Reti di Calcolatori

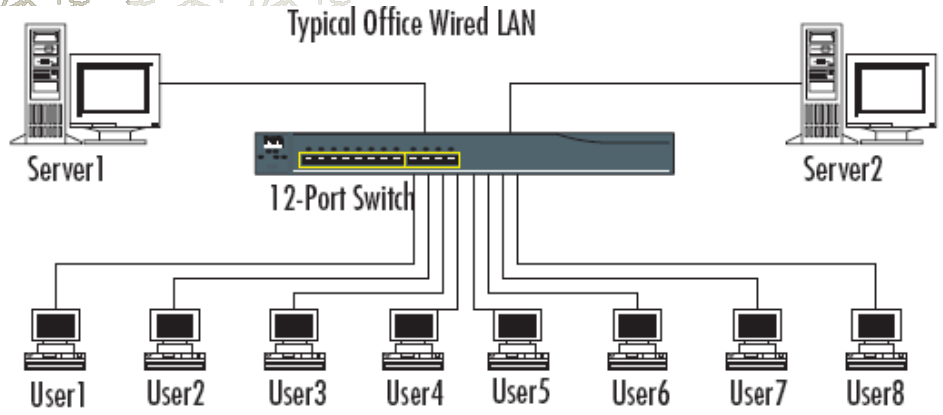
Protocolli data link layer per Wireless LAN

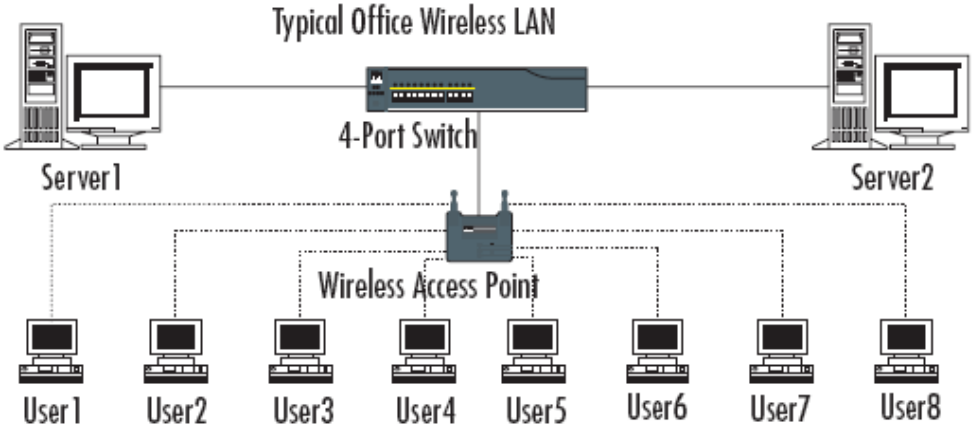
Reti wireless

- Motivazioni:
  - principalmente la diffusione di computer portatili, per offrire mobilita' senza perdita di connessione
  - un altro fattore e' l'estensibilita' della rete senza necessita' di cablaggio
- Bande trasmissive ISM
  - lo strato fisico e' realizzato con la trasmissione omnidirezionale in modulazione digitale di una portante
  - esistono bande di frequenza dedicate all'utilizzo senza necessita' 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, …

Vantaggi del *Wireless*

- Costi ridotti
- Meno problemi legati alle distanze (impiego di più AP o *wireless relaying*)
- Mobilità delle postazioni della rete





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 velocita' ad 1 o 2 Mbps nella banda a 2.4 GHz
  - IEEE 802.11b a velocita' 1, 2, 5.5 e 11 Mbps nella banda a 2.4 GHz
  - IEEE 802.11a con velocita' fino a 54 Mbps nella banda a 5 GHz
  - IEEE 802.11g fino a 54 Mbps nella banda a 2.4 GHz
  - IEEE 802.11n (WiFi 4) fino a 300 Mbps con tecnologia MIMO nella banda a 2.4 e 5 GHz
  - IEEE 802.11ac (Wi-Fi 5) fino a 1 Gbps con tecnologia MIMO nella banda a 5 GHz
  - IEEE 802.11ax (Wi-Fi 6) fino a 10 Gbps con tecnologia MIMO nella banda a 1, 5 e 7 GHz

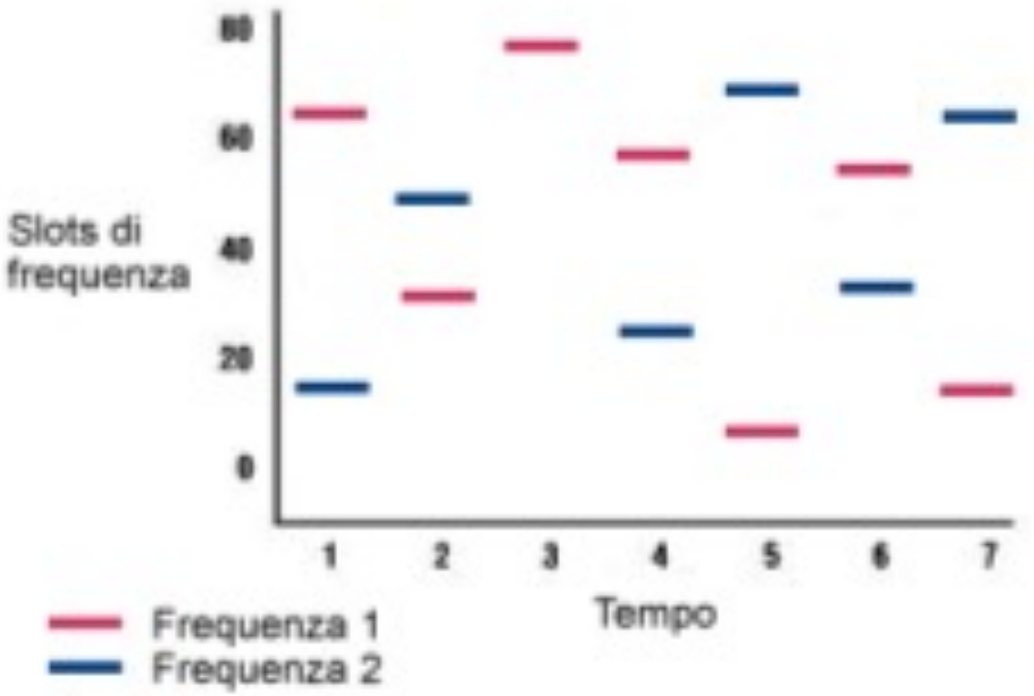
Tecniche a Divisione di Spettro

- Tecniche a divisione di spettro (SST):
  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

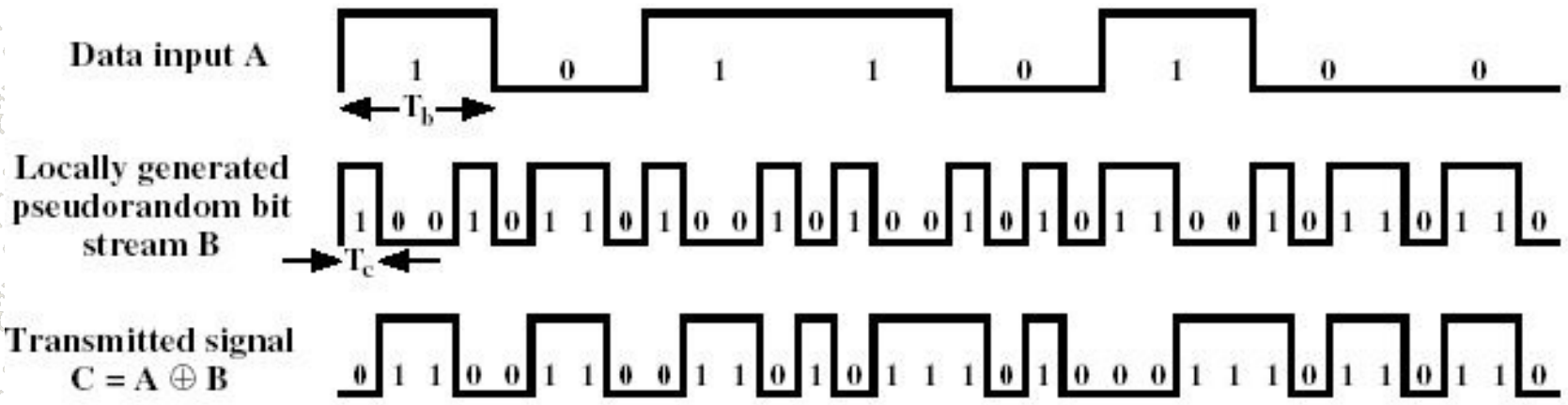
Strato fisico per le reti 802.11

- 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 e' 1 MHz
  - questa tecnica fornisce sicurezza (impossibile seguire la comunicazione senza conoscere la sequenza pseudocasuale) e solidita' contro il multipath fading (quando arriva il segnale riflesso la ricezione e' gia' spostata su un altro canale)
  - supporta standard ad 1 e 2 Mbps, con codifiche a 2 o 4 simboli con (G)FSK



Strato fisico per le reti 802.11 (cont.)

