

6 LA TRASMISSIONE WIRELESS

6.1 Sistemi a onde radio

Le trasmissioni wireless possono utilizzare le **onde radio** (RF, Radio Frequency) o i **segnali infrarossi** (IR, InfraRed) per comunicare attraverso l'aria.

Quindi, a differenza delle reti wired, formate da cavi elettrici o fibre ottiche, quelle **wireless** non utilizzano alcun tipo di cavo: il segnale è trasportato nell'aria tramite la propagazione di onde emesse da un'antenna.

L'intero spettro elettromagnetico è mostrato in **FIGURA 26**.

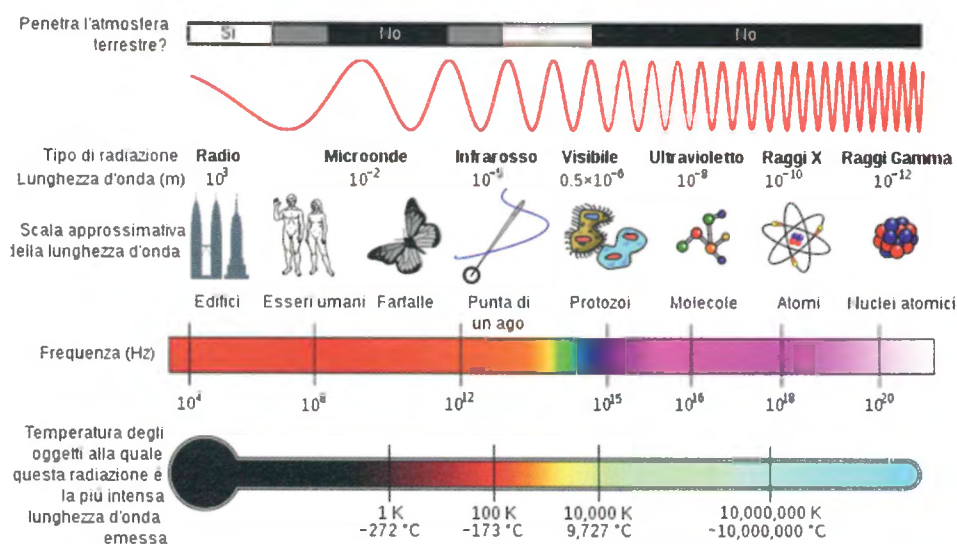


FIGURA 26 Spettro elettromagnetico

L'utilizzo delle onde radio ha portato alla nascita di alcuni tra i più diffusi standard per le comunicazioni e per le reti (Bluetooth, Wi-Fi, WiMAX), in grado di coprire anche l'intero pianeta grazie alle trasmissioni satellitari che possono ricevere le frequenze radio e ritrasmetterle sulla Terra.

L'utilizzo dei segnali infrarossi è invece limitato alla comunicazione diretta tra dispositivi posti a breve distanza, come la tastiera e il mouse con il Personal Computer.

#prendinota

L'intensità delle onde radio diminuisce con il quadrato della distanza. Per esempio: a 10 m dall'antenna il segnale ha solo 1/100 della sua energia originale.

Le onde radio sono onde elettromagnetiche nella banda di frequenza compresa tra 0 e 300 GHz.

Le onde radio possono attraversare o meno i materiali: i metalli le riflettono, mentre gli isolanti in genere le deviano (rifrazione).

La presenza di onde elettromagnetiche, in particolare in ambienti chiusi, pone però problemi di salute in quanto tali onde possono creare danni ai tessuti organici, quindi è necessario limitare la loro energia senza limitare la velocità di trasmissione.

La soluzione adottata prevede l'utilizzo di trasmettitori con potenze molto basse (100 mW per il Wi-Fi e 10 mW per il Bluetooth); limitando la potenza si ha anche il vantaggio di ridurre i consumi e aumentare la durata delle batterie dei sistemi portatili.

La limitazione di potenza ha ovviamente determinato un accorciamento delle distanze di utilizzo di un singolo trasmettitore, distanze che si riducono ulteriormente se sono presenti muri.

In particolare, si possono distinguere sistemi a banda stretta (Narrow Band, **NB**) e sistemi a spettro espanso (Spread Spectrum, **SS**).

Con il termine *segnali narrow band* sono indicati quei segnali cui viene assegnata una porzione di banda limitata: tutta la potenza del segnale è contenuta in una porzione di banda a RF paragonabile con la banda del segnale che porta l'informazione. Appartengono a questa categoria i segnali radio convenzionali.

Nei sistemi *Spread Spectrum* invece, il segnale viene distribuito con un'operazione di **spreading** su una porzione di banda molto più larga rispetto a quella del segnale di "informazione" (FIGURA 27). Questa operazione di modulazione rende il segnale simile al rumore (*noise-like*) e porta come vantaggio una maggiore resistenza all'interferenza. Il risultato è quello di un segnale di ampiezza minore distribuito su una banda più ampia.

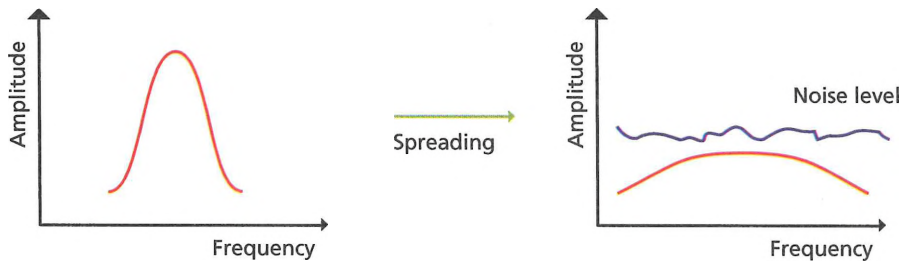


FIGURA 27 Spreading

I sistemi a banda stretta risultano più semplici, soprattutto in termini di implementazione pratica, ma sono spesso inadatti a lavorare in ambiente digitale e a soddisfare la sempre più complessa e diversificata richiesta di servizi wireless.

