Tratto dal Testo
Ettore Panella - Giuseppe Spalierno
Corso di Telecomunicazioni 2
Edizioni Cupido

CAPITOLO QUINTO

RETI LOCALI E GEOGRAFICHE

1. Generalità

Una rete per trasmissione dati è costituita da un insieme di supporti hardware e software per il collegamento di due o più terminali di elaborazione dati.

La necessità di trasferire informazioni da un terminale remoto ad un altro o nella memoria centrale di un sistema di elaborazione dati ha portato alla progettazione ed allo sviluppo di tecniche hardware, alla messa a punto di protocolli di comunicazione, alla comparsa di software applicativo ed all'uso di supporti in parte già esistenti, per il trasferimento fisico delle informazioni.

Il panorama attuale annovera la costituzione di reti:

- locali
- metropolitane
- geografiche

Le prime sono costituite da un limitato numero di computer collegati tra loro nell'ambito di una stanza, di un edificio, o, in genere, di computer distanti tra loro qualche centinaia di metri.

Le reti geografiche, invece, interconnettono sistemi distanti tra loro anche migliaia di chilometri.

Le reti metropolitane hanno un ambito cittadino.

Negli anni '90 si è sviluppato in tutto il mondo una tecnica che consente di collegare tra loro reti locali, reti geografiche, singoli terminali anche eterogenei tra loro circa l'ambiente di sviluppo in cui operano.

Essa è una rete gigantesca costituita dall'insieme di una miriade di reti, sia geografiche che locali, sia grandi che piccole: è la rete delle reti nota col nome di **internet**.

Nel primo volume si è sviluppato un capitolo sulle reti di computer con particolare riferimento all'assemblaggio ed alla configurazione del software sia per la gestione di una rete locale che per il collegamento ad internet.

Nei paragrafi successivi, invece, si svilupperanno i concetti relativi alle reti locali e geografiche con particolare riferimento ai protocolli di comunicazioni ed ai servizi offerti.

2. Reti locali

Le reti locali, note col termine **LAN** (Local Area Network), sono reti private ad alta velocità di piccole estensioni utilizzate per la trasmissione dei dati tra due o più apparati che, generalmente, sono computer localizzati in un'area limitata.

La tecnologia più affermata è la Ethernet nella quale la massima velocità di trasmissione dei dati è di 10Mbit/s, 100Mbit/s nella Fast Ethernet e di 1Gbit/s nella Gigabit Ethernet.

Il tasso di errore di trasmissione è assai basso: 10^{-8} - 10^{-9}, ovvero un errore medio di un bit ogni 100 milioni – 1 miliardo di bit trasmessi correttamente.

Si rammenta che l'architettura di una rete locale è costituita da un insieme di **nodi** collegati tra di loro attraverso i **rami**.

Il nodo può essere un punto terminale di un ramo, cioè un punto della rete dove risiedono le risorse che si intendono condividere, o un punto di congiunzione in cui confluiscono due o più rami, cioè un apparato di rete come, ad esempio, Hub o Switch.

Il ramo rappresenta il canale di comunicazione che collega due nodi e si avvale di mezzi trasmissivi in cavo o ad onde elettromagnetiche.

I mezzi trasmissivi in cavo utilizzati sono:

- *doppino intrecciato*; è un mezzo economico; se non è schermato presenta una certa sensibilità ai disturbi elettromagnetici, consente notevoli velocità di trasmissione per distanze fino a qualche centinaio di metri.
- *cavo coassiale*; per la sua elevata larghezza di banda consente elevate velocità per distanze di diversi chilometri.
- *fibra ottica;* presenta una totale immunità al rumore elettromagnetico e consente velocità di trasmissione fino a 12Gbit/s avendo una larghezza di banda di oltre 10GHz.
- *rete elettrica;* si utilizza la normale rete elettrica presente negli edifici per collegare i computer alla rete locale. La distanza massima tra i computer è dell'ordine di 100m. e la velocità di trasmissione è intorno a 10Mbit/s. Sono in atto studi per perfezionare ulteriormente tale tecnica.

L'informazione può essere modulata in **banda base** o a **larga banda**.

Nel primo caso i dati sono trasmessi in linea in forma digitale ma opportunamente codificati: un codice molto utilizzato è il codice Manchester[1].

Nel secondo caso il segnale digitale è modulato da una o più portanti ad alta frequenza e poi viene trasmesso. Ciò consente di realizzare contemporaneamente più trasmissioni su uno stesso mezzo di comunicazione.

