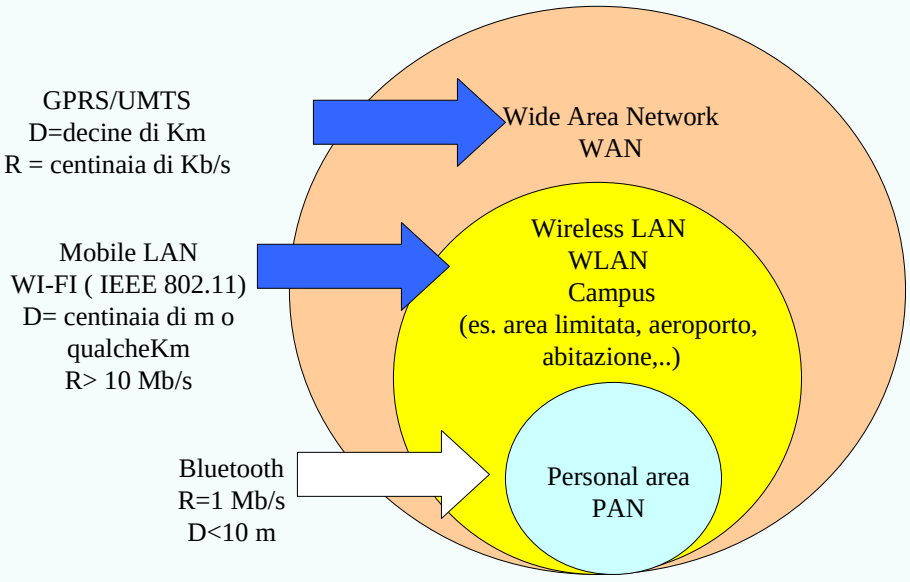
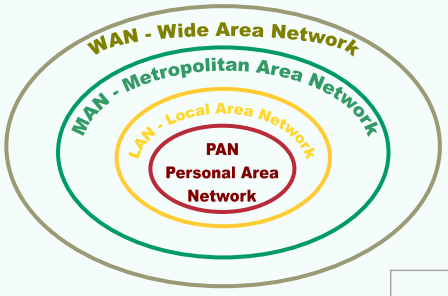
Wireless LAN
(WLAN)



Reti WLAN



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Speed	< 1 Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384 Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	Fixed, last mile access	PDAs, Mobile Phones, cellular access

Introduzione alle wireless LAN

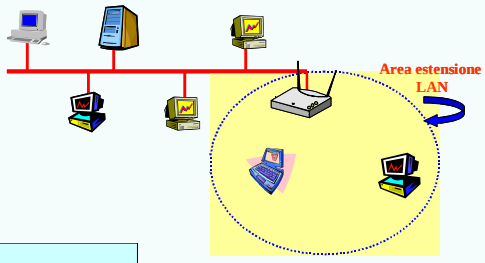
- Le reti locali wireless, indicate anche con la sigla WLAN (o Wireless LAN), rappresentano oggi soluzioni a basso costo per consentire l'accesso di un utente da qualunque posizione nell'area di copertura della rete stessa.
- Le WLAN hanno avuto un forte sviluppo negli ultimi anni grazie sia allo sviluppo di nuove tecnologie di comunicazioni mobili, sia alla disponibilità di terminali mobili sempre più potenti ed evoluti (esempio, PDA, notebook,…).
- Le WLAN presentano i seguenti vantaggi rispetto alle reti LAN cablate:
  - Non richiedono la cablatura di un ambiente
  - L'utente può accedere senza vincoli spaziali alla rete Internet o ad altre reti.

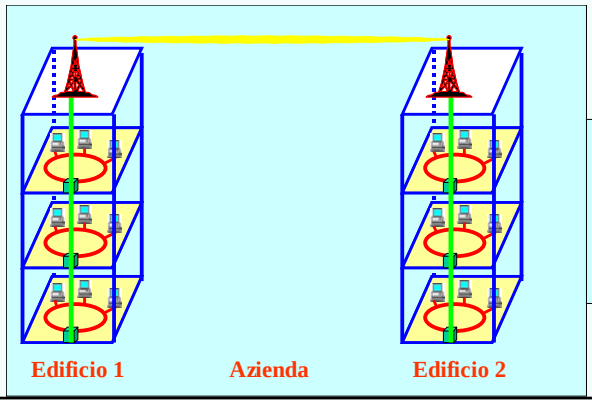
Applicazioni delle reti WLAN

- Le reti wireless LAN possono essere utilizzate per varie applicazioni:
  - Estensione di una rete locale;
  - Collegamento tra due sedi di una struttura;
  - Realizzazione di una rete locale dove non è possibile realizzare un cablaggio a causa di motivi architettonici (esempio in musei o ambienti storici)

Applicazioni delle reti WLAN

Estensione di una rete LAN in ambienti non cablati





Collegamento tra LAN in edifici diversi

Perché senza fili?

Aspetti salienti dei sistemi di telecomunicazioni senza fili odierni

- Unico investimento iniziale;
- Rapporto **QUALITÀ/PREZZO** più vantaggioso rispetto a molti sistemi cablati;
- Installazione rapida ed economica;
- Costi di manutenzione irrisori;
- Capacità trasmissiva elevata per dati e fonia;
- Elevata flessibilità e versatilità d'uso;
- Investimento riutilizzabile.



I sistemi di telecomunicazioni senza fili sono sicuri

Un telefono cellulare irradia dalle 20 alle 2000 volte la potenza irradiata dai comuni apparati per telecomunicazioni senza fili. Più precisamente:

- Potenza massima irradiata da un telefono cellulare GSM: **~ 2 Watt**;
- Potenza massima irradiata da un apparato per telecomunicazioni senza fili in tecnologia Spread Spectrum: **0.001 ÷ 0.1 Watt**.

Inoltre, l'intensità della radiazione emessa è inversamente proporzionale al quadrato della distanza

Alcune possibili applicazioni

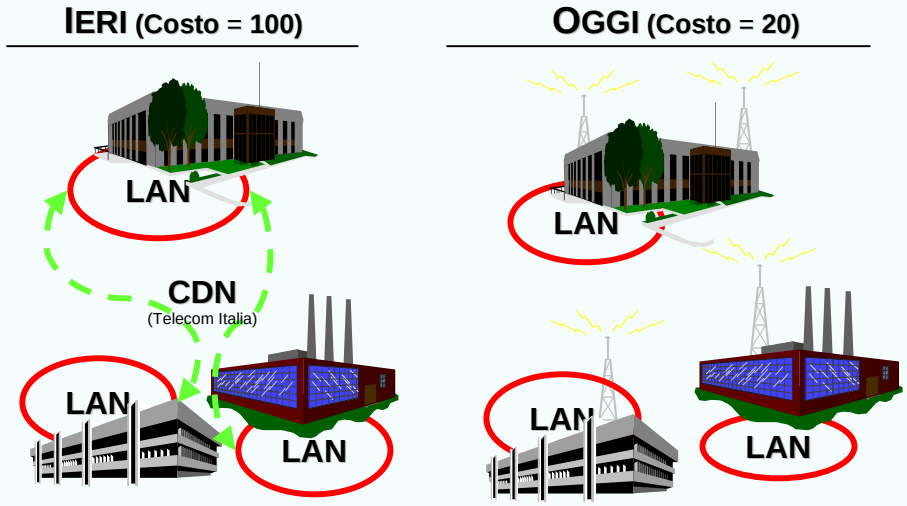
Utilizzo del wireless dove il cablato non è utilizzabile con successo:

- Collegamenti e reti per utenti in movimento;
- Realizzo di collegamenti, od intere reti, in tempi molto brevi (es. poche ore);
- Collegamenti di siti remoti non serviti da cavi;
- Sistemi di telecomunicazioni a carattere temporaneo: riutilizzo degli apparati, rapida riconfigurazione ed espansione delle reti.

Valutazione aziendale

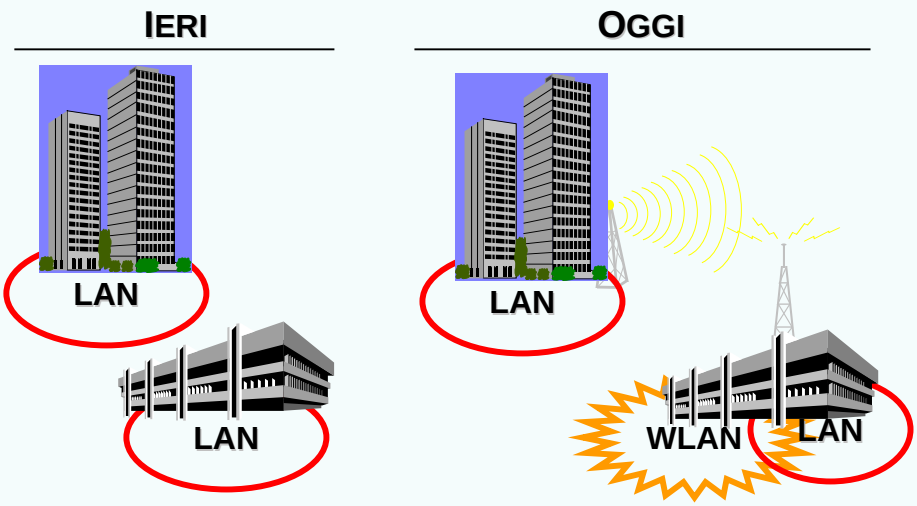
In alternativa all'acquisto di servizi di telecomunicazioni un'azienda può dotarsi di una propria rete di telecomunicazioni realizzata via cavo e via sistemi senza fili, per avere migliori prestazioni o costi complessivamente minori

MaxMara: Ponti radio outdoor



CDN: Linee digitali dedicate; LAN: Rete Locale Cablata

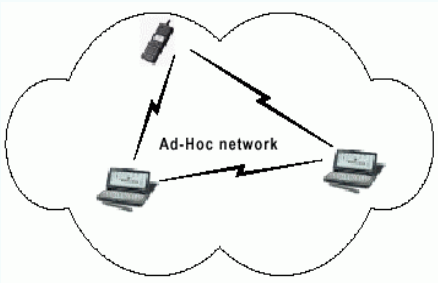
ISTAT: Reti senza fili in/outdoor



LAN: Rete Locale Cablata; WLAN: Rete Locale via radio

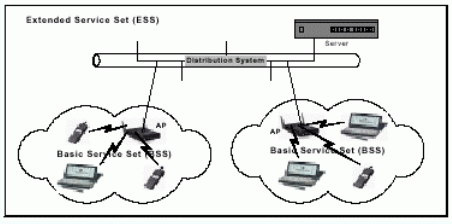
Reti Ad Hoc

- La comunicazione avviene tra i singoli terminali wireless
- Non è previsto accesso alla rete cablata
- Contesto di fiducia reciproca



Reti strutturate

- La rete è organizzata in celle, ciascuna governata da un Punto di Accesso (**AP** – **Access Point**)
- L'AP rappresenta il bridge tra rete cablata e wireless
- L'AP sovraintende alle comunicazioni tra i singoli apparati
- L'AP gestisce il **"roaming"** degli utenti



Caratteristiche dei sistemi Radio Narrow Band

- Capacità trasmissiva: da 2 x 2 Mbps a 2 x 622 Mbps;
- Portate molto lunghe, fino a 100 km per passo di ripetizione (50 km secondo le norme ITU);
- Supporto di tutti i protocolli: asincroni, sincroni ed isocroni;
- Operatività assolutamente sicura, affidabile e protetta dalla Legge;
- Manutenzione: minima, limitata al controllo periodico.