- 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



Spreading Spectrum

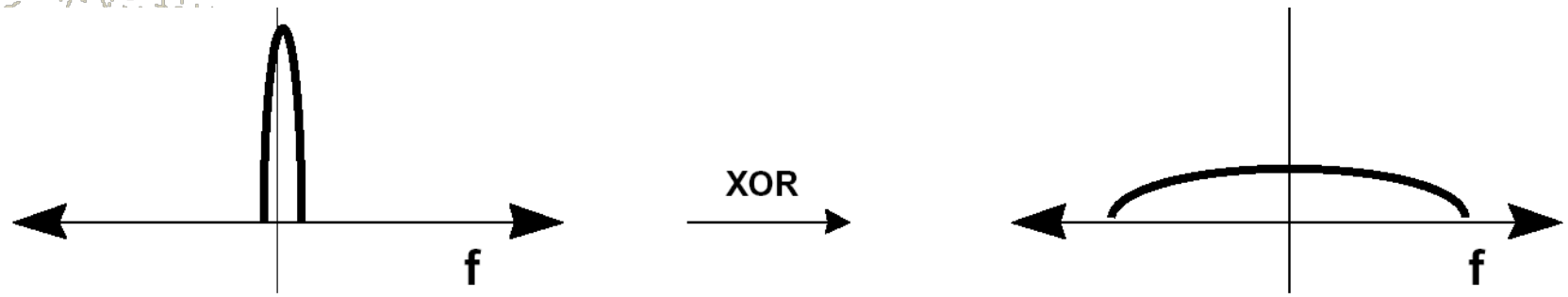


Figure 5a Effect of PN Sequence on Transmit Spectrum

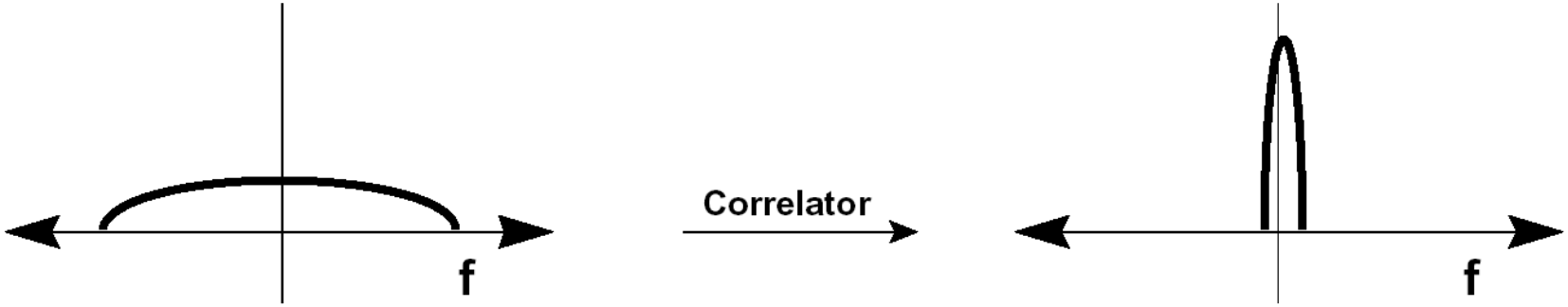


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

Strato fisico per le reti 802.11 (cont.)

- 802.11 DSSS (Direct Sequence Spread Spectrum) (cont.)
  - la banda disponibile e' 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 e' 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
    - poiche' l'ampiezza di banda del segnale inviato e' 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

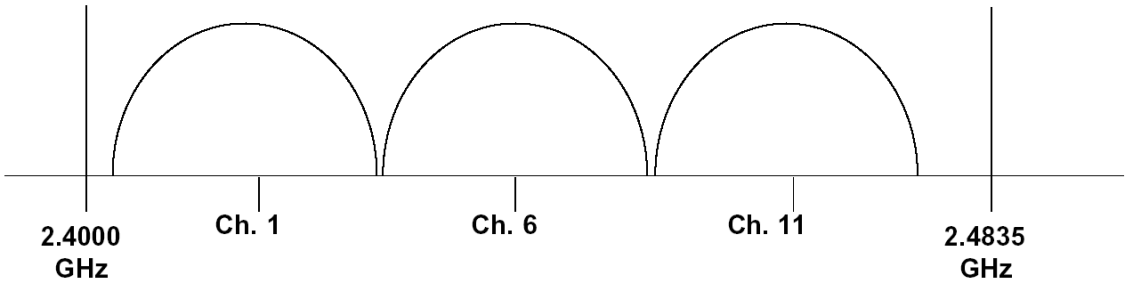


Figure 6 Three Non-Overlapping DSSS Channels in the ISM Band

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

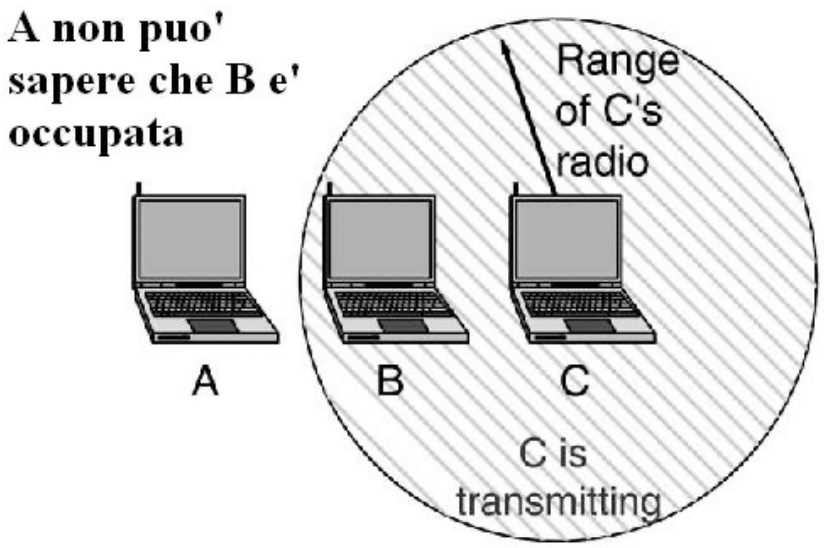
- DSSS:
  - Codifica ridondante ➔ più immune ai rumori
  - Maggiore spreco di banda (30 MHz per canale)
  - Possibilità di arrivare a 11 Mbps
- FHSS:
  - Più sicura
  - Molto limitata in banda (1 MHz)
  - Impossibile usarla nel WI-FI ad alti bit-rate

Dynamic Rate Shifting

- Dynamic Rate Shifting:
  - Data Rates adattati automaticamente alla natura del canale
  - 300 → 54 → 11 → 5.5 → 2 → 1 Mbps e viceversa
- Quando:
  - Luoghi rumorosi
  - Necessarie distanze maggiori

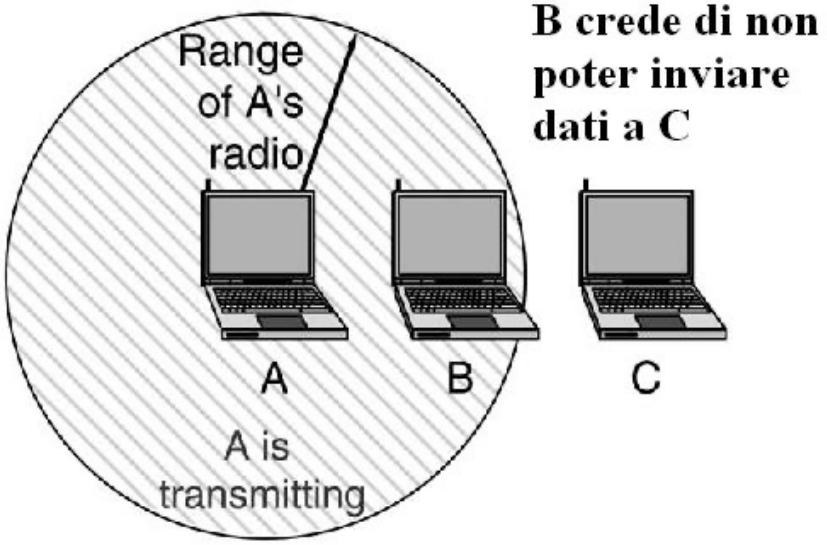
CSMA: stazione nascosta

- 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 potra' rilevare l'occupazione del canale in quanto e' fuori portata
- A iniziera' a trasmettere ed il suo segnale arrivera' a B interferendo con i dati che C sta' trasmettendo
- Questo e' detto problema della stazione nascosta



