Università di Genova
Facoltà di Ingegneria

Telematica

5. *Wireless* (Radiomobile e WLAN)

Prof. Raffaele Bolla

Telematica

Wireless (Radiomobile e WLAN)

- **Introduzione**
- **Radiomobile Cellulare**
- **IEEE 802.11**
- ***Bluethoot***
- ***HomeRF***

Introduzione

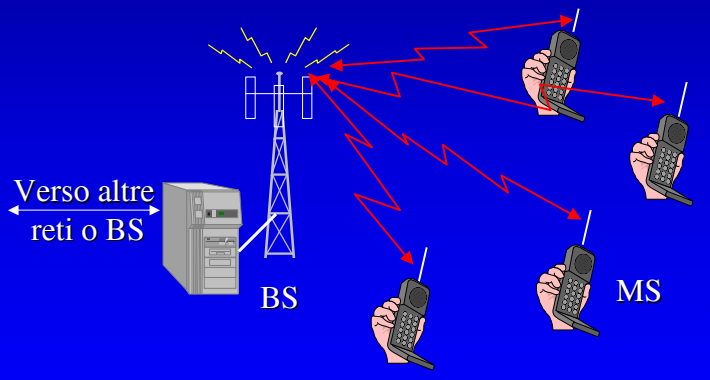
Wireless

- Le **reti *wireless*** sono reti in cui i terminali accedono alla rete tramite canali "senza fili" (radio in genere).
- Le **reti radiomobili** sono reti *wireless* dove i terminali utenti possono spostarsi sul territorio senza perdere la connettività con la rete.
- Le **reti cellulari** sono reti radiomobili la cui copertura geografica è ottenuta con una tassellatura di aree adiacenti e/o sovrapposte dette celle.
- Le ***Wireless* LAN** (WLAN) sono reti *wireless* che forniscono coperture e servizi tipici di una LAN.

3

Punto di accesso fisso

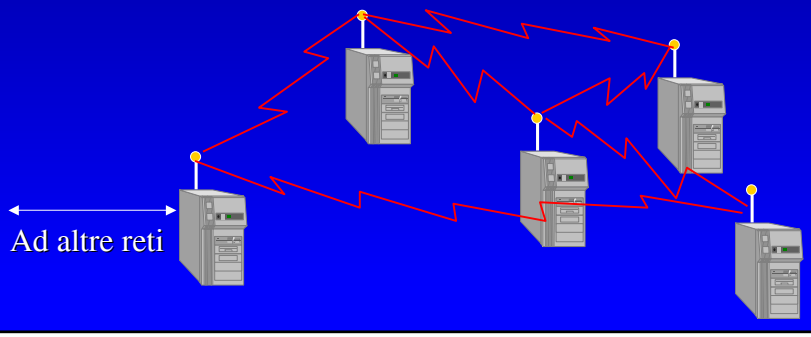
- I terminali mobili (*Mobile Station*, MS) non comunicano mai direttamente ma sempre tramite un stazione fissa (*Base station*, BS) di riferimento.



4

Autoconfiguranti

- I terminali (sia mobili che non) comunicano direttamente fra loro creando una rete autoconfigurante (*ad hoc network*). Uno o più terminali fissi fanno da "*gateway*" verso altre reti.
- Se i vari terminali possono funzionare anche da nodi di transito l'architettura viene detta di tipo *peer-to-peer*.



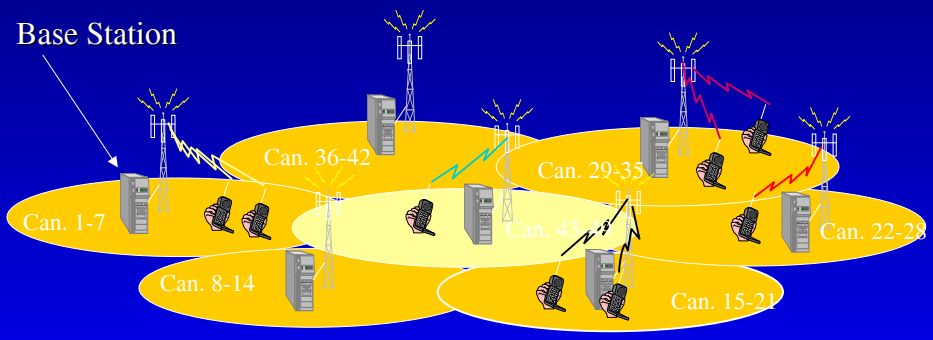
5

Reti cellulari

- La velocità di trasmissione nelle reti *wireless* è limitata dalla porzione di spettro disponibile.
- Per servire un numero elevato di utenti, come nel caso della telefonia mobile, una soluzione consiste il territorio in aree dette celle, ed assegnare ad ogni cella uno spazio dello spettro (canali in frequenza).
- Questa suddivisione spaziale permette un riuso delle frequenze (riutilizzare gli stessi canali in celle diverse), che deve essere fatto in modo da minimizzare l'interferenza tra celle vicine; il risultato è un significativo aumento della capacità totale disponibile.
- La struttura delle reti cellulari prevede un punto di accesso fisso (Base Station) per ogni cella ed ogni cellulare utilizza la BS della cella in cui al momento risiede.

6

Reti Cellulari



7

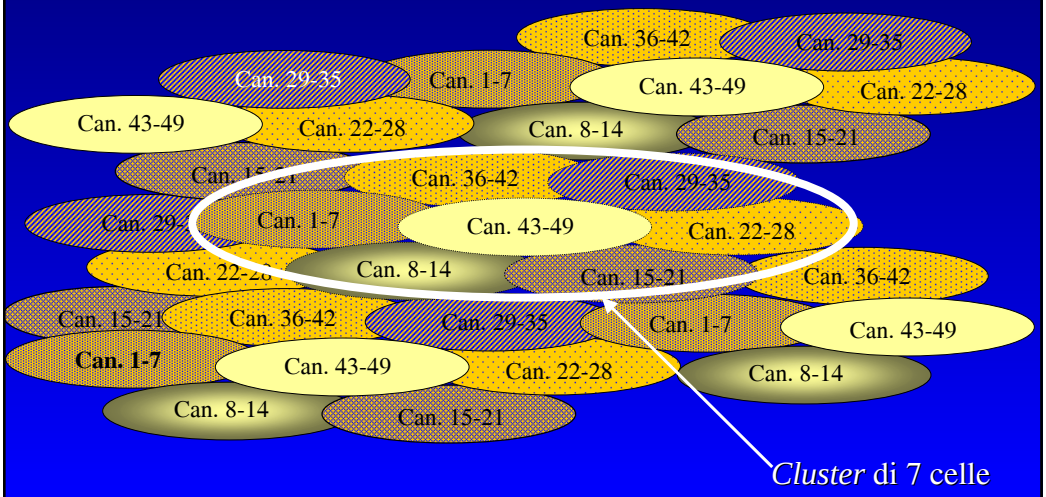
Reti Cellulari

- L'efficienza nelle reti cellulari viene misurata essenzialmente in base al riuso dei canali radio disponibili in celle adiacenti.
- Se si potessero riusare tutti i canali in ciascuna cella si avrebbe efficienza unitaria.
- Le celle vengono organizzate in "*cluster*" di N celle: all'interno di un *cluster*, ciascuna cella utilizza un sottoinsieme unico di canali.
- La dimensione del *cluster* è una misura dell'efficienza del sistema: più sono grossi i *cluster* (cioè più celle li compongono) meno efficiente è il sistema.
  - Sistemi analogici con accesso FDMA (AMPS, TACS, NMT): *cluster* di 19 o 21 celle
  - Sistemi numerici con accesso di tipo TDMA o misto FDMA/TDMA (GSM, D-AMPS, JCD): *cluster* di 7 o 9 celle
  - Sistemi numerici con accesso CDMA (IS-95): *cluster* di 1 cella (almeno in linea di principio)

8

Cluster

49 Canali totali disponibili



9

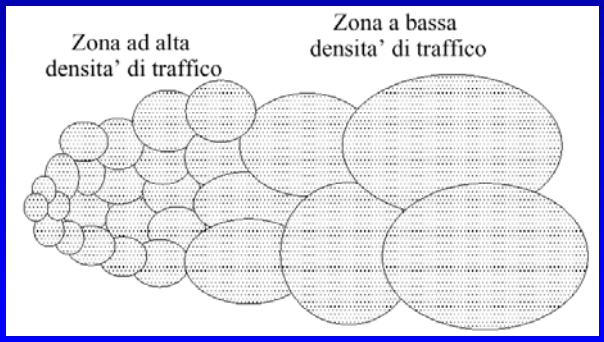
Rete Cellulare

- Consideriamo una superficie da servire di 400.000 km² (corrispondente circa alla superficie dell'Italia comprese le acque territoriali), ed indichiamo con R il raggio della cella, A la sua area, N il numero totale delle celle.
- Supponiamo di avere a disposizione 490 canali (ogni canale corrisponde allo spazio in freq. necessario ad una conversazione telefonica) e *cluster* di 7 celle (quindi 70 canali per cella):
  - Con un'unica cella potremmo avere al massimo 490 conversazioni contemporanee
  - Con R = 60 Km avremmo per ogni cella (supponiamo celle uguali) $A = 60^2 * \pi \approx 11.300$ Km², quindi N = 400.000/11.000 ≈ 36 quindi un totale di 36*70 = 2520 conversazioni contemporanee.
  - Con R=10 Km avremmo A ≈ 314 Km², N = 400.000/314 ≈ 1274, e quindi N= 1274*70 = 89.180 conversazioni contemporanee.
  - Con R=1 Km avremmo A ≈ 3,14 Km², N = 400.000/3,14 ≈ 127324, e quindi N= 127324 *70 = 8.912.680 conversazioni contemporanee.