Applicazioni dei sistemi Radio Narrow Band

I sistemi per telecomunicazioni Radio Narrow Band sono particolarmente indicati per:

- Trasporto di fonia e dati critici con Qualità di Servizio (QoS) e Classe di Servizio (CoS) ben definibili e stabili nel tempo;
- Dorsali geografiche ad alta capacità;
- **Collegamenti di qualsiasi tipo, fino a 150 km in tratta singola**.

Caratteristiche dei sistemi Radio Spread Spectrum

- Capacità trasmissiva:
  - Sistemi asincroni: da 1 x 354 kbps a 3 x 11 Mbps;
  - Sistemi isocroni: da 1 x 2 Mbps a 2 x 2 Mbps;
- Portate fino a 20 km (fino a 40 km a bassa velocità);
- Supporto dei protocolli asincroni e isocroni;
- Operatività soggetta regolamentata da Direttiva Europea 99-05 (R&TTE) e Decisione ERO 96-17;
- Manutenzione: minima, limitata al controllo periodico.

Applicazioni dei sistemi Radio Spread Spectrum

I sistemi per telecomunicazioni Radio Spread Spectrum sono particolarmente indicati per:

- Trasporto di fonia e dati critici con Qualità di Servizio (QoS) e Classe di Servizio (CoS) ben definibili e stabili nel tempo;
- Tratte medie a media capacità;
- Collegamenti di Wireless Local Loop (WLL);
- **Collegamenti di qualsiasi tipo fino a 15 km**.

Applicazioni dei sistemi senza fili

Lunghezza collegamento	Tecnologia consigliata
Breve (Fino a 1÷2 km)	**Ottica** (LED o LASER) **Radio** Spread Spectrum
Media (Fino a 10÷15 km)	**Radio** Spread Spectrum **Radio** Narrow Band
Grande (Oltre 5 km)	**Radio** Narrow Band



Storia WLAN

- 1990 : Motorola crea una prima rete WLAN commerciale
- 1990 : IEEE inizia la progettazione di una rete wireless mediante il gruppo IEEE 802.11
- 1997: IEEE rilascia lo standard 802.11
- 1999: IEEE rilascia lo standard 802.11a

Le tecnologie trasmissive

- Le reti WLAN possono essere realizzate mediante due diverse tecnologie:
  - Tecnologie radio: sono soggette a norme molto precise per evitare interferenze con altri servizi e problemi di inquinamento elettromagnetico; le bande radio di trasmissione sono spesso sature.
  - Tecnologie ottiche: presentano numerosi problemi su distanze superiori a qualche Km e risentono di condizioni atmosferiche particolari, come la presenza di nebbia.

- Le reti WLAN radio utilizzano presenti oggi sul mercato utilizzano prevalentemente la banda di frequenze ISM (Industrial –Scientific – Medical band) composta dalle seguente zone:
  - 902 – 928 MHz
  - 2,400 – 2,480 GHz
  - 5,150 – 5,250 GHz

Evoluzione delle reti WLAN

- Le reti WLAN sono state sviluppate in primo luogo dal gruppo IEEE 802.11, che è stato costituito nel 1989 e che ha sviluppato diverse classi di reti.

WLAN standardizzate da IEEE 802.11

Rate fino a **54 Mbps**
Compatibile con 'b'

- ***IEEE 802.11 (1997):*** questa rete opera ad una velocità di 2 Mb/s nella banda di frequenze ISM (2,4 - 2,4835 GHz)
- ***IEEE 802.11b (Wi-Fi):*** questa rete, nota con la sigla Wi-Fi, opera ad una velocità massima di 11 Mb/s (ma anche 5,5, 2 e 1 Mb/s) nella banda di frequenze ISM (2,4 - 2,4835 GHz)
- ***IEEE 802.11a (WI-FI 5):*** questa rete opera nella banda 5-40 GHz e presenta una velocità fino a 54 Mb/s
- ***IEEE 802.11g:*** questa rete presenta una velocità fino a 54 Mb/s e risulta compatibile con la rete 802.11b e 802.11a.

Caratteristiche delle reti WLA IEEE 802.11

	802.11	802.11a	802.11b	802.11g
Approvazione standard	Luglio 1997	Settembre 1999	Settembre 1999	Giugno 2003
Larghezza di banda	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Frequenze di lavoro e tecnologia	2.4-2.4835 GHz DSSS e FHSS	5.15-5.35; 5.725-5.825 GHZ OFDM	2.4-2.4835 GHz HR-DSSS	2.4-2.4835 GHz DSSS e OFDM
Numero di canali non sovrapposti	3 *indoor/outdoor*	4 *indoor* (UNII1) 4 *indoor/outdoor* (UNII 2) 4 *outdoor* (UNII 3)	3 *indoor/outdoor*	3 *indoor/outdoor*
Tipi di modulazione	**DQPSK** (DSSS 2 Mbps) **DBPSK** (DSSS 1 Mbps) **4GFSK** (FHSS 2 Mbps) **2GFSK** (FHSS 2 Mbps	**BPSK**(6, 9 Mbps) **QPSK** (12, 18 Mbps) **16-QAM** (24, 36 Mbps) **64-QAM**(48, 54 Mbps)	**DQPSK/CCK** (11,5.5 Mbps) **DQPSK** (2 Mbps) **DBPSK** (1 Mbps)	**OFDM/CCK** (6,9,12,18,24,36,48, 54 Mbps) **OFDM** (6,9,12,18,24,36,48, 54 Mbps) **DQPSK /CCK** (33,22,11,5.5 Mbps) **DQPSK** (2 Mbps)

Regolamentazione in Italia

- **In Italia, l'installazione e l'esercizio di sistemi che impiegano bande di frequenze di tipo collettivo, ovvero condivise, sono disciplinati dal Regolamento Licenze Individuali ed Autorizzazioni Generali di Telecomunicazione - DPR 447 del 5-10-2001 (GU 300 del 28-12-2001)**
- **La normativa è conforme al Piano Nazionale Ripartizione delle Frequenze (D. M. del 8-luglio-2002 e successive**

Regolamentazione in Italia

- **Le norme in Italia prevedono :**
  - **in ambito privato (all' interno di un edificio o di un singolo ufficio) le Wireless LAN, come strumento di accesso alla rete, sono di libero uso e possono essere utilizzate senza alcuna formalità burocratica;**
  - **tra edifici diversi che insistono su di un sito facente capo alla medesima proprietà degli edifici stessi le Wireless LAN, utilizzate come strumento di connessione tra le reti fisse dei singoli edifici, sono altresì di libero uso;**
  - **Le Wireless LAN utilizzate come strumento di connessione tra reti fisse di singoli edifici (ambito privato) divisi dalla presenza di suolo pubblico, sono assoggettate alla disponibilità di un'autorizzazione generale.**
  - **Le Wireless LAN di operatori WISP utilizzate per la fornitura dell'accesso al pubblico (nella banda 2.4 GHz e 5 GHz) alle reti e ai servizi di telecomunicazione in locali aperti al pubblico o in aree confinate a frequentazione pubblica (aeroporti, stazioni ferroviarie, centri commerciali, ecc..) sono assoggettate alla disponibilità di un'autorizzazione generale.**

Regolamentazione in Italia

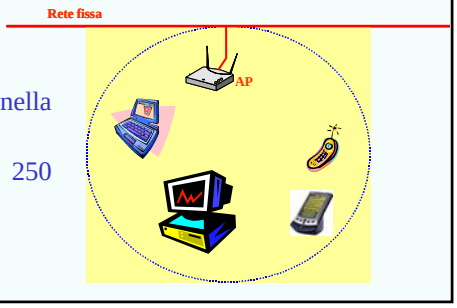
- **Le WLAN operanti nella banda 5.150-3.350 MHz in ambito pubblico, ai fini della limitazione delle interferenze dannose ad altri servizi previsti nel PNRF, possono essere installati solo all'interno di edifici.**
- **Sono in corso studi e sperimentazioni per estendere l'uso di questi sistemi in reti "outdoor" sulla base dello standard 802.11h (standard approvato nel 2003 e che migliora il livello fisico e il livello MAC di IEEE 802.11a nella banda di 5 GHz.**
- **Si sta analizzando la possibilità di uso della banda ISM 5.725-5.875.**

Componenti di una rete WLAN IEEE 802.11

Access Point (AP):

- Un Access Point rappresenta una stazione radio ripetitore del segnale ricevuto che opera normalmente connessa alla rete fissa;
- Un AP consente generalmente di connettere la rete wireless alla rete cablata.
- Gli AP possono essere implementati in:
  - **hardware**
  - **software** utilizzando per esempio un PC, o notebook dotato sia dell'interfaccia wireless sia di una scheda di LAN cablata.





- Un AP gestisce i terminali mobili presenti nella propria cella
- Un AP può gestire in certi casi fino a 250 terminali.