Infatti tutti i sistemi a banda stretta, a causa del limite fisico della risorsa radio, dovranno essere sempre regolamentati rigidamente per evitare reciproca interferenza e il conseguente degrado delle comunicazioni.

I sistemi SS appaiono, rispetto ai sistemi NB, come una tecnica di trasmissione più evoluta ed efficiente (in termini di utilizzo delle bande disponibili), in quanto consentono un accesso alla risorsa in maniera più disinvolta e permettono di ridurre drasticamente sia le interferenze sul segnale utile, sia le interferenze che lo stesso segnale utile produce sulle altre comunicazioni in corso.

Queste sono le condizioni essenziali affinché possa avvenire un salto di qualità in termini di incremento del numero di utenti che condividono la stessa risorsa rispetto ai sistemi a banda stretta. Sono dunque le tecniche SS quelle che si sono sviluppate nell'ambito delle reti.

6.2 Le tecniche Spread Spectrum nelle trasmissioni wireless

Nei sistemi Spread Spectrum l'allargamento spettrale è ottenuto dalla correlazione, mediante una XOR, tra la sequenza dati da trasmettere e una sequenza periodica di codice (Pseudo Random Noise Code o più semplicemente **PN code**) che deve essere unica per ogni utente e nota al ricevitore interessato a quella trasmissione (FIGURA 28).

Il ricevitore, conoscendo la sequenza di codice dell'utente, decodifica il segnale ricevuto e ricostruisce i dati originali. Tutto ciò è possibile finché la correlazione incrociata (*cross-correlation*) tra il codice dell'utente desiderato e i codici degli altri utenti

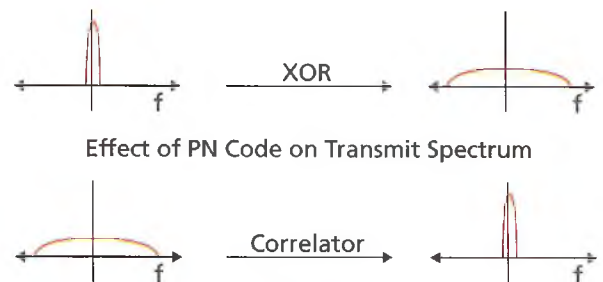


FIGURA 28 Correlazione mediante XOR

è bassa. La banda del segnale “codice” è scelta molto più larga rispetto alla banda del segnale informazione.

In questo modo il processo di codifica allarga (*spread*) lo spettro del segnale.

Una tecnica di modulazione a spettro espanso è caratterizzata, quindi, da due criteri:

- la larghezza di banda del segnale trasmesso è molto più larga della larghezza di banda del segnale informazione;
- la larghezza di banda risultante a RF è determinata, oltre che dall’informazione che è stata inviata, da una sequenza di codice: in questo modo la larghezza di banda è indipendente dal segnale informazione.

Prendiamo per esempio in considerazione la banda di frequenza ISM (Industrial, Scientific and Medical) da 2,412 GHz fino a 2,484 GHz utilizzata nelle principali tecnologie di rete wireless.

I due metodi più importanti utilizzati per la modulazione ad ampio spettro in questa banda sono:

- Direct Sequence - Spread Spectrum (**DS-SS**): dispersione di spettro in banda base;
- Frequency Hopping - Spread Spectrum (**FH-SS**): dispersione di spettro a salto di frequenza.

Le tecnologie USB wireless e Wi-Fi usano **DS-SS**, mentre Bluetooth e telefonia mobile utilizzano la modulazione FH-SS. La tecnica DS-SS è la più nota e usata tra le tecniche di espansione spettrale. Lo spreading è ottenuto correlando, mediante l’operazione logica XOR, la sequenza di informazione in banda base con la sequenza periodica di codice **PN code**, avente caratteristiche pseudo-casuali o di pseudo-rumore e **frequenza** ($1/T_c$) molto maggiore rispetto alla frequenza della sequenza informazione ($1/T$) (**FIGURA 29**).

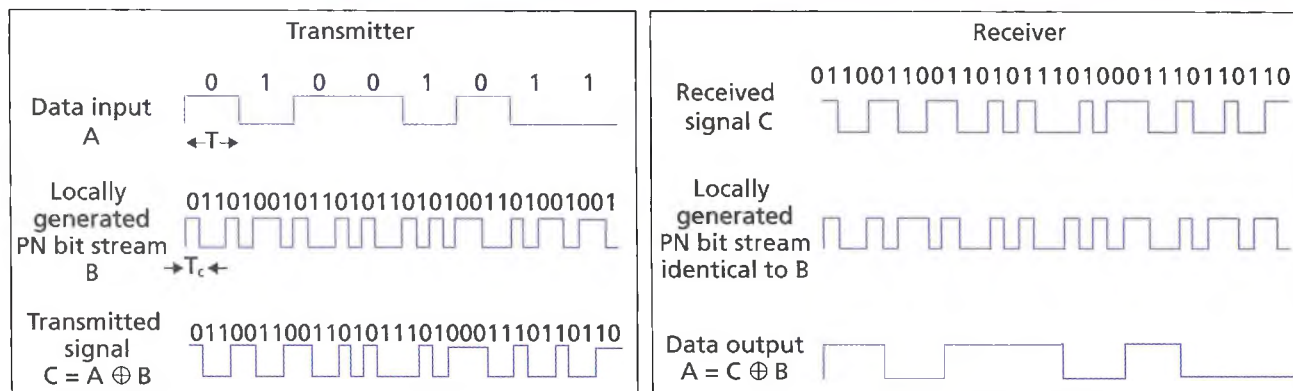


FIGURA 29 Codifica e decodifica di un segnale mediante DS-SS

Questo codice ridondante contribuisce a rendere il segnale resistente alle interferenze e alla ricostruzione dei dati originali, qualora risultino danneggiati dalla trasmissione.