10

Rete cellulare

- Ovviamente il complessivo aumento di capacità con celle di egual superfice viene realmente sfruttato solo se l'utenza risulta equamente distribuita sul territorio.
- Se per assurdo, tutti gli utenti si concentrassero in una cella, in realtà negli esempi precedenti il numero massimo di conversazioni si ridurrebbe comunque a 70.
- Per mantenere alta l'efficienza le celle vengono realizzate di dimensioni più piccole in corrispondenza di aree con elevata concentrazione di utenza (centri abitati, strade).



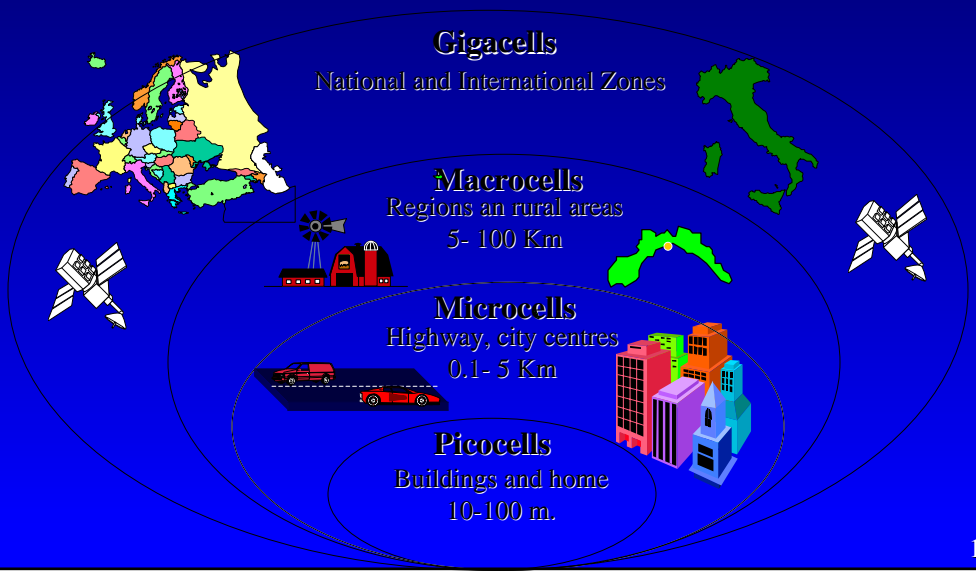
11

Rete cellulare

- Le celle di copertura non sono necessariamente cerchi (o esagoni) regolari tutte delle stesse dimensioni
- L'effettiva dimensione della cella è determinata dalla potenza degli apparati, dai ritardi di propagazione e dalla densità di traffico.
- E' possibile usare antenne direzionali per avere celle di forma e dimensione particolare
- E' possibile avere celle di dimensione (e forma) diversa per esigenze diverse
- E' possibile avere celle stratificate (celle a ombrello)

12

Rete cellulare

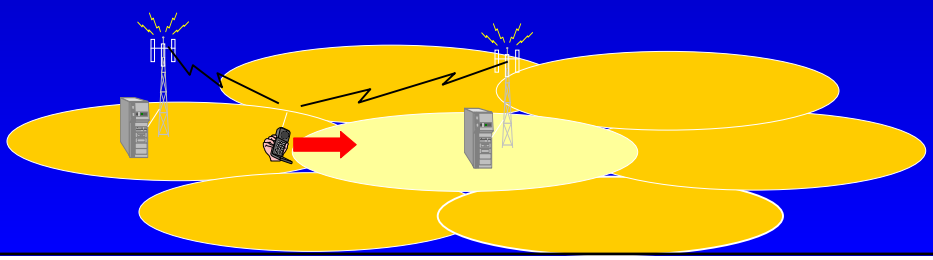


13

Rete Cellulare

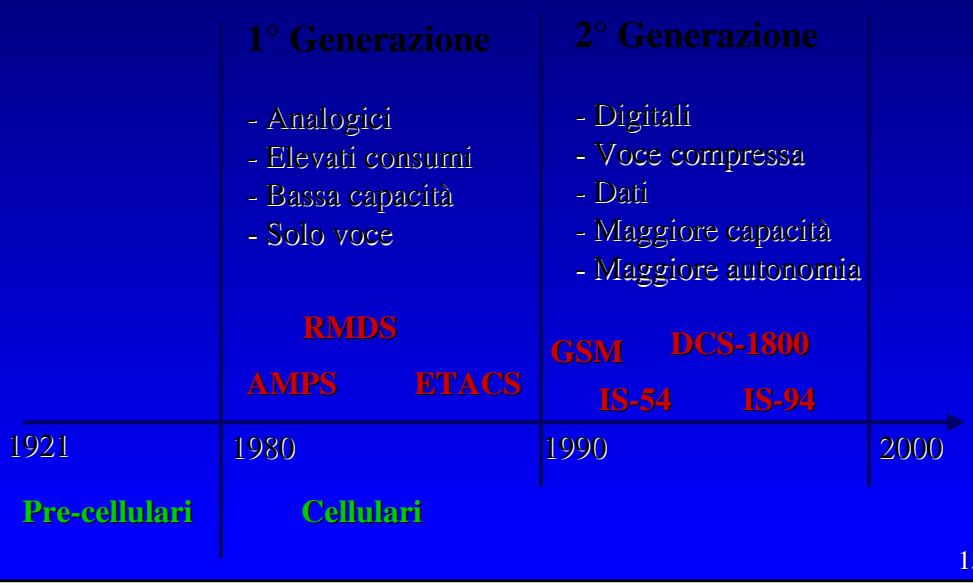
Handoff (o *Handover*)

- E' la procedura che consente il trasferimento di una chiamata da una cella alla successiva, mentre il terminale mobile si sposta all'interno della rete.
- Di fatto e l'elemento distintivo tra le reti cellulari ed ogni altro tipo di rete di TLC
- E' una operazione complessa che pone alla rete notevoli requisiti in termini di architettura di rete, di protocolli e di segnalazione per la gestione delle procedure connesse agli handover



14

Evoluzione delle reti radiomobili



15

Evoluzione delle reti radiomobili

3° Generazione

- Servizi multimediali
- Mobili Veloci 144 Kb/s
- Mobili Lenti 384 Kb/s
- Uffici 2 Mb/s
- Pacchetto e circuito
- Collegamenti asimmetrici
- Flessibilità ed efficienza

4° Generazione

- Larga Banda
  (≥ 2 Mb/s)

- Universal Mobile Telecommunication Systems (**UMTS**)
- Future Public Land Mobile Telecomm. Systems /International Mobile Telecomm.- 2000 (**FPLMTS/IMT-2000**)

16

GSM
La storia

- **1982**: la CEPT (*Conference Europeenne des Administrations des Postes et des Telecomunications*) istituisce un gruppo speciale per lo studio di un insieme uniforme di regole per lo sviluppo di una futura rete cellulare pan-europea: il *Groupe Special Mobile* da cui GSM
- **1984**: istituzione di 3 *Working Parties* (WP3) per la definizione dei servizi da fornire in GSM: l'interfaccia radio, i formati di trasmissione e i protocolli di segnalazione, le interfacce e l'architettura di rete
- **1985**: definizione della lista di raccomandazioni che il GSM deve produrre (finiranno per essere circa 130: 5000 pagine in 12 volumi!)
- **1986**: viene istituito il cosiddetto nucleo permanente con lo scopo di coordinare il lavoro del GSM, soprattutto visto il forte interesse da parte dell'industria

17

GSM
La storia

- **1987**: viene firmato un primo *Memorandum of Understanding* (MoU) tra operatori Telecom in rappresentanza di 12 Nazioni (europee) con i seguenti obbiettivi:
  - co-ordinare lo sviluppo temporale delle reti GSM europee e verificarne il loro standard
  - pianificare l'introduzione dei servizi
  - concordare politiche di instradamento e la tariffazione (modalità e prezzi)
- **1988**: con l'istituzione di ETSI (*European Telecommunication Standards Institute*) il lavoro relativo a GSM viene "spostato" in questo foro
- **1990**: viene deciso di applicare le speciche GSM anche al sistema DCS1800 (*Digital Cellular System on* 1800 MHz), un sistema di tipo PCN (*Personal Communication Networks*) inizialmente sviluppato in U.K.

