WIRELESS LAN

Prof. Ing. Maurizio Casoni

And many thanks to Prof. Sergio Palazzo (Università di Catania)

Dipartimento di Ingegneria dell'Informazione
Università degli Studi di Modena e Reggio Emilia

WIRELESS LAN: STORIA

- **1970s**:
  - IBM Labs in Svizzera: progetto di una rete wireless indoor nel campo dell'infrarosso
  - HP Labs: progetto di un sistema radio DS-CDMA per comunicazioni fra terminali
  - Entrambi i sistemi avevano velocità di 100 Kbit/s e non furono mai commercializzate
- **1981**: Negli U.S.A. la Federal Communication Commission (FCC) comincia a pensare di assegnare bande per applicazioni commerciali di tipo wireless
- **1990** : primi prodotti sul mercato in tecnologia spread-spectrum nelle bande ISM, 18-19 Ghz ed infrarosso

LICENSED vs. UNLICENSED BANDS

- UNLICENSED BANDS: due insiemi di bande **ISM** (Industrial, Scientific, Medical) e **PCS** (Personal Communications Services)
  - 1985: Vennero concesse tre bande ISM a condizione di usare tecniche spread spectrum
    - 902-928 Mhz
    - 2400-2483.5 Mhz
    - 5725-5850 Mhz
  - bande PCS a 1.9 Ghz (1850-1990 Mhz)
    - 1910-1920 Mhz: operazioni asincrone o a commutazione di pacchetto
    - 1920-1930 Mhz: applicazioni sincrone o a commutazione di circuito
    - La parte rimanente della banda per applicazioni con concessione
  - Di recente FCC ha aperto la banda dei 300 Mhz per operazioni senza concessione a 5Ghz: questa è la banda più promettente per applicazioni radio a pacchetto
- LICENSED BANDS: l'uso di queste bande richiede l'autorizzazione della FCC, processo lungo e difficile: è perciò preferibile per applicazioni outdoor (e.g. distribuzione domestica a larga banda)

WIRELESS LAN: STORIA

- ***1990***: IEEE nomina il comitato 802.11 per definire uno standard per wireless LANs

- ***1992***: In Europa ETSI comincia un'attività di standardizzazione per HIPERLAN (High Performance Radio LAN)

- ***1993***: UE concede le bande 5.2 e 17.1 Ghz ad HIPERLAN

ASPETTI del LIVELLO FISICO

- Livello fisico: trasmissione dei dati sul mezzo fisico
- Al momento, apparati radio operanti in modalità burst e ad accesso multiplo non sono commercialmente disponibili per velocità maggiori di 54 Mbps
- Il problema principale è combattere la ricezione **multi-path** da oggetti stazionari e mobili che comporta un canale dispersivo variante nello spazio e nel tempo

INFRAROSSO vs. RADIO

- Sistemi di comunicazione con trasmissione nell'infrarosso possono essere meno costosi da realizzare di quelli radio: ricevitori si basano sulla rilevazione dell'ampiezza o della posizione dei segnali, e non della frequenza o fase (i.e. facile rilevazione di potenza)
- Frequenze dell'infrarosso non sono regolamentate: non occorre licenza
- Vantaggi di privatezza: trasmissioni sono confinate entro una stanza
- E' possibile diffondere un raggio infrarosso mediante una lente: sistema simile a quello radio in termini di copertura di un'area indoor
- Infrarosso ha un "range" minore del radio: si usa quando l'interferenza elettromagnetica è un problema (ospedali)
- Problemi: come la radio, soffre del *multi-path* e della sincronizzazione; pure l'accesso multiplo è difficile
- Esistono prototipi a 100 Mbps ma richiedono una trasmissione in visibilità ed un'elevata accuratezza nel puntamento del fascio infrarosso (difficile in ambienti affollati indoor ed outdoor)

INFRAROSSO vs. RADIO

- Per reti a pacchetto wireless indoor o outdoor, radio è la soluzione preferita: non necessita di trasmissione in visibilità; puntamento ed accesso multiplo sono più semplici
- Infrarosso è una scelta possibile per reti ad alta velocità con collegamenti punto-punto o per evitare problemi di interferenza e.m.
- A basse velocità , sono possibili WLANs diffuse limitate a singola stanza

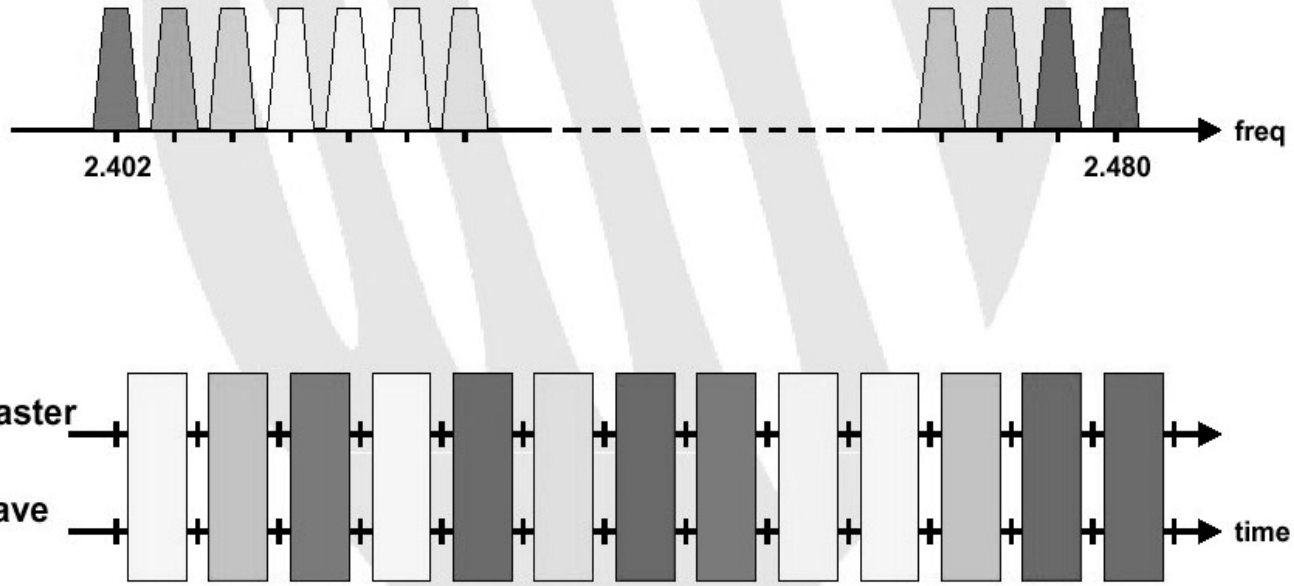
FREQUENZE di FUNZIONAMENTO

- Frequenze di funzionamento: aspetto importante da considerare quando si realizza un sistema wireless ad alta velocità
- Esistono limiti fisici e di legge
- **Limiti fisici** sono dati dai *limiti degli apparati*: tecnologia al silicio opera bene fino a 13-15 Ghz; a frequenze superiori può operare l'Arseniuro di Gallio (GaAs) ma a costi più elevati
  - Comunque sono già operativi dimostratori integrati al silicio BiCMOS SiGe per WLAN a 60 GHz
- …e dalla *propagazione*: attenuazione del segnale aumenta con la radice quadrata della frequenza
- **Limiti di legge:** sotto i 10 Ghz, può essere necessario ottenere una concessione o autorizzazione;

SPREAD SPECTRUM

- Esistono due tipi di tecniche SS: *direct sequence* e *frequency hopping*
- Per un sistema a 10 Mbps, con DS-SS e guadagni di processo di 10-100, occorrono velocità di chip da 100 Mbps a 1 Gbps : arduo da conseguire
- FH-SS è realizzabile e combatte il problema del multi-path ma ha problemi di sincronizzazione
- Sebbene alcune WLANs attuali usino SS, erano state concepite per operare nelle bande ISM, dove peraltro era obbligatorio l'uso di tecniche SS
- Per sistemi wireless ad alta velocità, con elevate bit rates, lo SS è difficile da impiegare
- Quinidi si ritiene che per i sistemi wireless ad alta velocità le tecniche Spread Spectrum non siano idonee

FREQUENCY HOPPING



MODULAZIONE

- Tecniche di modulazione lineare (BPSK, QPSK, DPSK, QAM) sono possibili per lo spettro radio
- Costellazioni multi-livello sono difficili da realizzare a causa del rumore e della difficoltà di equalizzazione
- Schemi di modulazione ad ampiezza costante (MSK, GMSK) possono risolvere il problema dell'amplificazione del segnale e sono implementati usando anche architetture di tipo a quadratura
- OFDM (Orthogonal Frequency Division Multiplexing) semplifica l'equalizzazione
- Radio funzionante a 25 Mbps usando uno schema QPSK o GMSK è fattibile; OFDM è attraente ma richiede ulteriori sforzi di ricerca e sviluppo prima di essere adottato su ampia scala

ANTENNE MULTIPLE

- Antenne multiple migliorano le prestazioni
- La scelta di quella col miglior rapporto segnale-interferenza fornisce un preciso miglioramento di prestazioni
- Tecniche più complicate, come *adaptive antenna arrays*, migliorano le prestazioni in modo significativo
- In generale, un sistema radio può raggiungere un'efficienza di 1-2 bps/Hz con una singola antenna non direzionale e questo valore aumenta linearmente con il numero di antenne

