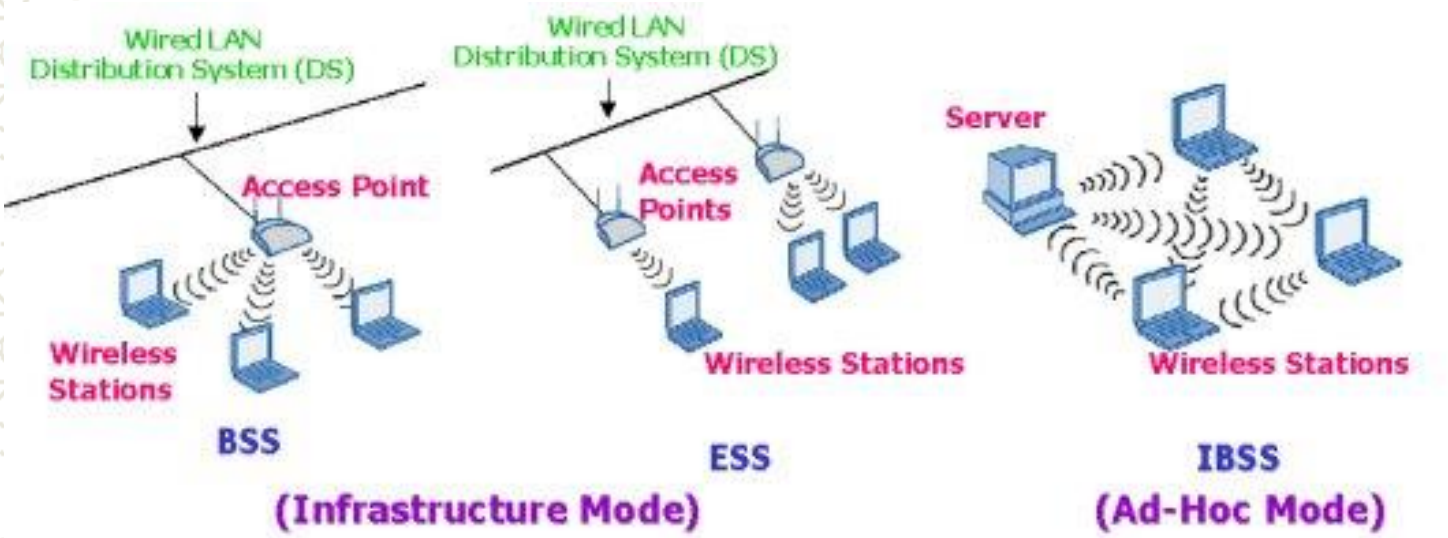


L'architettura delle WLAN IEEE 802.11

- L'architettura 802.11 è costituita da diversi componenti e servizi che interagiscono al fine di garantire la mobilità delle stazioni in modo trasparente agli strati più alti dello stack di protocolli
- Il componente di base della WLAN 802.11 è la **stazione**
  - È una qualsiasi unità che contiene le funzionalità del protocollo 802.11
  - Le stazioni 802.11 possono essere mobili (palmari), portatili (PC) o stazionarie (Access Point)
- Un insieme di stazioni costituisce un **Basic Service Set** (BSS)

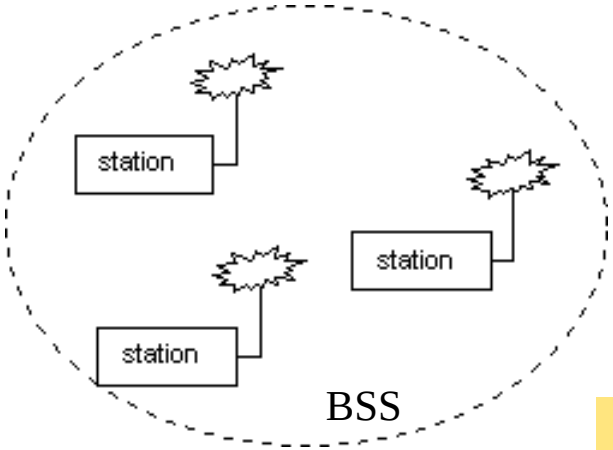
Topologie di rete per IEEE 802.11

- Esistono due modalità di funzionamento
  - Independent Basic Service Set (IBSS) o Ad Hoc Network
  - Infrastructure Basic Service Set o Infrastructure Mode



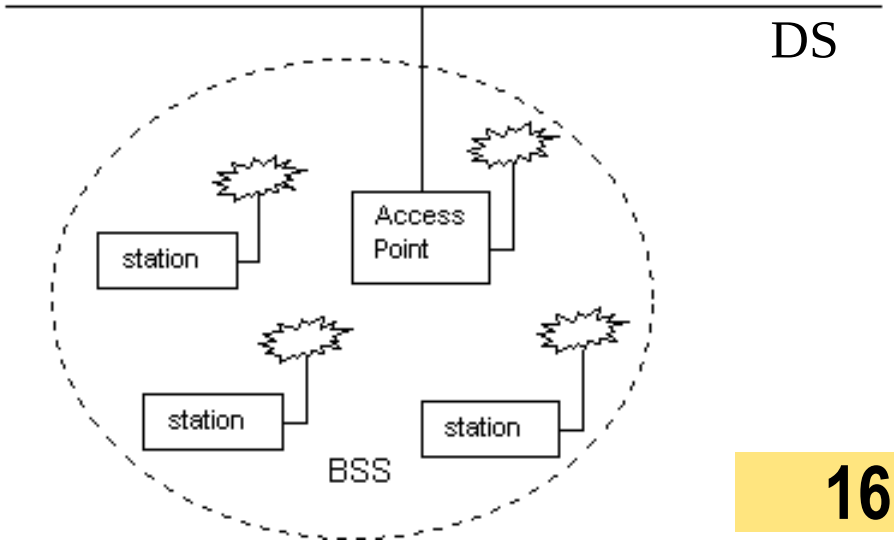
Independent Basic Service Set

- È la topologia più semplice dove un insieme di stazioni si sono identificate reciprocamente e sono interconnesse tra di loro in modalità peer-to-peer
- In un IBSS le stazioni comunicano direttamente tra loro
- In una IBSS non ci sono funzioni di relay
  - una stazione è raggiungibile solo se situata entro il raggio di copertura



Infrastructure Basic Service Set

- È una BSS con un componente chiamato **Access Point** (AP) che fornisce la funzione di relay per la BSS
- L'architettura dell'Infrastructure BSS è di tipo cellulare
  - Il sistema è diviso in celle costituite dalle BSS
  - Ciascuna cella è controllata dall'AP
  - La comunicazione tra stazioni avviene solo attraverso l'AP
- L'AP può fornire la connessione al **Distribution System**