Con la tecnica **FH-SS** l’espansione dello spettro è ottenuta facendo *saltare* il segnale, ovvero facendo saltare la porzione di banda che questo occupa su un certo numero di frequenze portanti, scelte in base a una logica regolata da una sequenza PN Code nota (come nel caso DS-SS) solo al trasmettitore e al ricevitore interessati alla comunicazione in atto. La potenza assegnata al segnale inoltre rimarrà costante per ogni salto.

In altri termini, il segnale modula, nel corso del tempo di salto T_h (quindi a una frequenza di salto $1/T_h$) una portante sempre diversa (FIGURA 30).

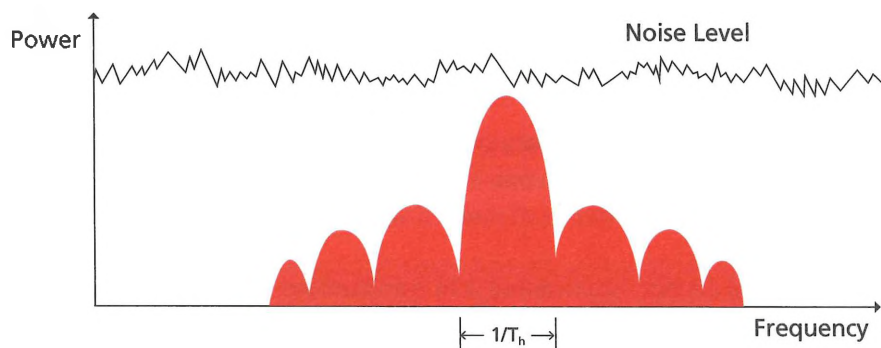


FIGURA 30 Distribuzione FS-SS con tecnica di salto

Un sistema FH-SS di fatto non altera la distribuzione spettrale del segnale originale, contrariamente a quanto avviene nel caso DS-SS e, pertanto, trasmettitore e ricevitore avranno sempre a che fare con segnali che possono essere considerati a tutti gli effetti a banda stretta.

Il maggiore impiego di banda, rispetto all'impiego che caratterizzerebbe un sistema a banda stretta, si realizza per effetto dei continui salti del segnale da una portante all'altra.

Un sistema FH-SS (FIGURA 31) produce la riduzione dell'effetto delle interferenze attraverso una forma di *evasione*; in altri termini, il sistema sfugge continuamente al disturbo. Questa tecnica di evasione sarà tanto migliore quanto maggiore sarà la frequenza di salto ($1/T_h$).

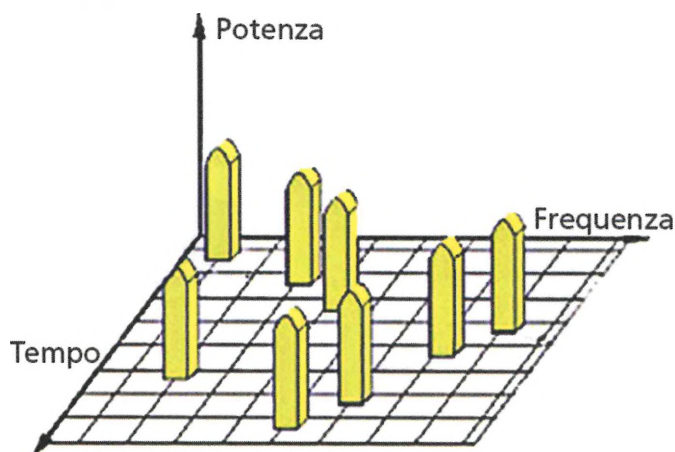


FIGURA 31 Distribuzione FS-SS con tecnica di salto a evasione

Si distinguono sistemi FH-SS slow (**SFH-SS**) e FF-HH fast (**FFH-SS**) per discriminare la velocità con cui avvengono i salti in frequenza; allo stato attuale i sistemi veloci FFH-SS, decisamente superiori, non hanno trovato una larga diffusione a causa della elevata complessità che li caratterizza. Tale complessità è da imputare alla necessità del ricevitore di effettuare le sue funzioni (demodulazione, decodifica, amplificazione, ecc.), mantenendosi sempre sincronizzato con i salti del segnale che deve recuperare; questo problema, già rilevante per sistemi SFH-SS, diventa quasi ingestibile nei sistemi FFH-SS.