I mezzi trasmissivi che sfruttano l'etere per il trasporto delle informazioni si dividono:

- *a radiofrequenza (ponti radio, satelliti, onde radio al suolo);*
- *a infrarossi.*

Le reti che utilizzano l'etere sono definite **senza fili** (wireless).

La scelta del mezzo fisico di collegamento dipende dalla distanza dei nodi da collegare, dalla velocità di funzionamento desiderata, dalla affidabilità della trasmissione e dai costi di installazione che si è disposti a sopportare.

Un altro problema che una rete locale deve poter risolvere è la diversità degli ambienti operativi dei singoli nodi : DOS, Windows, UNIX, Linux, ecc.

[1] Codice bipolare che evita lunghe sequenze di 0 o di 1.

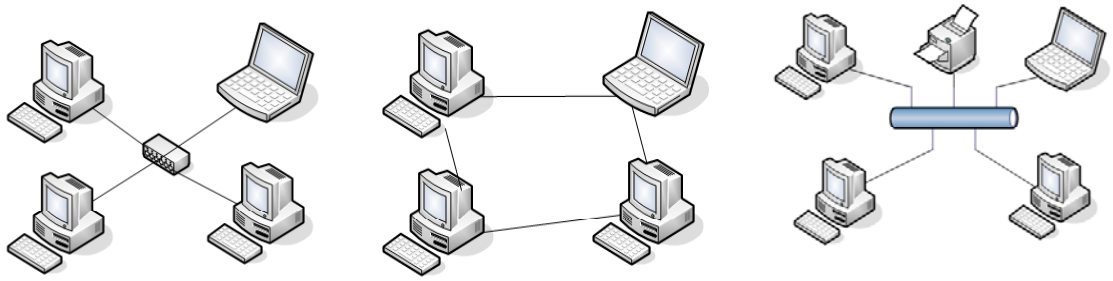
2.1 Topologia delle reti locali

Le strutture delle reti sono numerose ma tutte riconducibili a tre tipiche configurazioni fondamentali che sono:

- rete a stella;
- rete ad anello;
- rete a bus.

Per ciascuna di esse è possibile scegliere il mezzo trasmissivo da utilizzare, la tecnica di modulazione, il metodo di accesso alla rete ed il relativo tipo di controllo.

Nella **rete a stella** si individua un nodo centrale a cui sono collegati gli altri nodi attraverso trasmissioni bidirezionali. In fig.1a si mostra una tipica configurazione di rete LAN a stella.



a) Rete a stella **b) Rete ad anello** **c) Rete a bus**

Fig.1. – Tipologie delle reti.

Questo tipo di collegamento presenta il vantaggio di un basso costo, facilità di espansione ed agevole manutenzione. Il centro stella spesso è un apparato di rete come Hub o Switch. Svantaggio: in caso di avaria del centro stella la rete è paralizzata. Vantaggi: l'apparato di rete rigenera i livelli elettrici del segnale. L'hub riceve i dati da un nodo e li smista su tutti gli altri nodi, intasando così tutte le linee disponibili. Lo switch è più intelligente: "legge" i dati ricevuti, individua il destinatario ed invia i dati solo al nodo del destinatario evitando, così, di intasare tutte le linee come fa l'hub.

Nella **rete ad anello** ogni nodo risulta connesso ai due nodi adiacenti da rami con collegamento punto-punto unidirezionale. La struttura realizza un percorso chiuso come si mostra in fig.1b.

Ciascun nodo deve essere in grado, attraverso il confronto del proprio indirizzo con quello associato al flusso dei dati, di riconoscere se il messaggio che transita in rete è destinato ad esso. In caso contrario il nodo ritrasmette il messaggio al nodo adiacente.

I vantaggi presentati da questo tipo di rete derivano dal fatto che ogni nodo rigenera elettricamente il segnale ricevuto: ciò consente di realizzare reti di lunghezze più elevate rispetto alle altre; un altro vantaggio consiste nella semplificata procedura di instradamento in quanto il messaggio ricevuto deve essere inviato solo al nodo adiacente.

Fra gli svantaggi annoveriamo la possibilità di paralisi della rete derivante da un guasto ad un nodo o alla linea. Per ovviare a tale inconveniente si impiegano reti ad anello bidirezionali per cui, in caso di guasto sulla rete o in un nodo, i dati possono transitare dal trasmettitore al ricevitore seguendo l'altro percorso.