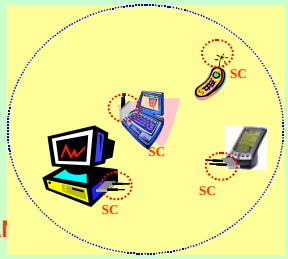
Configurazione di una WLAN

- Una rete WLAN 802.11 e, in particolare Wi-Fi, può essere configurata nei seguenti modi:
  - Peer to peer, in cui due o più terminali mobili dialogano direttamente tra loro;
  - Client e Access Point (AP), in cui le diverse stazioni dialogano tra loro o con una rete fissa mediante un access point
  - Access Point multipli, che consentono il roaming tra le diverse celle controllate da ciascun AP
  - Uso di Extension Point (EP):
  - Uso di antenne direzionali

Configurazione di un a rete WLAN

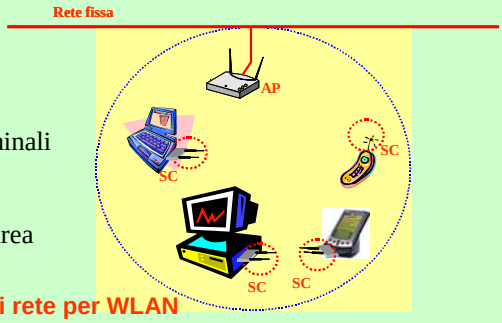
Peer-to-peer

- Due o più terminali mobili stabiliscono una connessione e comunicano direttamente tra loro. Questa rete prende il nome anche di rete ad hoc
- Nell'esempio la cella indica l'area di copertura del notebook
- **SC: Scheda di rete per WLAN**



Client e AP

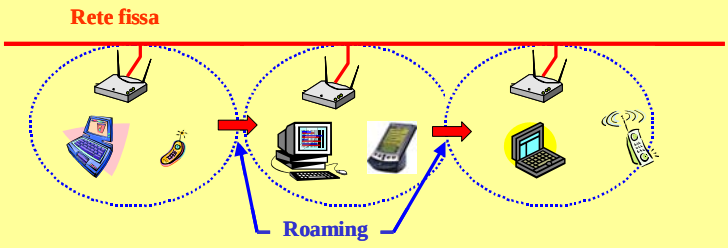
- In questo caso un access point è utilizzato per consentire la comunicazione tra i diversi terminali e tra un terminale e la rete.
- Ogni AP può gestire un piccolo gruppo di utenti (15-50) su un'area che va dai 30 ai 300 metri.
- **SC: Scheda di rete per WLAN**



Configurazione di un a rete WLAN

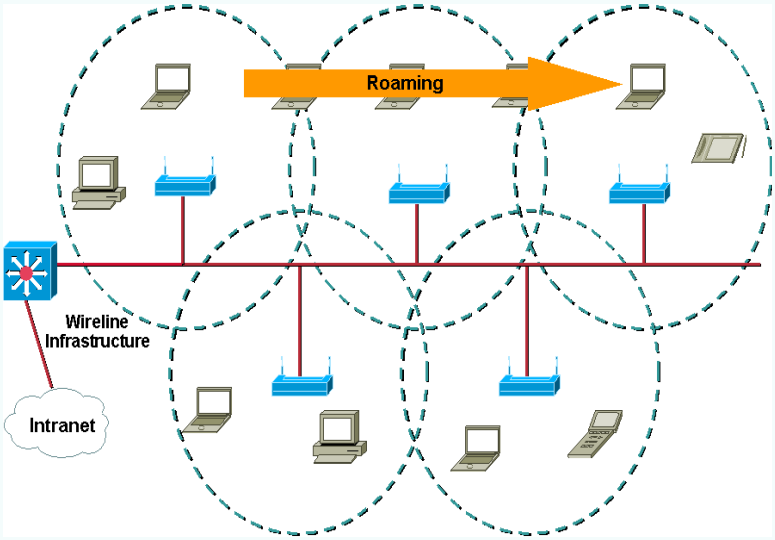
Vari AP e roaming

- Può essere realizzata in questo modo una vera e propria rete locale, le cui dimensioni dipendono dal numero di AP e, quindi di celle, dal numero di utenti e dall'ambiente in cui si vuole realizzare la rete.
- In un ambiente chiuso si può ad esempio mettere un AP per ogni stanza (o gruppi di stanze adiacenti).



- Una soluzione di questo tipo è oggi molto diffusa per l'accesso a Internet in ambienti strutturati, quali aeroporti, alberghi, aziende,..

Rete aziendale WLAN



Wi – Fi
Wireless Fidelity

Caratteristiche di Wi - Fi

- Le frequenze rese disponibili per Wi-Fi in Italia sono 2,4 – 2,4835 GHz
- *Questa banda non è soggetta a licenza* in molti paesi, tra cui l'Italia e può quindi essere usata da chiunque purché siano rispettati i limiti di potenza di trasmissione pari a 100 mW (in Italia)

Sicurezza nelle reti WLAN

- Principali aspetti della sicurezza
  - **Autenticazione**: l'utente dichiara la propria identità. Quando si parla di identità ci si riferisce all'identificazione accurata e certa degli utenti della rete, degli host, delle applicazioni, dei servizi e delle risorse. Le tecnologie standard che permettono questo includono alcuni protocolli di autenticazione come RADIUS (Remote Authentication Dial-In Users Service), Kerberos. Inoltre nuove tecnologie che si fondano su Certificati Digitali, Smart Card e Token si stanno imponendo sempre più nelle soluzioni per la definizione d'identità
  - **Integrità dei dati**: assicurarsi che il messaggio non sia stato modificato nel tragitto.
  - **Segretezza o Riservatezza**: cifrare i dati in modo che non siano intercettati
  - **Controllo Accessi**: gli accessi alle risorse devono essere controllati da e per il sistema.
  - **Disponibilità**: un sistema dev'essere disponibile solo agli utenti accreditati.

Tipi di attacchi

- I tipi di attacchi contro cui è necessario difendersi sono:
  - **Intercettazione**: l'hacker in ascolto può ascoltare e copiare informazioni rimanendo invisibile (*sniffing*).
  - **Modifica**: consiste nell'intercettare un pacchetto, aprirlo, modificarlo, richiuderlo e rispedirlo senza che né mittente né destinatario si accorgano di nulla.
  - **Contraffazione**: consiste nell'invio di falsi messaggi creati ex-novo con le credenzialità di un utente autorizzato dal sistema.

Problemi di sicurezza nello standard IEEE 802.11b

- Banda ISM (Industrial Scientifical and Medical) a 2.4 GHz
  → **interferenza** dovuta a diversi apparati (forni a microonde, cordless, Bluetooth etc.)

- Debolezze del protocollo **WEP:**
  - scelta dell'algoritmo di cifratura dati RC4, non efficiente in un contesto wireless
  - gestione inappropriata della chiave di cifratura dei dati e della **SSID** (**Server Set ID**)
  - lo standard prevede l'utilizzo del WEP solo come **opzione**

SSID (Server Set ID)

- L'SSID identifica univocamente ogni punto di accesso all'interno della rete. Tramite una configurazione corretta, soltanto i dispositivi che utilizzano la corretta SSID possono comunicare con i punti di accesso. Infatti, l'SSID serve come password condivisa tra i terminali ed il loro punto di accesso.
- Quest'ultimo viene configurato con SSID predefiniti, che dovranno essere sostituiti all'atto dell'installazione, per evitare facili attacchi.
- Di seguito vengono riportate le password predefinite più comuni:
  - ***"tsunami"***
    - Punto di Accesso **CISCO AIRONET Serie 340** 11 Mbps DSSS
    - Scheda di rete wireless PCI **CISCO AIRONET Serie 340** – WEP 128 bit
  - ***"101"***
    - Punto di Accesso **3COM AirConnect** 11 Mbps
    - Scheda di rete PCI **3COM AirConnect** 11 Mbps
  - **"*RoamAbout Default Network Name*"**
    - Punto di Accesso **AVAYA ORINOCO AS-2000** (Lucent/Cabletron)
    - Scheda di rete **AVAYA ORINOCO PC Gold Card** (Lucent/Cabletron)
- Gli SSID viaggiano in chiaro sulla rete se il WEP è disabilitato, permettendo quindi la loro cattura monitorando semplicemente il traffico.

Interfacce per la Configurazione –

- Ogni modello di AP dispone di più interfacce per la modifica della configurazione.
- Di seguito verranno elencate le varie possibilità nei tre modelli di cui sopra:
  - **Cisco –** *SNMP*, *seriale*, *Web*, *telnet*
  - **3Com -** *SNMP*, *seriale*, *Web*, *telnet*
  - **Lucent/Cabletron -** *SNMP*, *seriale*
- I modelli 3Com forniscono molte informazione tramite l'interfaccia web: all'aggressore è sufficiente individuarne uno per poi ricavare l'SSID dal menù *Proprietà di Sistema*. Inoltre i prodotti 3Com richiedono l'uso di una password per modificare la configurazione attraverso l'interfaccia web: per impostazione predefinita è identica alla password di comunità SNMP, quindi gli AP 3Com risultano esposti ad elevati rischi se lasciati con la password *comcomcom* predefinita.

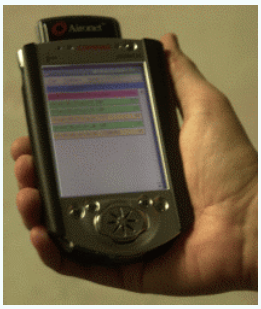
Tecniche di intrusione nella rete

- Inserimento di apparati wireless non autorizzati
- Intercettazione passiva e monitoraggio del traffico di rete
- Disturbo del segnale (**jamming**)
- Attacchi ai meccanismi di cifratura, grazie alle debolezze riscontrate nel protocollo WEP
- Errori nella configurazione della rete wireless

Strumenti di amministrazione

- IBM **Wireless Security Auditor (WSA)**
  Permette di gestire un'inventario e verificare lo stato degli apparati wireless presenti nella rete

- **AirSnort** e **WEPCrack**
  Sfruttano le debolezze del protocollo WEP per riportare tutto il traffico di rete catturato in chiaro



Strumenti di amministrazione - 2

- **NetStumbler**

  E' stato il primo strumento ed il più completo per l'individuazione e monitoraggio di reti wireless