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 realta' il canale sarebbe disponibile (nella ipotesi che la destinazione della trasmissione di A sia fuori dalla portata di B) perche' in C i segnali non interferirebbero
- Questo e' il problema della stazione esposta



MACA

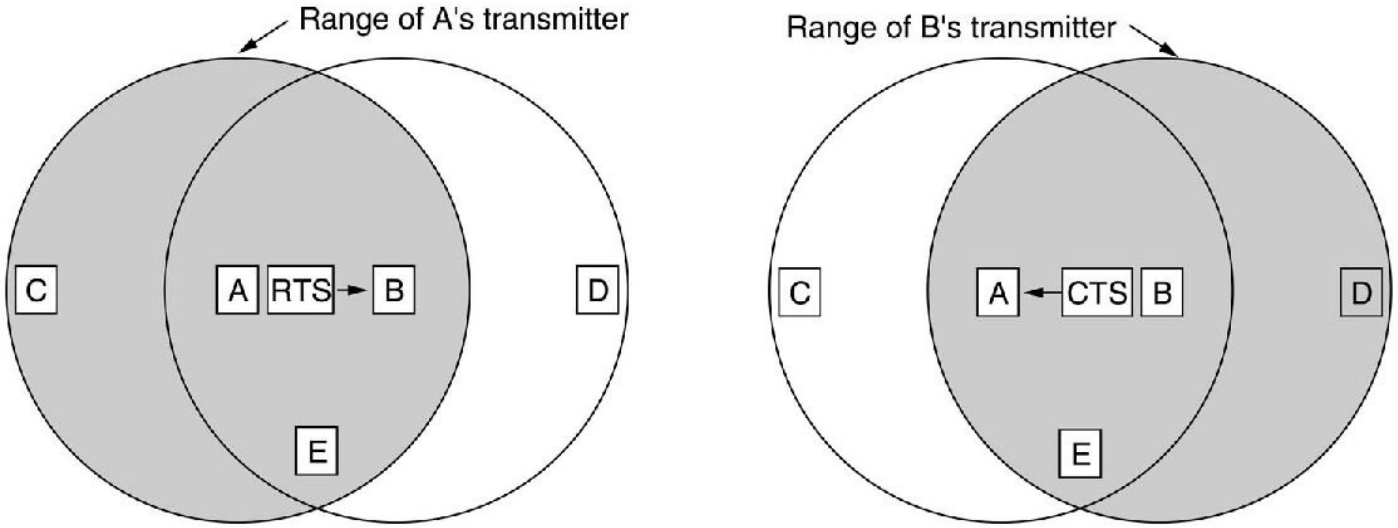
- L'inefficacia del protocollo CSMA deriva dal fatto che per le trasmissioni wireless quello che conta e' l'interferenza in prossimita' del ricevente, mentre l'analisi della portante che puo' fare una stazione e' solo in prossimita' di se stessa, cioe' del trasmittente
- Il protocollo MACA (Multiple 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 la lunghezza
  - 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

MACA (cont.)

- Tutte le stazioni che ricevono il frame RTS sanno che
  - B rispondera' con un CTS
  - in seguito A trasmettera' un frame di dati di lunghezza specificata in RTS
- Queste stazioni attenderanno senza trasmettere un tempo sufficiente alla trasmissione dei dati
- Le stazioni nascoste non vedono il frame RTS, ma vedono il frame CTS, quindi sanno che
  - trasmesso il CTS B dovra' ricevere il frame di dati, di lunghezza specificato nel CTS
- Queste stazioni attenderanno senza trasmettere per il tempo necessario alla trasmissione del frame di A (che loro non vedranno in quanto nascoste, ma sanno che ci sara')

MACA (cont.)

- 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

MACAW

- Il protocollo MACAW (MACA 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 e' stato introdotto l'utilizzo di frame di ACK con meccanismo stop-and-wait
  - si e' anche notato che CSMA puo' essere utilizzato per impedire ad una stazione di trasmettere un RTS durante la trasmissione di un altro RTS verso la stessa destinazione
  - infine si e' modificato l'algoritmo di backoff in modo da applicarlo separatamente ai diversi flussi trasmissivi

Protocollo del sottostrato MAC di 802.11

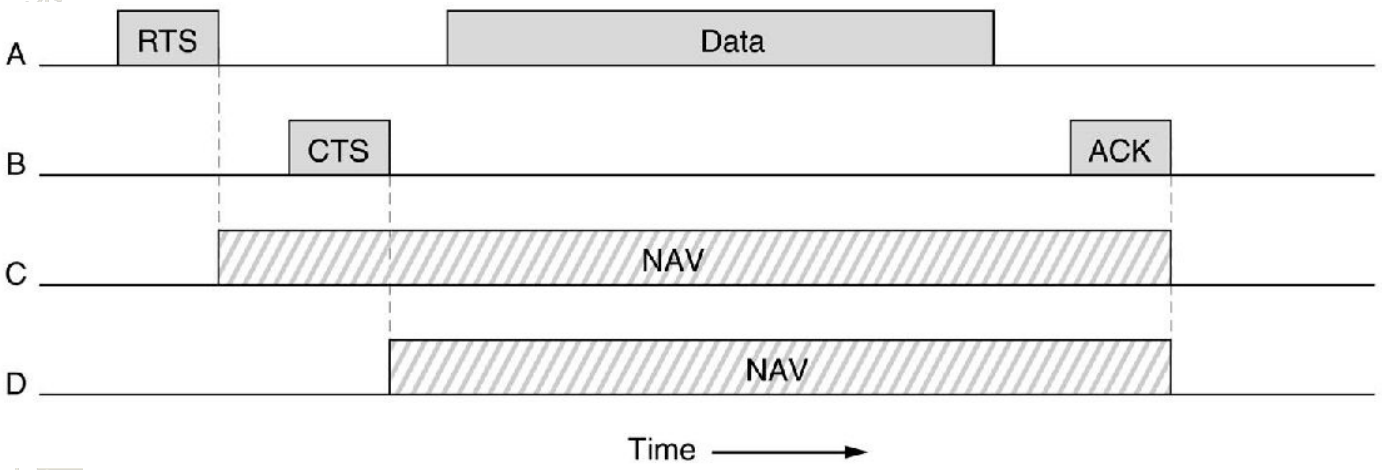
- 802.11 supporta due modalita' operative:
  - DCF (Distributed Coordination Function)
    - prevede la comunicazione tra stazioni senza un arbitraggio centralizzato
    - questa modalita' prevede la contesa del mezzo e la gestione delle collisioni
    - nota come rete ad hoc
  - PCF (Point Coordination Function)
    - prevede che ci sia una stazione base che coordina la trasmissione di tutti
    - in questa modalita' non ci sono collisioni perche' l'ordine delle trasmissioni e' determinato dalla stazione di controllo
- Tutte le schede wireless devono supportare la trasmissione DCF, mentre quella PCF e' opzionale (ma molto diffusa)

Protocollo in modalita' DCF

- In questa modalita' si utilizza il protocollo CSMA/CA (Carrier Sense Multiple Access Collision Avoidance) che opera in due modi
  - la stazione controlla se il canale e' libero (per quello che puo' vedere)
    - se e' libero trasmette (senza collision detection)
    - se e' occupato, aspetta che si liberi e trasmette
    - se si verifica una collisione (rilevata) utilizza il backoff esponenziale binario e ritenta

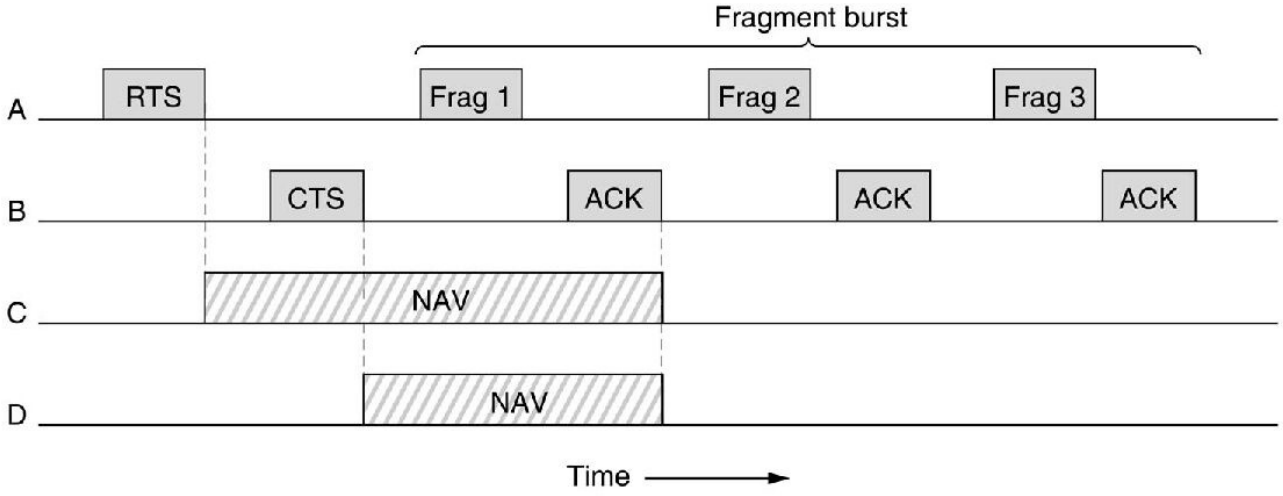
Protocollo in modalita' DCF (cont.)