18

GSM
La storia

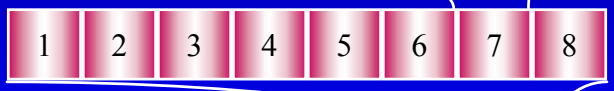
- **1991**: (luglio) il lancio commerciale del GSM, pianificato per questa data, viene rimandato al
- **1992** per la mancanza di terminali mobili conformi allo standard (?!?)
- **1992**: viene rilasciato lo standard definitivo relativo a GSM, che a questo punto diventa l'acronimo di *Global System for Mobile communications*
- **1992**: introduzione ufficiale dei sistemi GSM commerciali
- **1993**: il MoU di GSM raccoglie 62 membri di 39 paesi; inoltre altre 32 organizzazioni in rappresentanza di 19 paesi partecipano come osservatori in attesa di firmare il MoU
- **1993{98**: rapidissimo sviluppo dell'utenza e notevole miglioramento della qualità del servizio offerto, nonchè del numero di servizi offerti

19

GSM
Struttura della trama

time slot = 156.25 bits = 577 µs
tasso = 270.833 kbit/s

trama = 8 slots = 4.62 ms

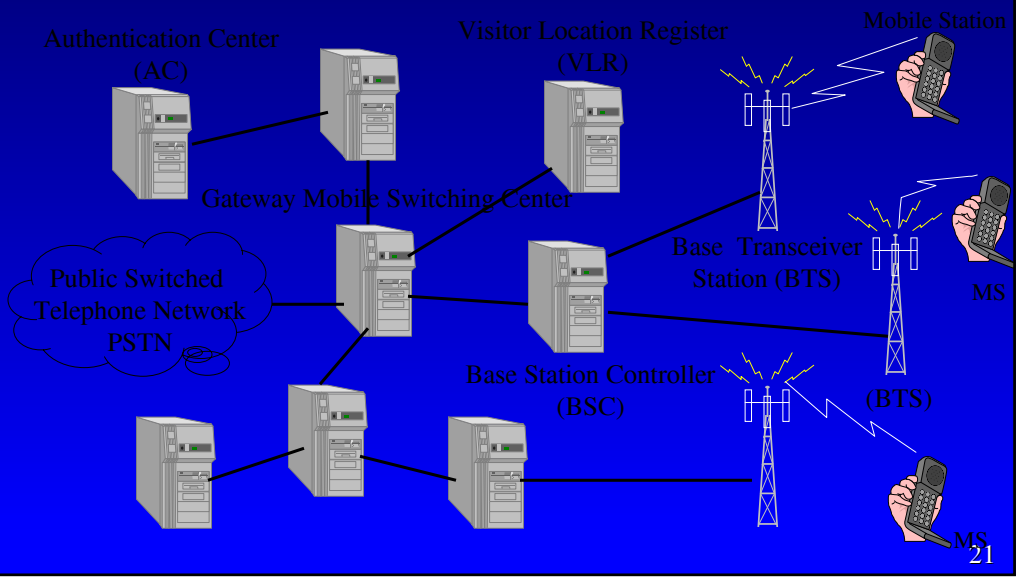


multitrama = 26 trame = 120 ms

*: Informazione di controllo

20

GSM
L'architettura



21

GSM
Canali di controllo

- I canali di controllo (***C**ontrol **CH**annel*, **CCH**) del GSM sono:
  - Canale di diffusione (***B**roadcast* **CCH**, *BCCH*)
  - Canale di controllo comune (***C**ommon* **CCH**, **CCCH**)
  - Canale di controllo dedicato "autonomo" (***S**tand-alone **D**edicated* **CCH**, **SDCCH**)
  - Canale di controllo associato (***A**ssociated* **CCH**, **ACCH**)

22

GSM
Canali di controllo

- BCCH
  - Unidirezionale BST - MS, diffonde informazioni di sistema e di sincronizzazione (ID della cella, struttura dei canali, condizioni di accesso, parametri radio utilizzabili (es. contr. di pot.)). È usato anche dalla MS per effettuare misure sulle celle adiacenti.
- CCCH
  - Bidirezionale. Da BST a MS serve ad inviare:
    - » Messaggi di chiamata (***P**aging **CH**annel* **PCH**)
    - » Messaggi di assegnazione risorsa (*Access Grant Channel*, **AGCH**)
  - Da MS a BST è gestito tramite accesso casuale (***R**andom **A**ccess **CH**annel*, **RACH**) e permette l'invio di richieste di chiamate.

23

GSM
Canali di controllo

- SDCCH
  - Bidirezionale che porta segnalazioni specifiche ad una connessione.
- ACCH
  - Bidirezionale, è associato ad un canale di traffico. Ce ne sono di due tipi:
    - » Lento, *Slow* -**ACCH** (**SACCH**), usato nel corso della trasmissione per la gestione della stessa.
    - » Veloce, *Fast*-**ACCH** (**FACCH**), usato per *handover*, ottenuto eliminando trame informative.

24

GSM

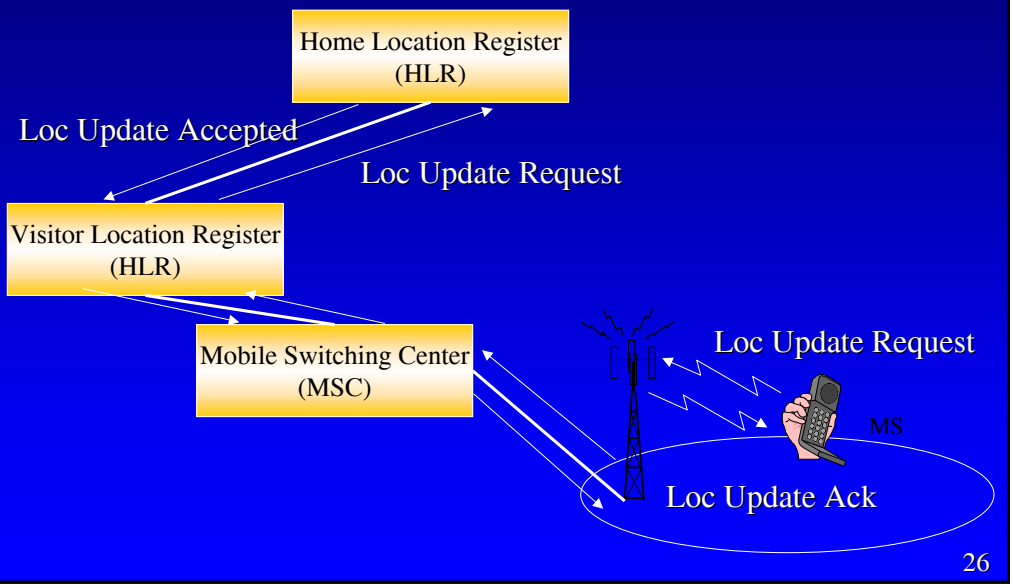
Canali di controllo

Canale	Velocità (bit/s)	Ritardo (ms)
FACCH	9200	58
SDCCH	782	250
SACCH	391	485
BCCH	782	250
AGCH	782	250
PCH	782	250
RACH	34	236