- **EtheReal**

  Potente sniffer, già impiegato per le reti Ethernet

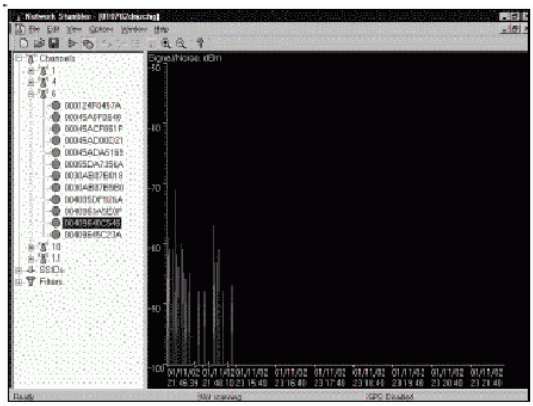
IBM WIRELESS SECURITY AUDITOR

- Il *Wireless Security Auditor* (*WSA*) è un prototipo di agente di monitoraggio di reti wireless sviluppato da **IBM**, eseguito sotto *Linux Red Hat 7.1* su notebook o sotto la distribuzione Linux *Familiar*, con la libreria **ftlk**, su un **COMPAQ IPAQ**
- WSA automaticamente monitora la rete per verificare un corretto livello di sicurezza, in aiuto agli amministratori per prevenire eventuali attacchi.
- Gli altri pacchetti software che svolgono il ruolo di analizzatori di reti (**wlandump**, **ethereal**, **Sniffer**) attualmente a disposizione sono rivolti a personale esperto, che voglia analizzare in maniera molto dettagliato il contenuto dei pacchetti.
- WSA è rivolto ad uno spettro più ampio di utenti, installatori di reti o amministratori, che vogliano un sistema semplice ma efficace per esaminare la configurazione della rete wireless sotto il profilo della sicurezza, senza conoscere in dettaglio lo standard 802.11.
- L'amministratore di rete ottiene con questo strumento una facile risposta alle seguenti domande:
  - Che tipo di punti di accesso sono installati sulla rete?
  - Dove sono?
  - Sono correttamente configurati?
  - Possiedono l'ultima versione del firmware?
- Nel dettaglio le funzioni svolte dal WSA sono:
  - Esamina i pacchetti di sincronizzazione (*beacon packets*) per trovare tutti i punti di accesso.
  - Determina l'SSID e il nome degli AP.
  - Esamina i pacchetti sonda (*probe packets*) e le risposte a questi.
  - Esamina i pacchetti dei dati.
  - Determina la presenza di meccanismi di cifratura.
  - Esamina i pacchetti di autenticazione ed il relativo metodo.
  - Esamina il numero di client nella rete.

NetStumbler

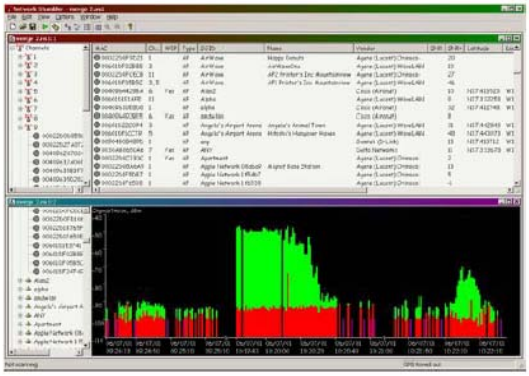
- E’ un progetto che si è esteso per tutto il territorio degli Stati Uniti
- Costituisce una banca dati di reti wireless individuate tramite questo strumento software
- Sfrutta una debolezza dello standard nota come **SSID broadcast**
- E’ in grado di collezionare un numero cospicuo di informazioni su una rete wireless semplicemente analizzandone passivamente il traffico

Misura del segnale con NetStrumbler



Intercettazione e Monitoraggio

- **Intercettazione di traffico su una rete LAN**
- **Wireless sniffer:** Un attaccante utilizza un tool di sniffing wireless (NetStumbler, AirSnort) con il quale intercetta il traffico radio, anche da parecchie centinaia di metri di distanza, cercando soprattutto le informazioni di sessione (username e password).



Intercettazione e Monitoraggio

- Intercettazione del traffico di rete su una Wlan:
- **Spoofing Arp:** Un attaccante utilizza un tool come Dsnifftramite il quale, corrompendo la tabella ARP dell'access point, può trasparentemente far transitare tramite di se il traffico destinato da un client ad un'altra macchina (server, gateway..) sniffandolo.

- Intercettazione del traffico di rete su una Wlan:
- **Hijacking SSL e SSH:** utilizzando la tecnica dello spoofing Arp tramite Dsniff, un attaccante può dirottare sessioni TCP comprese SSL e SSH. Il Client riceve solo un warning che le credenziali dell'host e del certificato sono cambiate chiedendo conferma dell'accettazione di quelle nuove.

Errate Configurazioni

- Access Point con configurazioni di default **Installazione plug&play:** molti vendor, per rendere semplice l'installazione degli access point, mettono di default molti parametri ed abilitando il DHCP in modo che l'access point funzioni immediatamente e velocemente.
- L'installatore si trova con apparati 'plu&play' che funzionano al volo ma senza una parametrizzazione avanzata possono rilevarsi molto vulnerabili.

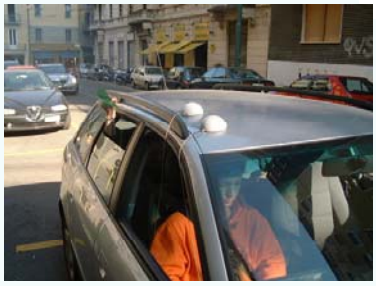
War Driving

- Attività di hacking delle reti wireless dove una stazione mobile wireless (Pc, scheda wireless, GPS ed antenna direzionale) dotata di sniffer radio, è posta in un veicolo e coprendo una certa area si va alla ricerca degli access point
- Tramite l'attività di War Driving, vengono create delle mappe del territorio con la localizzazione degli access point scoperti e le loro eventuali vulnerabilità,(senza WEP ad esempio)
- Queste mappe sono pubbliche e inserite su internet



War Driving

- Andare a caccia di reti wireless con una normale scheda è possibile. Questa soluzione non consentirebbe però la massima efficienza e il massimo grado di rilevazione, in quanto il basso guadagno dalle piccole antenne incluse nelle pcmcia non ci permettere di ricevere i segnali radio provenienti dagli Access Point situati nei piani alti degli edifici.
- Per individuare questi Access Point e per individuare tutti i segnali che, per una ragione o per l'altra, sono spesso molto deboli (AP posizionati verso le facciate interne degli edifici; AP presenti nelle vicinanze, il cui segnale giunge riflesso dalle case etc...) è quindi necessario disporre della giusta attrezzatura.



- **Esempio di kit tipico:**
- 2 Computer portatili
- 1 Inverter 12V - 220V per autovetture
- 2 schede wireless Cisco Aironet LCM352 (questo specifico modello ci consente di collegare fino a 2 antenne esterne per scheda)
- 2 Antenne Omnidirezionali da 2.2dBi di guadagno con base magnetica (per poterle porre sul tetto della macchina)
- 1 Antenna Direzionale Log Periodic da 8dB



Le linee guida della Sicurezza Wireless Wi-Fi

- Progettazione della architettura della Wireless Lan e corretta installazione degli apparati
- Trattare la rete Wireless come una rete ‘insicura’, definire delle politiche di sicurezza che portino, ad esempio, ad introdurre meccanismi di strong authentication che implichino l’identificazione dell’utente
- Utilizzare meccanismi di criptazione che utilizzino una generazione dinamica delle chiavi di criptazione, al limite in ogni sessione.
- Security assessment ed auditing della infrastruttura wireless, dei firewall e degli eventuali sistemi IDS

Progettazione della Architettura

- Effettuare un network assessment della **attuale** rete cablata al fine di identificarne la corretta topologia e gli eventuali punti didebolezza **a prescindere** dalla futura implementazione della Wlan.
- Definire le politiche di chi utilizzerà il wireless, identificarli, raggrupparli, decidere a quali risorse potranno accedere ed in che tempi
- Installare una Wlan pilota **NON in produzione** al fine di verificare che l’integrazione alla attuale rete fisica non generi problemi.
- Verificare in quella sede che le politiche di sicurezza siano applicabili, le prestazioni accettabili, valutare le eventuali modifiche da compiere sugli applicativi al fine di migliorare le prestazioni e la sicurezza degli stessi.

Progettazione della Architettura

- Studio della planimetria del sito al fine di individuare il numero di Access Point necessari e la loro posizione rispetto la propagazione con la scelta della migliore antenna e suo corretto posizionamento tenendo conto dei lobi di propagazione e delle riflessioni.
- Nel caso di access point adiacenti, utilizzare canali diversi per minimizzare problemi di crosstalk che potrebbero diminuire le prestazioni.
- Verifica strumentale del sito per verificare la posizione corretta degli AP, per garantire la massima copertura radio interna con la minima fuoriuscita del segnale radio dal sito per non favorire

Installazione
Identificare la Wlan

- Negli access point configurare un SSID a livello di password sicura (15 caratteri, simboli, cifre, lettere) e non utilizzare l'SSID di default.
- Disabilitare, se possibile, il Broadcast dell'SSID

- Access list: MAC Filtering
- Inserire direttamente l'elenco dei MAC address delle NIC autorizzate a collegarsi ad un dato access point
- Mantenere l'anagrafe interna delle NIC radio per evitare furti o sparizioni
- Per prevenire l'ARP spoofing, usare tabelle di ARP statiche negli access point per accedere a servizi ben determinati

Abilitare il WEP

- Nonostante siano riconosciute le debolezze dell'algoritmo di criptazione adottato dall' 802.11, il WEP consente di proteggerci dai tentativi di intrusione più semplici e rende comunque non leggibili i nostri dati alla maggioranza dei malintenzionati.
- La suamancata adozione consente letteralmente a chiunque di introdursi sul nostro network.
- L'eventuale tempo e costo per un intrusore per decriptare i nostri dati è direttamente proporzionale alla loro sensibilità.
- Nel caso comunque di presenza di wireless in un sito sensibile, si adotteranno contromisure aggiuntive come le VPN.

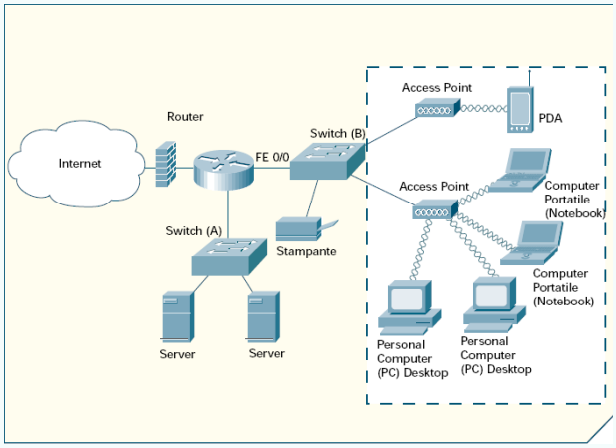
Progettare una WLAN

- Gli amministratori di rete, che devono installare una rete wireless, si trovano spesso di fronte a problematiche molto diverse da quelle associate alle reti cablate:
  - Analizzare i servizi che la rete deve fornire
  - il problema principale è relativo alla sicurezza di rete,
  - Identificare le tecnologie da adottare,
  - pianificare la copertura del segnale radio,
  - come monitorare le prestazioni della rete.