- la seconda modalita' e' derivata da MACAW, con utilizzo di RTS, CTS ed ACK per ogni frame trasmesso
  - l'interfaccia della stazione che rileva un RTS o un CTS rivendica per se' un canale virtuale NAV (Network Allocation Vector) che impedisce alla stazione di trasmettere per tutto il tempo che deve durare la trasmissione in preparazione, fino all'ACK



Protocollo in modalita' DCF (cont.)

- Poiche' le reti wireless sono molto rumorose, il protocollo prevede la possibilita' di spezzare il frame in frammenti, ciascuno trasmesso e riscontrato individualmente
- i frammenti vengono inviati tutti di seguito, senza bisogno di invio di RTS
- le stazioni in ascolto utilizzaranno il NAV per attendere solo fino al primo riscontro: per evitare colisioni con gli altri frammenti si utilizza un meccanismo che vedremo piu' avanti



Protocollo in modalita' PCF

- Nella modalita' PCF la stazione base sonda le altre stazioni per vedere se hanno frame da trasmettere
- La trasmissione e' regolata ed autorizzata dalla stazione base e non avvengono collisioni
- Il protocollo specifica la modalita' di interrogazione, e prevede che le stazioni si registrino con la stazione base per entrare nel meccanismo delle interrogazioni
- La stazione base regola tutto il meccanismo della trasmissione, comprese le informazioni sulle sequenze di salto di frequenza (per FHSS) e le temporizzazioni
- Il protocollo, ottimizzato per i computer portatili, prevede anche che la stazione base possa imporre alla stazione mobile di mettersi in modalita' di sospensione, al fine di risparmiare batteria

Coesistenza PCF e DCF

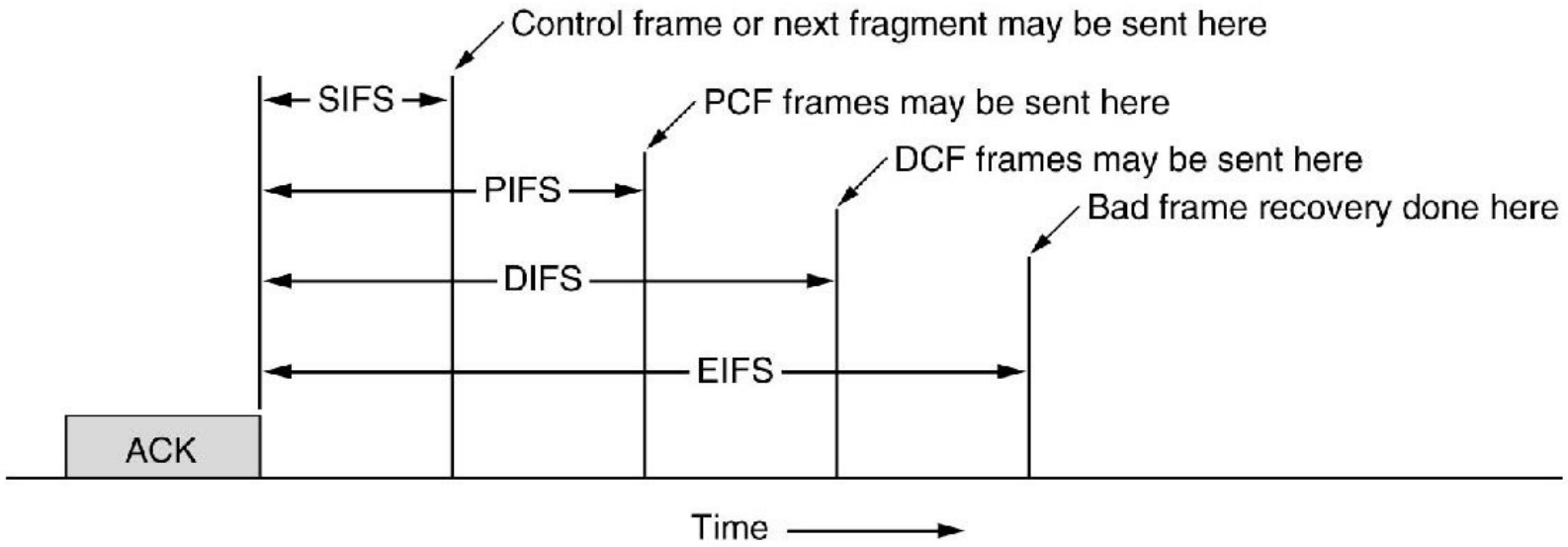
- 802.11 prevede un meccanismo di attesa a tempi differenziati che permette la coesistenza di PCF e DCF
  - terminata una trasmissione, inizia un periodo di tempo detto SIFS (Shotr IntreFrame Spacing), dopo il quale pou' trasmettere solo:
    - una stazione che ha ricevuto l'ACK di un frammento ed invia un altro frammento (in questo modo la stazione potra' trasmettere tutti i frammenti senza perdere il controllo del canale)
    - una stazione che ha ricevuto un RTS ed invia un CTS (gli altri aspettano)
    - una stazione che ha ricevuto una interrogazione (in modalita' PCF) e puo' rispondere (solo lei)
  - in ogni caso c'e' sempre al massimo una stazione che puo' trasmettere dopo un intervallo SIFS, quindi non ci possono essere collisioni
  - l'intervallo SIFS permette alle stazioni con trasmissioni in corso (dopo un frammento, dopo un RTS, dopo una interrogazione) di portare a termine la trasmissione

Coesistenza PCF e DCF (cont.)

- il secondo intervallo temporale in ordine di lunghezza e' detto PIFS (PCF IFS); se nessuno ha trasmesso tra lo scadere del SIFS e lo scadere del PIFS, sono autorizzate le trasmissioni che la stazione base utilizza in modalita' PCF per interrogare le stazioni
  - in questo modo la stazione base ha la priorita' su tutto il traffico "non in corso"
  - esiste un meccanismo per evitare che una stazione base allochi per sempre il canale con trasmissioni di interrogazione, lasciando spazio alle eventuali trasmissioni DFS
- il terzo intervallo di tempo e' detto DIFS (DCF IFS): se nessuno ha trasmesso frame PCF entro la scadenza del DIFS, iniziano le regole di contesa relative alle trasmissioni in modalita' DCF
  - questo e' il momento per poter trasmettere un frame RTS

Coesistenza PCF e DCF (cont.)

– L'ultimo intervallo (EIFS: Extended IFS) e' utilizzato (alla priorita' piu' bassa) dalle stazioni che hanno ricevuto un frame danneggiato per annunciare il fatto



Collisioni su wireless: CA

- CD non utilizzabile in WLAN:
  - ***Non si è sicuri che ogni WT ascolti tutte le altre WT della BSS***