6.3 Sistemi a infrarossi

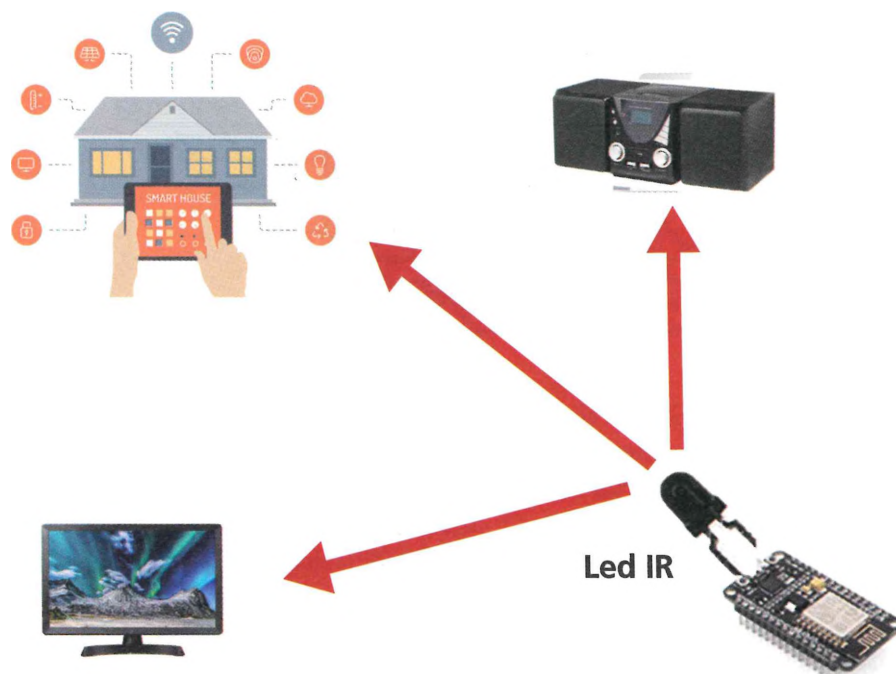
Le sorgenti a infrarossi (*infrared*) emettono una radiazione elettromagnetica con lunghezza d'onda di frequenza all'incirca fra i 300 GHz e i 400 THz. In pratica, si estende dall'estremo superiore dello spettro delle microonde (*microwave*) all'estremo inferiore (rosso) dello spettro delle onde luminose (*visible light*), come precedentemente mostrato in Figura 26.

La tecnologia a raggi infrarossi è usata per comunicazioni a brevissima distanza (pochi metri), infatti la luce infrarossa non è in grado di attraversare alcun ostacolo (anche il vetro di una finestra attenua di molto il segnale!).

L'**IrDA** (Infrared Device Application) è lo standard per la trasmissione dati tramite infrarossi, è bidirezionale e point-to-point tra i dispositivi con collegamento "a vista" (LoS, Line of Sight). Come si è detto, tali dispositivi sono indicati per comunicazioni a breve distanza e non per le reti vere e proprie.

Telecomandi e apparecchi IrDA usano diodi emettitori di radiazione infrarossa (comunemente detti **LED infrarossi** o LED IR) per comunicare con i più svariati dispositivi in grado di ricevere il segnale e per interagire con le apparecchiature di uso comune (impianto stereo, TV, climatizzatore) che non sono connesse alla rete locale o che non sappiamo controllare con un'unica interfaccia o applicazione (FIGURA 32). Se prendiamo in considerazione il telecomando di un TV, quando premiamo uno dei pulsanti verrà emesso, tramite il LED IR, una sequenza di accensioni e spegnimenti del LED IR a frequenza fissata (tipica è la frequenza di 38 kHz) secondo uno schema specifico per ogni pulsante premuto. A ogni pulsante è associato uno schema specifico (detto pattern) di 0 ed 1. A ogni stato logico è associata la frequenza di 0 Hz nel caso si voglia inviare uno 0 logico ed una frequenza di 38 kHz nel caso si voglia inviare un 1 logico. Gli schemi sono in genere costituiti da sequenze 12 o 32 bit.

FIGURA 32 Sistema a infrarossi



Un LED a emissione di luce infrarossa può essere comandato da un segnale **PWM** (Pulse Width Modulation) usando le principali schede IoT (Arduino, Raspberry Pi e ESP8266) per la trasmissione dei bit di codice.

La PWM è un tipo di modulazione digitale in cui l'informazione è codificata sotto forma di durata nel tempo di ciascun impulso. Viene introdotto un **duty cycle** come rapporto tra la durata dell'impulso positivo e la durata dell'intero periodo.

Grazie ai moderni microcontrollori, è possibile attivare o disattivare un interruttore ad alta frequenza e allo stesso modo rilevare lo stato e il periodo di un impulso.

In **FIGURA 33** è mostrato un esempio di PWM per codificare un byte (da 0 a 255 in decimale, da 00000000 a 11111111 in binario). A ogni percentuale di durata del duty cycle corrisponderà un valore numerico diverso nel range prestabilito.

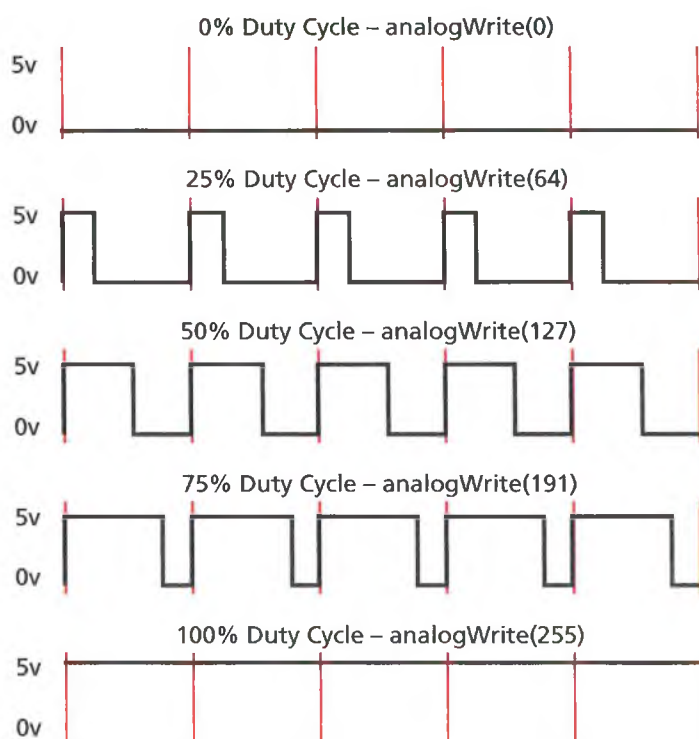


FIGURA 33 PWM

La radiazione infrarossa emessa è catturata da apposite lenti e modulata, cioè accesa e spenta molto rapidamente, per rappresentare i bit da trasmettere. Il ricevitore usa un fotodiodo al silicio per convertire la radiazione infrarossa incidente in corrente elettrica. Anche la luce usata nelle fibre ottiche è spesso infrarossa.