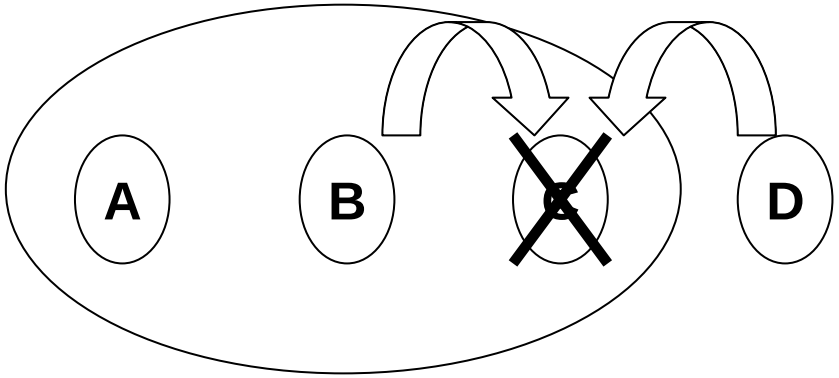
WIRELESS LANs

- Trasferimento di informazioni tra dispositivi di rete usando sistemi radio che operano a determinate frequenze
- Stazioni potrebbero pure essere mobili
- Topologie principali:
  - "Ad hoc": assenza di qualuque infrastrttura e gli utenti mobili comunicano direttamente
  - Infrastrutturata: esiste una stazione particolare che ha funzioni di controllo (i.e. per l' accesso radio) e può fare da ponte verso reti fisse

PROBLEMI DA AFFRONTARE

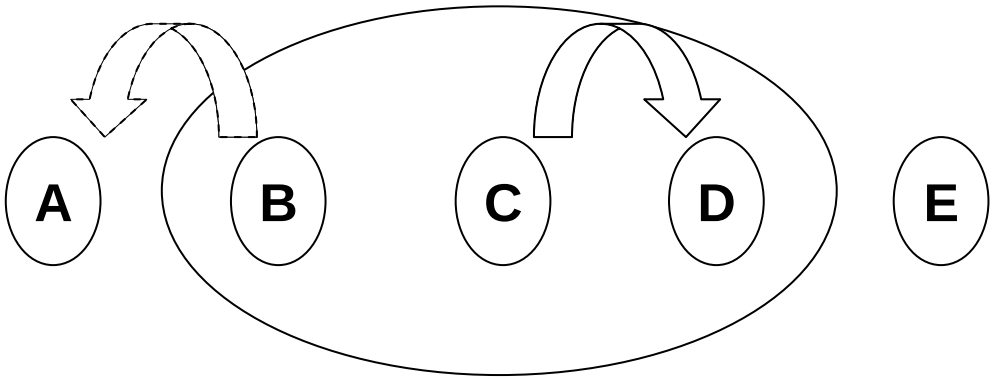
- Limited wireless transmission range
- Broadcast nature of the wireless medium
  - **Hidden terminal problem**
  - **Exposed terminal problem**
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions

PROBLEMA del TERMINALE NASCOSTO



A transmission from B to C is heard by A but not by D. A hidden terminal problem results when D attempts to transmit to C without knowing the ongoing transmission

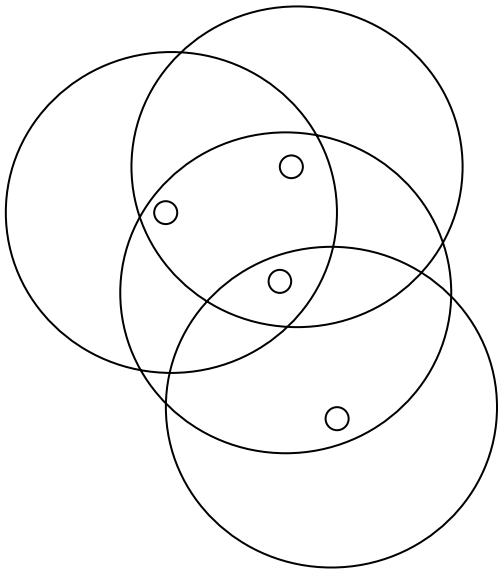
PROBLEMA del TERMINALE ESPOSTO

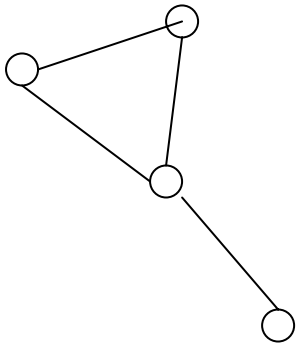


A transmission from C to D is heard by B but not by A.
An exposed terminal problem occurs when B remains silent even if its transmission to A will not cause any collision

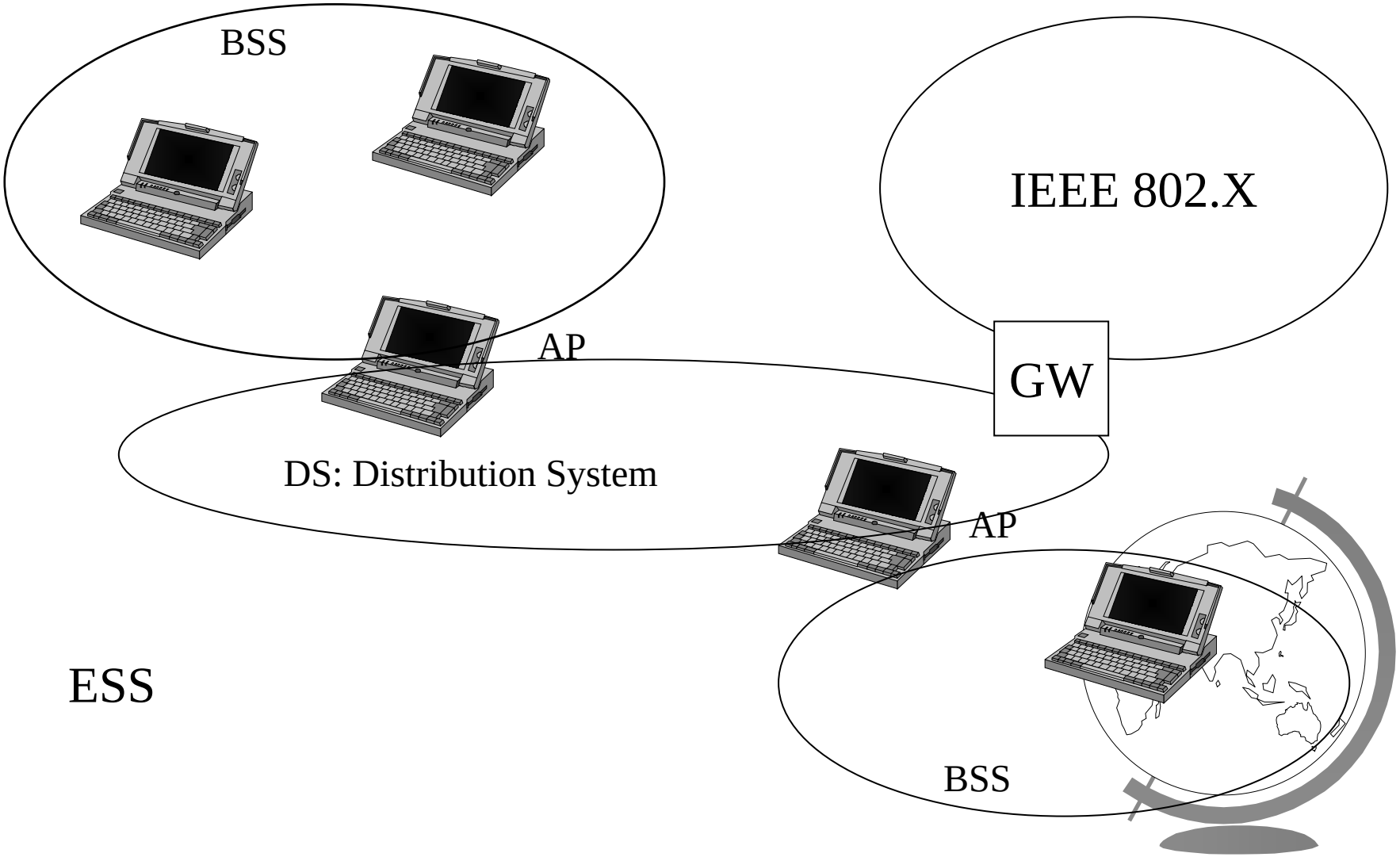
MULTIHOPPING

- Data routes may traverse multiple links to reach a destination.
- It increases overall network capacity since the spatial domain could be reused for concurrent but physically separate sessions
- It conserves transmit energy resources $\Rightarrow$ reduces interference