Progettare una WLAN
Fase di indagine

- Studio e sopralluogo dell'area da coprire con il segnale wireless.
- Lo studio è essenziale per pianificare la posizione e il numero dei dispositivi (Access Point) che garantiscono una copertura radio ottimale nell'area d'interesse, tenendo in considerazione che, nella maggior parte dei casi, ogni stazione base deve disporre di una connessione alla rete cablata e una per l'alimentazione.
- Spesso molti Access Point possono operare in modalità bridge, ovvero come semplici replicatori di segnale, senza la necessità di essere collegati al network cablato;
- Un altro aspetto da tenere in considerazione è la propagazione radio sia per analizzare l'area di copertura, sia per determinare se esistono interferenze da parte di altre reti o di altri segnali. Due accesso point vicini possono interferire tra loro perché la frequenza di trasmissione è messa di deafult uguale
- Per questo è possibile utilizzare un notebook e un programma shareware come Network Slumber

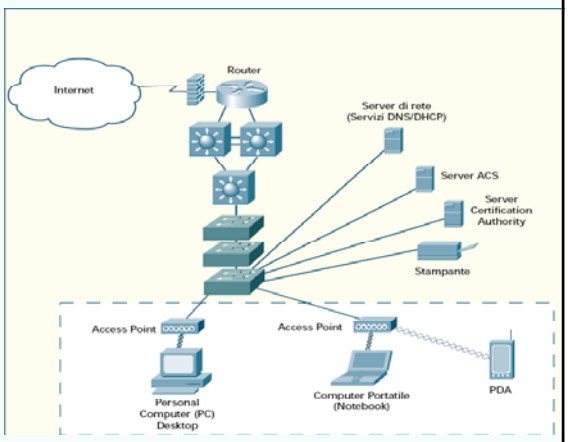
Esempio di rete WLAN
Piccolo ufficio



- Sistema di cablaggio per la creazione di un segmento di backbone;
- Una quantità necessaria di Access Point di accesso LAN a radiofrequenza da parte dell'utenza servita;
- I server;
- Uno switch per l'interconnessione di tutti gli Access Point; uno switch per l'interconnessione dei server;
- Un router per l'accesso ad Internet e un firewall dedicato alla gestione della sicurezza di rete;

Esempio di rete WLAN - Azienda medie dimensioni

- Un sistema di cablaggio per la creazione di un segmento di backbone;
- Una quantità opportuna di dispositivi Access Point di accesso LAN a radiofrequenza da parte dell'utenza servita;
- Switch per l'interconnessione di tutti gli Access Point;
- un server di rete tipo DHCP (Dynamic Host Configuration Protocol) per la configurazione automatica dei parametri di rete degli apparati wireless in dotazione dei client o DNS (Domain Name Server) per gestire la corrispondenza tra nomi e indirizzo IP;



- un server ACS (Access Control Server) per il controllo degli accessi centralizzato. Il server ACS offre un controllo centralizzato per l'autenticazione, autorizzazione ed accounting di tutti gli utenti e distribuisce questo tipo di controllo alle centinaia o migliaia di punti di accesso su tutta la rete;
- un server Certification Authority (CA) per la produzione e gestione dei certificati digitali;
- un router per l'accesso ad Internet e un firewall per la gestione della sicurezza di rete;

Reti PAN
Personal Area Network

Le reti PAN con maggiore diffusione

- Le tecnologie PAN consentono di trasmettere dati e segnali a piccole distanze (dell'ordine al massimo di un centinaio di metri).
- Negli ultimi anni si sono diffusi vari sistemi. I più noti sono:
  - IrDA (Infrared Device Application): tecnologia wireless che utilizza per la trasmissione dei dati connessioni point to point a raggi infrarossi tra dispositivi posti in vista e alla distanza massima di 1 – 2 metri e con un bit rate di 4 Mb/s.
  - Bluetooth: che utilizza trasmissioni radio fino a distanze di 100 m con una velocità fino a 100 Mb/s.
  - HomeRF: progettata soprattutto per piccole reti domestiche e piccoli uffici con distanze fino a 15 m e velocità di trasmissione fino a 10 Mb/s.

I sistemi ottici

Caratteristiche dei sistemi ottici

- Capacità trasmissiva: da 2 x 2 Mbps a 2 x 1.25 Gbps;
- Portata in condizioni meteo medie: fino a 2 km;
- Necessitano di visibilità ottica tra i punti da collegare
- Compatibili con qualsiasi protocollo: asincrono, sincrono ed isocrono (Sistemi Virtual Fiber);
- Garantiscono l'assoluta riservatezza delle informazioni trasmesse;
- Manutenzione praticamente assente: pulizia delle ottiche ogni 6 ÷ 12 mesi;
- **Uso libero e gratuito**.

Applicazioni dei sistemi ottici

I sistemi per telecomunicazioni wireless ottici sono particolarmente indicati per:

- Trasporto di fonia e dati critici con Qualità di Servizio (QoS) e Classe di Servizio (CoS) ben definibili e stabili nel tempo;
- Tratte brevi ad alta capacità, anche di dorsali geografiche;
- **Collegamenti di qualsiasi tipo entro 2 km**.

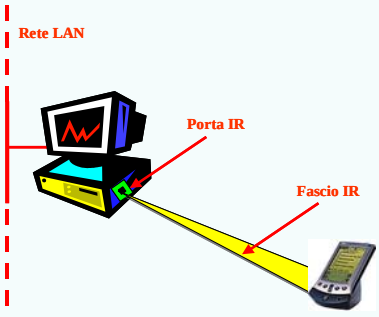
IrDA

Caratteristiche di IrDA

- La tecnologia IrDA (Infrared Data Association) utilizza raggi infrarossi (IR) ed è ormai diffusa da molti anni.
- Attualmente i sistemi IrDA sono presenti in milioni di dispositivi, ad esempio per collegare dispositivi (mouse, tastiera, PDA, scanner,...) a un computer.
- La tecnologia IrDA consente velocità di trasmissione fino a 4 Mb/s e nel nuovo standard (FIR) la velocità di 16 Mb/s.
- La tecnologia IrDA presenta bassi costi (una porta IrDA ha un costo di circa 2 $)

Principali limitazioni della tecnologia IrDA

- Le distanze limitate (pochi metri)
- I dispositivi devono essere in visibilità diretta
- il raggio d'azione è abbastanza limitato perché presenta anche un'angolazione molto stretta per cui i segnali al di fuori di un cono di 30 gradi e distanti più di un metro non sono ricevuti.



HomeRF

Caratteristiche di HomeRF

- HomeRF è stata sviluppata dall'HomeRF Working Group, un gruppo guidato dalla Proxim, ma che include anche altre importanti aziende quali la Compaq, la Motorola, l'Intel e la Cayman Systems.
- HomeRF è una tecnologia progettata per piccole reti domestiche e piccoli uffici e utilizza la banda ISM (banda di frequenza a 2,4 GHz)
- *HomeRF non richiede punti d'accesso (access point) poiché le connessione tra i dispositivi, sono point to point.* Questa caratteristica riduce notevolmente i costi.
- HomeRF consente di comunicare a distanze fino a 15 m e presenta una velocità massima di 10 Mb/s.

Bluetooth

Storia del Bluetooth

- Il sistema Bluetooth è stato originariamente proposto da Ericsson ed è stato espressamente per realizzare la comunicazione senza fili per apparecchi di piccole dimensioni e per distanze limitate.
- Bluetooth è stato standardizzato nel 1999
- Bluetooth è in grado di farinteragire fra loro dispositivi diversi (telefoni, stampanti, notebook, PDA, impianti HiFi, tv,computer, PC, cellulari, elettrodomestici, device,etc..) senza la necessità di collegamenti via cavo.
- Per fare ciò ciascun dispositivo deve possedere all'interno di un chip, integrato, in grado di trasmettere e ricevere informazioni via radio.



Tipico chip Bluetooth

- Il nome deriva da condottiero vichingo di un famoso condottiero scandinavo del Medioevo, Arald II Bluetooth, re vichingo che unificò le regioni norvegesi a quelle danesi.



Principali caratteristiche del Bluetooth

- Bluetooth utilizza la banda di 2,4 GHz ISM (Industrial Scientific Medical)
- La distanza massima che può essere raggiunta è di 30 m.
- La velocità di trasmissione è di 1 Mb/s.
- La trasmissione può avvenire sia mediante onde radio, sia mediante infrarossi.

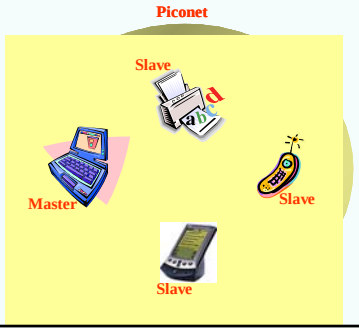
- Bluetooth è un sistema di comunicazione personale e può servire a connettere qualunque terminale o dispositivo senza necessità di connessioni fisse.



La struttura delle reti Bluetooth

- La struttura base più semplice di rete Bluetooth è indicata con il nome di Piconet.
- Piconet è formata da 2 or più unità Bluetooth che condividono lo stesso canale
- In una piconet una stazione è indicata con il nome di master, mentre le altre stazioni sono indicate come slave.
- La stazione master regola le comunicazione degli slave.

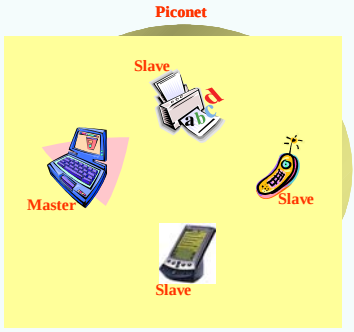
- Una stazione master può essere contemporaneamente collegato a massimo 7 slave per piconet.



La struttura delle reti Bluetooth

- La tecnologia Bluetooth è basata su una rete del tipo Master - Slave in cui il dispositivo che inizia la comunicazione assume il ruolo di *master* mentre il ricevente divento lo *slave*.
- Ogni master può gestire fino ad un massimo di 7 slaves allo stesso tempo.