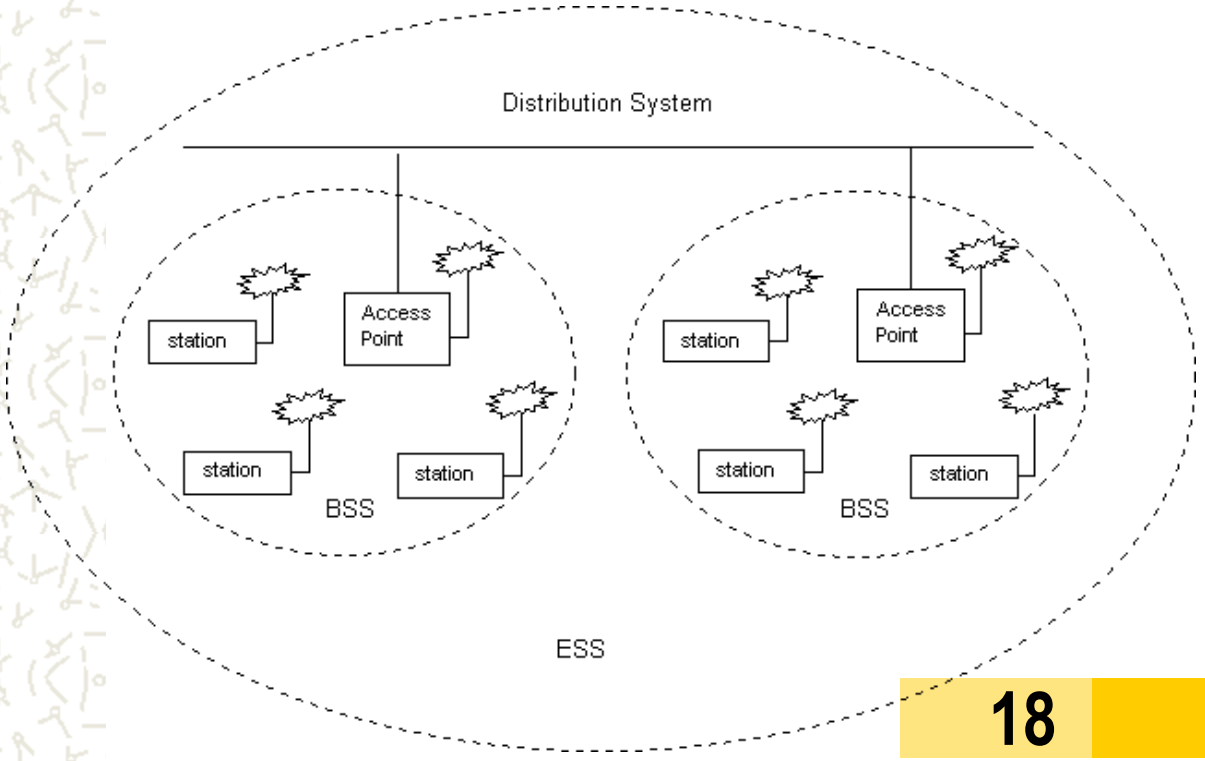


Il Distribution System (DS)

- Funzionalmente è uno strato residente in ciascun AP che funge da dorsale della WLAN, attraverso il quale un AP comunica con un altro AP per
  1. Scambiare pacchetti destinati alle stazioni nei rispettivi BSS
  2. Girare pacchetti per inseguire le stazioni mobili che si spostano da un BSS ad un altro
  3. Scambiare pacchetti con una rete su cavo
- Lo standard 802.11 non pone nessun vincolo su come il DS deve essere implementato, ma solo sui servizi che deve fornire
  - Il DS si può basare sia su una LAN 802.3 su cavo, che su una rete wireless 802.11

Extended Service Set

- In 802.11 l'**Extended Service Set** (ESS) estende la mobilità delle stazioni ad un raggio di azione arbitrario
- Un ESS è un insieme di Infrastructure BSS, dove gli AP comunicano tra di loro attraverso il DS per trasportare il traffico da una BSS all'altra, agevolando lo spostamento delle WS tra BSS



L'ESS nel modello OSI

- Gli elementi di rete al di fuori dell'ESS vedono l'ESS e tutte le sue stazioni mobili come una singola rete al livello MAC dove tutte le stazioni sono fisicamente stazionarie
- L'ESS quindi nasconde la mobilità delle stazioni mobili a quanto situato al di fuori dell'ESS, ed è visto dai livelli superiori del modello OSI come una singola rete 802
- Questa caratteristica di 802.11 consente ai protocolli di rete esistenti, che non possiedono il concetto della mobilità, di operare correttamente con una WLAN che supporta la mobilità

Tecnologie e protocolli dello strato fisico

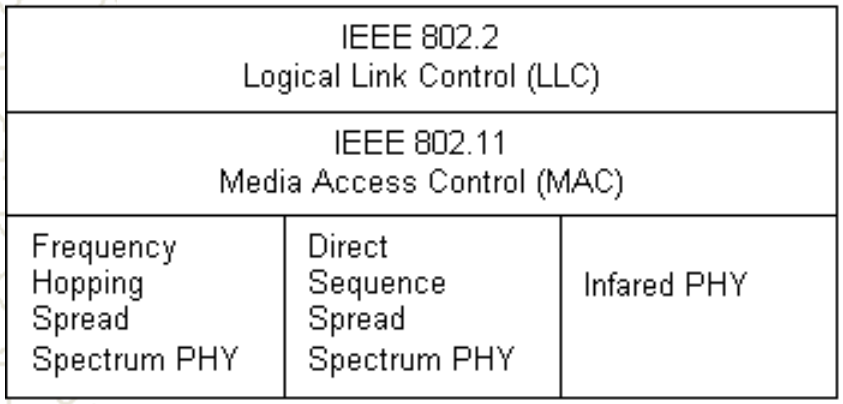
Lo strato fisico deve:

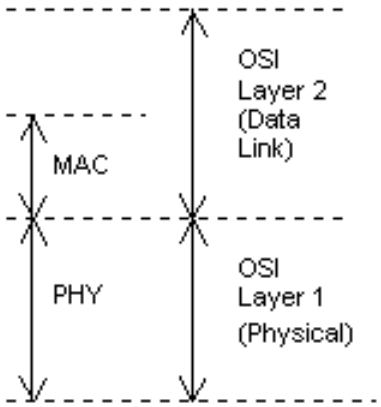
- Fornire un'interfaccia per lo scambio di frame con lo strato MAC per la trasmissione e la ricezione dei dati
- Fornire al MAC un'indicazione sull'attività del mezzo (meccanismo di carrier sense fisico)
- Trasmettere fisicamente i frame attraverso il mezzo fisico nella banda di frequenze assegnata

Proprietà del PHY di IEEE 802.11

- Lo standard 802.11 definisce tre tecnologie (diverse tra di loro e quindi non interoperabili) ad 1 e 2 Mbit/sec nella banda a 2.4 GHz
  - **Frequency Hopping Spread Spectrum** (FHSS)
  - **Direct Sequence Spread Spectrum** (DSSS)
  - **Infrarossi**

Spread Spectrum





Estensioni del PHY IEEE 802.11

- 802.11b è l'estensione del PHY 802.11 nella banda a 2.4 GHz per il supporto di 5.5 e 11 Mbit/sec, in tecnologia DSSS

- 802.11a è l'estensione del PHY 802.11 nella banda a 5 GHz per il supporto fino a 54 Mbit/sec, in tecnologia **Orthogonal Frequency Division Multiplex** (OFDM)

Spread Spectrum

- Il segnale è sparpagliato, a pari potenza totale, su una banda più ampia di quanta realmente necessaria per la trasmissione