RETE INFRASTRUTTURATA



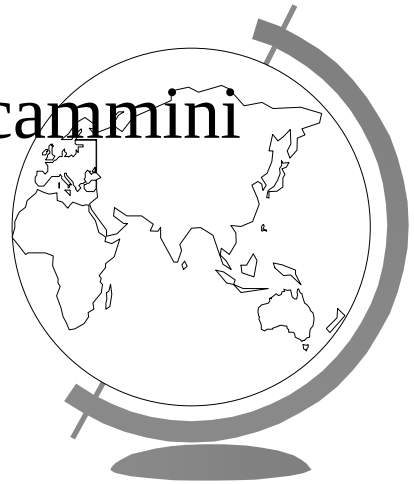
TECNICHE di TRASMISSIONE

Proprietà di una WLAN ad alta velocità:

- bit rates @ decine di Mbps
- complessità e consumo di potenza limitati negli apparati

Alcune soluzioni:

- Spread spectrum: usato sistemi radio cellulari (CDMA)
- Antenne direttive : per ridurre l'effetto dei cammini multipli
- Modulazione a portanti multiple
- Modulazione con singola portante



IEEE 802.11

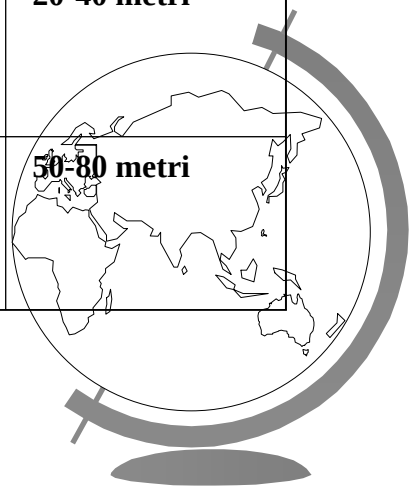
Sono stati definiti tre livelli fisici:

- ad infarosso in banda base: modulazione OOK @ 1Mbps
- DS-SS: QPSK @ 2Mbps
- FH-SS: QPSK @ 1 e 2 Mbps
- I sistemi SS operano nella banda ISM 2400-2483.5 Mhz

- Viene impiegato il protocollo DFWMAC (Distributed Foundation Wireless MAC) con 2 *coordination functions*:
  - metodo distribuito di base per l'accesso : traffico asincrono
  - metodo centralizzato opzionale per l'accesso : traffico real time

IEEE 802.11: diverse versioni

Standard	Frequenza	Data Rate	Modulazione	Copertura
IEEE 802.11	2,4 GHz	1-2 Mbps	QPSK/ DSSS	Pochi metri
IEEE 802.11b (Wi-Fi)	2,4 GHz	5,5 – 11 Mbps	QPSK/ DSSS	50-100 metri
IEEE 802.11a (Wi-Fi 5)	5 GHz	fino a 54 Mbps	OFDM	20-40 metri
IEEE 802.11g	2,4 GHz	fino a 54 Mbps	OFDM	50-80 metri



IEEE 802.11: ARCHITETTURA

- Velocità minima : 1 Mbps per applicazioni dati
- Supporto per applicazioni real-time
- Supporto della mobilità, almeno pedestre
- **BSS** (Basic Service Set): insieme di stazioni sotto il controllo della stessa Coordination Function (CF)

  Coordination Function: funzione logica che in un BSS assegna alle stazioni i diritti a trasmettere e ricevere; ne sono state definite 2:
- *Distributed Control Function* (DCF): per l' accesso distribuito di base
- *Point Coordination Function* (PCF): accesso centralizzato opzionale

  Basic Service Area (BSA): area di comunicazione dei membri del BSS

  Distribution System (DS): dorsale per collegare più BSSs e può essere radio o cablata

  Access Point (AP): stazione punto di accesso ad un DS

Distributed Control Function

Metodo di base per l'accesso multiplo ed impiega:

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Random back-off
- Explicit acknowledgment

  anche se wireless è un mezzo broadcast, il tradizionale CSMA/CD non funziona perché una stazione non riesce ad ascoltare il canale per eventuali collisioni mentre sta trasmettendo

  Carrier sensing viene eseguito sia all'interfaccia radio (Carrier sensing fisico) sia al sottolivello MAC (carrier sensing virtuale):

- Carrier sensing fisico: rileva la presenza di altri utenti attraverso la potenza relativa del loro segnale
- Carrier sensing virtuale: usato da una stazione sorgente per informare le altre del BSS della durata di utilizzo del canale

TIME INTERVALS

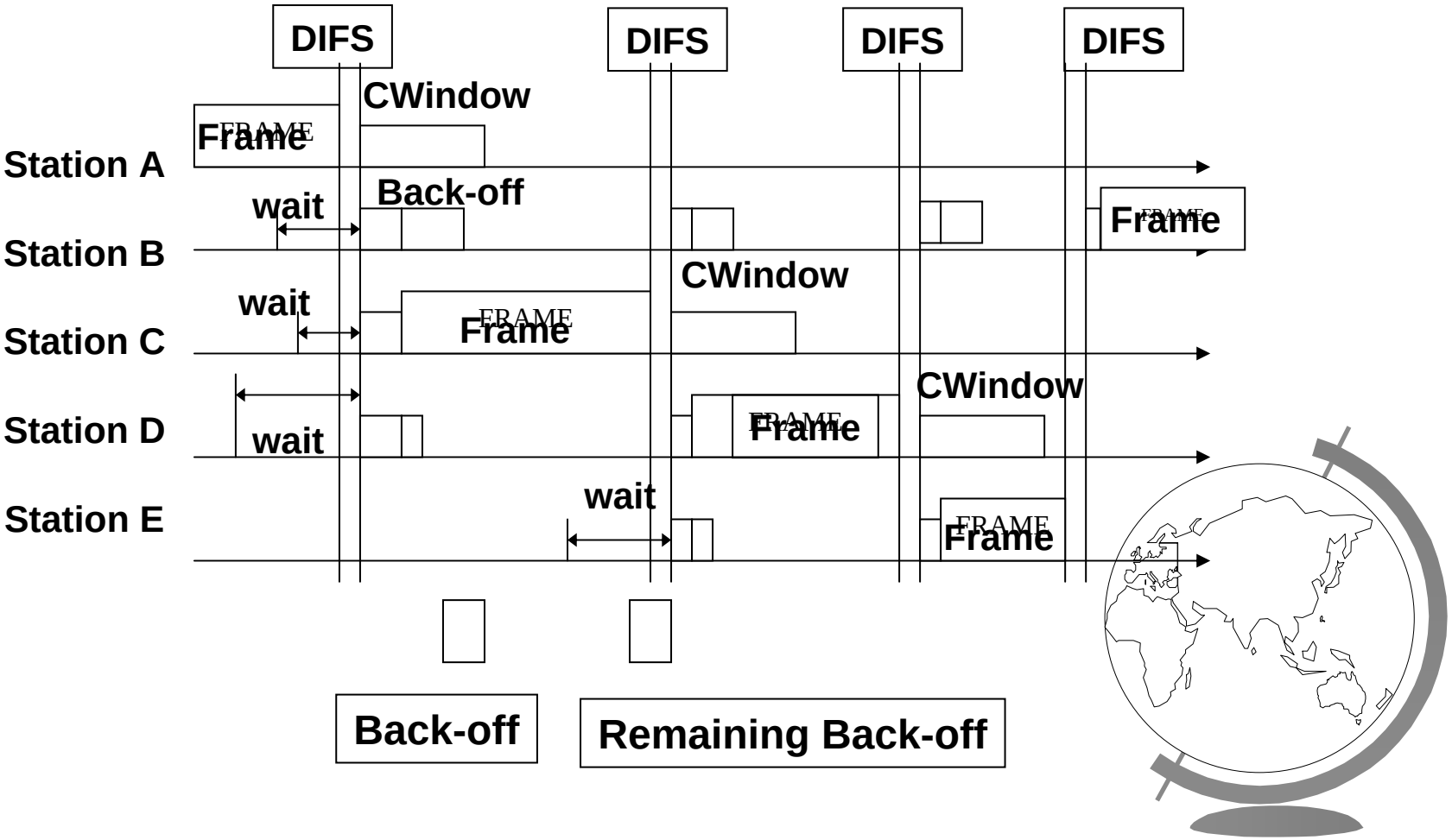
- Il protocollo DFWMAC adotta differenti livelli di priorità per supportare applicazioni asincrone e real time mediante diversi intervalli di non attività
- Inter Frame Spacing (IFS): intervallo di tempo tra 2 frames ed una stazione sente il canale in accordo a precisi intervalli di tempo

Tre diversi IFS sono stati definiti:

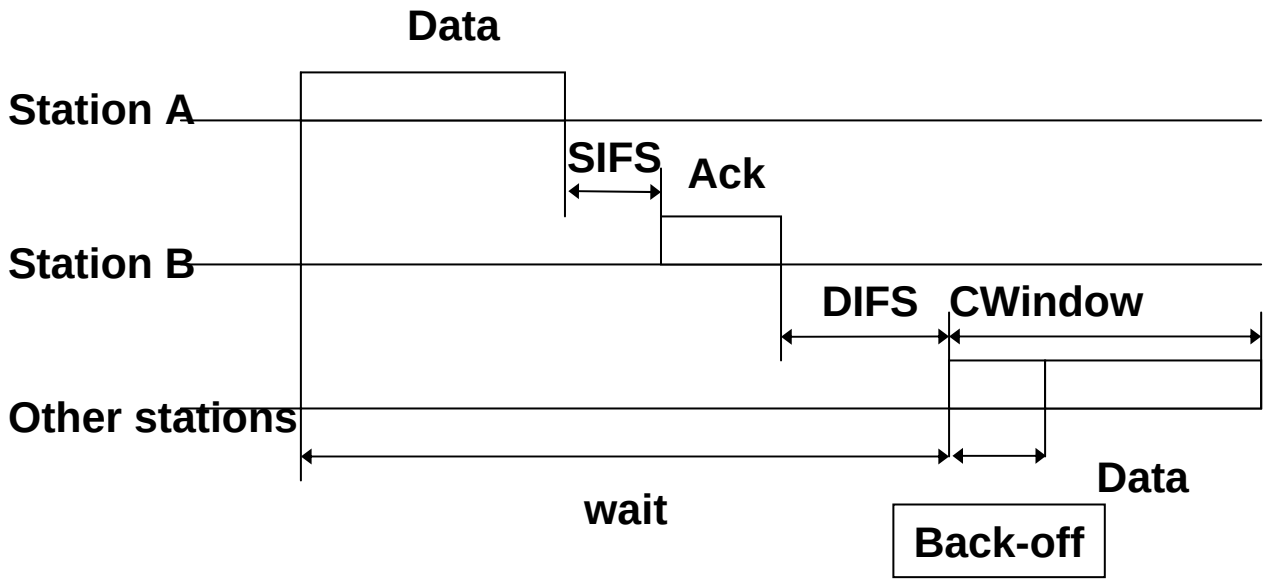
- Short Inter Frame Space (SIFS): per la trasmissione di ACK, RTS, CTS
- PIFS: Point Coordination Function IFS
- DIFS: Distributed Coordination Function IFS

Prima di trasmettere, ogni stazione deve attendere un intervallo pari a DIFS per non collidere con trasmissioni a priorità più elevata, corrispondenti ad intervalli di tempo più corti, i.e. SIFS or PIFS

TIME INTERVALS: Procedura di Back-off



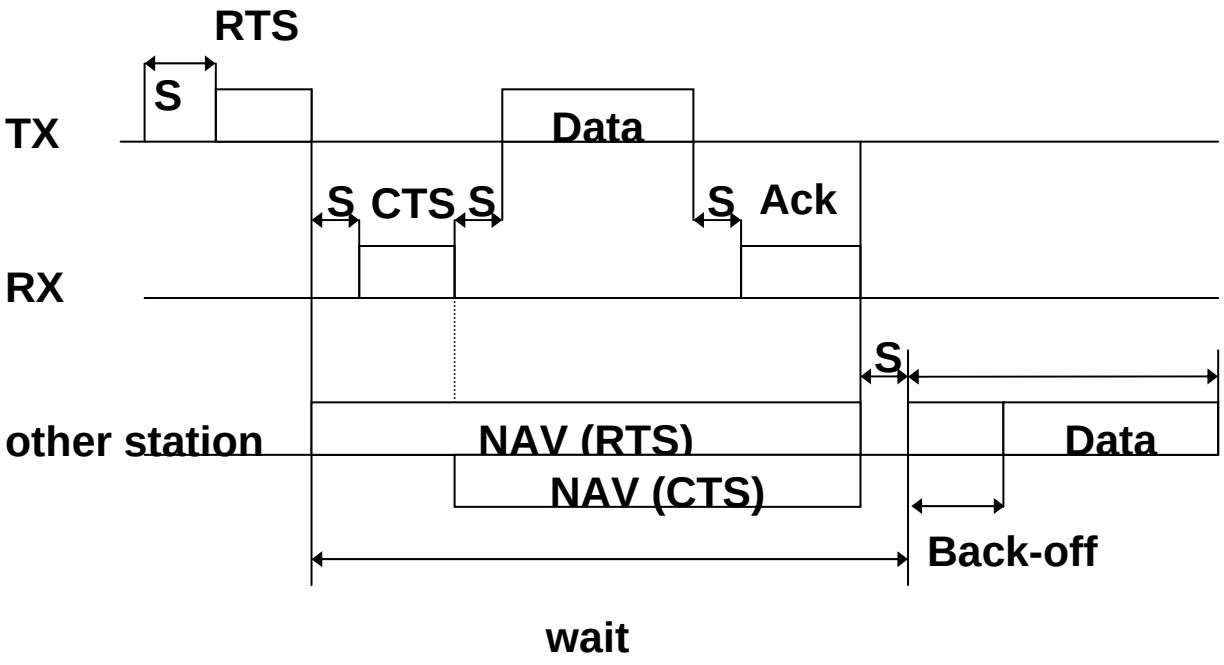
TIME INTERVALS: SIFS and DIFS



Point Control Function

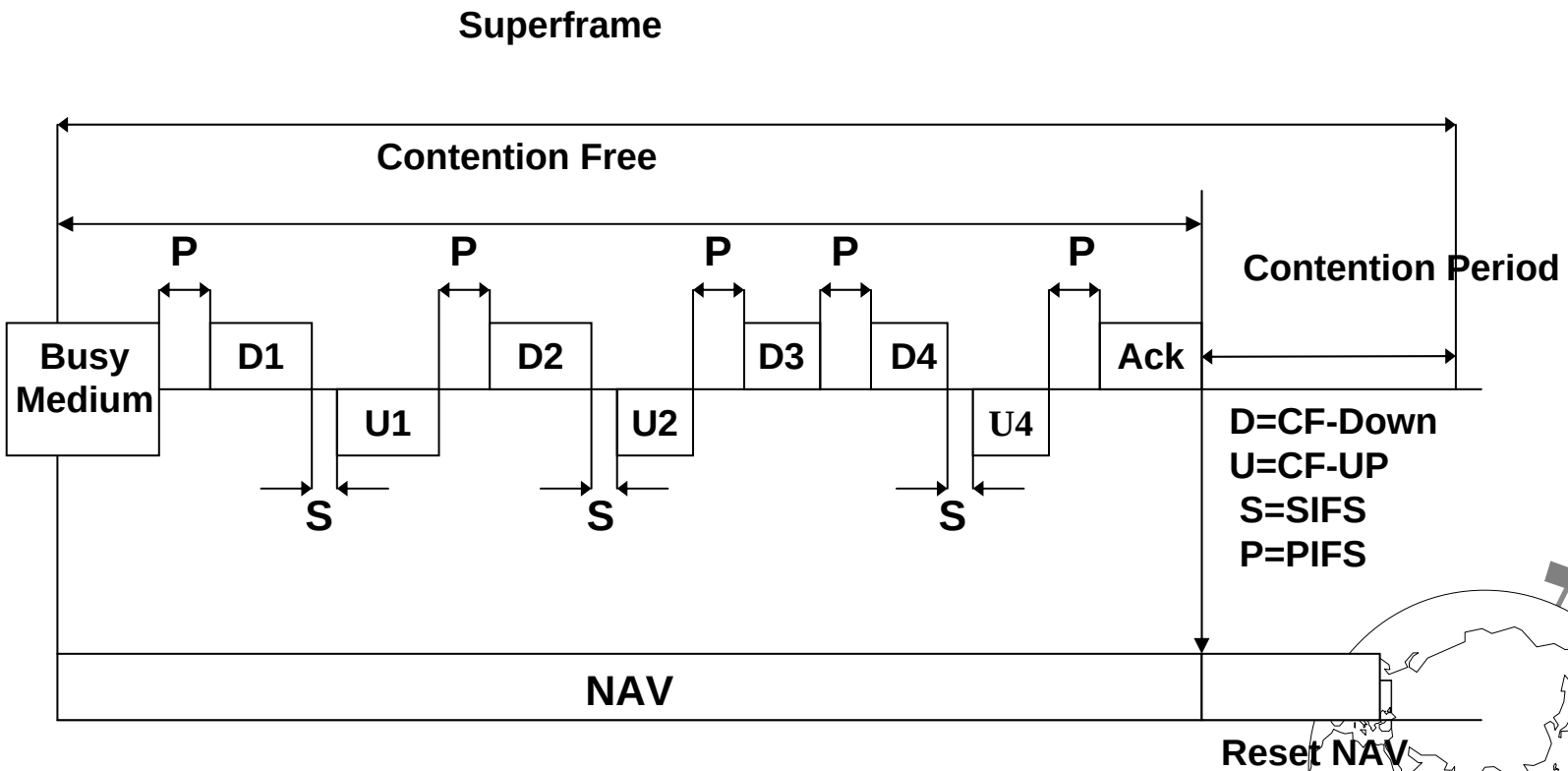
- Una stazione qualsiasi può essere Point Coordinator (PC)
- PC ha priorità più alta perché usa intervalli più corti (PIFS)
- PC agisce su tutte le stazioni in un BSS e di solito è pure l'Access Point
- PC usa meccanismo a polling per evitare la collisione fra stazioni che operano col PCF
- Una stazione, quando è il suo turno, può inviare un frame di dati o un ACK

Net Allocation Vector (NAV)