FISSA LE CONOSCENZE

- Quali sono i più diffusi standard per le comunicazioni e per le reti che utilizzano le onde radio?
- Qual è la differenza tra i sistemi a banda stretta (*Narrow Band*) e i sistemi a spettro espanso (*Spread Spectrum*)?
- Quali sono i due metodi più importanti utilizzati per la modulazione ad ampio spettro nella banda ISM?
- A quali tipi di comunicazioni è limitato l'uso dei segnali infrarossi?

7 GLI APPARATI DI RETE

7.1 La scheda di rete

FIGURA 34 NIC PC Card PCMCIA



FIGURA 35 NIC USB

#prendinota

La PC Card **PCMCIA** è uno standard sviluppato dalla Personal Computer Memory Card International Association al fine di permettere l'espansione delle funzionalità dei dispositivi portatili.

#prendinota

Forse a qualcuno può sembrare impossibile che vi siano sufficienti indirizzi MAC diversi per tutti pensando al gran numero di PC sparsi per uffici e abitazioni private.

In realtà con 12 cifre esadecimali, pari a 48 bit, è possibile indirizzare 2^{48} schede di rete diverse. Ricordando che

$2^{10} \approx 10^3$ $2^{20} \approx 10^6$
 $2^{30} \approx 10^9$ e $2^{40} \approx 10^{12}$
 risulta che

$$2^{48} \approx (2^8 \cdot 10^{12}) \approx (256 \cdot 10^{12})$$

cioè circa 256.000 miliardi. Sulla Terra siamo circa 7 miliardi e mezzo: gli indirizzi MAC sono sufficienti!

La scheda di rete (**NIC**, Network Interface Card) è un circuito stampato che collega l'host al mezzo trasmissivo (cioè il PC al cavo). È chiamata anche **LAN adapter**. Solitamente la NIC si trova integrata nella scheda madre del computer. Nel caso in cui si volesse installare una seconda interfaccia di rete (per esempio, perché ha prestazioni migliori di quella integrata) si può ricorrere a una NIC in formato PCIe, per i computer desktop, o in formato PC Card PCMCIA (FIGURA 34) o USB (FIGURA 35) per i computer notebook.

Le schede di rete sono anche note con il nome di **schede Ethernet** poiché forniscono una porta standard Ethernet per il collegamento alla rete tramite connettore RJ45 e cavo di rete in rame di tipo doppino telefonico (twisted-pair).

Anche le schede di rete possono supportare diverse velocità di trasmissione come i cavi. La scheda Ethernet standard prevede 10Mbps, la **Fast Ethernet 100Mbps**, la **Gigabit Ethernet 1000Mbps (1Gbps)** e la **10 Gigabit Ethernet 10Gbps** (FIGURA 36). Lo standard Gigabit Ethernet è disponibile anche per cavi in fibra (FIGURA 37).

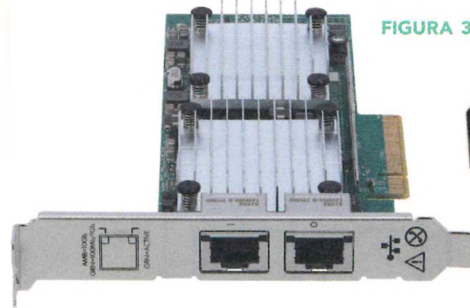


FIGURA 36 NIC PCIe 2 porte 10 gigabit ETH rame

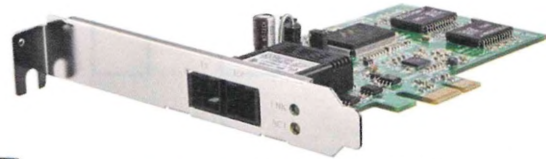


FIGURA 37 NIC PCIe Gigabit ETH fibra

Le schede di rete sono caratterizzate da un indirizzo fisico univoco chiamato **MAC address** (Media Access Control) costituito da 12 cifre esadecimali (6 byte) come mostrato in FIGURA 38.

I primi tre ottetti sono detti **OUI** (Organization Unique Identifier), in quanto identificano l'azienda produttrice della scheda, le altre tre coppie sono detti **UAA** (Universally Administered Address) e rappresentano il numero progressivo cronologico di produzione della scheda da parte di una determinata azienda (numero seriale). La caratteristica fondamentale dell'indirizzo MAC è di essere univoco: non esistono due indirizzi MAC uguali in tutto il pianeta cioè non ci sono due schede di rete (quindi due host) con lo stesso MAC.

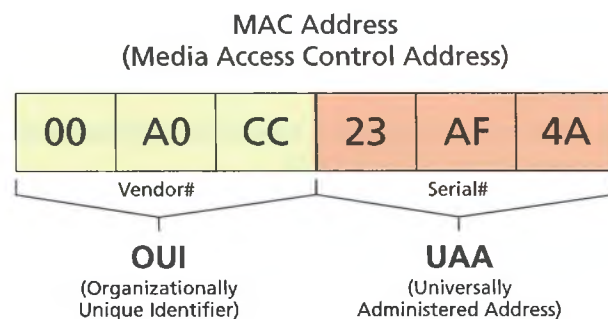


FIGURA 38 MAC Address

7.2 L'hub

L'**hub** ha come compito principale quello di ricevere le informazioni dai vari nodi presenti sulla rete e di inoltrarle agli altri nodi collegati alle sue porte. È un apparato presente sul mercato con un numero molto variabile di porte standard Ethernet (FIGURA 39), essendo utilizzabile in una rete domestica come in una LAN aziendale per collegare le NIC dei singoli computer a un centro stella di rete (topologia a stella o stella estesa).