- Ha uno spettro con banda larga e bassi valori di modulo e, quindi, risulta difficilmente distinguibile dal rumore di fondo (utile per Applicazioni militari)

- In questo modo si riduce l'efficienza del sistema perchè non si utilizza l'intera capacità di banda

Spreading Spectrum

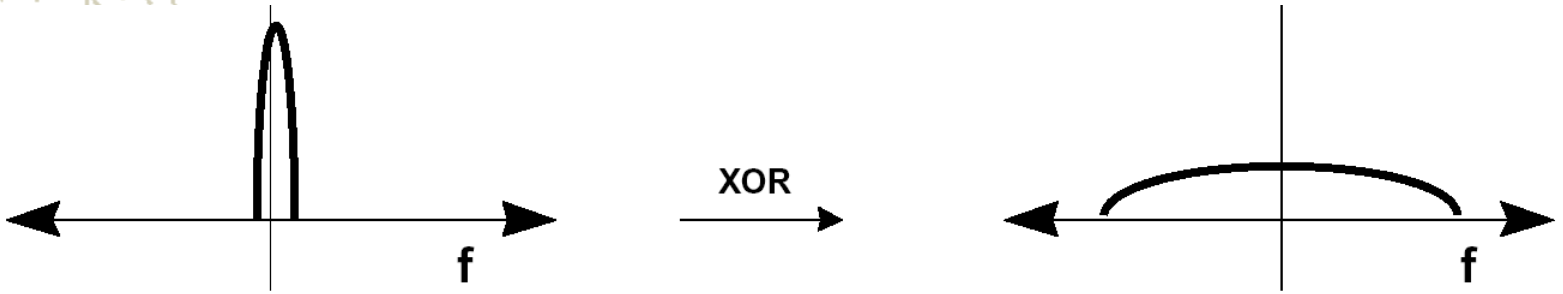


Figure 5a Effect of PN Sequence on Transmit Spectrum

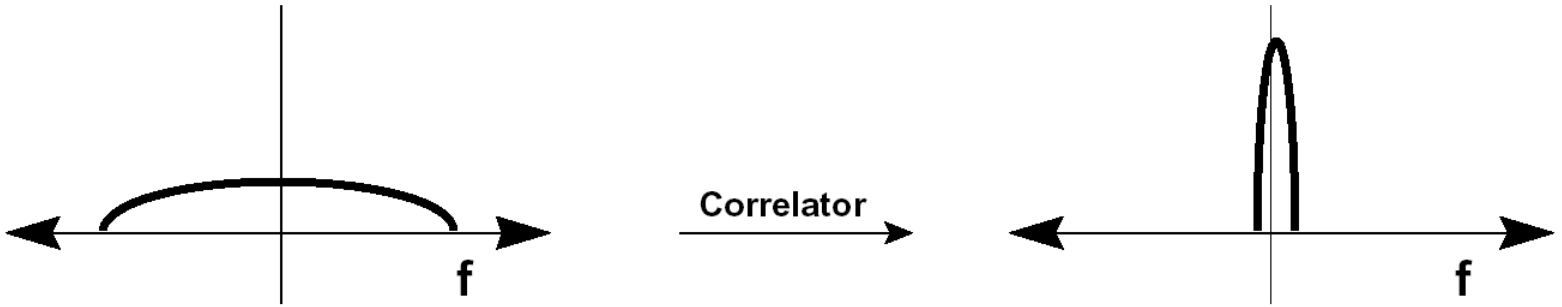


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

Vantaggi dello Spread Spectrum

- Impedendo a ciascun sistema di usare l'intera capacità di banda, sistemi indipendenti possono essere sovrapposti nella stessa banda con un impatto trascurabile sulle prestazioni
- Viene ridotto l'impatto sul sistema di interferenze localizzate
  - Si ha maggiore robustezza in ambienti disturbati
- Si può far vedere che lo Spread Spectrum può aiutare a ridurre il delay spread dovuto al multipath
  - Si garantiscono prestazioni migliori in ambienti dove il multipath è maggioromente accentuato (ad es. ambienti indoor), con un aumento del raggio d'azione e del rate raggiungibile

Tecniche a Divisione di Spettro (SST)

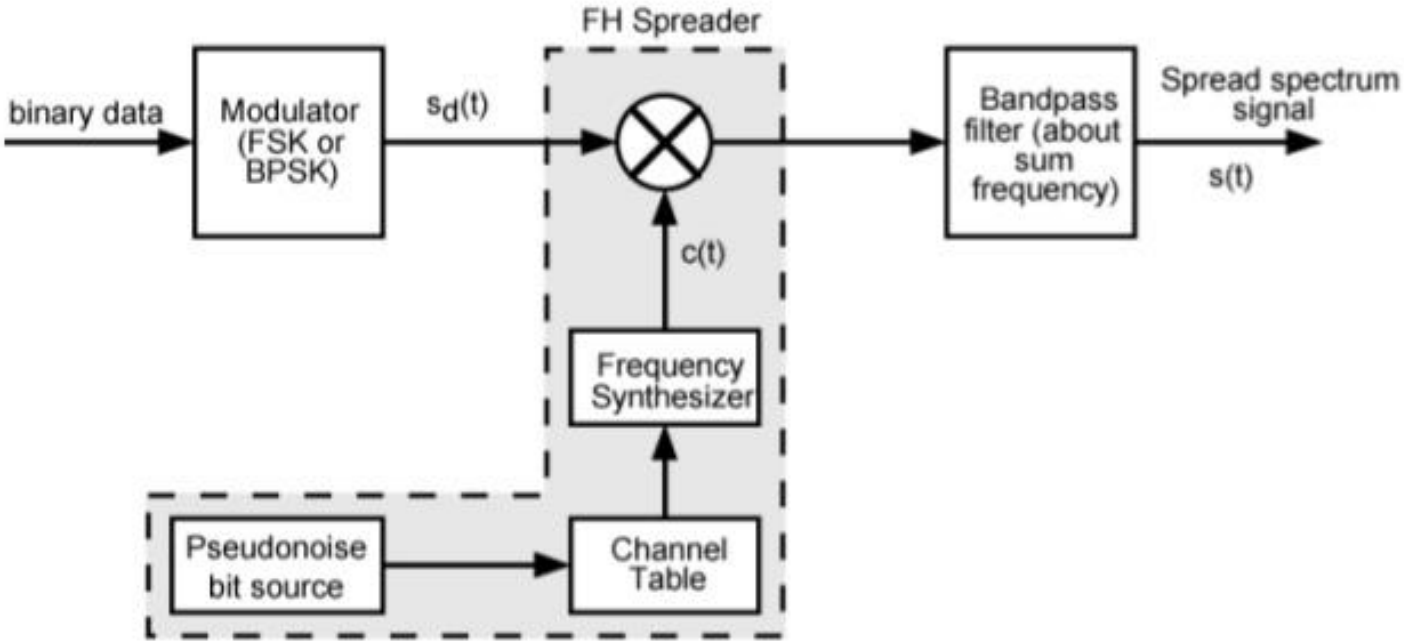
Esistono varie procedure per allargare lo spettro di un segnale:

1. FH – salto in frequenza (Frequency Hopping)
2. DS – sequenza diretta (Direct Sequence)

- Occupano più banda del necessario ma
  - Aumentano l'immunità al rumore (DS)
  - Aumentano la sicurezza della comunicazione

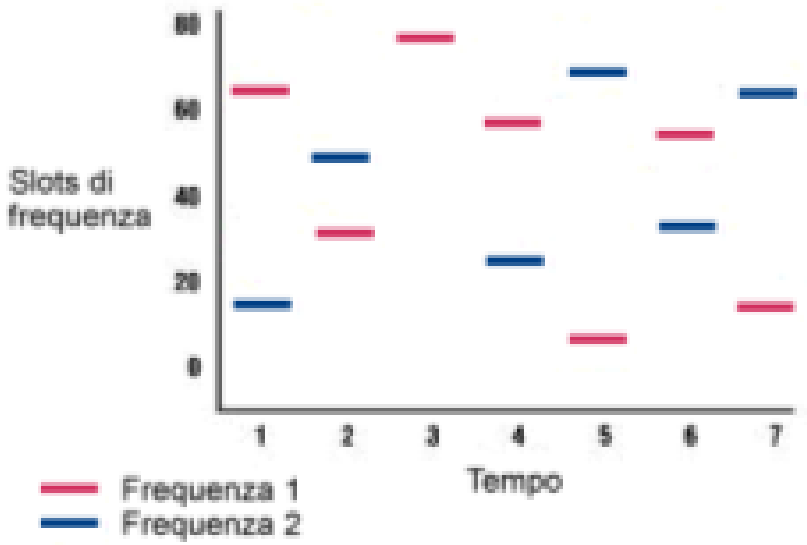
FHSS

Frequency Hopping Spread Spectrum System (Transmitter)



802.11 FHSS

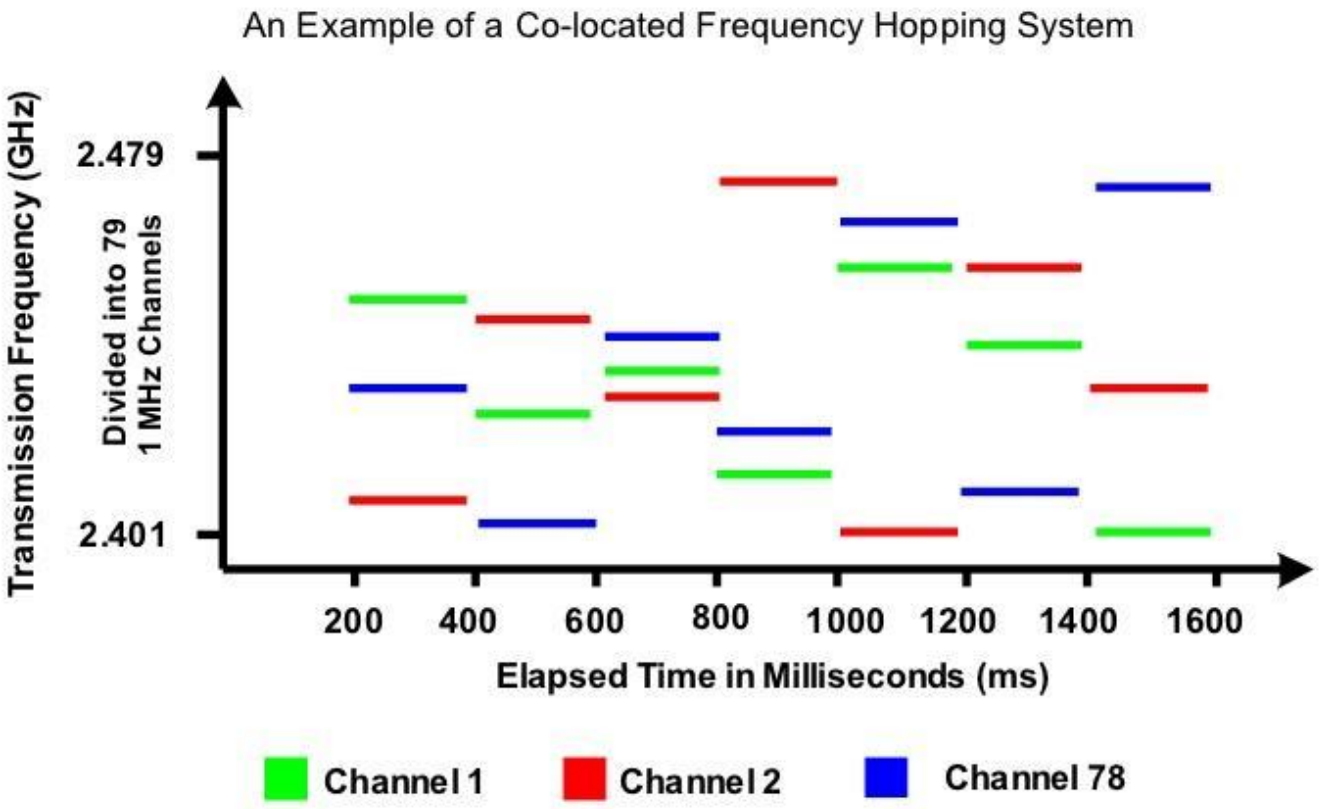
- 802.11 FHSS (Frequency Hopping Spread Spectrum)
  - utilizza 79 canali ad 1 MHz a partire da 2.4 GHz con la tecnologia Frequency Hopping:
  - la trasmissione salta ad intervalli temporali definiti (minori di 400 ms) da una frequenza ad un'altra secondo una sequenza pseudocasuale nota a tutti
  - la banda disponibile è 1 MHz
  - supporta standard ad 1 e 2 Mbps, con codifiche a 2 o 4 simboli con (G)FSK



- questa tecnica fornisce sicurezza (impossibile seguire la comunicazione senza conoscere la sequenza pseudocasuale) e solidità contro il multipath fading (quando arriva il segnale riflesso la ricezione è già spostata su un altro canale)