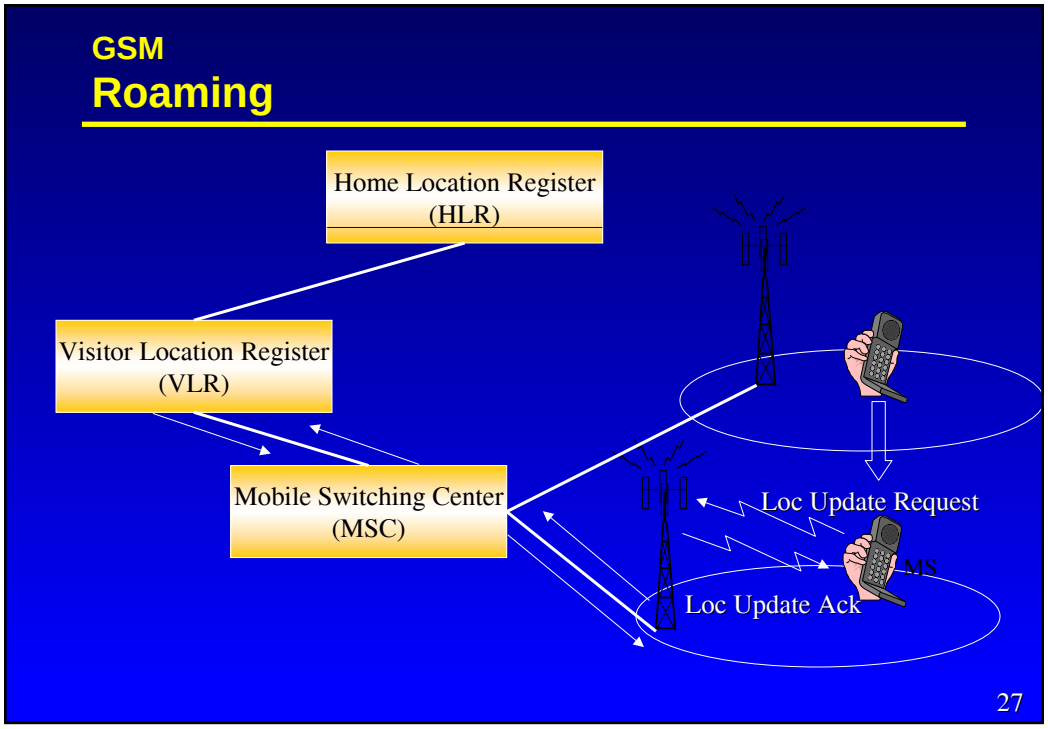
25

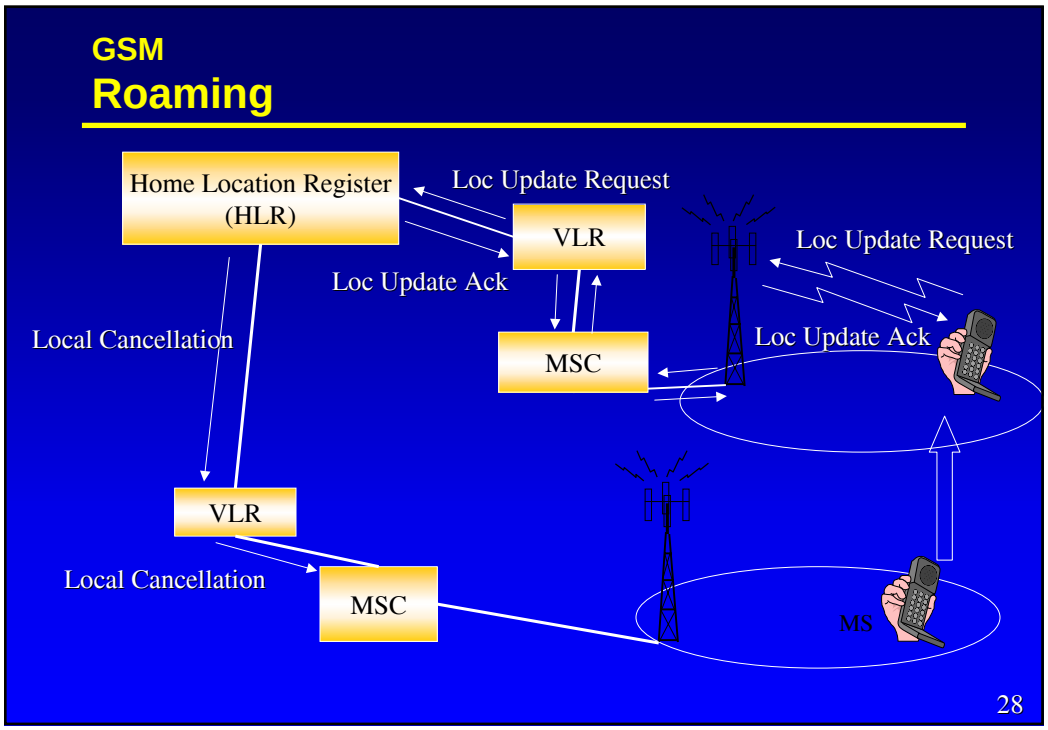
GSM

Roaming

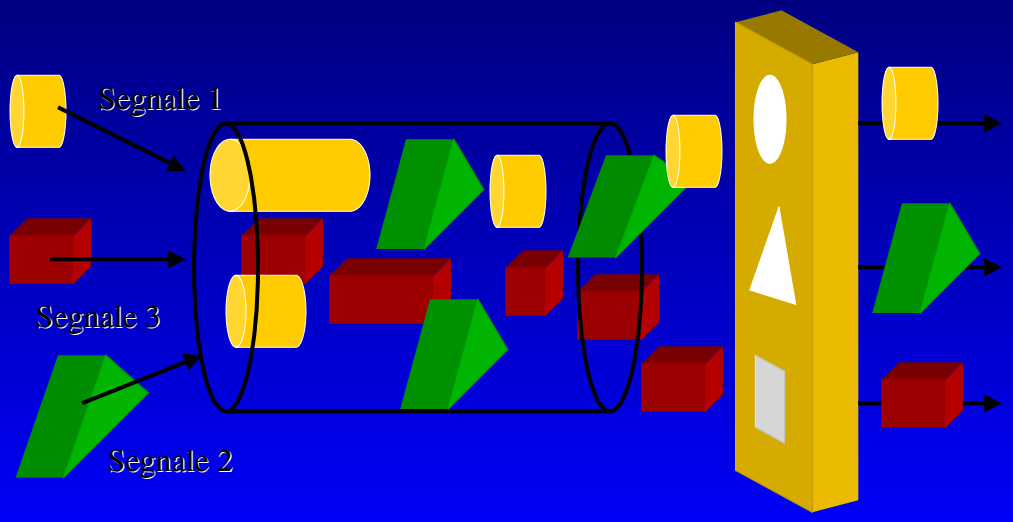


26


GSM
Roaming
Home Location Register
(HLR)
Visitor Location Register
(VLR)
Mobile Switching Center
(MSC)
Loc Update Request
MS
Loc Update Ack
27


GSM
Roaming
Home Location Register
(HLR)
Loc Update Request
VLR
Loc Update Request
Loc Update Ack
Local Cancellation
MSC
Loc Update Ack
VLR
Local Cancellation
MSC
MS
28

CDMA



29

CDMA

- ***Frequency hopping***
  - ogni quanto di tempo le stazioni cambiano frequenza di trasmissione, secondo una sequenza prefissata.
- ***Direct sequence***
  - La velocità base di trasmissione è molto più alta di quella della singola stazione, ed a ogni bit generato dalla stazione vengono trasmessi più bit (*chip*) dal trasmettitore.
    Ad ogni stazione viene associata una codifica particolare che sia il più possibile scorrelata con quella degli altri.
- L'effetto in ambedue i casi è uno "*spreading*" nello spettro delle singole trasmissioni; queste tecniche vengono quindi chiamate di tipo "***Spread-spectrum***".

30

CDMA

- Vantaggi
  - Sicurezza, difficile da decodificare
  - Poco sensibili a disturbi su parti ristrette dello spettro
  - Non hanno bisogno di avere un sincronismo comune, basta un sincronismo fra ricevitore e trasmettitore
  - Permettono a stazioni base adiacenti di comunicare con lo stesso mobile (soft-*handoff*).
  - Non esiste un limite fisso (*hard*) sul numero massimo di stazioni.
  - Non si deve realizzare una pianificazione di frequenza.

31

CDMA

- Svantaggi
  - E' complesso da realizzare
  - Richiede un controllo di potenza accurato (tutti i trasmettitori trasmettono sullo stesso canale)
  - Richiede la disponibilità di larghi tratti di spettro liberi.
- Si osservi che, anche se la ri-utilizzabilità delle frequenze da cella a cella sembra indicare una maggiore efficienza del CDMA sul TDMA, in realtà da questo punto di vista i due metodi sono equivalenti.

32

WirelessLAN

- Si tratta di reti in area locale in cui i le stazioni terminali (e talvolta anche i nodi intermedi) usano collegamenti senza fili.
- Sono anch'esse pensate come reti mobili, ma la mobilità è in genere intesa come relativamente lenta.
- Il loro scopo è quello sia di agevolare i cablaggi che "liberare" gli utenti da postazioni di lavoro fisse.

33

WirelessLAN

- Fra gli standard importanti in questo ambito vanno citati:
  - IEEE 802.11
  - HIPERLAN (*European HIgh PERformance* LAN)
  - Bluetooth
  - HomeRF - Shared Wireless Access Protocol - Cordless Access (SWAP-CA)

34

WirelessLAN - 802.11

- Lo standar iniziale é stato pubblicato nel 1997; é stato aggiornato con l'IEEE 802.11:1999 ed é stato adottato dall'OSI/IEC co,e 8802-11:1999
- Il sito ufficiale é www.ieee802.org/11/
- Ci sono diversi gruppi di lavoro sul progetto 802.11:
  - » 802.11D: Additional Regulatory Domains
  - » 802.11E: Quality of Services
  - » 802.11F: Inter-Access Point Protocols (IAPP)
  - » 802.11G: Higher data Rates at 2.4 GHz
  - » 802.11H: Dynamic Channel Selection and Transmission Power Control
  - » 802.11i: Authentication and Security
- Ad oggi sono presenti due versioni dello standard:
  - 802.11b: opera nella banda di 2.4 GHz ed é già utilizzato largamente
  - 802.11a: opera nella banda dei 5 GHz a velocità superiori

35

WirelessLAN

IEEE 802.11

- Mezzi trasmissivi:
  - Onde elettromagnetiche attraverso l'etere (radio, luce visibile o infrarossi)
- Terminali supportati:
  - Fissi, spostabili, mobili a velocità pedestre ed eventualmente veicolare.
- Estensione, due configurazioni previste:
  - *Basic Service Area* (BSA): interconnessione diretta fra nodi terminali
  - *Estended Service Area* (ESA): la comunicazione fra stazioni avviene tramite un sistema di distribuzione.