- Algoritmo di prevenzione:
  - CA – Collision Avoidance
  - 4 – Way Handshake

CA Collision Avoidance 1

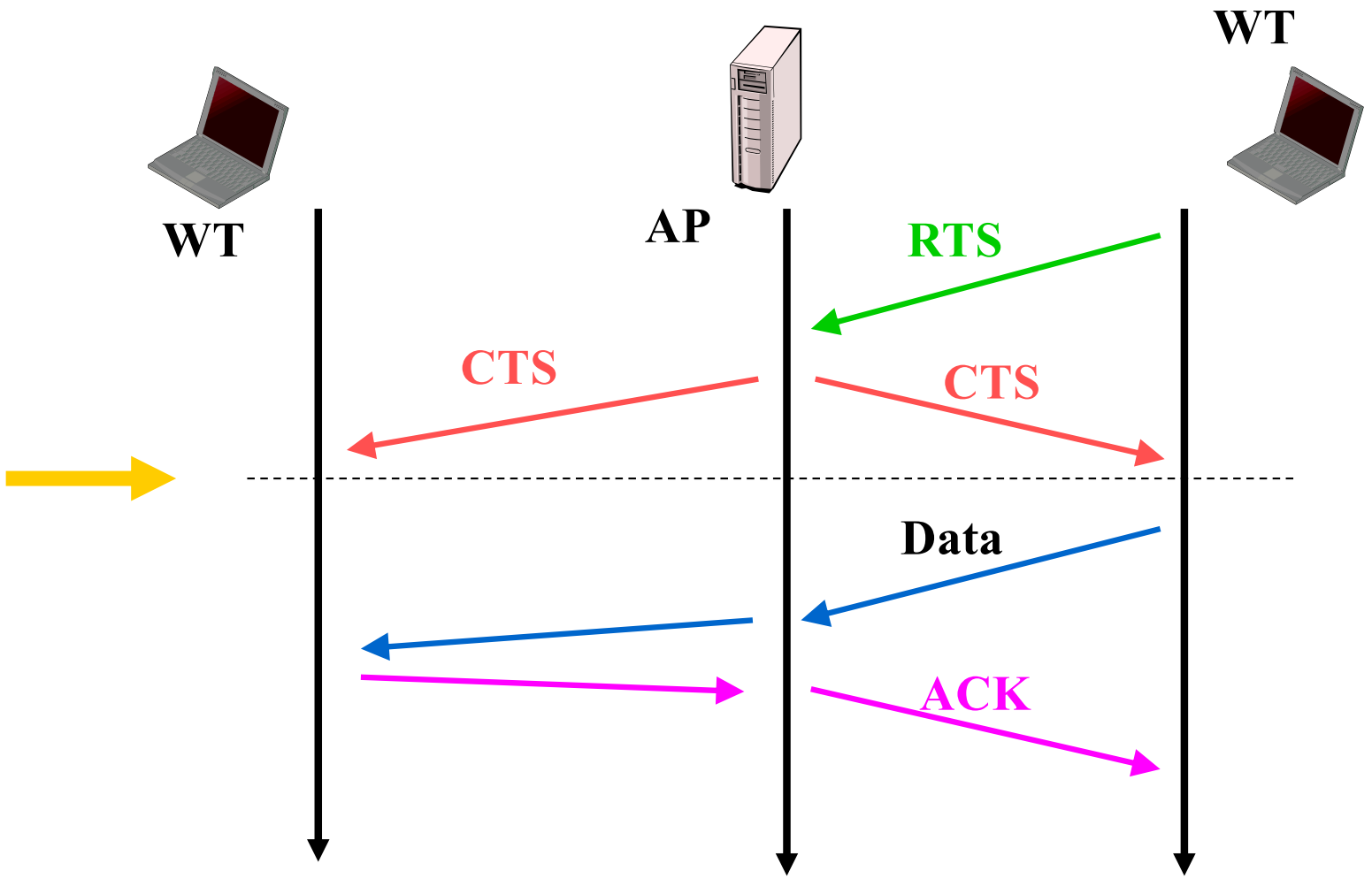
- Tx ascolta il canale
  - Carrier Sense (CS)
- Se Tx trova il mezzo libero per un tempo DIFS (Distribuited Inter Frame Space) trasmette
- Tx trasmette un breve messaggio di controllo RTS (Request to Send)
  - Lunghezza del MSG
  - Mittente e Destinatario
- L'AP riceve l' RTS e risponde, dopo un tempo SIFS, con un breve messaggio CTS (Clear to Send)

CA Collision Avoidance 2

- Tutte i WT che “vedono” i messaggi RTS e/o CTS settano il NAV-Network Allocation Vector alla durata della trasmissione
  - Virtual Carrier Sense
- Nota:
  - CTS è visto sicuramente da tutte le WT della BSS
- Tx riceve il CTS ed inizia la sua Tx
- Rx riceve il msg e controlla il CRC:
  se OK risponde con un ACK
- Se Tx non riceve ACK entro un tempo T1, ritrasmette il msg.

4-Way Handshake

Da qui non sono più possibili collisioni



CA: Caratteristiche

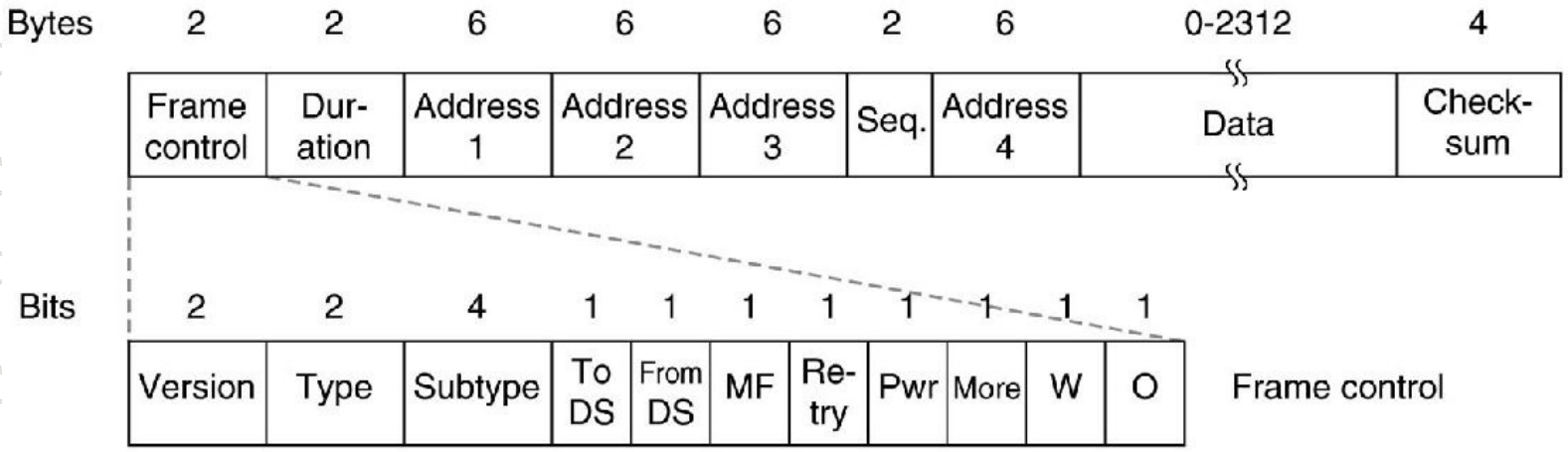
- Brevi messaggi (RTS e CTS):
  a) Minor P() di collisioni
  b) Minor costo di una collisione
- Ogni WT sa che il canale è occupato
  - RTS è visto dai WT vicini a Tx
  - CTS è visto da tutti (mandato dall'AP)
- Se il pacchetto dati è piccolo non conviene usare RTS/CTS

Frame in 802.11

- Esistono tre tipi di frame
  - dati: dedicati al trasferimento dei dati dei protocolli superiori
  - gestione: dedicati alle funzioni di gestione della cella, quali associazione, autenticazione, interrogazione
  - controllo: sono i frame ACK, RTS, CTS

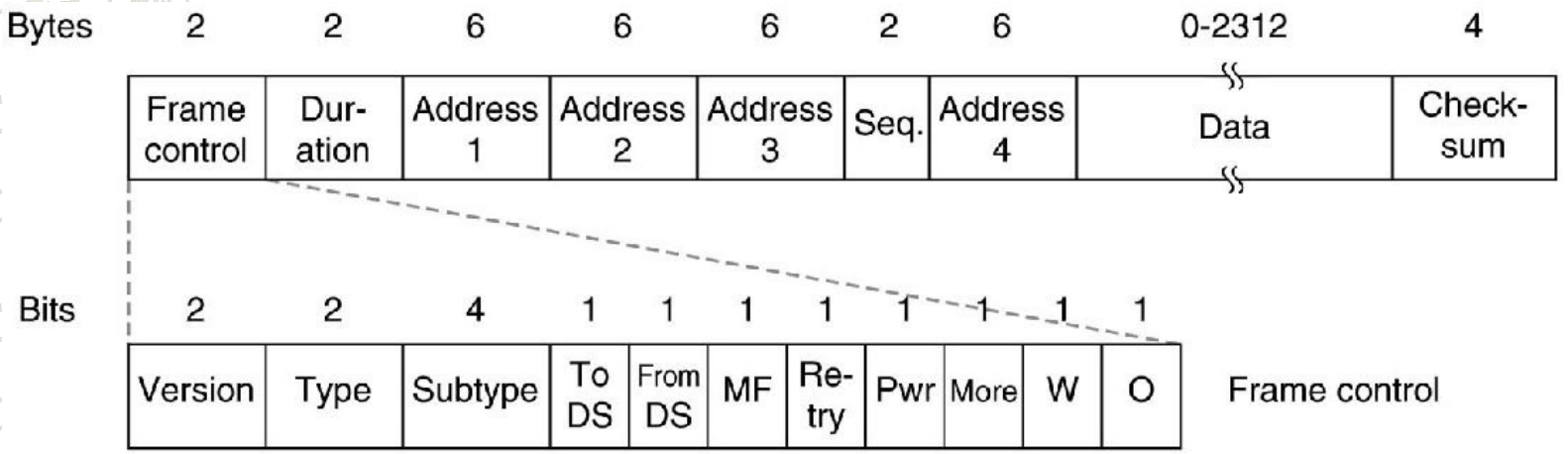
Frame di dati

- La struttura del frame di dati e' costituita da divesri campi
  - frame control: definisce la versione del protocollo, il tipo di frame, se il frame proviene o e' diretto alla rete di distribuzione (Ethernet, ad esempio), se sara' seguito da altri frammenti, se e' una ritrasmissione, se e' stata utilizzata crittazione
  - durata: specifica per quanto tempo il frame occupera' il canale



Frame di dati (cont.)