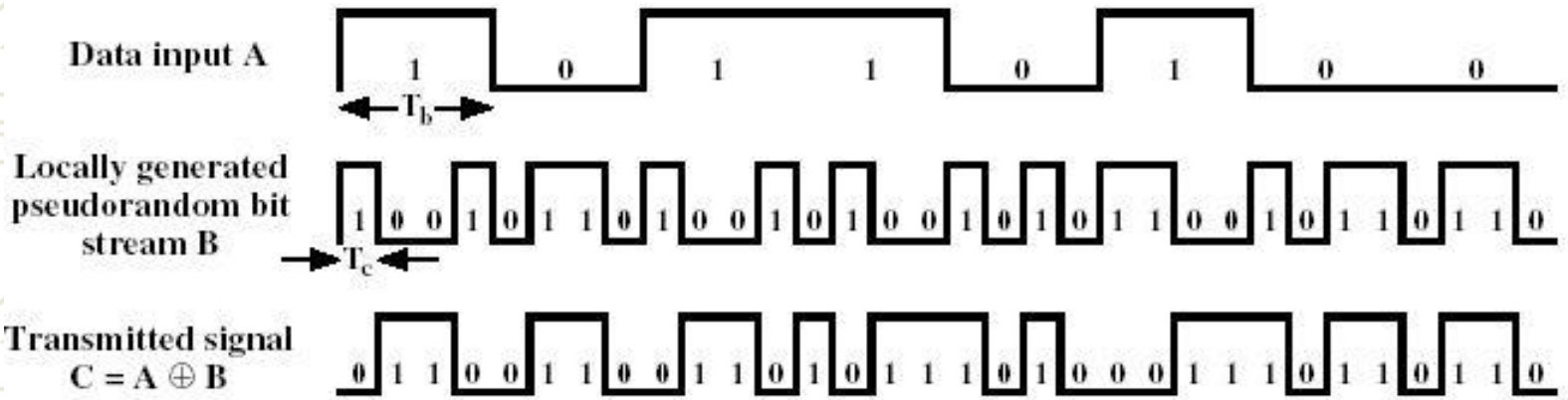
802.11 FHSS

Frequency Hopping Spread Spectrum



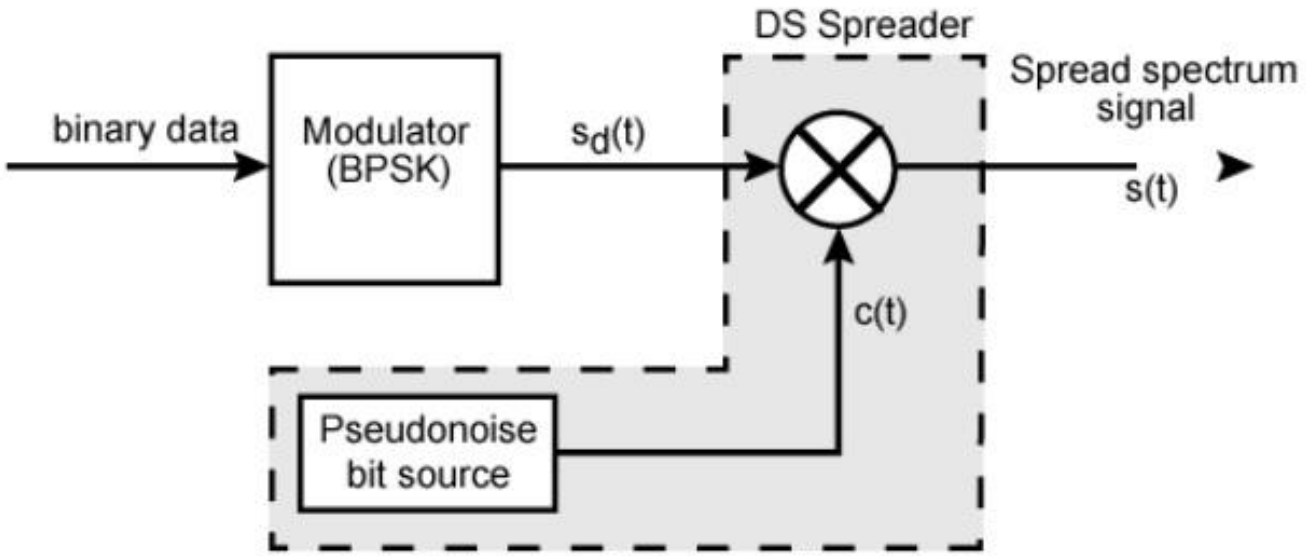
DSSS

- 802.11 DSSS (Direct Sequence Spread Spectrum)
  - Per far fronte al rumore si usa la tecnica “chipping”:
  - Ogni bit è convertito in una serie di bit ridondanti (chip)
    - il tempo di un bit viene suddiviso in *m* intervalli temporali
    - il valore trasmesso e’ la combinazione in or esclusivo dei bit dei dati (di durata Tb) combinati con una sequenza pseudocasuale o predefinita di bit, ciascuno di durata Tc=Tb/m, detti chip
  - lo standard opera nella banda a 2.4 GHz ed utilizza una sequenza fissa di 11 chip (sequenza di Barker) per codificare un bit di dati



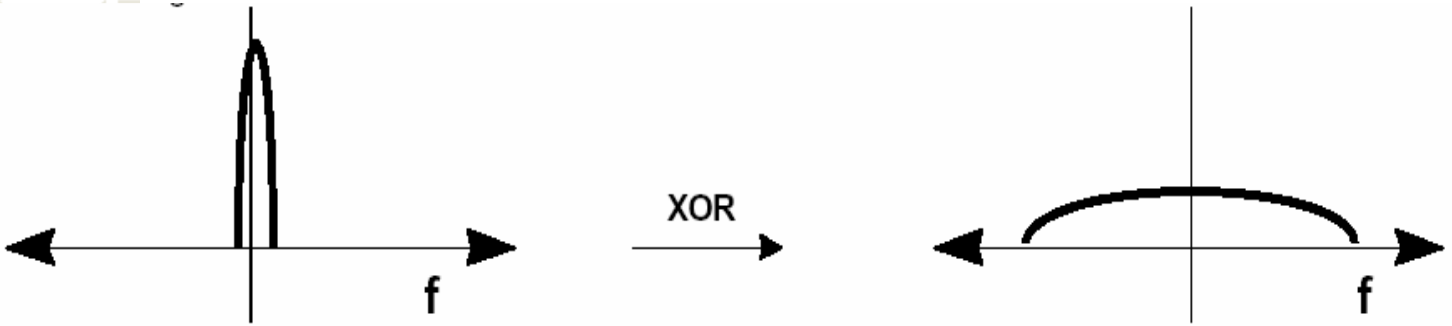
DSSS

Direct Sequence Spread Spectrum Transmitter

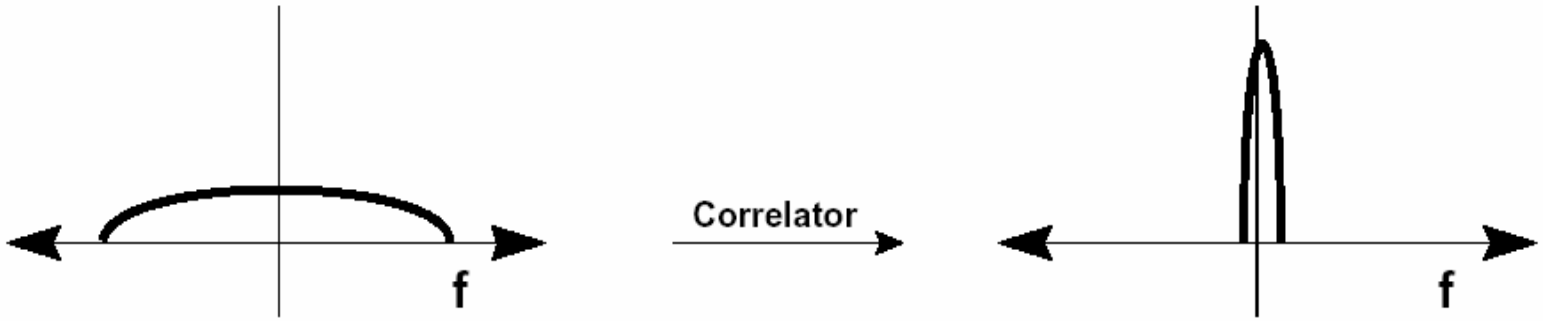


DSSS

La sequenza PN provoca un'allargamento (**spread**) della banda passante del segnale risultante (da cui il termine **spread spectrum**) con una conseguente riduzione del picco di potenza.