36

WirelessLAN

IEEE 802.11

- Velocità:
  - 802.11b: inizialmente 1-2 Mb/s (1997), 5.5-11 Mb/s nella seconda versione (1999).
  - 802.11a: 6,9,12,18,24,36,48 e 54 Mb/s (6, 12 e 24 sono obbligatori).
- Coperture:
  - 50-100 mt (802.11b) and 15-30 mt (802.11a) con antenne omnidirezionali; con antenne direzionali ad alto guadagno é possibile arrivare fino a 40 Km.
- Servizi:
  - con e senza vincoli sul ritardo
- Tecnica di accesso multiplo:
  - unica per diversi livelli fisici.

37

WLAN-IEEE 802.11

Peculiarità dell'ambiente *wireless*

- Tipo di mezzo "difficile"
  - Interferenze e rumore
  - Qualità variabile nello spazio e nel tempo
  - Condiviso con eventuali elementi 802.11 "non richiesti"
  - Condiviso con elementi non-802.11
- Non si può assumere la connettività completa (stazioni nascoste)
- Diversi regolamenti internazionali

38

WLAN-IEEE 802.11

Peculiarità dell'ambiente *wireless*

- Presenza della mobilità
  - Variazione della affidabilità del collegamento
  - Funzionamento a batteria: *power management*
  - Gestione del movimento
- Sicurezza
  - Nessun confine fisico
  - LAN sovrapposte

39

WLAN-IEEE 802.11

Specifiche

- Un singolo MAC che supporti diversi livelli fisici
  - Canali singoli e multipli
  - Differenti caratteristiche di "*Medium sense*"
- Permettere la sovrapposizione di più reti nella stessa area geografica
- Robustezza all'interferenza
- Risolvere il problema dei nodi nascosti
- Fornire supporto ai traffici con requisiti di ritardo massimo

40

WLAN-IEEE 802.11

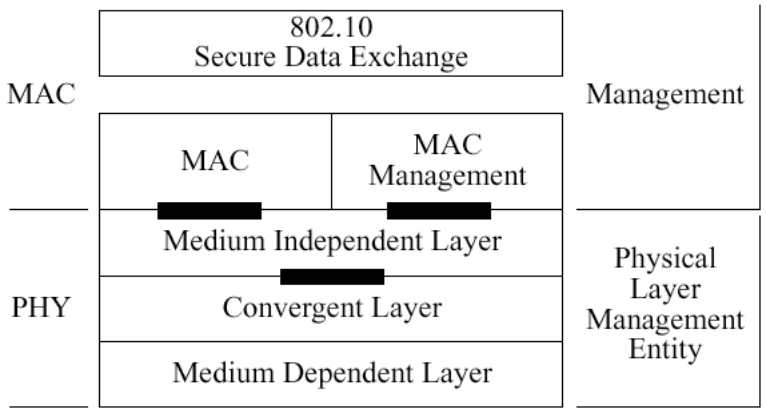
Caratteristiche

- Il MAC supporta attualmente 3 livelli fisici
  - *Frequency Hopping Spread Spectrum (FHSS)*
  - *Direct Sequency Spread Spectrum (DSSS)*
  - *Infrared*
- Permette due tipi di configurazioni
  - Infrastruttura
  - Indipendente (Ad Hoc)
- Usa la tecnica CSMA/CA (*Collision Advoidance*) con un punto di "coordinamento" opzionale.

41

WLAN-IEEE 802.11

Architettura



42

WLAN-IEEE 802.11

Architettura

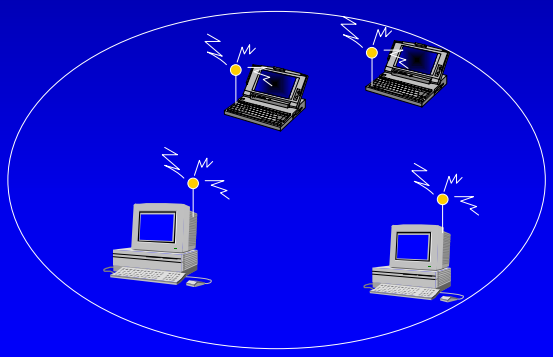
- MAC Entity
  - Meccanismo di accesso
  - Frammentazione
  - Encriptaggio
- MAC Management
  - Sincronizzazione
  - *Power management*
  - *Roaming*
- Physical Convergence
  - Riunisce le funzionalità comuni
  - L'individuazione *clear channel* (canale libero)

43

WLAN-IEEE 802.11

Architettura - Indipendente

- "Ad hoc" network
- Comunicazioni dirette
- Copertura limitata

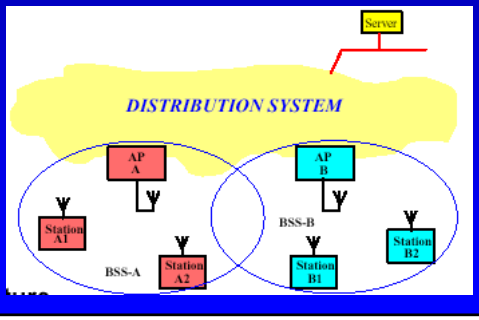


44

WLAN-IEEE 802.11

Architettura - Infrastructura

- Infrastruttura: *Access Point* (AP) e Stazioni
- Il *Distribution System* (DS) interconnette le diverse celle (*Basic Service Set* - BSS) attraverso gli AP per formare un *Extended Service Set* (ESS):
  - La connessione fra può essere sia *wireless* che *wired*.
  - la struttura interna del DS non è definita dallo standard
- Una stazione, detta *Portal*, presente sul sistema di distribuzione interconnette la WLAN con altre reti.



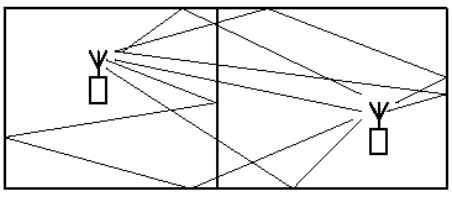
45

WLAN-IEEE 802.11

Frequency Hop Spread Spectrum

- Banda: 2.4 GHz (2.4 - 2.4835)
- Modulazione: Gaussian shaped FSK a 2 o 4 livelli
- Velocità minima 1 Mb/s, massima 2 Mb/s
- Fino ad massimo di 26 reti co-locate
- Permette un buona robustezza al fading dovuto ai cammini multipli (comuni nell'ambienti "indoor")

•Percorsi di propagazione multipli, interferendo l'uno con l'altro, creano del *fading* selettivo in frequenza
•Le fluttuazioni sono correlate a frequenze adiacenti ma si scorrelano, in ambiente indoor, dopo pochi MHz



46

WLAN-IEEE 802.11

Frequency Hop Spread Spectrum

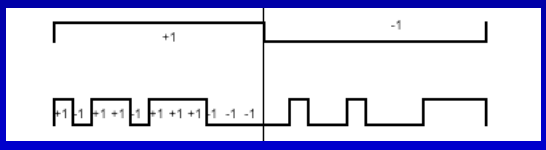
- Lo spettro complessivo è diviso in 79 canali da 1 MHz ciascuno
- Un elaboratore predesignato genera una lista con le 79 frequenze in un ordine specifico
  - Ogni "salto" (*hop*) deve distare almeno 6 canali.
  - Le diverse possibile sequenze (78) sono ottenute spostando l'inizio della sequenza di un *offset* e ricalcolandola con modulo 79
- Le 78 sequenze sono organizzate in 3 insiemi di 26 elementi
- Il *throughput* continua a salire fino a 15 reti colocate, in condizioni di traffico elevato.