- Sender transmits RTS frame
- Receiver replies with CTS frame
- Neighbours:
  - see CTS: keep quiet
  - see RTS but not CTS: transmit
- Receiver sends ACK when gets frame
  - neighbors silent until see ACK
- Collisions
  - no collision detection
  - known when CTS is not received
  - exponential back-off

Superframe and PCF protocol



AMBITO NORMATIVO ITALIANO 1/2

- Libero uso su Fondo Privato (D.P.R. 447 art.6 5/10/2001)
  - Sono di libero uso apparecchiature che impiegano frequenze di tipo collettivo, senza alcuna protezione,….come reti locali radiolan (802.11b Wi-Fi)…nell'ambito del fondo

- Autorizzazione Generale negli altri casi (D.P.R. 447 art.5 5/10/2001)
  - È necessaria un'autorizzazione generale per l'installazione e l'esercizio di sistemi che impiegano bande di frequenza colletive….come installazione ed esercizio di reti locali radiolan (802.11b Wi-Fi)…

- NUOVO PIANO RIPARTIZIONE DELLE FREQUENZE (20/7/2002)
  - Disciplina l'uso delle frequenze radio
  - In banda ISM 2.4 GHz è previsto il servizio radiolan per il solo uso Privato ai sensi del DPR 447

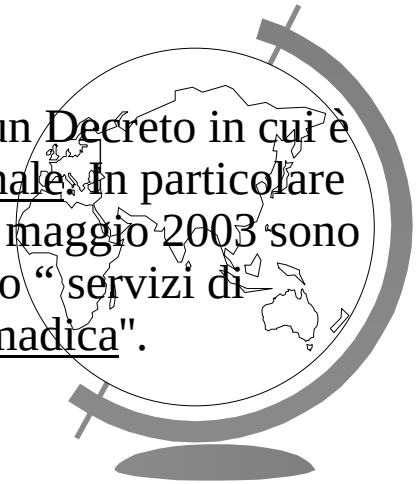
AMBITO NORMATIVO ITALIANO 2/2

Il 28 Maggio 2003 è stato promulgato da parte del Ministero delle Comunicazioni un Decreto Ministeriale di regolamentazione dei servizi Wi-fi ad uso pubblico

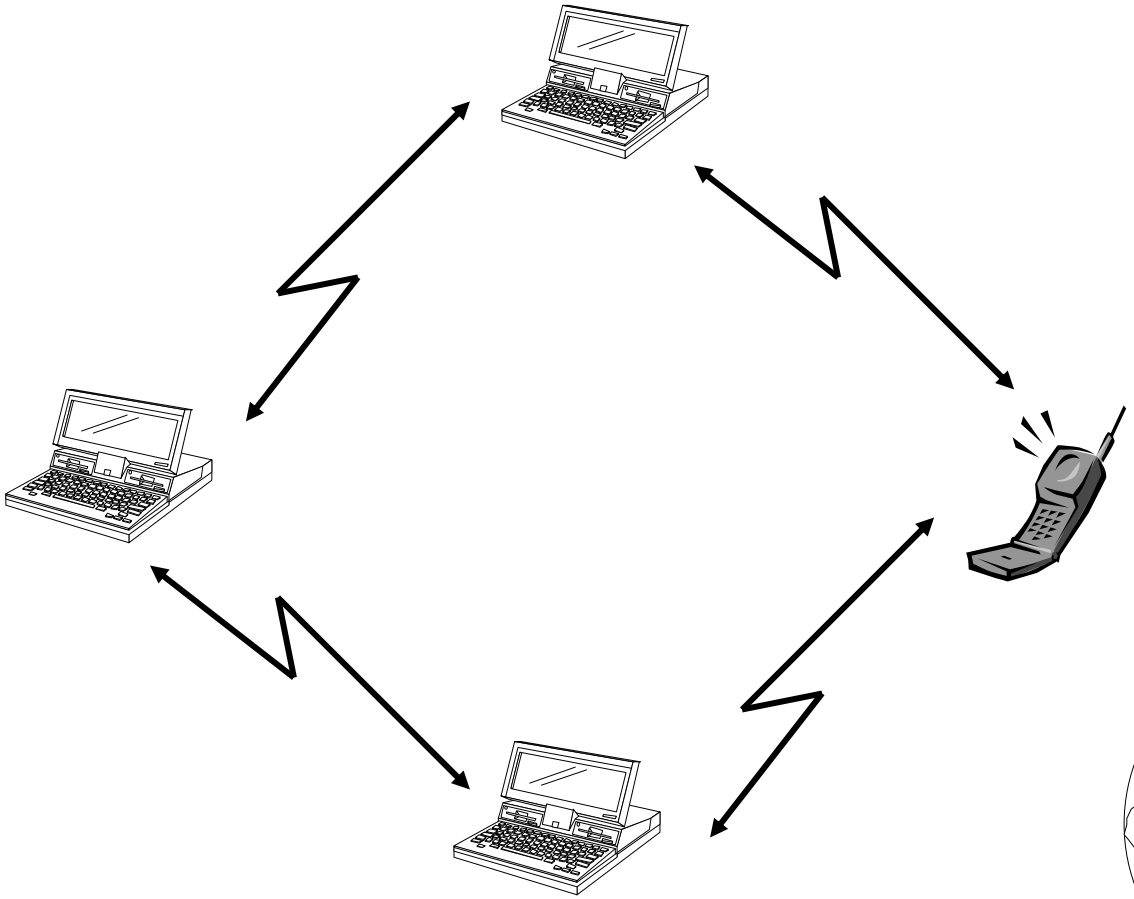
All'art.2 si precisa che:

- Il presente provvedimento fissa le condizioni per il conseguimento dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN nella banda 2.4 GHz o nelle bande 5 GHz, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni, in locali aperti al pubblico o in aree confinate a frequentazione pubblica quali aeroporti, stazioni ferroviarie e marittime e centri commerciali.
- Ai fini della limitazione delle interferenze dannose ad altri servizi previsti dal Piano nazionale di ripartizione delle frequenze, gli access point operanti nella banda 5.150-5.350 MHz possono essere installati all'interno di edifici...

Il 4 Ottobre 2005 il Ministero delle Comunicazioni ha promulgato un Decreto in cui è stata estesa la regolamentazione del Wi-Fi a tutto il territorio nazionale. In particolare all'art.1 si dice che "All'art. 2, comma 1, del decreto ministeriale 28 maggio 2003 sono soppresse le parole da “locali aperti”, fino alla fine del comma; dopo “ servizi di telecomunicazioni” si aggiungono le parole “in modalità fissa e nomadica".



BLUETOOTH



Bluetooth Networking

- Il nome
  - Harald Blatand “Bluetooth”, Vichingo e Re di Danimarca (940-981)

- IEEE 802 project
  - **802.15:** *Wireless Personal Area Network*

Bluetooth SIG

- The Bluetooth Special Interest Group SIG comprende le industrie promotrici:
  - 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia e Toshiba, e
  - più di 2000 aziende collegate
- SIG obiettivo:
  - guidare l'evoluzione della tecnologia e
  - proporla sul mercato

Bluetooth Networking?

- Personal Area Network
  - veloce setup di una PAN
    (es. cellulare + PC + stampante)
- Accesso a LAN/ WAN
  - sostituzione di cavi...
- Conferenze, meeting, riunioni,...
- Giochi interattivi ad-hoc
- Home Networks:
  - interconnessione e controllo apparecchi domestici
  - applicazioni industriali
  - controllo remoto di robot

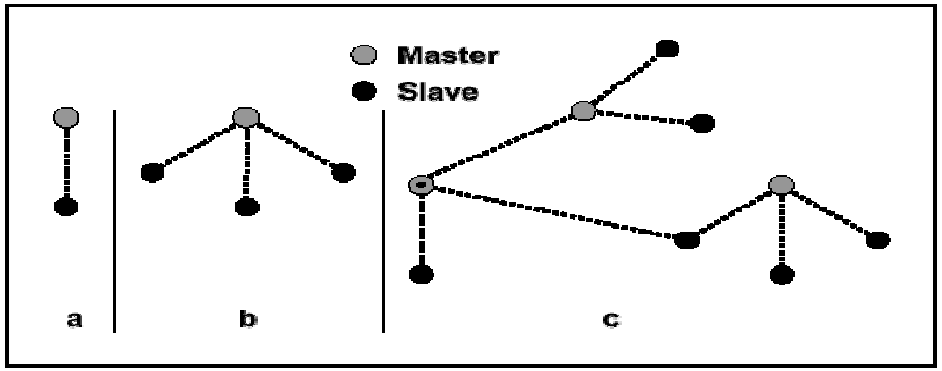
Bluetooth

- 2.4 GHz ISM (Industrial Scientific Medicine):
  - banda senza licenza, 89 MHz di spettro disponibile
- tecnica FH - SS (1600 hops/ s su 79 distinte sottobande, ognuna larga 1 MHz)
  - USA, Europa :

    2.400 - 2.4835 GHz
- velocità lorda: 1 Mbit/ s
- schema di modulazione : GFSK, con indice compreso tra 0.28 e 0.35

BLUETOOTH

- ✓ A short range (10-100 m) and low-cost wireless network system to replace cables and give RF connection between consumer devices
- ✓ Allows creation of small ad hoc networks (***piconets)*** consisting of at most 8 simultaneously active devices (1 master+up to 7slaves)
- ✓ Many piconets may coexist in the same area (interconnected or not) ⇒ ***scatternet***.
- ✓ All devices are identical and have the same probability to be a master or a slave in a piconet
- ✓ Dynamic reconfigurability gives a very flexible system suited to many environments.