Il segnale ricevuto è correlato alla sequenza PN al fine di ricostruire i dati originari e di filtrare eventuali interferenze.



DSSS

- 802.11 DSSS (Direct Sequence Spread Spectrum) (cont.)
  - la banda disponibile è divisa in 14 canali di 5 MHz, a partire da 2.412 GHz
    - le stazioni debbono essere configurate per determinare il canale utilizzato
    - non tutti i canali sono disponibili in tutti i paesi
    - in USA il canale 14 è proibito, in Spagna sono ammessi solo il 10 e l'11, in Italia sono tutti ammessi
  - le antenne trasmettono a 11 MHz; con modulazioni PSK a 2 o 4 livelli e 11 chip per bit lo standard permette trasmissioni a 1 o 2 Mbps
    - poichè l'ampiezza di banda del segnale inviato è intorno ai 22 MHz, nonostante i filtri dell'elettronica per non interferire due trasmissioni indipendenti nella stessa area debbono utilizzare canali separati da almeno 5 canali

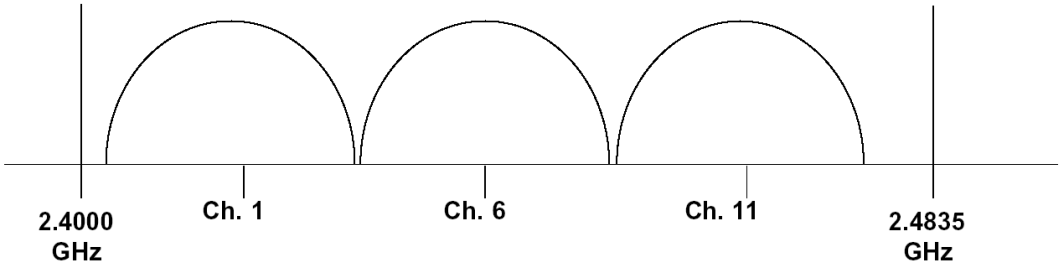


Figure 6 Three Non-Overlapping DSSS Channels in the ISM Band

Canali DSSS

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

DS vs. FH

- DSSS:
  - Codifica ridondante ➔ più immune ai rumori
  - Maggiore spreco di banda (30 MHz per canale)
  - Possibilità di arrivare a 11 Mbps
- FHSS:
  - Più sicura
  - Molto limitata in banda (1 MHz)
  - Impossibile usarla nel WI-FI ad alti bit-rate

Dynamic Rate Shifting

- È un meccanismo del PHY di 802.11b che consente di modificare automaticamente la velocità di trasmissione dei dati al fine di compensare le variazioni del canale
  - Il rate varia in funzione della
    - Attenuazione dovuta alla distanza tra la stazione e l'access point (potenza, fattore al numeratore del SNR)
    - entità delle interferenze (rumore, fattore al denominatore del SNR)
- Tale tecnica è trasparente all'utente ed agli strati superiori dello stack di protocolli

Protocollo di accesso al mezzo nella 802.11

CSMA/CA

(Carrier-Sense Multiple Access with Collision Avoidance)

- Come per il CSMA, lo strato fisico sonda il livello di energia sulla frequenza radio per determinare se c'è o no un'altra stazione che sta trasmettendo e fornisce questa informazione al livello MAC
- Se il canale è rilevato libero per un tempo >= DIFS (Distributed Inter Frame Space), la stazione trasmette.
- Se il canale è occupato, aspetta un tempo casuale (crescente) e riprova
- Come in CSMA, il frame sarà ricevuto se non ci sono state collisioni
- Quando il ricevitore riceve correttamente il frame, essa aspetta un breve periodo di tempo (SIFS – Short Inter Frame Spacing) e poi invia un frame di riscontro al sender.

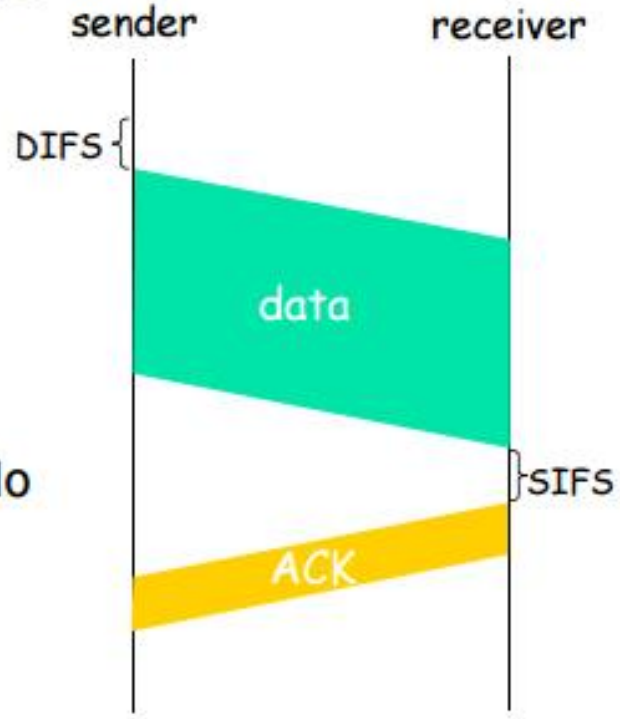
CSMA/CA

802.11 sender

- se il canale è inattivo per un tempo pari a **DIFS** (Distributed Inter Frame Space) allora
  - Trasmette un'intera frame (senza CD)
- se il canale è occupato
  - Sceglie un *backoff time* casuale
  - Il timer viene decrementato mentre il canale è inattivo
  - Allo scadere del timer, trasmette una frame
  - Se non riceve ACK, incrementa l'intervallo di backoff casuale, torna al passo 2

802.11 receiver

- se la frame è ricevuta in maniera corretta
  - restituisce un ACK dopo un tempo **SIFS** (Short Inter Frame Space)



CSMA/CA

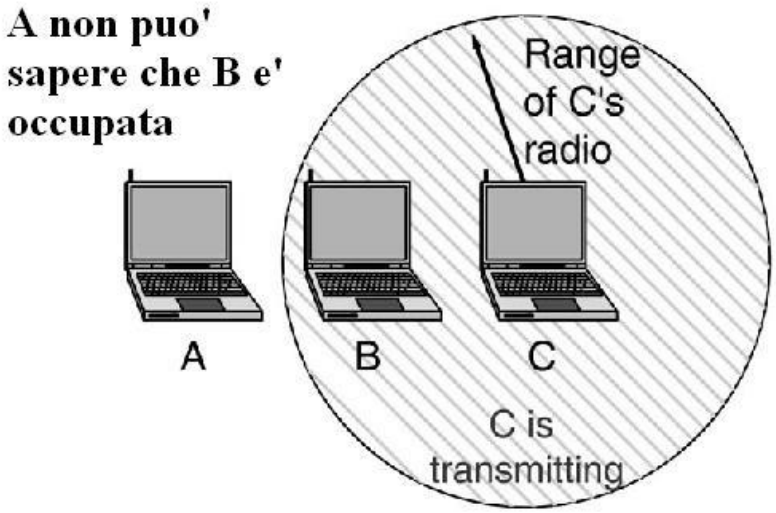
CSMA/CA non rileva le collisioni

- Motivo 1: La rilevazione delle collisioni richiede l'abilità di spedire e ricevere allo stesso tempo. Ciò può essere costoso.