47

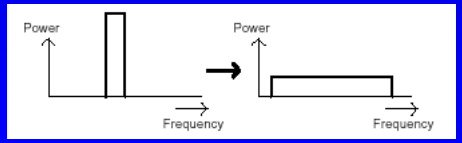
WLAN-IEEE 802.11

DirectSequence Spread Spectrum

- Il segnale relativo ad un simbolo viene "sparso" su una sequenza:



- Banda più larga
- Potenza meno "densa"



48

WLAN-IEEE 802.11

DirectSequence Spread Spectrum

- Banda: 2.4 GHz (2.4 - 2.4835)
- Prima versione: velocità minima 1 Mb/s (*Differential Binary Phase Shift Key* DBPSK), massima 2 Mb/s (*Differential Quadrature Phase Shift Key* DQPSK)
- Seconda versione (Higher Rate DSSS): velocità minima 5.5 Mb/s, massima 11 Mb/s
- Tasso di simbolo 1 MHz
- *Chipping* rate 11 MHz
- 7 canali complessivi, radunati in coppie (in Europa uno dei canali della prima coppia non può essere usato); i canali di ogni coppia possono operare simultaneamente senza interferenza.

49

WLAN-IEEE 802.11

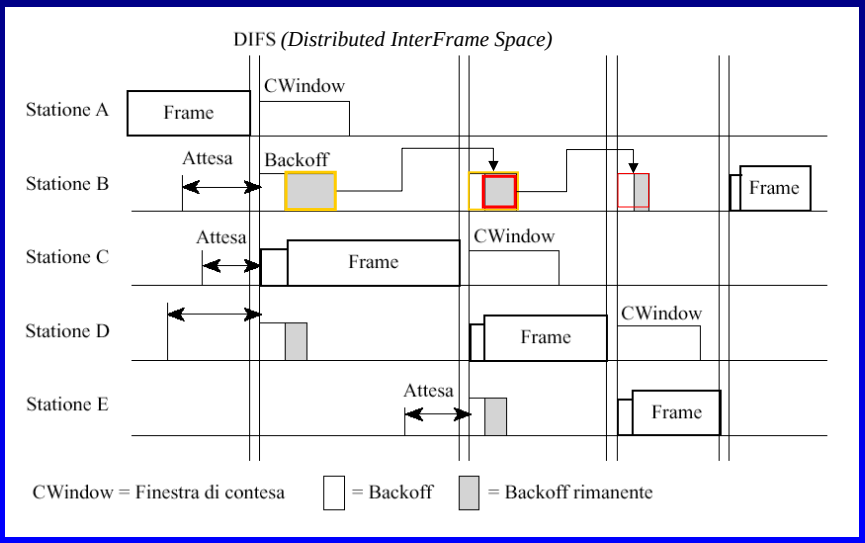
MAC

- La tecnica scelta è il Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
- Due funzionalità presenti
  - *Distribution Coordiantion Function*
    - » Realizza il meccanismo di MAC in forma completamente distribuita
  - *Point Coordination Function*
    - » Versione centralizzata per permettere le realizzazione di servizi "*delay bounded*"

50

WLAN-IEEE 802.11

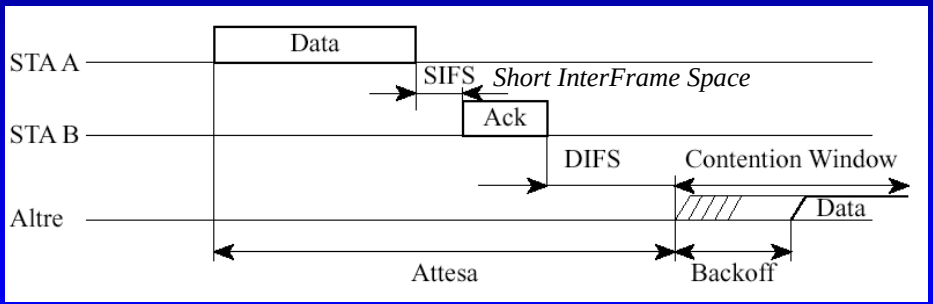
MAC - DCF



51

WLAN-IEEE 802.11

MAC - DCF



52

WLAN-IEEE 802.11

MAC - Inter Frame Spaces

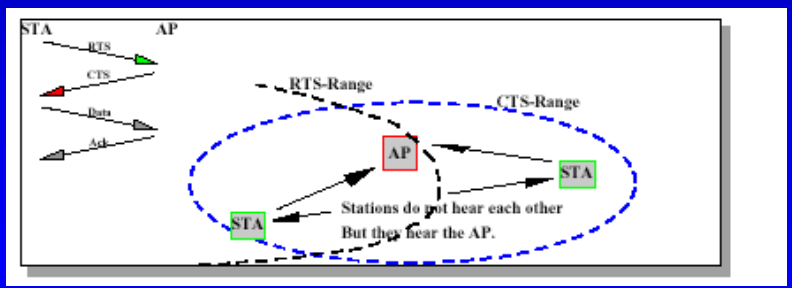
- **SIFS** (*Short Inter Frame Space*) - separa la trasmissione di pacchetti appartenenti allo stesso dialogo (es. Pacchetto + ACK). Viene calcolato in base ai tempi necessari agli apparati hw per commutare tra tx/rx.
- **PIFS** (*Point Coordination Inter Frame Space*) - é utilizzato dal Point Coordinator per gestire il polling. É pari allo SIFS + il tempo di una slot
- **DIFS** (*Distributed Inter Frame Space*) - il tempo che una stazione deve attendere prima di accedere al canale. Corrisponde al PIFS + il tempo di una slot.
- **EIFS** (*Extended Inter Frame Space*) - utilizzato da una stazione che non riceve correttamente il pacchetto per non collidere con un pacchetto successivo appartenente allo stesso dialogo.

53

WLAN-IEEE 802.11

MAC - DCF

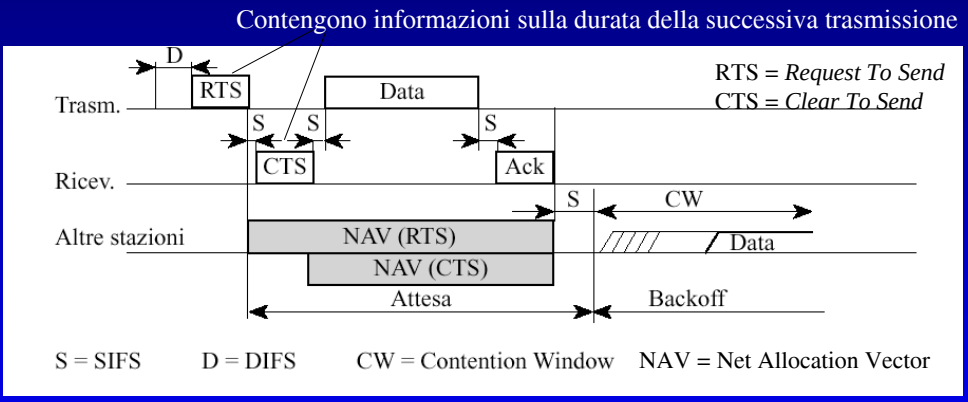
- Le collisioni non sono evitate completamente per due motivi:
  - Tempi di backoff simili
  - Stazioni nascoste



54

WLAN-IEEE 802.11

MAC - DCF

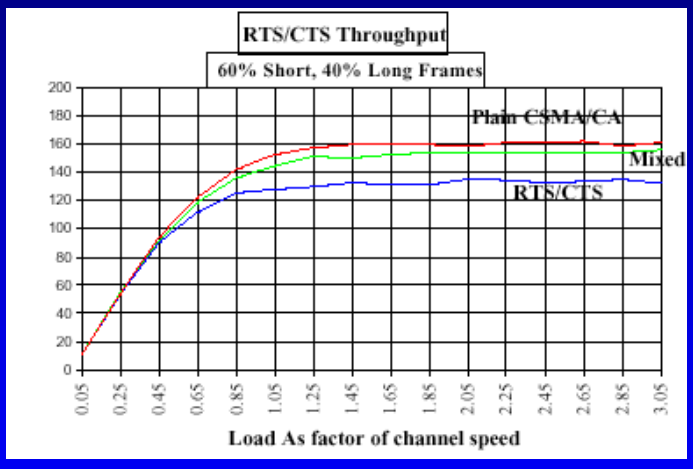


Se i pacchetti sono molto corti il sistema è inefficiente per cui per lunghezze sotto una certa soglia è prevista la tx senza RTS/CTS;
La tx diretta viene effettuata anche nel caso di broadcast

55

WLAN-IEEE 802.11

MAC - DCF



56

WLAN-IEEE 802.11

MAC - DCF

- Si osservi che il MAC prevede sia una funzione di frammentazione e recupero di errore (solo per *point to point*);
- Questo perché
  - Nei collegamenti radio la BER è alta e la probabilità di avere un pacchetto errato aumenta con la lunghezza del pacchetto stesso;
  - Più i pacchetti sono corti, meno *overhead* genera una eventuale ritrasmissione;