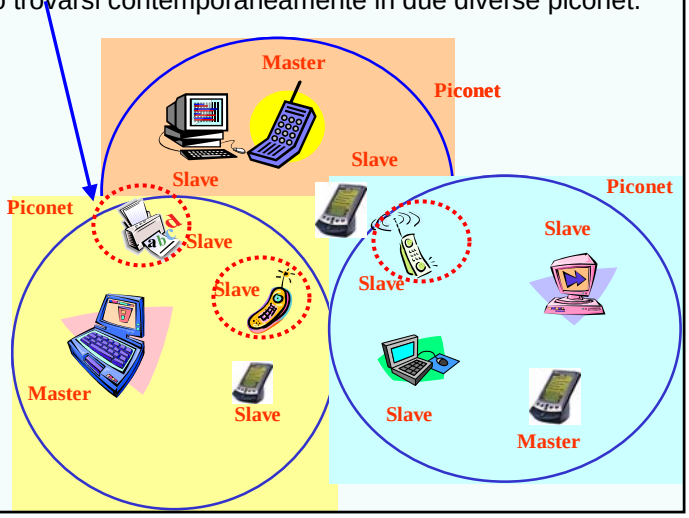
- Il master ha un controllo globale sulla rete che sta amministrando dando il clock a tutti gli slaves;
- Ogni slave deve rispettare tale clock se vuole trasmettere o ricevere le informazioni da e verso l'unità master.



La struttura delle reti Bluetooth

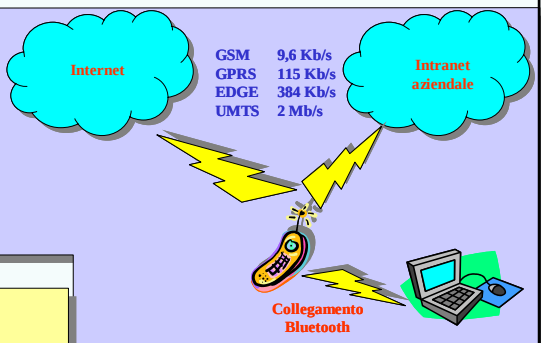
Scatternet (almeno 2 piconet)

- Una scatternet è formata da almeno due piconet.
- Un terminale può trovarsi contemporaneamente in due diverse piconet.



Esempi di applicazioni di Bluettoth

- Trasferimento dell'informazione tra il cellulare (o PDA) e un computer: il cellulare può servire a trasferire le informazioni contenute in esso (ad esempio la rubrica) oppure informazione recuperata da Internet o dalla rete aziendale.

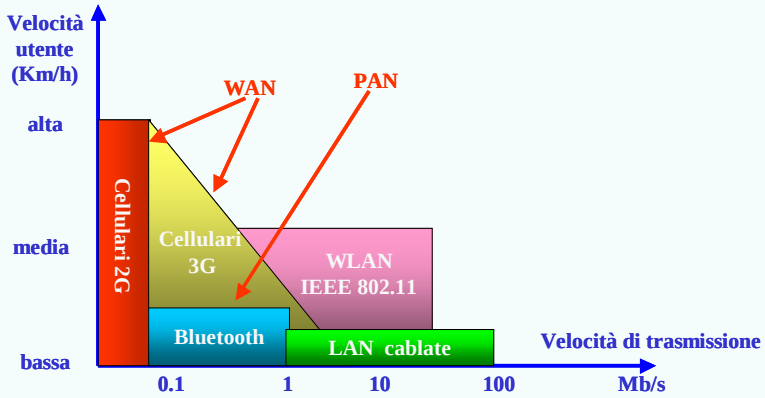




- Trasferimento di dati da un computer verso le sue periferiche o verso altri computer mediante rete ad hoc

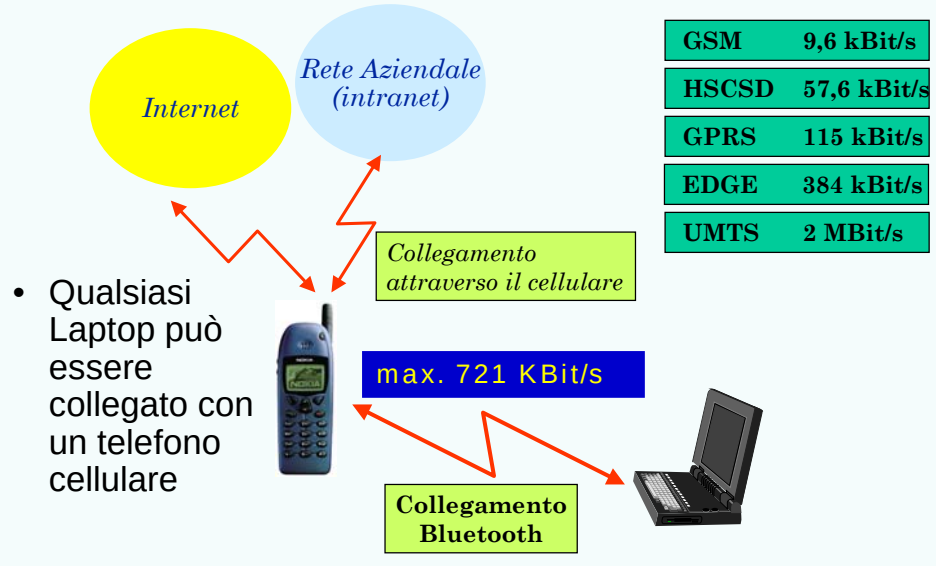
Confronto tra alcune tecnologie wireless

- Nella figura viene mostrato schematicamente il confronto in termini di velocità di trasmissione tra le principali tecnologie wireless.



Bluetooth: esempi di applicazione

Un esempio di applicazione per Blutooth

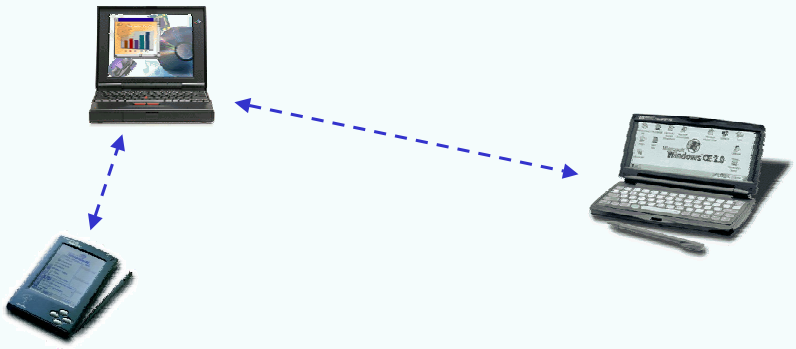


- Qualsiasi Laptop può essere collegato con un telefono cellulare

Reti ad-hoc wireless personali

– Trasferimento wireless di files

– Collegamento di un computer con le sue periferiche

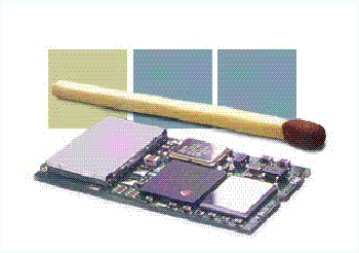


Sostituzione del cavo tra dispositivi

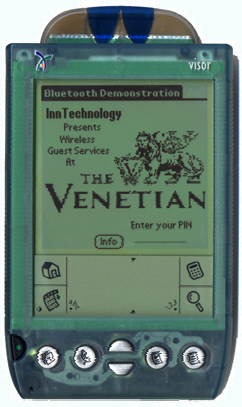
- Accessori dei PC
  - Mouse e tastiera senza fili
  - Collegamento alla stampante
  - Collegamento a Organizer e a modem
- Cuffia Cordless
  - Da usarsi col telefono
    - Chiamate a voce
  - Da usarsi col PC
    - Scrivere a voce
    - Ascoltare l'audio



Modulo radio Bluetooth della Ericsson



Uno scenario d'uso

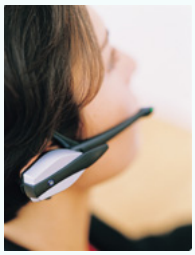


Bluetooth può essere usato per:

- Connettersi a LANs
- Collegamenti diretti tra dispositivi
- Collegarsi a Internet
- Collegarsi alle periferiche

Il primo dispositivo Bluetooth: la cuffia radio di Ericsson

- La cuffia serve per connettersi via radio al cellulare
- Massima distanza raggiungibile: 10 m
- Il peso della cuffia è 20 grammi





La PCMCIA Bluetooth Card di IBM

Bluetooth PC Card from IBM at a glance

Part number	09N9812
Wireless PAN standard	Bluetooth* compliant
Form factor	Type II PC Card
Data rates	up to 721 Kbps asymmetric; 478Kbps full duplex
Frequency band*	2.4GHz ISM
Range*	up to 10m (33ft)
Bluetooth profiles supported	Service discovery; Serial port; Dial-up networking; FAX (as data terminal); LAN Access
Data encryption	128 bit
Output power	0dBm
Power consumption (5V power supply)	Doze mode: <=41 mA Receive mode: <= 175 mA Transmit mode: <= 521 mA (full duplex)
Receive sensitivity	-84dBm
Dimensions (HxWxD)	5x54x118mm (0.2"x2.1"x4.6")
Operating environment Temperature Relative humidity	 -20-29°C (-5-85°F) 90% maximum (non-condensing)
Agency approvals	Safety: UL 1950, IEC 60950 EMC: ETS 300 826, FCC CFR47 part 15.249, VCCI Radio: ETS 300 328, FCC CFR47 part 15.249, TELEC ARIB STD-T66, IC RSS 139 212
Limited warranty*	One year
Systems*	For the most up-to-date compatibility information, please visit our Web site at **ibm.com**/pc/europe/options
Software	Bluetooth Software Suite
Operating systems	Microsoft® Windows® 95; Windows 98; Windows 98SE; Windows 2000; Windows ME (future)

IBM

IBM United Kingdom Limited
emea marketing and publishing services (emaps)
Normandy House
PO Box 32
Bunnian Place
Basingstoke
RG21 7EJ
United Kingdom

The IBM home page can be found on the Internet at **ibm.com**/pc/europe

IBM is a registered trademark of International Business Machines Corporation.

* ThinkPad is a trademark of International Business Machines Corporation.

** Microsoft and Windows are trademarks of Microsoft Corporation.

Bluetooth is a trademark owned by Telefonaktiebolaget L M Ericsson, Sweden and licensed to IBM.

* Bluetooth operates in the unlicensed 2.4GHz radio spectrum.

* Many factors affect range, including building material and external interference sources. Range may vary and may be lower than the stated range.