- Motivo 2 (più importante): La capacità di rilevare le collisioni non garantisce l'assenza della collisione
  - Problema della stazione nascosta
  - Problema della stazione esposta
  - Attenuazione (fading)

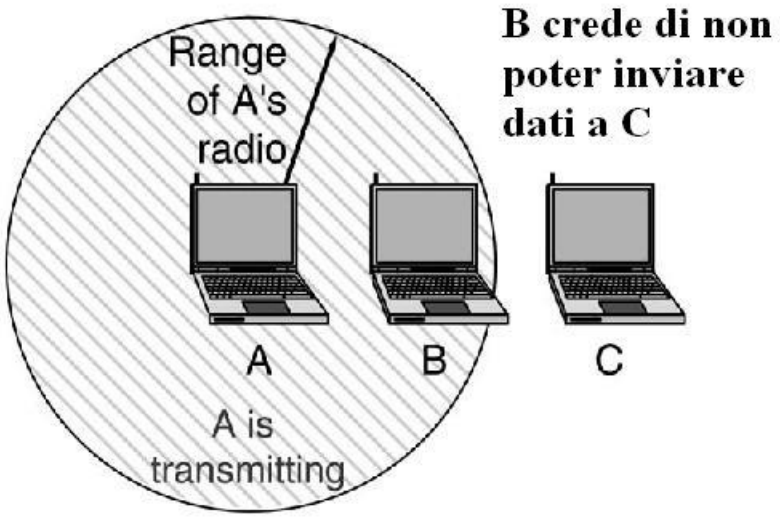
CSMA: stazione nascosta

- Come esempio consideriamo tre stazioni A, B e C tali che B sia a portata di A e di C, ma A e C non possano rilevare le rispettive trasmissioni
- Se C sta trasmettendo dati a B, A non potrà rilevare l'occupazione del canale in quanto è fuori portata
- A inizierà a trasmettere ed il suo segnale arriverà a B interferendo con i dati che C stà trasmettendo



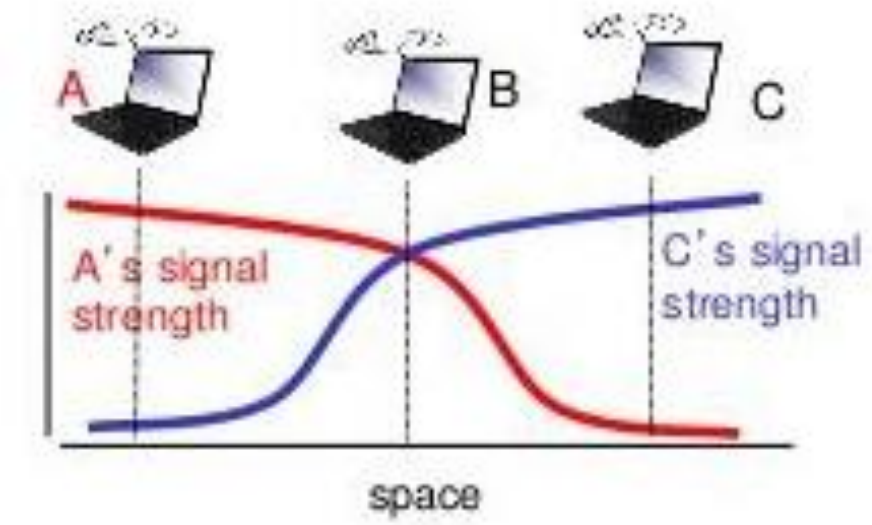
CSMA: stazione esposta

- Se nelle stesse ipotesi supponiamo che A stia trasmettendo verso un'altra destinazione, e che B desideri inviare dati a C
- B ascolta il canale e lo trova occupato, quindi non trasmette
- In realtà il canale sarebbe disponibile (nella ipotesi che la destinazione della trasmissione di A sia fuori dalla portata di B) perchè in C i segnali non interferirebbero



CSMA: Fading

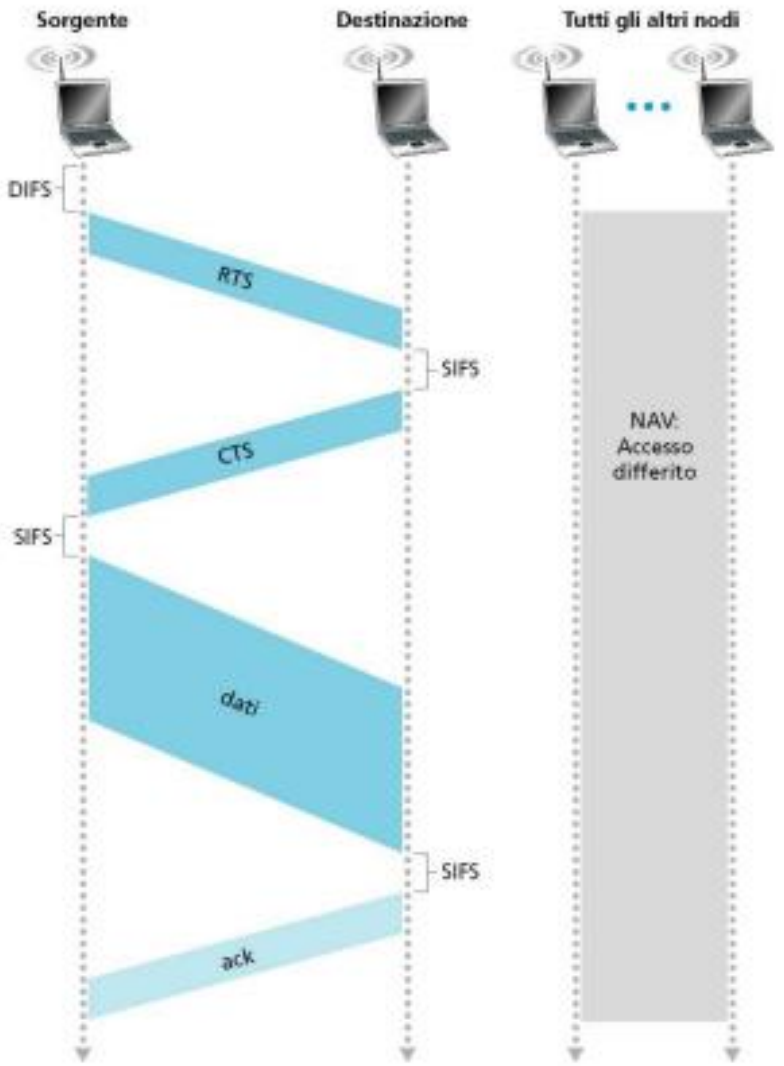
- A e C sono situati in modo che la forza del loro segnale non è sufficiente per rilevare le rispettive trasmissioni,
- ma il loro segnale è abbastanza forte da interferire con la stazione B