57

WLAN-IEEE 802.11

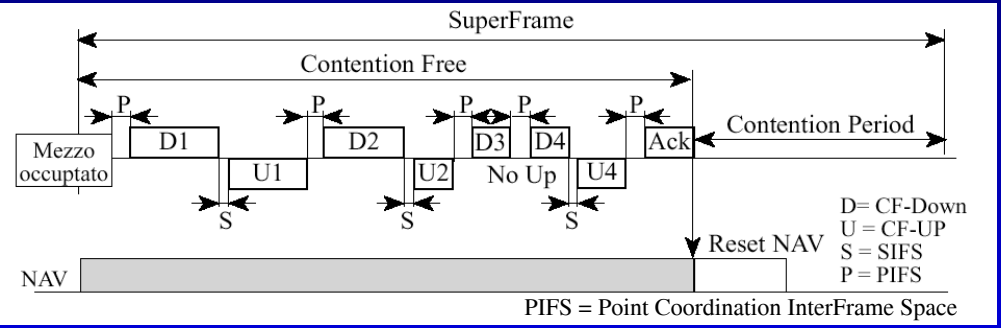
MAC - PCF

- Viene gestita da alcune stazioni specializzate (per es. AP) che vengono chiamate *Point Coordinator (PC)*.
- Una PCF non può sovrapporsi ad un'altra sullo stesso canale trasmissivo.
- In sostanza viene creata una struttura temporale detta Superframe divisa in due parti:
  - Contention free period: gestita da un PC con un meccanismo polling
  - Contention period: gestito come nel DCF.
- Serve a fornire servizi con requisiti di ritardo.

58

WLAN-IEEE 802.11

MAC - PCF



- L'ack viene inserito nel frame successivo di una tx (trannel'ultimo)
- Le stazioni che non trasmettono per più di un certo numero di turni vengono escluse

59

WLAN-IEEE 802.11

Sicurezza

- Un aspetto fondamen tale nelle WLAN é rappresentato dalla sicurezza
- Lo standard 802.11 presenta meccanismi di protezione non completamente adeguati
- Utilizza la cosiddetta *Wireless Equivalency Privacy* (WEP), che ha come obiettivo quello di fornire un livello di protezione equivalente a quello delle reti cablate; questo non é considerato sufficiente
- Esistono varie tecniche per le quali é stata dimostrata la capacità di violare con successo la protezione

60

WLAN-IEEE 802.11

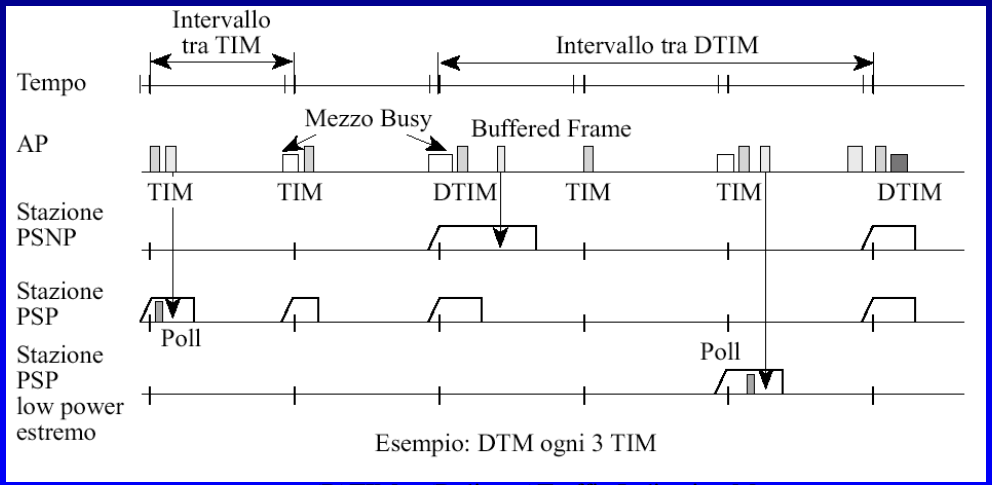
Sicurezza

- Due sono gli aspetti legati alla sicurezza:
  - Prevenire l'utilizzo da parte della rete da parte di stazioni non autorizzate
  - Evitare l'ascolto del traffico della LAN da parte di stazioni esterne
- Le WLAN prevedono una fase di autenticazione della stazione che desiderano entrare nella LAN (richiedendo la conoscenza di una chiave segreta)
- La cattura del traffico locale viene evitata criptando il traffico trasmesso
- La chiave di criptatura può essere a 64, 128 o 154 bit

61

WLAN-IEEE 802.11

Controllo di potenza



(D)TIM = (Delivery)Traffic Indication Map

62

WLAN-IEEE 802.11

Sicurezza

- Un elemento fondamentale per le wireless LAN è rappresentato dalla sicurezza.
- L'IEEE 802.11 soffre di meccanismi di protezione attualmente non del tutto adeguati
- Usa quello che è chiamato *Wired Equivalent Privacy* (WEP), che ha l'obiettivo di fornire una protezione equivalente a quella fornita dalle "*wired LAN*" che non è considerata sufficiente
- Sono stati dimostrati e divulgate varie tecniche per effettuare con successo "attacchi" allo standard.

63

WLAN

HiperLAN

- La prima proposta viene presentata nell'ETSI nel 1995
- La copertura prevista va da 10 a 100 m
- Lo spettro allocato dal CEPT è 5.15-5.30 GHz (5 canali) e 17.1-17.2 GHz
- Velocità di trasmissione 23.529 Mbit/s, GMSK
- *Packet error rates* < 10^{-3}, (*adaptive equalization based on a training sequence per packet*)
- *Multi-hop routing* che usa database dinamici nei nodi
- *Carrier Sense Multiple Access* a tre fasi - *prioritization, elimination, yield*; probabilità di collisione < 3% (relativamente diverso dal IEEE 802.11)
- *Power saving in Hardware*.

64

WLAN

HiperLAN

	HIPERLAN Type 1	HIPERLAN Type 2	HIPERLAN Type 3	HIPERLAN Type 4
Link type	Wireless LAN MAC	Wireless ATM MAC	Wireless high speed remote access MAC	Wireless very high speed wireless infrastructure MAC
Link Frequency	5 GHz	5 GHz	5 GHz	17 GHz
Data Rate	> 20 Mbit/sec	> 20 Mbit/sec	> 20 Mbit/sec	155 Mbit/sec

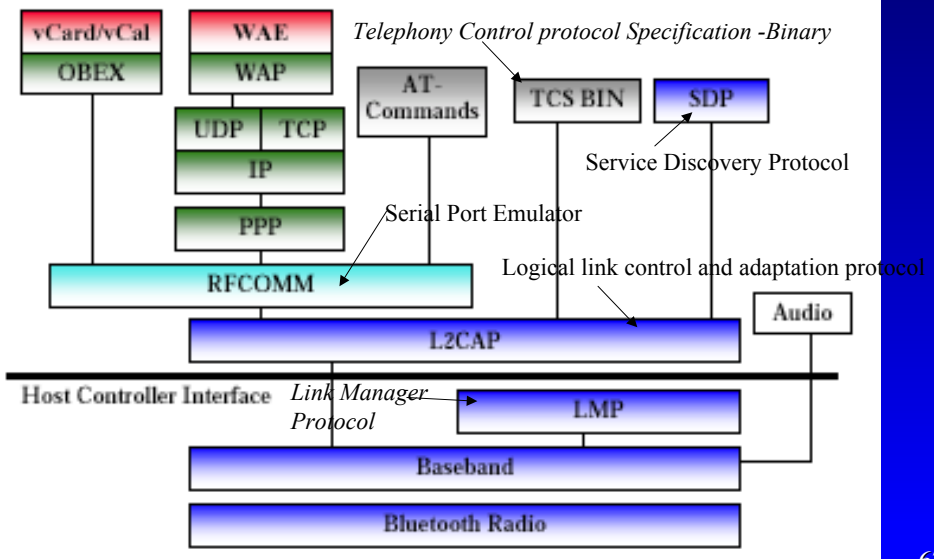
65

Bluethoot

- Si tratta di un tipo di rete studiata per l'interconnessione di apparati (pc con stampanti, modem, telefoni fissi e cellulari, …) all'interno di una stanza o comunque di un ambiente di piccole dimensioni.
- Realizza quella che talvolta viene chiamata *Personal Area Network* (PAN).
- L'estensione della rete dovrebbe quindi essere intorno alla decina di metri, ma lo standard prevede anche apparati con potenze sufficienti a raggiungere la 50 di metri di copertura (portandosi a competere con 802.11 e *HomeRF*).

66

Bluethoot
Architettura



67

Bluethoot
Livello Radio

Spettro (Frequency Hopping)

Geography	Regulatory Range	RF Channels
USA, Europe and most other countries[1)]	2.400-2.4835 GHz	f=2402+k MHz, k=0,…,78

Table 2.1: Operating frequency bands

Note 1. The Bluetooth Specification includes a special frequency hopping pattern to provide provisions for compliance with national limitations like in France. The frequency range for France is 2.4465 - 2.4835 GHz and the corresponding RF channels are f = 2454 + k MHz, k= 0,...,22..