* For information regarding the terms and conditions or copies of IBM's Statement of Limited Warranty (not available in all countries), please contact your Business Partner or IBM marketing representative.

* Some configurations may not be compatible.

Other company, product or service names may be trademarks or service marks of others.

Options by IBM



Il modulo Bluetooth di Toshiba

- 15 x 30 x 3 mm in
- Il ricetrasmettitore non è più grande di un francobollo.
- Un modulo Bluetooth può essere connesso ad un PC tramite una card o attraverso la porta USB.
- Supporta una trasmissione asincrona e fino a tre sincrone.
- Il canale asincrono consente trasferimenti a 721 Kbit/s in una direzione e a 57.6 Kbit/s nell'altra. In una connessione simmetrica, si hanno invece fino a 432.6 Kbit/s in entrambe le direzioni.



Part Number	PA3053E-1PCC
Format	PC Card type II
Transmission Range	up to 100 metres
Transmission Power	+20dBm Bluetooth radio designed in accordance with specification of the Bluetooth System v1.0B
Compatibility	Any notebook featuring a PC Card slot type II. Any Blueto product certified to Bluetooth specification v1.0B
Software Included	Bluetooth Neighbourhood Suite, SPANworks 2000.
OS Support	Windows 98 SE/ME (further OS support available soon)
Warranty	1 year

Dispositivi della ACER

USB Dongle



Specifications

General Radio:	Carrier Freaquency Symbol Rate	2.402-2.495Ghz 1 Mbps
Radio Performance - Receiver:	Rx sensitivity @1e-3 BER	-70dBm
Radio Performance - Transmitter:	Power at Antenna Port (class 2)	-6 ~ +4 dBm
Antenna:	Integrated PCB Antenna (patent pending)	
Environmental:	Operating Temperature Storage Temperature	0°C ~ +65°C -30°C ~ +75°C
USB Adaptor:	USB Compliance System Support	Version 1.1 Win 98, Win 2000
Certification:	FCC, ETSI, TELEC Regulatory Compliant	
Power Management:	Support power management features as defined by Microsoft PC 98 and PC 99 guidelines, and Bluetooth specific power management	

Dispositivi della ACER

PDA Connect



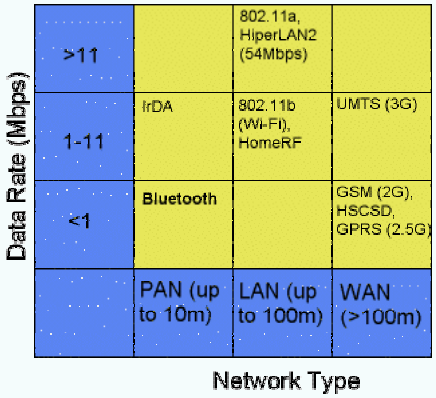
Specifications

Compliance:	Bluetooth specification Version 1.1 Springboard HDK
Data rate:	1 Mbps on the wireless channel
Antenna:	Internal built-in patch antenna
Radio:Frequency Range :	2.4 - 2.4835 GHz
Output power :	0 dBm to 20 dBm (software controlled)
Power:	drawn from VisorO battery pack - Current : Peak : 60 mA; typical : 40 mA
Regulatory Approval:	FCC Part 15
Color and material:	Color coordinated (to discuss with Handspring)

Bluetooth

Tipo di operazione	Frequenza radio
Banda di attività	ISM fra 2,402 GHz e 2,480 GHz
Modulazione	GSFK (Gaussian Frequency Shift Keying
Velocità di trasf. dati max	1 Mbps
Raggio	10 metri (100 metri opzionali)
Duplexing	Full-duplex, TDD (Time division Duplex)
Velocità salti di frequenza	1600 hop/secondo (3200 hop/secondo per richieste o pagine)
Ampiezza canale	1 MHz
Output RF	Classe 3 (raggio 10): 0 dBm (1mW);
Canali vocali	3 simultanei a 64 Kbps ciascuno
Canali dati	Full duplex a 432,6 Kbps, asimmetrica 721 Kbps in uscita e 56 Kbps in ingresso

Confronti con altre tecnologie wireless



Il livello radio

- Bassi costi (singolo chip)
- Tecnica *Frequency Hopping - Time Division Duplexing* (FH-TDD)
- Bassa potenza di trasmissione (bassi consumi ed elevata durata delle batterie).
- Robustezza all'interferenza grazie alla modalità di trasmissione di tipo FH.

Bande di frequenza

Paese	Gamma di frequenze	Canali RF	
Europa & USA	2400 - 2483.5MHz	F=2402 + k MHz	k = 0 a 78
Giappone	2471 - 2497MHz	F=2473 + k MHz	k = 0 a 22
Spagna	2445 - 2475MHz	F=2449 + k MHz	k = 0 a 22
Francia	2446.5 -2483.5MHz	F=2454 + k MHz	k = 0 a 22

Classi di potenza

Classe	Massima Potenza trasm.	Potenza uscita nominale	Potenza uscita minima	Controllo di potenza
1	100 mW (20 dBm)	Non definita	1 mW (0 dBm)	4 a +20 dBm -30 a 0 dBm, optional
2	2.5 mW (4 dBm)	1mW (0 dBm)	0.25 mW (-6 dBm)	-30 a 0 dBm, opzionale
3	1 mW (0 dBm)	Non definita	Non definita	-30 a 0 dBm, opzionale

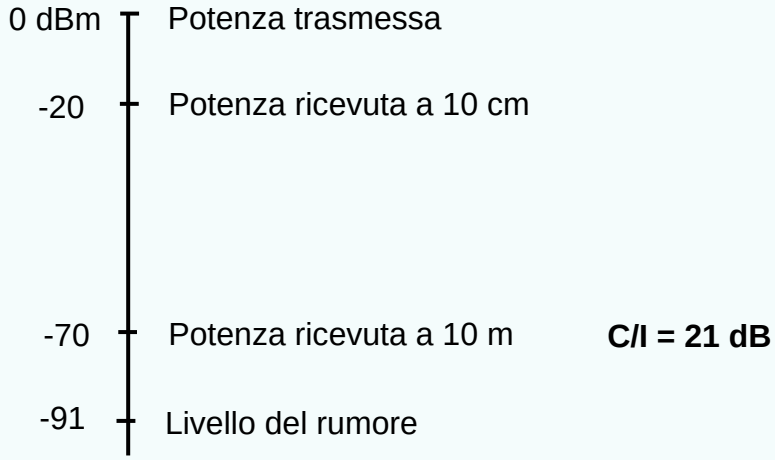
Il massimo salto di potenza è di 8 dB; il minimo è di 2 dB.

Un dispositivo di classe 1 con una potenza massima trasmessa di +20 dBm deve essere capace di controllare la sua potenza trasmessa fino a 4 dBm.

La modulazione usata

- Bit-rate: 1Mbit/s +/-20ppm
- GFSK (*Gaussian Frequency Shift Keying*) con BT=0.5
  - Bit 1 : Deviazione di frequenza positiva
  - Bit 0 : Deviazione di frequenza negativa
- La massima deviazione della frequenza deve essere compresa tra 140 KHz e 175 KHz
- Si hanno 1600 salti di frequenza (FH) al secondo, uno per slot.

Caratteristiche della attenuazione e della qualità



Bluetooth a confronto con le WLAN vere e proprie

- Bluetooth non è una vera e propria Wireless LAN perché:
  - non consente la mobilità (Roaming / Handover)
  - ha limitato bit-rate
  - ha un limitato numero di dispositivi
- L'aspetto vantaggio è che costa poco.
- La soluzione adeguata per WLAN in grado di supportare elevatissimi bit-rate tipici di trasmissioni real-time è data dallo standard HIPERLAN2.

RF-Id

Sistemi Radio per l'Identificazione Automatica

Introduzione ai sistemi di identificazione automatica

- Negli ultimi anni le procedure di identificazione automatica si sono sempre più diffuse sia nel campo industriale sia nei sistemi di circolazione dei materiali sia in ambiti logistici di acquisto e distribuzioni merci.
- L'obiettivo di tali tecnologie è fornire informazioni riguardo persone, animali, cose o prodotti in transito.

- I sistemi più utilizzati per l'identificazione nelle applicazioni industriali sono:
  - le etichette con codici a barre;
  - le smart card.

Introduzione ai sistemi di identificazione automatica
Codici a barre

- Vantaggi della tecnologia dei codici a barre:
  - bassi costi;
  - Semplici da utilizzare.

- Svantaggi della tecnologia dei codici a barre:
  - Bassa memoria
  - Impossibilità di riprogrammazione.

Introduzione ai sistemi di identificazione automatica

Smart card

- Le Smart Card sono dei dispositivi con capacità di elaborazione e di memorizzazione dei dati costituiti da un supporto plastico solitamente di dimensioni uguali a quelle di una carta di credito e da un circuito integrato incorporato che consente di memorizzare ed elaborare al loro interno particolari informazioni.
- Le Smart Card offrono numerosi vantaggi:
  - alta resistenza agli attacchi fisici/logici ;
  - possibilità di effettuare transazioni sicure
- Le Smart Card so dividono in due classi:
  - Carte a Memoria
  - Carte a Microprocessore



- Le smart card possono operare solo attraverso il *contatto* diretto tra la carta e un apposito lettore.

Tecnologie radio per l'identificazione

- Le tecnologie RF-Id nascono essenzialmente come strumenti per l'identificazione automatica di persone e cose in modo alternativo ai sistemi di codici a barre e di smart card.

La Tecnologia RF-Id nasce per sopperire ai limiti di :

Barcode → **Impossibilità di Riprogrammazione**

Barcode → **Memoria Ridotta**

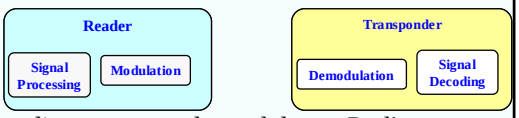
Smart Card → **Contatto**

Un sistema RF-Id sfrutta le onde elettromagnetiche per :

- **Garantire uno scambio di dati senza il minimo contatto fra ricetrasmettitori (e quindi riconoscere anche un utente o un oggetto)**
- **Fornire energia di alimentazione a dispositivi privi di batteria**

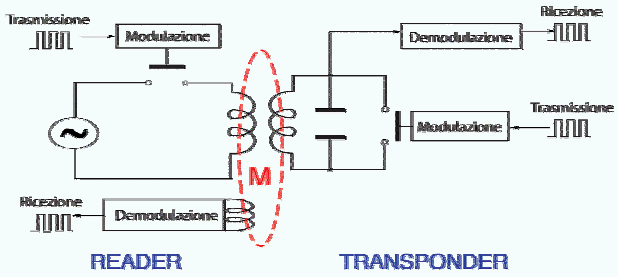
Caratteristiche dei sistemi RF-Id

- Un sistema RF-Id è costituito essenzialmente da tre componenti:
  - un Ricetrasmettitore (Reader);
  - uno o più Transponder (TAG);
  - Un'antenna.