L'hub non è in grado di verificare quale sia il reale destinatario di tali dati, per cui li invia su tutte le porte tranne quella da cui sono arrivati (modalità **broadcast**). Saranno gli stessi dispositivi riceventi a valutare se i dati inviati dall'hub siano o meno di loro pertinenza e, in caso contrario, a rifiutarli senza processarli.

Tale operazione, oltre a provocare un traffico inutile sulla rete, crea anche incertezze sulla sicurezza dei dati stessi. Bisogna infatti considerare che tutte le informazioni arriveranno a tutti i dispositivi collegati anche quelli a cui non sono realmente destinate.

Un altro compito tipico degli hub è quello di **repeater multiporta**. Il repeater è un apparato ripetitore che permette di ritrasmettere un segnale su una rete.

Ricordiamo che un segnale che transita su un supporto fisico tende ad attenuarsi dopo una certa distanza, oltre a essere distorto a causa del rumore, quindi può essere necessario rigenerarlo.

Un hub con funzioni di repeater quando riceve un segnale, lo rigenera riportandolo al livello originale, lo risincronizza e lo inoltra estendendo così la lunghezza del canale trasmissivo su LAN omogenee.

Per una rete LAN a 10/100Mbps Ethernet vale la regola dei 4 ripetitori, secondo la quale tra 2 host non possono esserci più di 4 ripetitori. Questo per evitare la latenza, cioè il ritardo di un segnale nell'arrivare a destinazione. Una latenza troppo alta rende la rete meno efficiente.

Ci sono 3 tipi di hub:

- **passivi**: servono solo come punto di connessione fisica, non vedono (non leggono) i dati che passano. Essendo passivi non necessitano di alimentazione elettrica;
- **attivi**: richiedono alimentazione elettrica per amplificare e ripulire i segnali che arrivano e trasmetterli sulle altre porte (funzione di repeater);
- **intelligenti**: chiamati anche *smart hub*, funzionano come gli hub attivi ma al loro interno hanno un microprocessore che fornisce informazioni di diagnostica. Sono più costosi degli hub attivi ma sono utili nelle situazioni di *troubleshooting* (ricerca del guasto).

I dispositivi collegati a un hub ricevono tutto il traffico che passa attraverso di esso (broadcast): più dispositivi ci sono e più facile sarà avere **collisioni**. Una collisione si ha quando due dispositivi trasmettono nello stesso istante; ciò causa la distruzione dei dati, che dovranno essere ritrasmessi provocando evidenti ritardi.

Per questo motivo gli hub sono adatti a reti di dimensioni ridotte o con traffico limitato.



FIGURA 39 Hub a 16 porte Ethernet

7.3 Lo switch e il bridge

Lo **switch** è un apparato in grado di analizzare il contenuto di un pacchetto di dati ricevuto e di inoltrarlo solo al reale destinatario, riducendo in tal modo il traffico superfluo nella rete e le possibili collisioni che invece crea l'hub.

Uno switch permette che avvengano più comunicazioni in parallelo, infatti durante la comunicazione collega solo le due porte interessate, rendendo possibili più scambi contemporaneamente con conseguente aumento della bandwidth totale.

Gli switch attuali offrono la funzionalità di autoconfigurazione, cioè sono in grado di riconoscere dinamicamente il dispositivo all'altro capo del cavo, adeguando di conseguenza il collegamento interno per garantire una corretta comunicazione. In questo modo non è più necessario usare cavi incrociati (crossover) e si possono usare sempre cavi dritti (straight-through), in quanto lo switch configura in automatico la porta in modo diverso se dall'altra parte del cavo c'è un altro switch oppure un PC. Esistono modelli di switch di tipo "ibrido" ossia con porte che usano differenti velocità, per esempio porte 10/100 Mbps e porte 1.000 Mbps. Nella FIGURA 40 è mostrato uno switch con 48 porte 10/100 Mbps e 2 porte Gigabit.

Gli switch sono associati a topologie a stella e stella estesa, dove svolgono funzioni di centro stella e sono adatti a reti di qualsiasi dimensione e con un elevato livello di traffico.

Il **bridge** è un apparato simile allo switch ma con meno porte (anche solo 2). Mentre lo switch collega direttamente gli host a un segmento di rete, il bridge serve a collegare tra loro due o più segmenti di rete (FIGURA 41).

Il compito del bridge è quindi anche quello di repeater grazie alla capacità di inoltrare i dati verso un altro segmento di rete.