La relativa lentezza nella trasmissione dipende dal numero di nodi costituenti la rete: infatti ogni nodo deve leggere e poi trasmettere al nodo successivo le informazioni che viaggiano in linea.

Per evitare conflitti dovuti alla richiesta simultanea della rete da parte di due o più nodi si utilizza la tecnica *Token-ring* per il controllo dell'accesso alla rete.

La tecnica consiste nel far circolare nella rete una particolare stringa binaria, denominata **token** (gettone). Il nodo in attesa di trasmissione che riceve il token ha il consenso all'utilizzo della rete. Alla fine della trasmissione il nodo cede il token a quello successivo. Se il nodo non deve trasmettere alcun dato, legge il token e lo rispedisce immediatamente a quello adiacente.

Una **rete a BUS** è costituita da un'unica linea multipunto a cui risultano collegati, tramite cavo coassiale, tutti i nodi della rete come si mostra in fig.1c. Le estremità del bus vanno chiuse con resistenze di terminazione.

È una configurazione concettualmente molto semplice, di facile espansione e caratterizzata da buona affidabilità e flessibilità.

I dati trasmessi da un generico nodo vengono immessi sul BUS e letti da tutti gli altri nodi. Essi saranno acquisiti solo dal nodo destinatario il quale confronta il suo indirizzo con quello associato al messaggio in transito.

Un vantaggio consiste nella immunità a situazioni critiche: se un nodo va in avaria la rete continua a funzionare correttamente con la sola esclusione, ovviamente, del nodo guasto.

Uno svantaggio di questa configurazione è la ridotta lunghezza della rete poiché non è possibile, a differenza della rete ad anello, rigenerare il segnale.

La rete a bus utilizza il cavo coassiale. La rete a stella, di norma, utilizza un cavo costituito da due coppie di fili conduttori intrecciati per la riduzione dei disturbi elettromagnetici, una coppia per la trasmissione e l'altra per la ricezione.

Esiste un'altra topologia, molto impiegata, che utilizza sia quella a stella che a bus; essa viene definita *rete mista.* Al bus principale, denominato *dorsale*, sono collegate delle bretelle ognuna delle quali porta al centro di una sotto-rete locale a stella come si mostra in fig.2. Il centro stella è un dispositivo concentratore di rete (HUB o SWITCH) che ha il compito di dirigere il traffico di rete e di individuare eventuali problemi. Un concentratore può controllare un numero limitato di nodi (da 4 a 24, tipicamente). Per la gestione di una stella con un numero più elevato di nodi si utilizza di solito uno chassis nel quale si sistemano due o più SWITCH collegati tra loro (*stackable*).

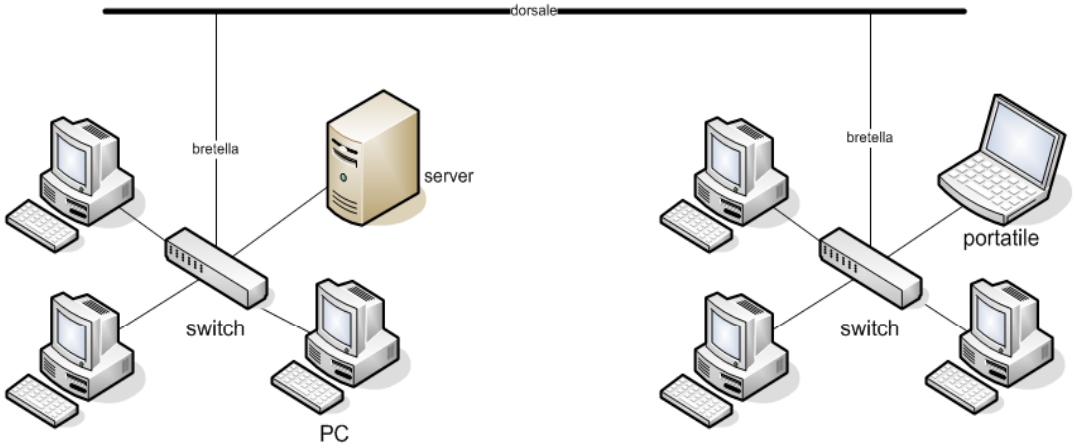


Fig.2. – Esempio di rete locale mista.

2.2. Tecniche di accesso alla rete

Le tecniche di accesso descrivono le modalità con le quali i nodi terminali utilizzano il mezzo trasmissivo al fine di realizzare una corretta trasmissione delle informazioni.