- quattro indirizzi, che definiscono
  - destinazione del frame (per il recapito)
  - sorgente del frame (usato per l'ack)
  - stazione base di partenza del frame
  - stazione base di arrivo del frame
- queste distinzioni servono, ad esempio, per distinguere il fatto che il frame 802.11 e' trasmesso da A verso l'access point B, ma la destinazione e' la stazione C che si trova sulla rete cablata oltre l'access point
- Il campo sequenza numera i frammenti
- Infine i dati (fino a 2312 byte) ed il checksum con CRC a 32 bit



Altri frame

- I frame di gestione hanno un formato simile, ma solo due campi address in quanto il loro traffico e' confinato entro la cella
- I frame di controllo non hanno campo dati ne' sequenza; l'informazione del controllo inviato (RTS, CTS, ACK) e' contenunto nel campo subtype dei byte di controllo di frame

Control Frames

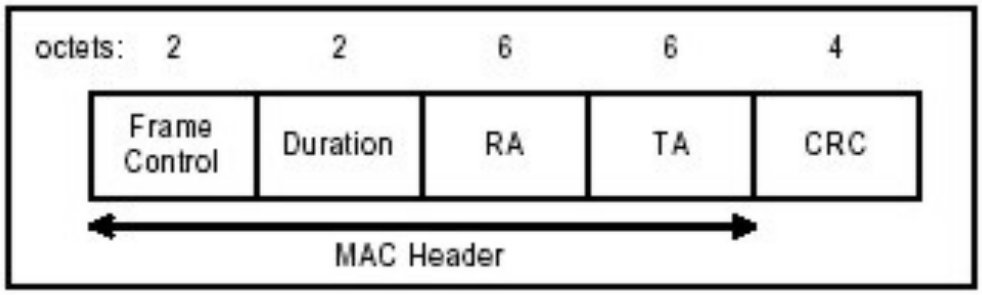
RTS:

DA – destinatario

TA – mittente

Duration – in µs

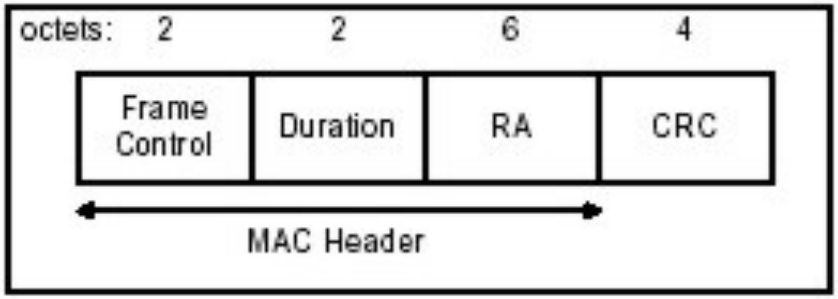
data frame + 1 CTS + 1 ACK + 3 SIFS



CTS:

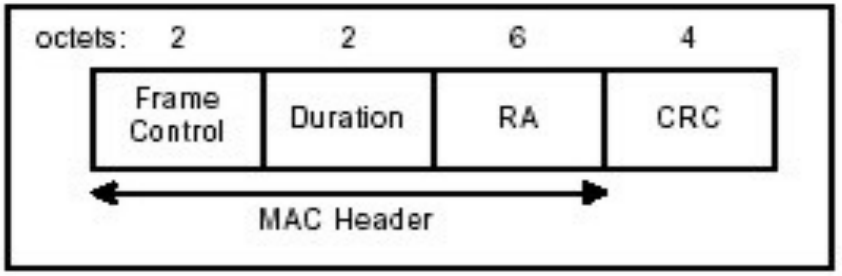
RA – è il TA del precedente RTS

Duration – duration del RTS – CTS – 1 SIFS



ACK:

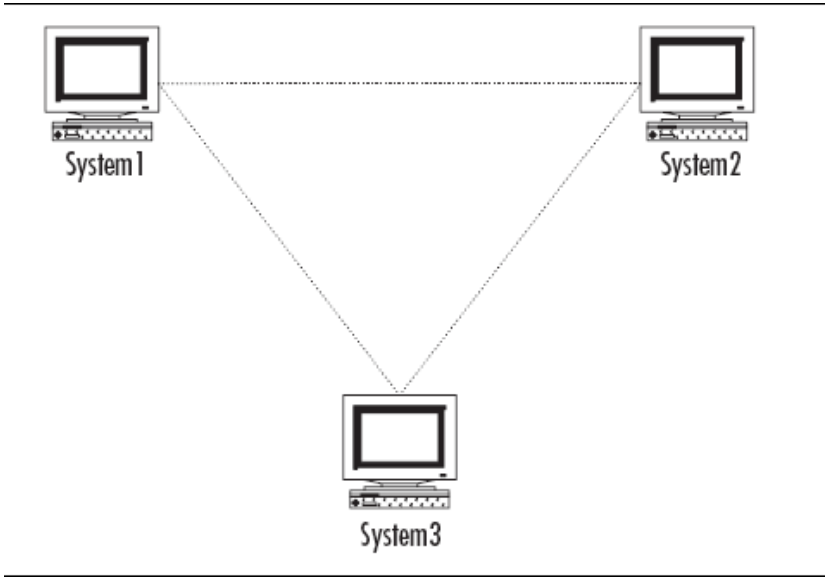
RA – è l'indirizzo A2 del precedente frame



Modalità operative delle WLAN

Modalità *ad hoc* (*o infrastructureless*)

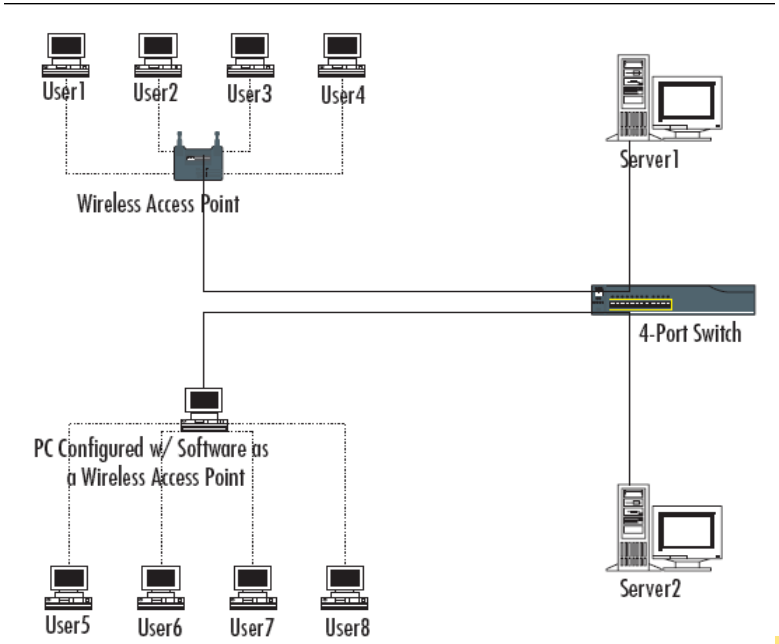
I computer possono comunicare direttamente l'uno con l'altro solo grazie alla propria interfaccia di rete *wireless*



Modalità operative delle WLAN

Modalità AP (o *infrastructured*)

La comunicazione in rete avviene grazie ad ***Access Point*** (**AP**) hardware o software che sono parte integrante della rete WLAN, e per mezzo delle interfacce di rete *wireless* installate e configurate su ciascuna postazione in modo da comunicare con specifici AP per collegarsi a specifiche WLAN



Modalità operative delle WLAN: considerazioni

Modalità ad hoc

- Semplice da configurare
- È semplice aggiungere nuove postazioni
- Non è possibile alcuna gestione centralizzata
- Ideale per piccole reti

Modalità AP

- Più complessa da configurare
- Richiede AP hardware o software nel progetto della rete
- È possibile la gestione centralizzata (a vantaggio anche della sicurezza)
- Ideale per reti più grandi