Inter-Piconet Communication

- A slave can belong to two different piconets, but <u>not at the same time</u>
- A slave can leave its current piconet (after informing its current master about the duration of the leave) and join another piconet
- A master in one piconet can also act as a slave in another piconet

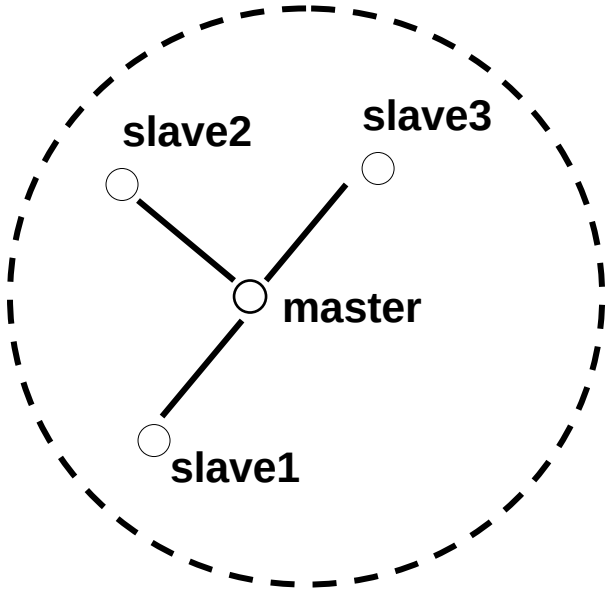
SCATTERNET

Each piconet in a scatternet uses a different hopping sequence

Since two independently chosen hopping patterns may simultaneously select the same frequency with non-zero probability, some collisions between piconets are possible, thus reducing effective throughput

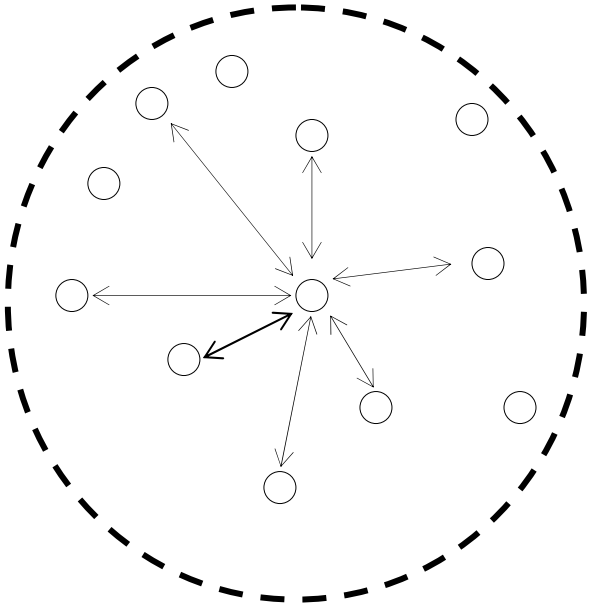
Topologia di Rete - Piconet

- Una piconet è l'unità base
  - creata ad-hoc
  - sul concetto master/slave
  - master e slaves sono identici, ma con ruoli distinti basati su:
    - polling e reservation
  - slaves sono identici, ma possono avere diversi profili di traffico



Piconet: creazione

- Set-up ad-hoc
  - nodo qualunque può essere il master
  - il master determina lo schema di FH, quindi ogni piconet è definita dalla sua sequenza di frequency hopping
  - tutte le unità Bluetooth della piconet sono tempo e hop sincronizzate sul canale



- **master**
- **active slaves**
- **parked slaves**
- **standby, connecting slaves**

BLUETOOTH: POSSIBILI SCENARI

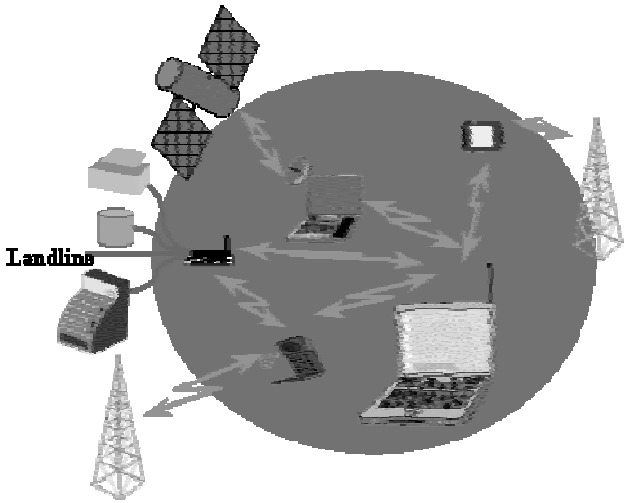


Figure 1: Voice/data access points

Figure 2: Peripheral interconnects

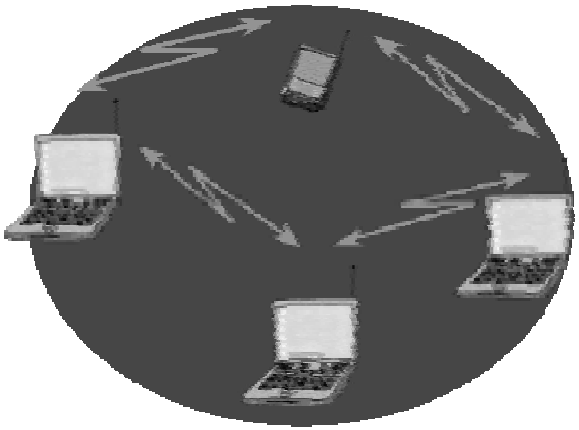
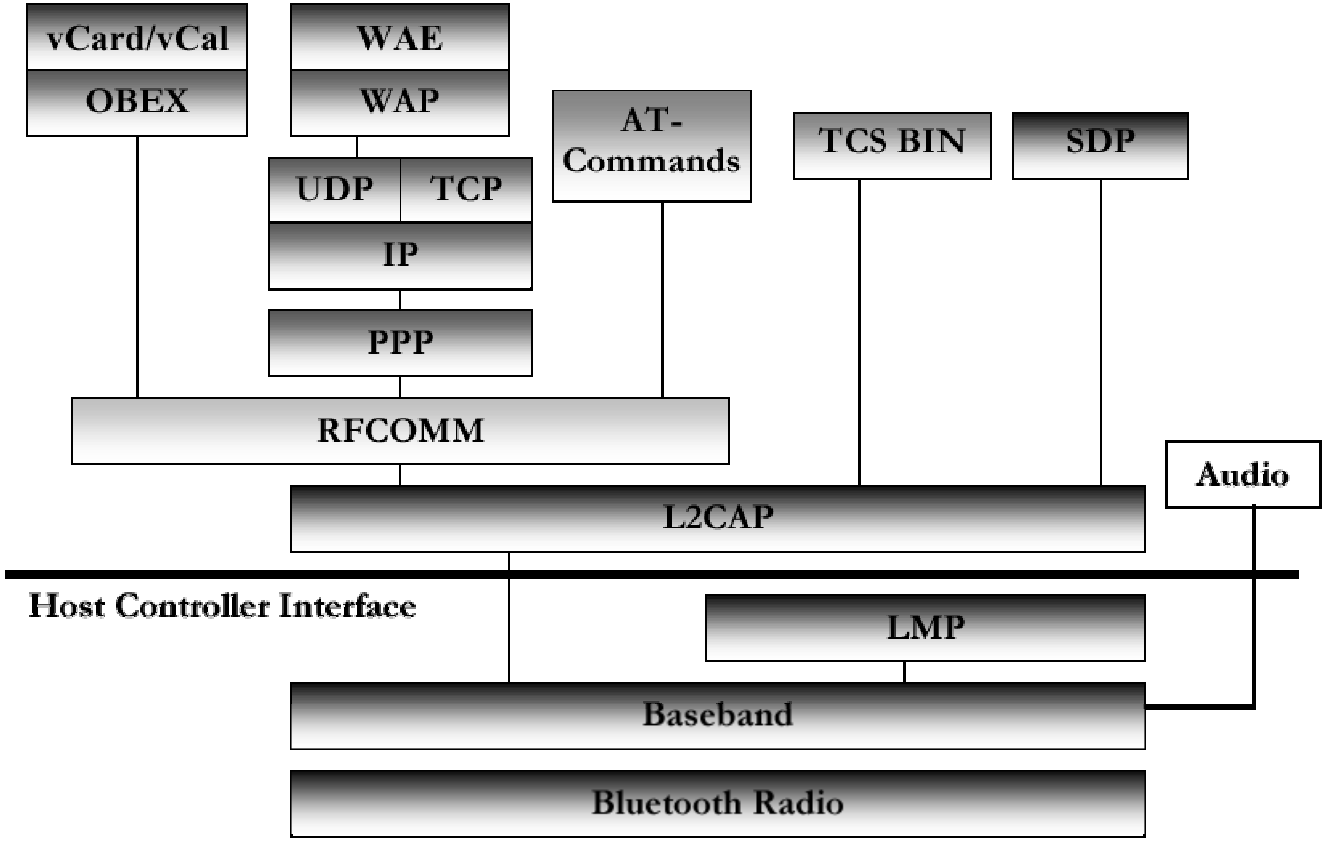