- Reader e TAG comunicano fra loro mediante un segnale modulato a *Radio Frequenza (RF).*

- Schema di funzionamento di un RF-Id.



- Il transponder può non essere alimentato: la potenza necessaria per trasmettere il segnale al reader viene fornita in questo caso dal segnale incidente generato dal reader

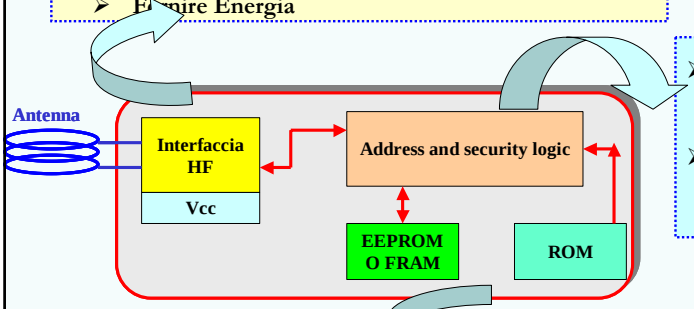
Transponder passivi e attivi

- I transponder utilizzati negli RF-Id possono diversi in due classi:
  - Transponder passivi: il transponder non possiede una propria batteria interna, per cui la potenza necssaria per funzionare viene fornita direttamente dalla sorgente RF (reader) che interroga il transponder.
  - Transponder attivi: il transponder possiede una sorgente di alimentazione propria (generalmente una batteria)

Architettura di un transponder

Le principali funzioni svolte sono:

- Demodulare il segnale ricevuto
- Trasmettere i dati
- Fornire Energia



- Gestisce tutti i processi che coinvolgono il chip
- Può contenere un'unità per la cifratura

- Le memorie contengono le informazioni e i codici relativi al transponder.

Principali caratteristiche dei transponder passivi

- I Transponder passivi non possiedono invece alcuna batteria interna: la potenza necessaria al loro funzionamento viene derivata direttamente dalla sorgente RF (reader) esterna che dialoga con il Transponder.
- *I transponder passivi sono più leggeri, più piccoli e meno costosi di quelli attivi;*
- I transponder passivi hanno un ciclo di vita praticamente infinito.
- I transponder passivi sono costituiti da:
  - Un chip, costituito generalmente da un circuito di trasmissione e da una memoria non volatile che contiene un codice unico che viene trasmesso al reader oppure un microprocessore in grado di elaborare i dati provenienti dal reader e ritrasmettere i risultati richiesti.
  - Un'antenna che svolge i seguenti compiti:
    - ✓ per trasmettere e ricevere i dati;
    - ✓ Trasformare l'energia elettromagnetica proveniente dal reader in energia elettrica utile per alimentare il transponder.
- I transponder passivi permettono di arrivare a distanze fino a qualche m. In molti casi le distanze sono ancora più piccole.

Bande di frequenza per i transponder passivi

I Transponder passivi operano nelle seguenti bande:

Basse frequenze (120 – 145 KHz):

- Basse velocità di trasmissione (1 – 2 Kb/s)
- Grande varietà di formati

Medie frequenze (13.56 MHz):

- La banda ISM (Industrial, Scientific and Medical band) è attualmente la banda su cui si pensa di realizzare la maggior parte delle nuove applicazioni;
- Buone velocità di trasmissione (28 Kb/s).
- In condizioni ottimali distanze di lettura pari a 3.5m, che nella pratica si riducono all'ordine del metro

Alte frequenze (860 - 930 MHz e 2,45 GHz):

- La banda 900 MHz non può essere utilizzata in Europa perché assegnata al GSM.
- La frequenza 2,45 GHz consente elevate velocità di trasmissione, ma risente in modo sensibile delle condizioni atmosferiche.
- Velocità di trasferimento fino a 40 Kb/s.

Principali caratteristiche dei transponder attivi

- I transponder attivi contengono una sorgente di alimentazione propria, in genere una piccola batteria al litio.
- Rispetto a quelli passivi i transponder attivi consentono:
  - Maggiori distanze maggiori rispetto a quelle passive: la portata radio può arrivare fino a 100 m;
  - Operare a frequenze più elevate;
  - Maggiori velocità di trasmissione;
  - Gestire maggiori quantità di informazioni e memorie.



- L'utilizzo di una batteria limita il ciclo di vita del Transponder; tuttavia, il basso consumo energetico del circuito assicura comunque una funzionalità di almeno dieci anni.
- La durata della batteria può allungarsi o accorciarsi in base alle temperature di lavoro ed al numero di cicli di lettura e scrittura effettuati.

- I transponder attivi hanno un costo più elevato rispetto a quelli passivi (circa 10 volte)

Classificazione dei transponder
Scrittura dati

- I metodi utilizzati per memorizzare i dati in un transponder possono essere divisi in tre categorie:
  1. Read-Only Transponder
  2. Writable Transponder;
  3. Transponder con funzioni crittografiche

Read-Only Transponder

- la memoria contiene un numero di identificazione non modificabile, costituito da pochi byte, e da una stringa di controllo;
- *La trasmissione può avvenire solo nella direzione dal transponder al reader;*
- Sistemi molto economici (costo spesso inferiore a 0,5 E).
- **Esempi di applicazioni**
  - l'identificazione di animali,
  - i controlli di accesso ad aree private
  - le automatizzazioni di attività industriali;
  - Gestione dei magazzini.

Classificazione dei transponder
Scrittura dati

Writable transponder

- I Transponder sui quali è possibile scrivere dati sono disponibili in diverse capacità che variano dal singolo byte ai 64 bytes.
- L'accesso in lettura e in scrittura al Transponder avviene spesso a blocchi di memoria costituiti da più bytes.
- Per cambiare parte del contenuto dati di un singolo blocco prima deve essere letto l'intero blocco, dopodiché deve essere riscritto inserendo i bytes modificati. I sistemi attuali utilizzano blocchi di 16 bits, oppure 4 o 16 bytes.
- **Tipi di memorie:**
  - EEPROM (*Electric Erasable Programmable Read-Only Memory*), sono le più utilizzate, ma presentano un alto consumo di energia nelle operazioni di scrittura.
  - FRAM (*ferromagnetic random access memory*) sono di recente sviluppo, poco utilizzati a causa di problemi riscontrati durante la fabbricazione; presentano un consumo energetico in lettura più basso di un fattore 100 e il tempo di scrittura 1000 volte più basso sempre rispetto alle EEPROM.
  - SRAM (*static random access*), vantaggiose per la rapidità con la quale svolgono i cicli di scrittura, ma richiedono una batteria ausiliaria

Classificazione dei transponder
Scrittura dati

Transponder con funzioni crittografiche

- Questo tipo di transponder serve a prevenire accessi non autorizzati.
- I transponder possono consentire diverse soluzioni per permettere l'accesso ai dati contenuti nella memoria:
  - Inserimento di password per la lettura e la scrittura;
  - Cifratura dei dati mediante l'utilizzo di chiavi segrete. La chiave segreta viene scritta al momento della fabbricazione in una parte di memoria riservata. Per ragioni di sicurezza tale area di memoria risulta illeggibile.

Classificazione dei sistemi RF-Id

In base al contesto nel quale sono inseriti, il mercato offre una classificazione dei Sistemi RF-Id in quattro categorie ben distinte :

EAS (Electronic Article Surveillance systems)

Gate reader



PDA (Portable Data capture Systems)



Networked Systems



Positioning Systems



Classificazione dei sistemi RF-Id

EAS (Electronic Article Surveillance systems)

- I sistemi EAS utilizzano generalmente transponder a 1 bit e servono a verificare la presenza di un prodotto all'interno di un'area.
- Il loro costo è di pochi centesimi di euro, poiché i transponder non necessitano di un chip.

Esempi di applicazione: Utilizzo in un centro di vendita al dettaglio per salvaguardare la struttura da eventuali furti.

- Ogni articolo viene dotato di un transponder. All'uscita del centro è posto un Reader (generalmente ingombrante) attraverso il quale ogni cliente deve passare prima di uscire



Gate reader

- Gestione del magazzino di un'azienda

Classificazione dei sistemi RF-Id

PDA (Portable Data capture systems)

- Nei sistemi PDA il reader RF-Id è integrato in un terminale mobile (PDA, cellulare,…), che ha lo scopo di recuperare i dati dal transponder ed eventualmente di trasmetterli al sistema di elaborazione.



Networked Systems

- In questi sistemi i reader RF-Id sono disposti in posizioni fisse di una determinata area e sono collegati a una rete per la gestione delle informazioni.
- I transponder possono essere fissi o mobili



Esempio: catena di montaggio.

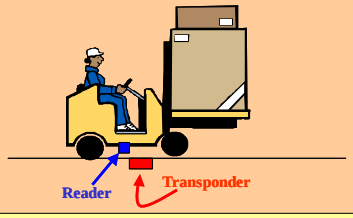
- I transponder si trovano in oggetti che devono essere assemblati, mentre i reader sono disposti sulla catena di montaggio e consentono di individuare i componenti da assemblare.

Classificazione dei sistemi RF-Id

Positioning Systems

- In questi sistemi i Transponder sono utilizzati per facilitare la localizzazione automatica e fornire un supporto di navigazione per veicoli guidati.
- I Reader sono posizionati sui veicoli e collegati ad un computer di bordo, il cui compito è quello di spedire dati al sistema informativo che gestisce i veicoli.
- I Transponder sono disposti sul pavimento dell'ambiente di lavoro e programmati per opportune identificazioni e localizzazioni dei mezzi..

Esempio: gestione di veicoli
e merci in un magazzino



Architettura Esterna del Transponder



Disc Transponder



Key Transponder



Smart Card



GlassTransponder



Plastic Transponder



Smart Label

Creazione di uno Scenario Reale : Centro Commerciale

Ad ogni cliente abitudinario verrà fornito un Key Transponder :



Generazione Profilo Avanzato



Raccolta Dati



Identificazione Profilo Avanzato

Nickname :

Messaggio Pubblicitario Personalizzato