Potenza

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Table 3.1: Power classes

68

Bluethoot
Livello Baseband

- Sono previsti due tipi di servizi:
  - ***Syncnronous Connection Oriented*** (SCO)
  - ***Asynchronous Connectionless*** (**ACL**)
- La rete è organizzata in gruppi di stazioni dette "***piconet***".
- Ogni *piconet* vede una stazione assumere il ruolo di master e le altre di slave.
- Il master fornisce il sincronismo e coordina le trasmissioni interrogando ciclicamente (*polling*) gli slave.

69

Bluethoot
Livello Baseband

Full-duplex via ***Time Division Duplex***

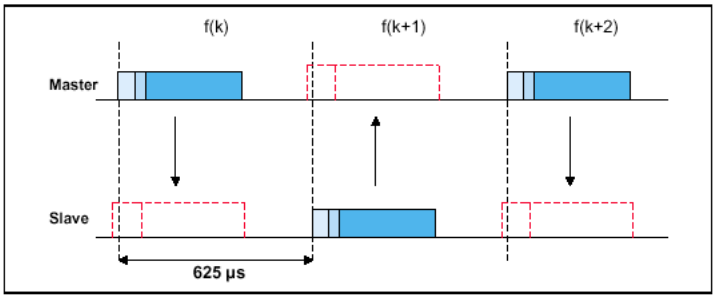


Figure 2.1: TDD and timing

70

Bluethoot

Livello Baseband

Tasso nominale di “salti” (*hop*) è 1600 hop/s.

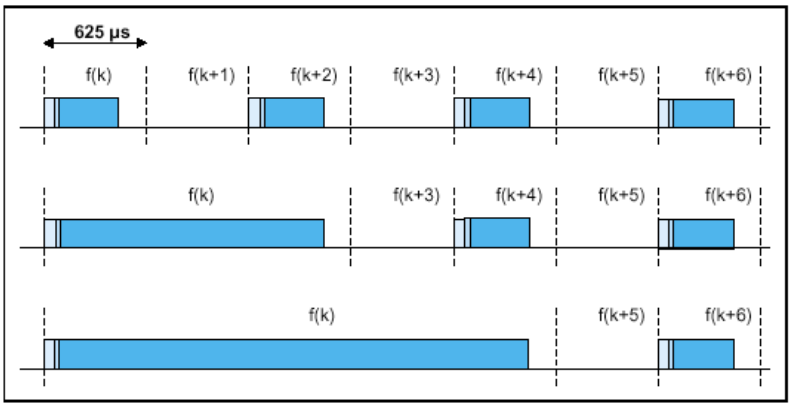


Figure 2.2: Multi-slot packets

71

Bluethoot

Livello Baseband

Tassi trasmissivi (ACL)

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX1	1	0-29	no	no	185.6	185.6	185.6

Table 4.10: ACL packets

72

Bluethoot

Tassi trasmissivi (ACL)

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	no	no	64.0
DV*	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D

Table 4.11: SCO packets

73

Bluethoot

Link Manager Protocol

- E' responsabile dell'instaurazione dei link
- Si occupa anche degli aspetti legati alla sicurezza quali
  - Autenticazione
  - Cifratura
  - Scambio delle chiavi di cifratura
- Controlla e negozia la dimensione dei pacchetti nel livello *baseband*

74

Bluethoot
Logical Link Control and Adaptation Protocol

- Lavora in parallelo all'LMP ma trasporta informazione d'utente (dati dei livelli superiori
- Fornisce servizi sia orientati alla connessione che no, può operare funzioni di *multiplexing*, di segmentazione e riassemblaggio e gestisce gruppi d'utente.

75

Home-RF v. 2.0

- Sono specifiche definite da un consorzio di aziende "*HomeRF Working Group Inc.* (HRFWG)" (http://www.homerf.org/) formatosi all'inizio del 1998
- Fanno parte del consorzio fra gli altri:
  - AT&T
  - Compaq Computer Corp.
  - Dolby Laboratories
  - Fujitsu, Ltd.
  - Motorola
  - National Semiconductor
  - Nokia, Inc.

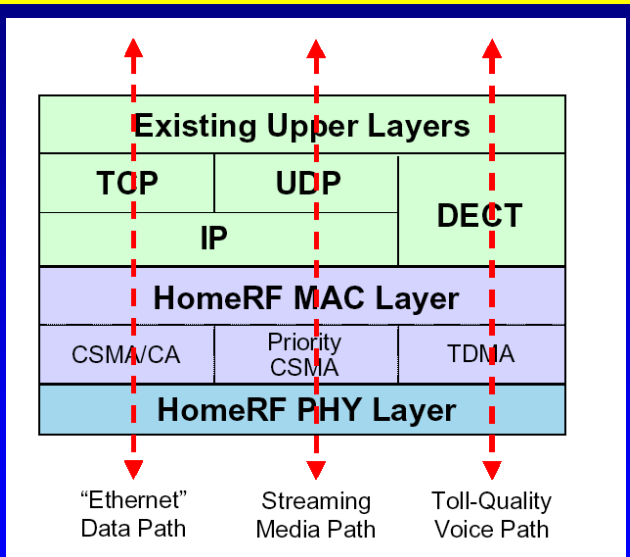
76

Home-RF v. 2.0

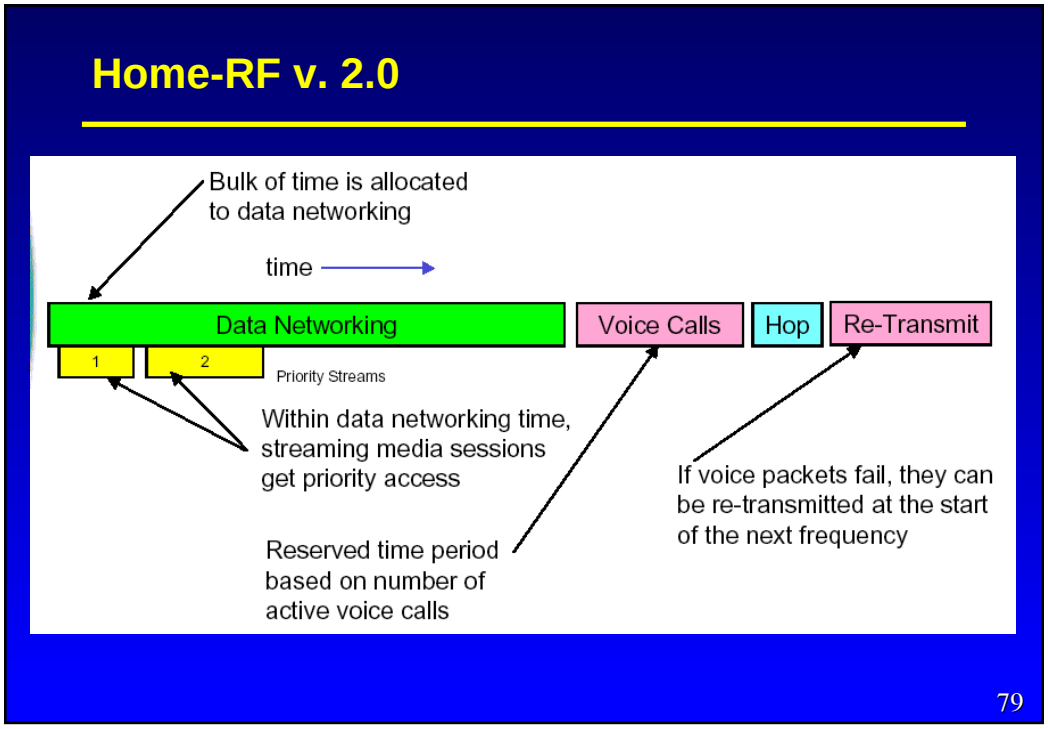
- 10 Mb/s di velocità massima con possibilità di scendere a 5 Mb/s, 1.6 Mb/s o 0.8 Mb/s in condizioni ambientali difficili
- Compatibile con lo standard HomeRF 1.2 a 1.6 Mb/s e 0.8 Mb/s
- Topologie simultaneamente attive sia di tipo host/client che peer to peer (ad hoc)
- Modalità con risparmio energetico elevato
- Efficaci misure per il diniego di accesso e la protezione
- Fino a 8 flussi prioritari simultanei per audio e video mono e bi-direzionali
- Fino a 8 conessioni a qualità vocale bi-direzionali simultanee (4 inizialmente)

77

Home-RF v. 2.0



78


Home-RF v. 2.0
Bulk of time is allocated to data networking
time
Data Networking
Voice Calls
Hop
Re-Transmit
1
2
Priority Streams
Within data networking time, streaming media sessions get priority access
Reserved time period based on number of active voice calls
If voice packets fail, they can be re-transmitted at the start of the next frequency
79