CSMA/CA

- L'inefficacia del protocollo CSMA deriva dal fatto che per le trasmissioni wireless quello che conta è l'interferenza in prossimità del ricevente, mentre l'analisi della portante che può fare una stazione è solo in prossimità di se stessa, cioè del trasmittente
- Il protocollo CSMA/CA (Multiple Access with Collision Avoidance) tenta di risolvere il problema nel seguente modo:
  - il trasmettitore A invia un piccolo frame (RTS: Request To Send) al ricevitore B
    - il frame RTS contiene la richiesta di trasmettere un frame a B, specificandone nel campo *duration* un'indicazione della durata della trasmissione dati.
    - Ciò darà agli altri la possibilità di conoscere per quanto tempo devono astenersi dalle trasmissioni
  - il ricevitore B trasmette un piccolo frame di conferma (CTS: Clear To Send) ad A, con le stesse informazioni del RTS
  - quando A riceve il CTS trasmette il frame di dati a B

CSMA/CA(cont.)



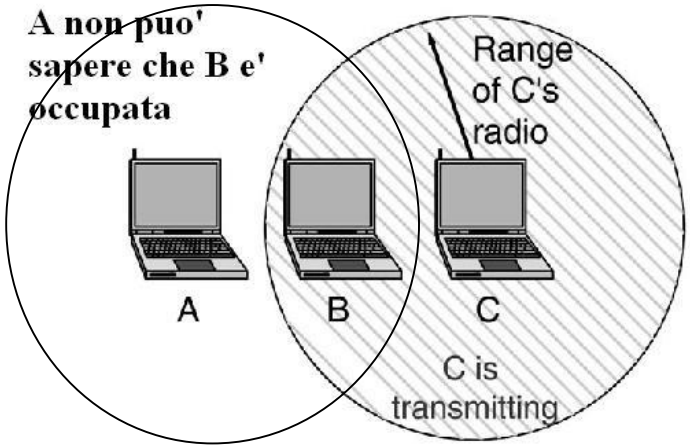
Tutte le stazioni che ricevono il frame RTS sanno che:

1. B risponderà con un CTS
2. in seguito, A trasmetterà un frame di dati per un tempo specificato in RTS

Queste stazioni attenderanno senza trasmettere per il tempo sufficiente alla trasmissione dei dati.

Il *NAV* (Network Allocation Vector) contiene l'intervallo minimo di tempo del quale le stazioni devono differire il loro accesso alla rete.

CSMA/CA: Soluzione Problema della stazione nascosta



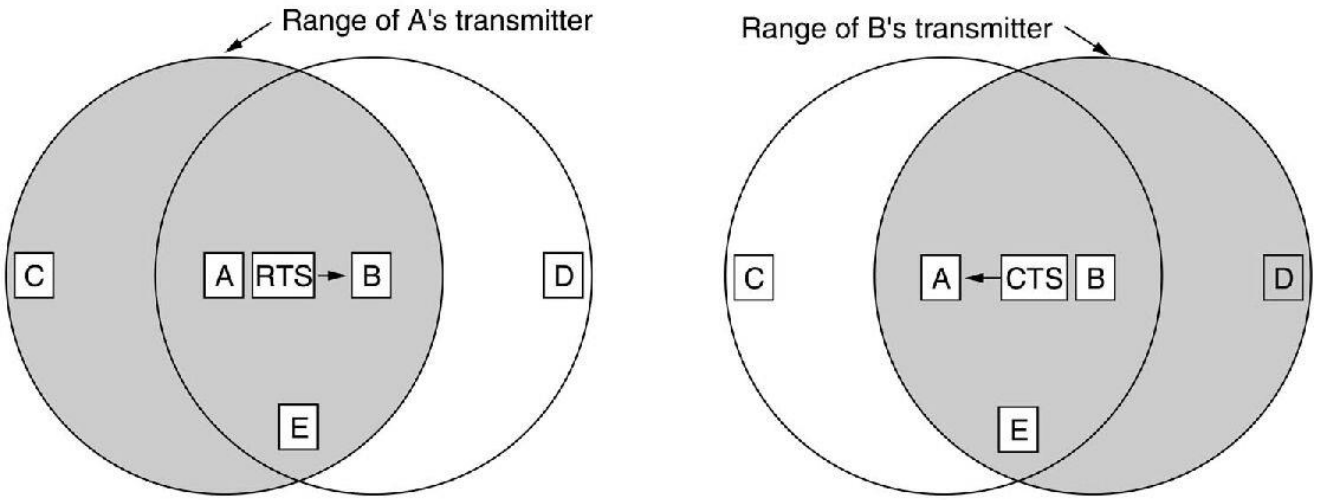
Problema della stazione nascosta:

- *A non vede C e viceversa*
- *B vede A e C*
- *A e C possono inviare dati simultaneamente a B creando una collisione*

- Le stazioni nascoste (A) non vedono il frame RTS (inviato da C), ma vedono il frame CTS (inviato da B), quindi sanno che:
  - trasmesso il CTS, B dovrà ricevere il frame di dati per un tempo specificato nel CTS
- Queste stazioni attenderanno senza trasmettere per il tempo necessario alla trasmissione del frame di C (che loro non vedranno in quanto nascoste, ma sanno che ci sarà) verso B.

CSMA/CA: Possibili collisioni

- Collisioni saranno possibili se un frame RTS venisse trasmesso contemporaneamente verso una destinazione collocata nel campo di ricezione dei due trasmittenti: i due frame andranno perduti
- In questo caso la stazione che non riceve il CTS dopo un timeout applica l'algoritmo di backoff esponenziale binario e ritenta



Exponential Backoff Algorithm 1

- Risolve i contenziosi del canale
  - Ogni stazione sceglie un numero random (*n*) compreso tra *0* e *m*
  - Attende (*n* x *slot time*) prima di riprovare
  - Ad ogni collisione *m* aumenta in maniera esponenziale
- Slot Time:
  - definito in modo che ogni stazione possa determinare se un'altra ha acceduto al canale nello slot precedente
  - questo riduce P(collisione) della metà

Exponential Backoff Algorithm 2

- Eseguito nei seguenti casi:
  - Tx trova il mezzo occupato
  - Dopo ogni ritrasmissione
  - Dopo una trasmissione andata a buon fine
- Non viene eseguito:
  - una stazione vuole tx un nuovo pacchetto ed il mezzo è libero

CSMA/CAW

- Il protocollo CSMA/CAW (CSMA/CA per Wireless) introduce migliorie specifiche per le applicazioni wireless
  - nella maggior parte dei casi la mancanza di ACK a livello 2 provoca la ritrasmissione solo a livello 4, con grossi ritardi
  - per questo motivo è stato introdotto l'utilizzo di frame di ACK con meccanismo stop-and-wait
  - si è anche notato che CSMA può essere utilizzato per impedire ad una stazione di trasmettere un RTS durante la trasmissione di un altro RTS verso la stessa destinazione
  - infine si è modificato l'algoritmo di backoff in modo da applicarlo separatamente ai diversi flussi trasmissivi