Figure 3: Personal Area Networking (PAN)

PROTOCOL STACK



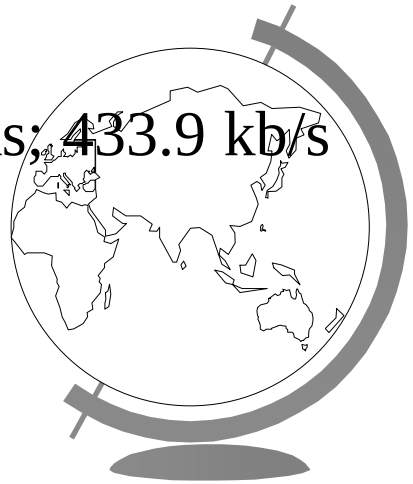
CANALE RADIO

✓ ISM (Industrial, Scientific and Medical) licence free band [2,4 - 2,483] GHz divided in 79 channels spaced by 1MHz

✓ Channel is temporally slotted (slots duration= 625 μs, frequency hopping=1600 hops/sec)

✓ Access: FH-CDMA Spread Spectrum can be used to minimize power waste and guarantee robustness to interference

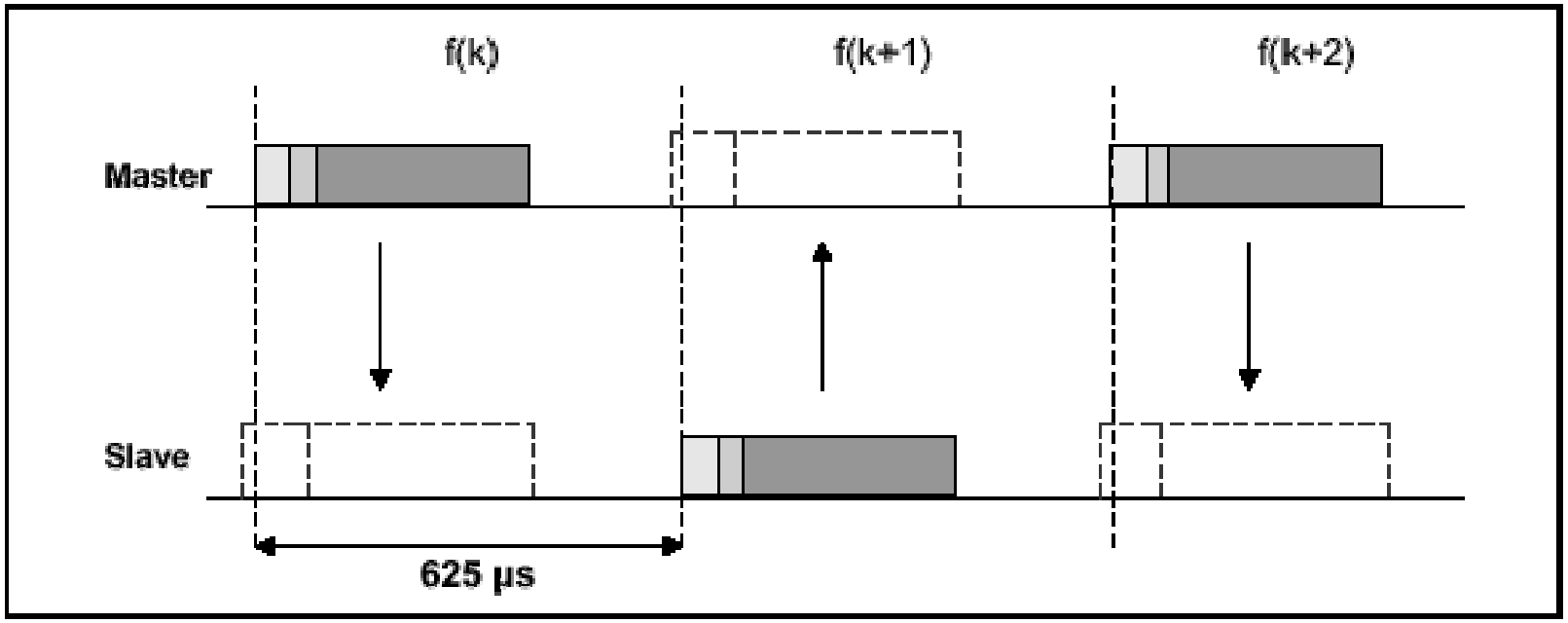
✓ Bandwidth: ≤ 1 Mbit/s (723.2 kb/s asymmetric links; 433.9 kb/s simmetric links)



CANALE FISICO

✓ A packet is transmitted, after each hop, within a single radio channel

✓ *Hopping Sequence*, that is only related to master's hardware address, is used to select the next radio channel

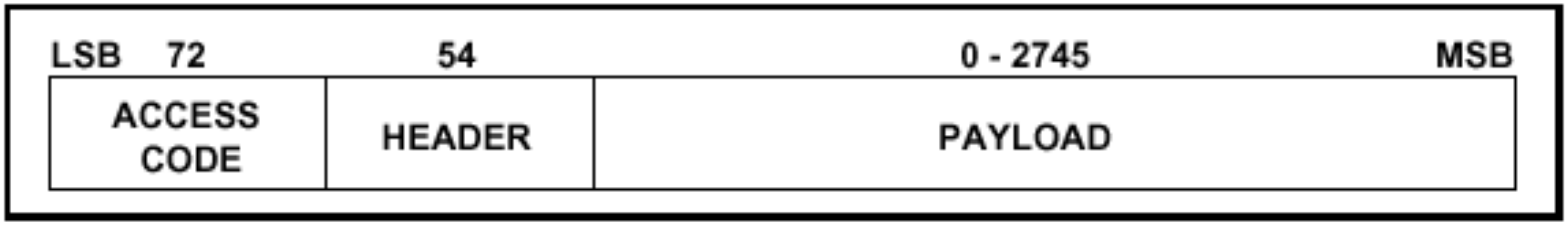


CANALE FISICO

Due tipi di collegamenti master-slave:

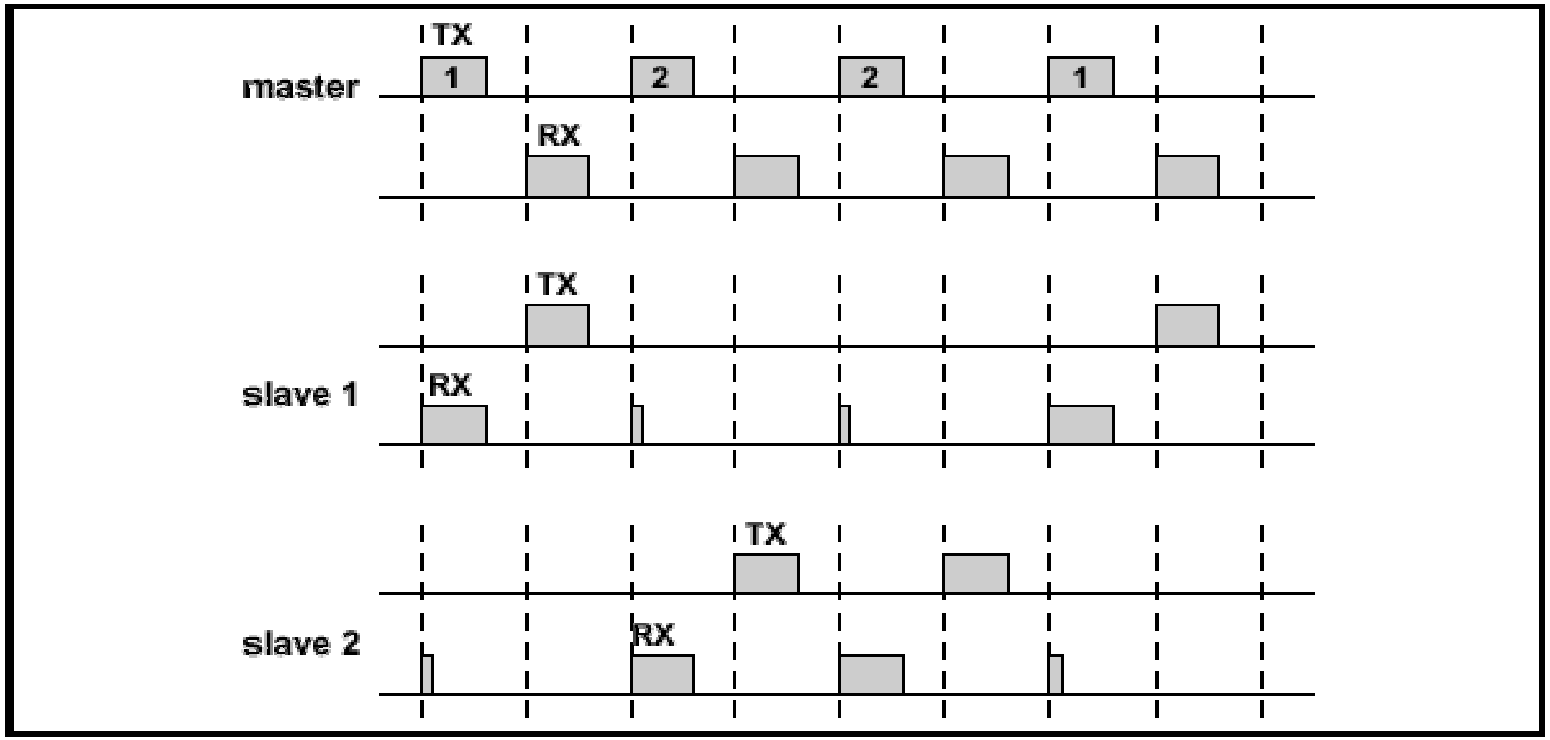
1. SCO (Synchronous Connection-Oriented)
2. ACL (Asynchronous Connection-Less)

pacchetto Bluetooth :