FIGURA 40 Switch a 50 porte Ethernet

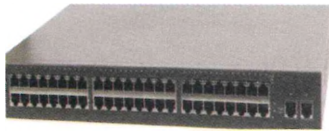
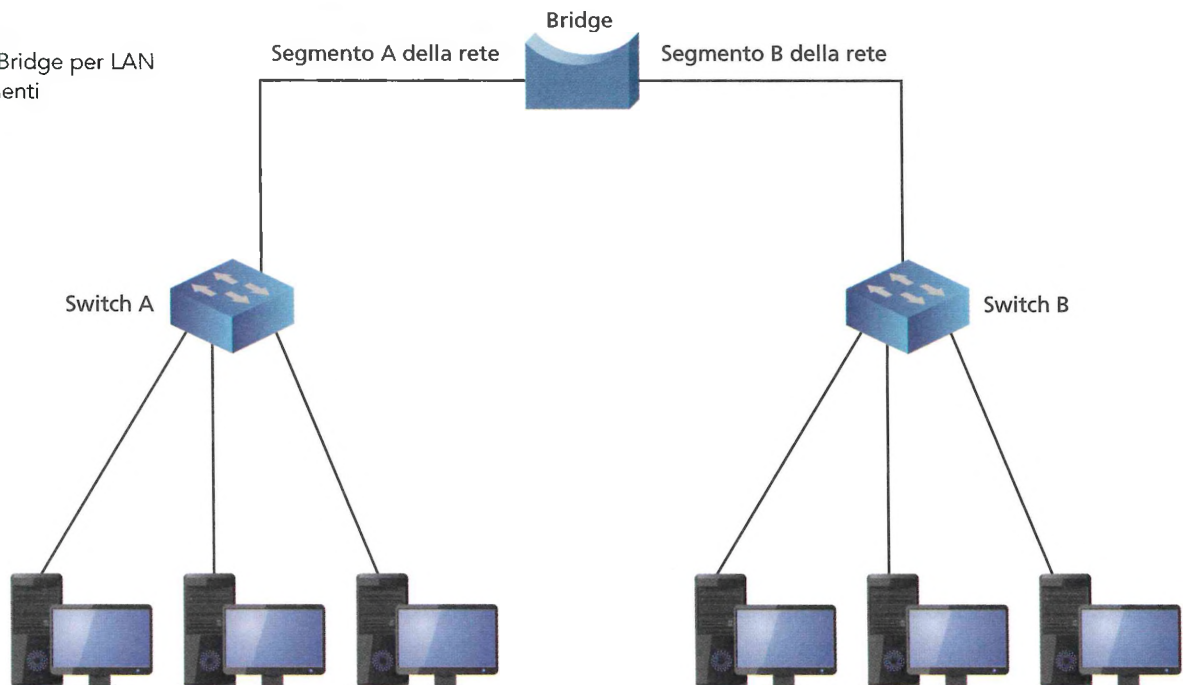


FIGURA 41 Bridge per LAN con 2 segmenti



I bridge permettono quindi la suddivisione di grosse reti in sottoreti in modo da facilitare la gestione e il controllo delle stesse, oppure permettono di creare delle macroreti partendo da reti locali già esistenti. È possibile in questo modo creare delle reti dipartimentali che verranno poi inglobate nell'unica rete aziendale.

7.4 Il router

Un **router** è un dispositivo hardware che si occupa di far comunicare tra loro reti differenti ed eterogenee instradando i pacchetti nella giusta direzione. Il router, in particolare, è il dispositivo utilizzato per permettere l'accesso di tutti i computer di una rete LAN a un'altra rete (per esempio a Internet).

Reti diverse parlano "linguaggi" diversi, quindi a livello di trasmissione fisica, di accesso e di controllo, per collegare tra loro due reti non è sufficiente metterle in comunicazione tramite un bridge o uno switch. È necessario invece che tra una rete e l'altra venga posto un apposito dispositivo, il router, che parli entrambi i protocolli delle due reti e provveda a leggere, tradurre e rispedire (*store and forward*) i dati che lo attraversano (FIGURA 42 e FIGURA 43).

Tipicamente i router che vengono impiegati nelle reti locali per la connessione a Internet integrano al loro interno le funzioni di modem, di conseguenza in rete viene installato un unico apparato con funzionalità di modem/router.

Il router, quindi, è connesso a due o più reti (FIGURA 44) e si occupa di indirizzare i messaggi decidendo quale percorso far compiere ai dati sulla base delle informazioni



FIGURA 42 Router per MAN-WAN



FIGURA 43 Router aziendale

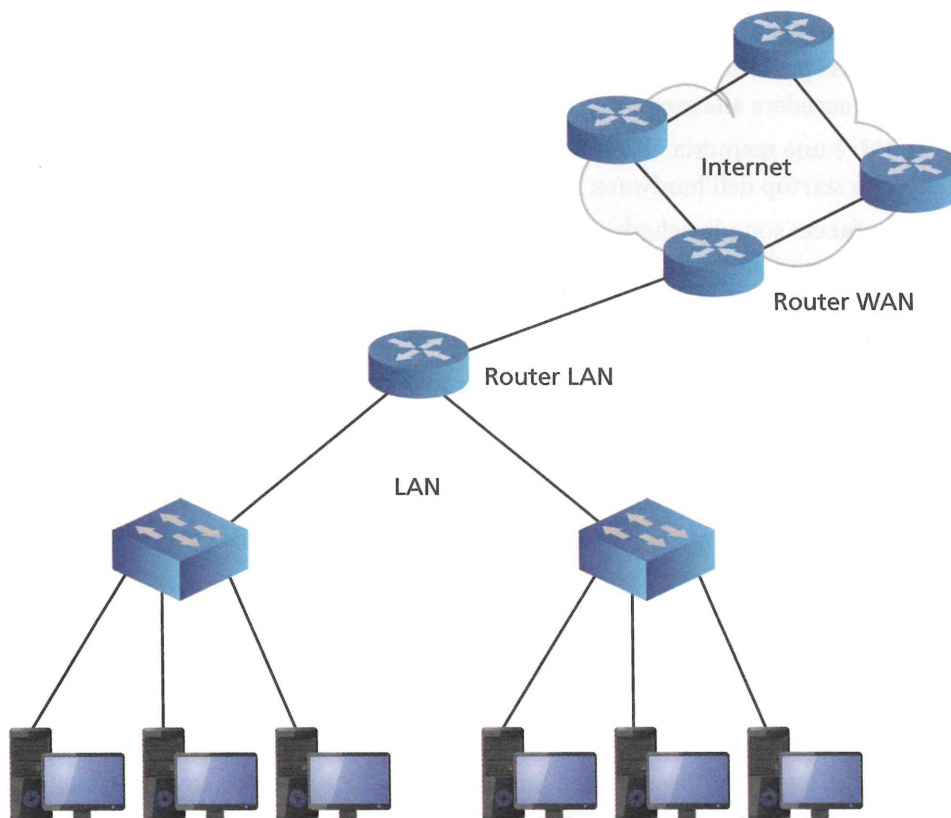


FIGURA 44 Router per LAN e per WAN

dello stato delle reti alle quali è collegato, cioè determinando il successivo punto della rete a cui inoltrare il pacchetto di dati ricevuto. In questo modo il router reindirizza i messaggi che vengono trasmessi tra reti di computer perché vengano instradati fino a raggiungere la destinazione finale.