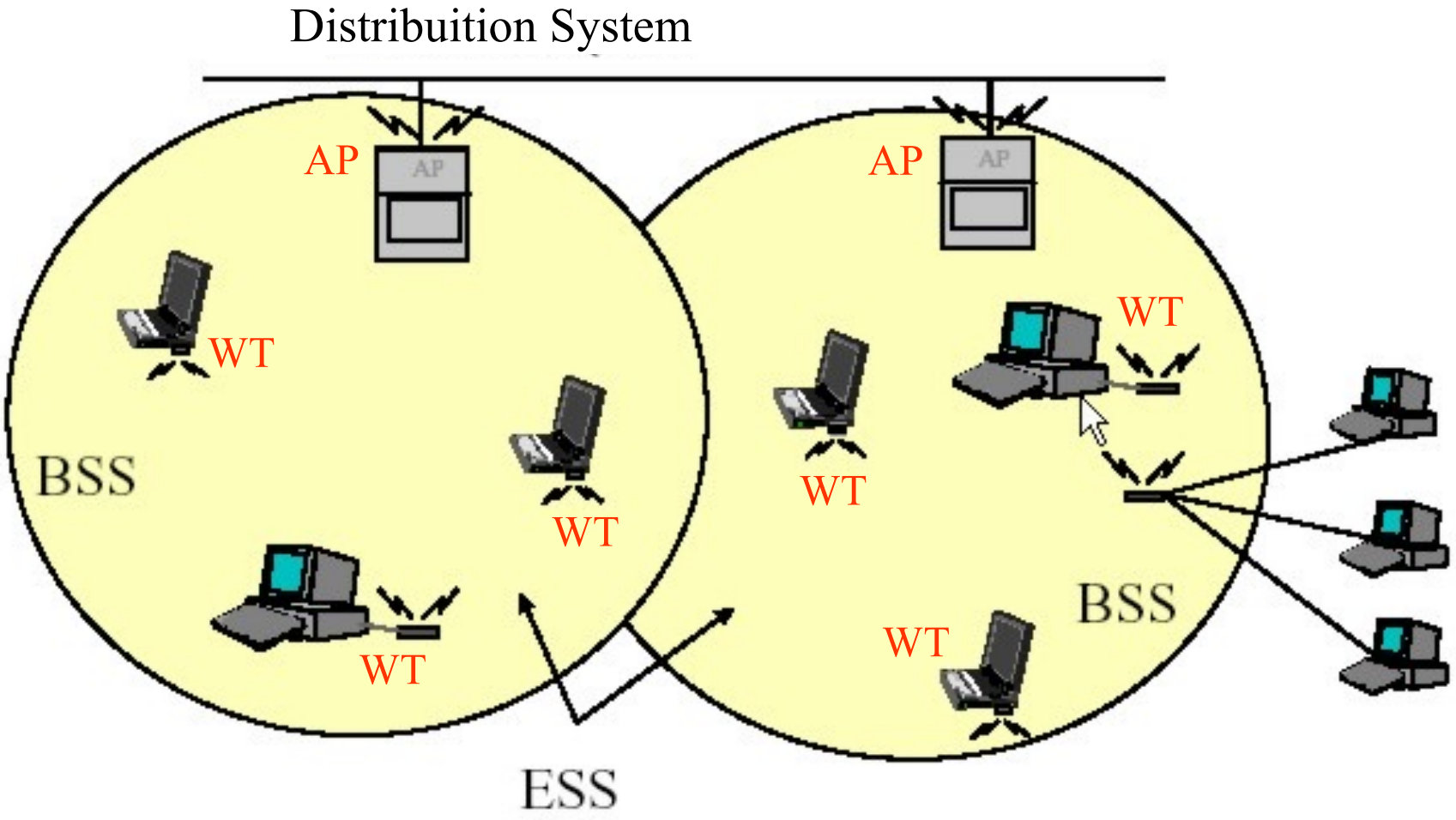
Access point

- Le reti wireless sono connesse alla rete cablata (una qualche rete 802.x) tramite una stazione che ha funzioni di bridge (converte il protocollo tra 802.11 ed il protocollo della rete cablata)
- Questa stazione e' detta access point
- L'access point ha anche funzioni di stazione di controllo della cella per le trasmissioni in modalita' PCF
- E' possibile realizzare topologie di estensione della rete tramite una catena di access point che rimpallano la trasmissione wireless di un frame fino a raggiungere la rete cablata

802.11 - Architettura

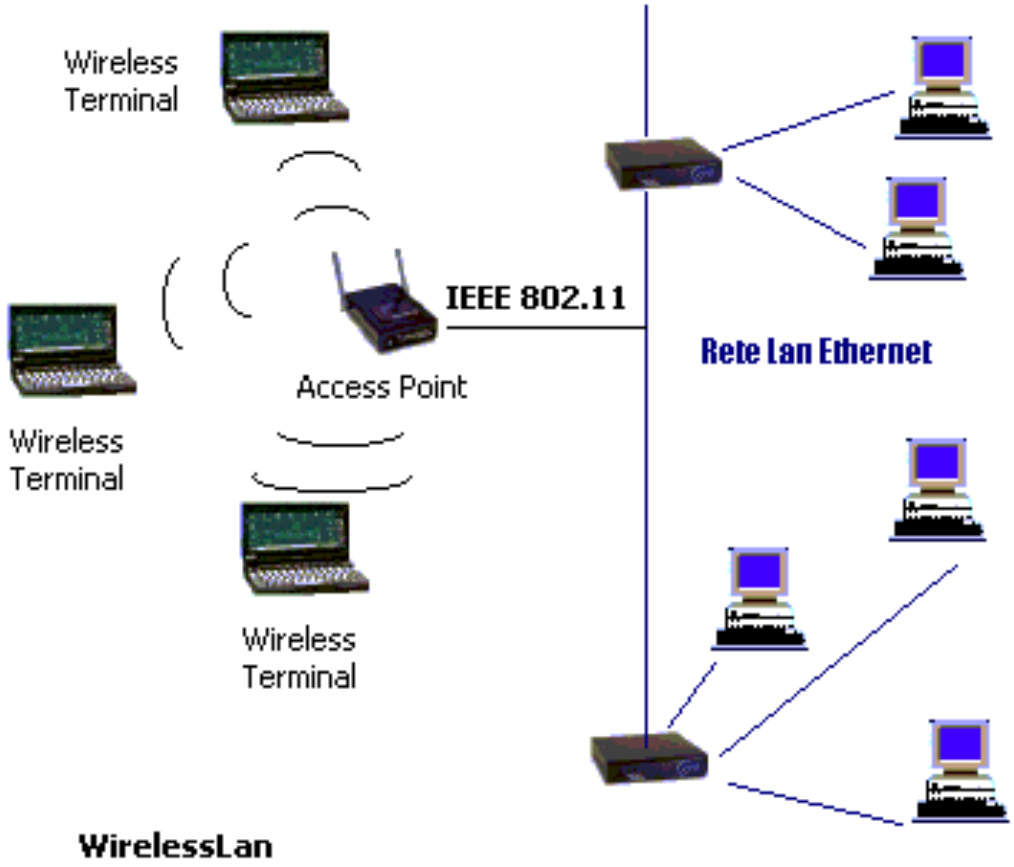
- Il sistema è suddiviso in celle (BSS – Basic Service Set)
- Ogni cella ha il suo Access Point (AP)
- Ogni WT (Wireless Terminal) è dentro una cella e agganciato ad un AP
- Gli AP sono collegati ad un Distribuition System (DS)
- L'insieme delle celle può essere visto come una rete (ESS – Extended Service Set)