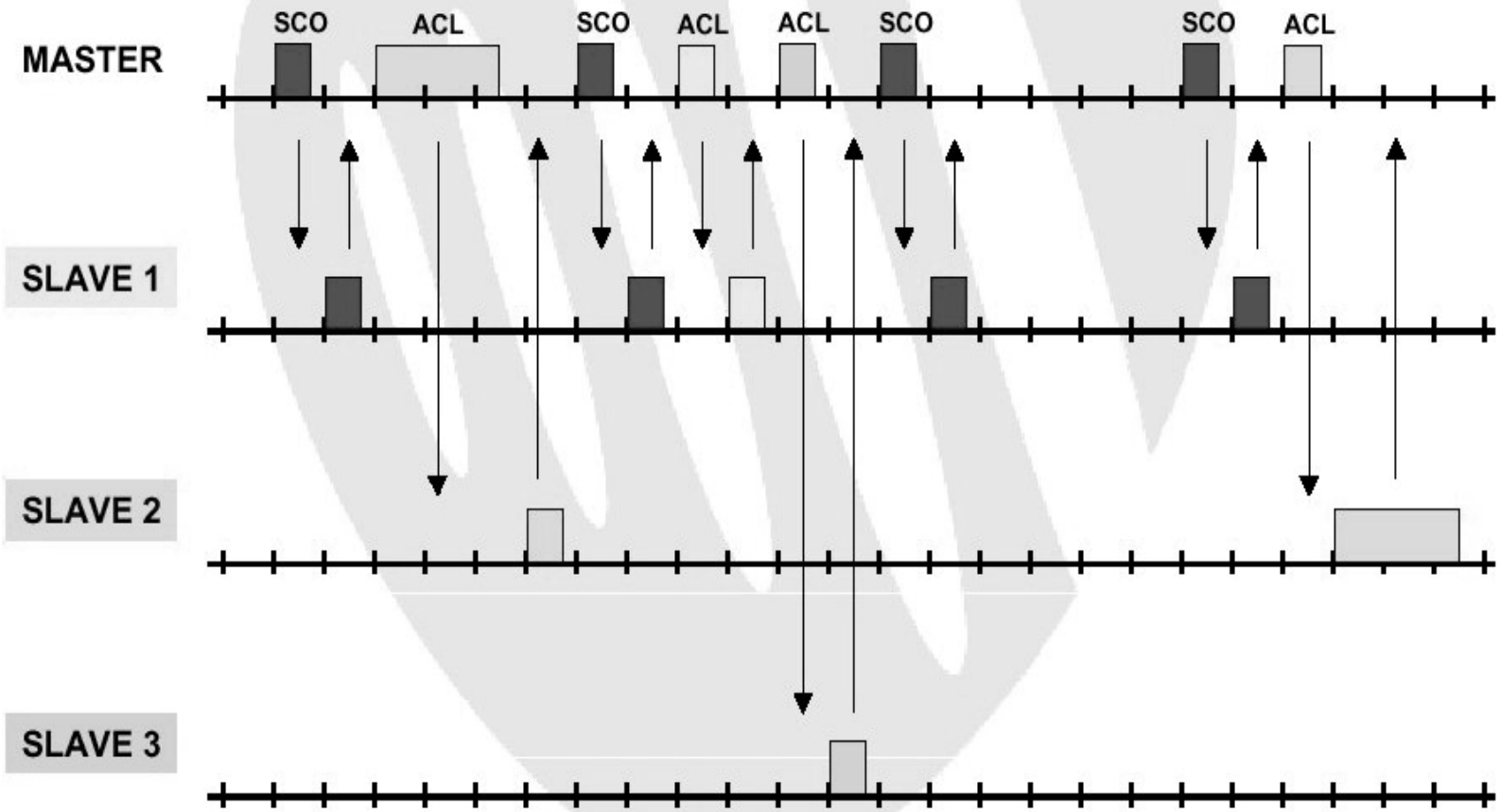


A slave can only transmit in the slot successive to that in which a poll packet was received from the master without transmission errors.

Example of a 3 units piconet



MIXED LINK EXAMPLE



INQUIRY

<u>Used to discover other devices and exchange synchronization</u>
(hardware address and clock)

• Asymmetric procedure

▪ To exchange information two nodes must agree on a common channel-hopping sequence

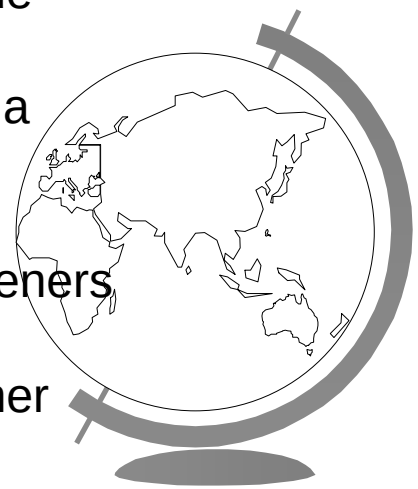
▪ Listener and sender hop using the same sequence but the sender hops faster than the listener

▪ When more than one listener are present, their replies may collide

▪ To avoid collisions, listeners defer their replies until expiration of a random back-off timer

▪ The sender collects device address and clock offset from the listeners

▪ This information is subsequently used to page the selected listener



PAGING

Used to establish connections and to define roles

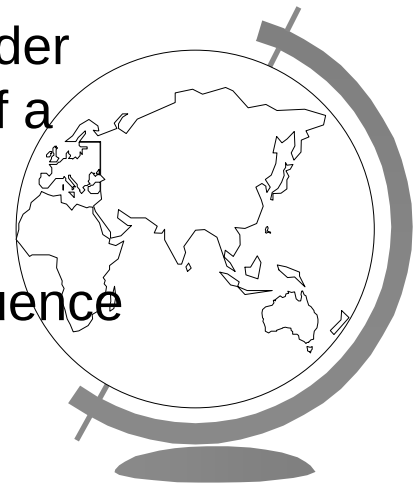
- Steps similar to Inquiry

- Exception: paging message is unicast to a selected listener ⇒ listener needs not back-off before replying

- The sender has also an estimate of the listener's clock ⇒ is enabled to communicate with the listener almost istantaneously

- Upon receiving an ACK for the paging message, the sender becomes the master and the listener becomes the slave of a newly formed piconet

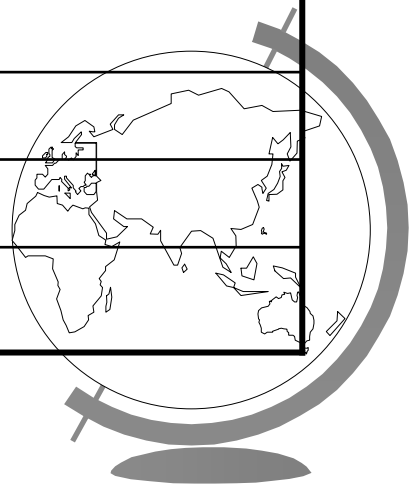
- Both nodes switch to the piconet's channel-hopping sequence



IEEE 802.15

IEEE 802.15 working group was created to develop a set of standards for short range wireless communication referred to as WPAN

Task Group	Goal
IEEE 802.15.1	Deriving a Wireless Personal Area Network standard based on the Bluetooth Specifications.
IEEE 802.15.2	Facilitating coexistence of WPAN and WLAN.The coexistence model tries to quantify the mutual interference of the two.
IEEE 802.15.3	Drafting and publishing a new standard for high-rate (20Mbit/s or greater) WPANs.
IEEE 802.15.4	Providing a standard for low data-rate wireless connectivity (LR-WPAN).

Bluetooth vs IEEE 802.11

Property	BT	IEEE 802.11b
Application	Cable replacement technology	Wireless version of Ethernet LAN
Type of devices	Ideal for Cellular Phones	Limited applicability for handheld devices
Bandwidth	ISM	ISM
Range	<10 meters	>100 meters
Data rate	1 Mbps	11 Mbps
Power Consumption	Limited	Expensive
Physical layer	FH-SS	DS-SS
Type of use	Very simple	Complex