Le due attività principali di un router sono dunque:

- scegliere il percorso migliore (**routing**);
- mettere i pacchetti sull'interfaccia di uscita corretta (**forwarding**).

Anche se un router può essere usato per segmentare una rete locale, il suo principale utilizzo è come dispositivo per reti geografiche.

Il router, essendo un **computer dedicato al routing** (instradamento dei pacchetti), necessita di un Sistema Operativo e dal punto di vista hardware dev'essere dotato di almeno due schede di rete e di:

- **microprocessore** con CPU specializzata nelle elaborazioni richieste;
- **RAM**: memoria volatile usata per memorizzare la tabella di routing, il file di configurazione, i pacchetti in attesa. La RAM viene condivisa come memoria del processore e memoria di input/output (I/O) per i pacchetti in attesa e in genere è dinamica (DRAM);
- **flash**: memoria di tipo read-only cancellabile e riprogrammabile, è usata per contenere il Sistema Operativo e mantiene il suo contenuto anche se non c'è alimentazione (a differenza della RAM);
- **NVRAM** (Non Volatile RAM): è usata per memorizzare il file di configurazione di startup (quello che viene eseguito all'accensione del router); come la memoria flash, mantiene il suo contenuto anche se non c'è alimentazione;
- **bus**: la maggior parte dei router contiene un System bus e un CPU bus. Il System bus si usa per le comunicazioni tra la CPU e le interfacce, mentre il CPU bus è usato per accedere alle memorie;
- **ROM**: è una memoria non volatile usata per contenere i programmi di diagnostica allo startup dell'hardware;
- **interfacce**: sono le schede di rete del router usate per le connessioni verso l'esterno; generalmente sono di 3 tipi: LAN, WAN, gestionale. Quelle LAN in genere sono di tipo Ethernet o Token Ring, quelle WAN possono essere seriali o ISDN. La porta gestionale (detta anche console o AUX) è usata per la configurazione del router.

Un router con almeno due schede di rete di cui una verso la LAN e una verso la WAN può essere configurato come **gateway** e, attraverso esso, si rende condiviso l'accesso a Internet per tutti i computer della rete locale. L'interfaccia del router che funziona da gateway LAN diventa la "via di uscita" degli host dalla LAN stessa.

7.5 L'Access Point

Gli **AP** (Access Point, **FIGURA 45**) hanno un doppio scopo: sono dei bridge che collegano la parte cablata (wired) della LAN con la parte wireless e consentono ai Wireless Terminal (dispositivi wireless quali: smartphone, tablet, netbook, ecc.) di collegarsi alla rete (agisce quindi da gateway). L'utilizzo degli AP è diventato indispensabile vista la presenza sempre maggiore di dispositivi mobili in una rete.



FIGURA 45 Access Point

Nelle reti domestiche di solito basta un AP che funge anche da router consentendo di collegarsi a Internet. Nelle reti aziendali invece più AP vengono cablati per creare un vero e proprio sistema di distribuzione wireless in cui ogni AP è una **base station** a cui i dispositivi wireless si collegano. Approfondiremo nel corso del quarto anno il principale standard per il wireless: l'IEEE 802.11 che ha dato origine al Wi-Fi sulle bande a 2.4 GHz e a 5 GHz.

La configurazione di un AP in una rete aziendale o domestica prevede l'impostazione di una serie di parametri. I principali sono i seguenti.

- **SSID** (Service Set Identifier): serve ad assegnare un nome alla rete wireless affinché gli utenti possano identificarla. L'AP può essere configurato per trasmettere in broadcast e in continuazione l'SSID attraverso un frame periodico detto **beacon**. In questo modo, i dispositivi wireless sono in grado di rilevare l'elenco delle reti wireless esistenti nel loro raggio d'azione.
- **Potenza**: la normativa ETS 300-328 dell'ETSI (European Telecommunications Standards Institute) impone di non irradiare segnali con una EIRP (Effective Isotropic Radiated Power), cioè la potenza che effettivamente è emessa dall'antenna in ogni direzione, superiore a 100mW per la banda a 2.4 GHz e 1 W per la banda a 5 GHz.
- **Canale**: poiché le bande sono divise in canali da alcuni MHz, si può impostare l'AP affinché lavori su uno qualsiasi dei canali disponibili. AP vicini non devono usare lo stesso canale per evitare interferenze.
- **Crittografia**: lo standard di crittografia e di autenticazione è la WEP (Wired Equivalent Privacy). È necessario attivarla come livello minimo di sicurezza. Si deve assegnare una chiave di crittografia a ogni utente perché possa collegarsi all'Access Point con dati crittografati. Le chiavi standard sono da 10 cifre esadecimali (40 bit) o da 26 cifre esadecimali (104 bit) corrispondenti alla crittografia rispettivamente a 64 o 128 bit per via dell'aggiunta, in entrambi i casi, di un vettore d'inizializzazione a 24 bit.

FISSA LE CONOSCENZE

- A che cosa serve la scheda di rete (NIC)?
- Che cosa è in grado di fare un hub "intelligente"?
- Che differenza c'è tra switch e bridge?
- Quali compiti principali svolge un router?
- Quali sono le caratteristiche hardware di un router?
- Che cos'è e a che cosa serve l'SSID?



Case study
Installazione di un
modem ADSL