802.11 - Architettura



802.11 - Architettura

- Una WLAN può essere interfacciata con una normale lan cablata



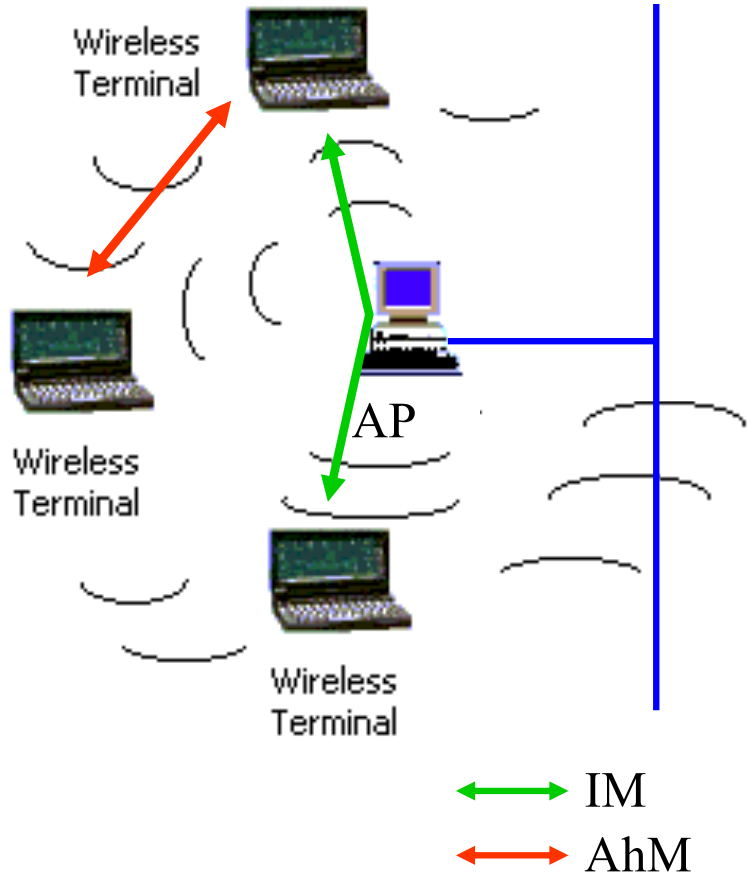
802.11 - Architettura

- AP
  - Gestiscono la cella (BSS)
  - Interfacciano WLAN con altre LAN (bridge)
  - Implementati Hw e Sw
  - Esistono AP-Router (bridging a livello di rete)
    - Es.
      router wifi-ADSL
- WT - Terminali mobili
  - Notebook
  - Cellulari
  - ecc..

802.11 - Architettura

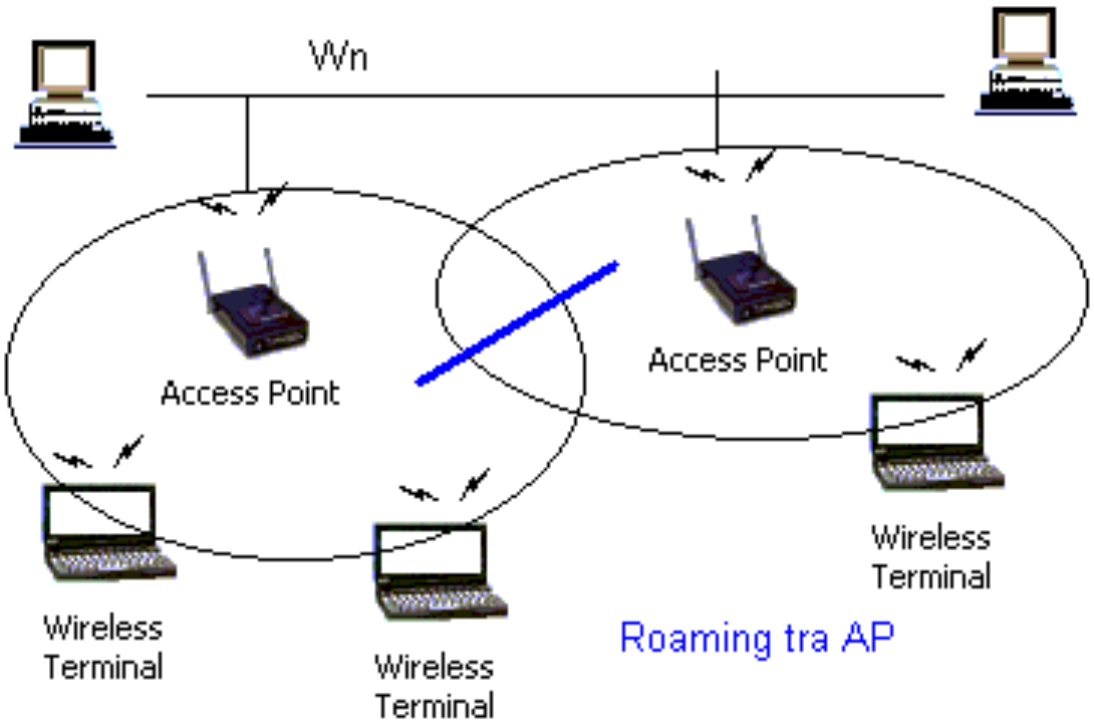
- **Mode Ad-hoc**
  comunicazione punto a punto tra due WT senza passare da un AP
  (IBSS, Indipendent-BSS)

- **Infrastructure Mode**
  i terminali comunicano tra loro tramite un AP (BSS-ESS)



802.11 - Roaming

- Un WT può passare da un AP ad un altro in modo del tutto trasparente (roaming)
- Ogni AP periodicamente invia un ***frame beacon***, per notificare ai client sia la propria presenza, sia informazioni sulla configurazione e sulla sicurezza.
- I client periodicamente inviano in *broadcast* e su tutti i canali, una ***probe-request frame*** attendendosi una ***probe-respone frame*** dagli AP vicini, con lo scopo di individuare potenziali destinatari di *roaming*, per compilarsi opportune liste da consultare per il roaming.



Autenticazione 802.1x

L'autenticazione 802.1x è una soluzione di livello 2 per gestire l'accesso alla rete, basato sul controllo a livello di porta usando le ***Port Access Entity* (*PAE*)**. Sostanzialmente definisce un *framework* per l'autenticazione che utilizza protocolli esistenti, come **EAP** e **RADIUS**, trasformando i messaggi di diversi tipi di autenticazione in appropriati *frame*.

I protocolli di autenticazione che possono essere impiegati sono essenzialmente di due tipi:

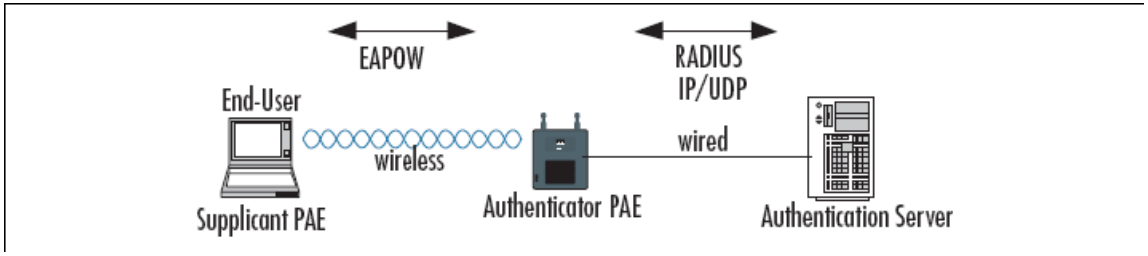
- ***End to End***: quando sono coinvolte due macchine collegate virtualmente, ma non fisicamente comunicanti (ad esempio **EAP**).
- ***Point to Point***: quando sono coinvolte due macchine direttamente connesse (ad esempio EAPoL, ma anche, astrattamente **RADIUS**).

Nel *framework* 802.1x vengono definiti 3 attori del processo di autenticazione:

***Supplicant* (*PAE*)** chi desidera accedere ai servizi della rete fornendo le credenziali

***Authenticator* (*PAE*)** chi applica le *security policies* prima di concedere l'accesso alla rete

Authentication Server chi verifica le credenziali di accesso alla rete



Extensible Authentication Protocol (EAP)

EAP è un protocollo di trasporto di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei metodi di autenticazione specifici, si hanno così:

- EAP-MD5
- LEAP
- PEAP
- EAP-MSCHAPv2
- EAP-TLS
- EAP-TTLS
- . . .

Remote Authentication Dial-In User Service (RADIUS)

- RADIUS è un protocollo **AAA** (***Authentication***, ***Authorization*** and ***Accounting***) che si basa su un modello *client/server*.
- Anche RADIUS è un protocollo di trasporto di meccanismi di autenticazione, ma può veicolare anche altri contenuti (*attributi RADIUS*) che servono a scopi specifici.

- Anche se lo standard 802.1x non specifica quale tipo di server di autenticazione deve essere implementato, RADIUS rappresenta lo standard *de facto* in 802.1x, rendendo sicuro il canale tra *Authentication Server* e *Authenticator*.

Autenticazione 802.1x: le fasi

Fase 1

•Il *Supplicant,* contenuto nel terminale WN, richiede all'*Authenticator*, contenuto nell'AP, l'accesso alle risorse della LAN. L'*Authenticator* richiede al terminale WN le credenziali d'accesso. In questa fase la connessione alla wired LAN tra *Supplicant* ed *Authenticator* avviene tramite la ***uncontrolled port*** che permette **solo traffico EAP**

Fase 2

•L'*Authenticator* inoltra le credenziali all'*Authentication Server* attraverso la ***uncontrolled port*** usando il protocollo **RADIUS**.

Fase 3

•Dopo l'avvenuta autenticazione, l'*Authentication Server* comunica all'*Authenticator* di spostare il terminale WN sulla ***controlled port*** permettendo l'accesso alle risorse della LAN.