L'obiettivo delle tecniche di accesso è quello di gestire in modo ottimale il traffico all'interno di una rete locale ovvero nella capacità di smaltire velocemente il traffico dati.

Esse si possono suddividere in due grandi categorie:

- accesso a contesa;
- accesso a domanda.

La prima tecnica è di tipo casuale e consente a ciascun nodo, in modo asincrono, di iniziare la trasmissione.

La tecnica di accesso a domanda cede ad un nodo il diritto di trasmettere sulla rete in determinati periodi di tempo.

2.2.1. Tecniche di accesso a contesa

Le tecniche di accesso a contesa sono utilizzate nelle reti locali a BUS e a stella in cui i vari nodi condividono lo stesso mezzo fisico con modalità asincrona.

Ciò determina una elevata probabilità di conflittualità che è possibile evitare introducendo opportuni controlli sull'accesso alla rete.

Tecnica CSMA (Carrier Sense Multiple Access)

La tecnica CSMA (accesso multiplo a rilevazione di portante) è una tecnica che consiste nell'*ascolto* del canale prima di passare alla trasmissione dei dati.

Se il canale è libero si procede alla trasmissione dei dati senza più preoccuparsi del controllo del canale.

Se il canale è occupato sono possibili due attività:

- aspettare che il canale si liberi prima di trasmettere;
- riascoltare il canale dopo un dato tempo di ritardo.

Questa tecnica non elimina del tutto la possibilità di collisione tra i dati trasmessi simultaneamente da due nodi perché potrebbe verificarsi il caso in cui due o più nodi, trovando il canale libero, inizino contemporaneamente la trasmissione generando, così, la collisione dei dati.

La sovrapposizione dei dati provenienti da più nodi impedisce il corretto riconoscimento dei dati stessi da parte dei nodi ricevitori introducendo, così, errori di lettura.

La probabilità di collisione aumenta col ritardo di propagazione del segnale e con la distanza tra due nodi concorrenti.

I nodi ricevitori si possono trovare davanti a due casi: ricevono il pacchetto di dati con errori o non ricevono alcun dato.

Nel primo caso rispondono con un messaggio di non riconoscimento (NAK), nel secondo caso non rispondono affatto.

Il trasmettitore, in entrambi i casi, non ha ricevuto in risposta la conferma ACK della corretta ricezione dei dati da parte del ricevitore ed è costretto, quindi, a ritrasmettere il pacchetto con inevitabile rallentamento della velocità di trasmissione.

L'aumento del numero dei nodi peggiora la situazione poiché aumenta la probabilità di collisione.

Per risolvere, almeno in parte, il problema della collisione sono state introdotte delle varianti una delle quali è descritta di seguito.

Tecnica CSMA/CD (Collision Detection)

Questa tecnica, utilizzata nelle reti Ethernet e pubblicata come standard IEEE802.3, differisce dalla precedente durante la trasmissione dei dati; infatti, nella tecnica precedente, il nodo inizia la trasmissione se rileva il canale libero e non si cura più dell'ascolto del canale.

Nella tecnica CSMA/CD (CSMA a rivelazione di collisione) il nodo continua l'ascolto del canale anche a trasmissione avviata: in caso di collisione la comunicazione in corso viene sospesa, il nodo trasmettitore genera una stringa binaria di 4-6 byte, nota come "sequenza di jamming", che permette a tutte le stazioni di rilevare la collisione e di scartare i bit ricevuti come frutto della collisione.

Il nodo trasmettitore ripete la procedura di inizio trasmissione dopo un intervallo di tempo di attesa pseudocasuale To.

In questo modo difficilmente i due nodi potranno rientrare in conflitto.

Questo metodo consente di ridurre fortemente la possibilità di collisione rendendo, così, la trasmissione più efficiente.

Il tempo di attesa To prima della ritrasmissione è un multiplo intero dello "slot time" pari a $t_s = 51.2\mu s$:

$$To = r \cdot t_s$$

ove: $0 \leq r \leq 2^k-1$, con $k = \min(n,10)$, ed n è il numero delle collisioni precedenti.

Ogni volta che avviene una collisione, r può aumentare e quindi anche To.

Dopo 16 collisioni viene inviato un messaggio di errore e la trasmissione è sospesa.

Lo slot time t_s rappresenta il tempo necessario per la trasmissione di un pacchetto di 64byte alla velocità di 10Mbps. Infatti:

$$64byte \cdot 8 / 10Mbps = 51.2\mu s$$

Supponendo che la velocità dei dati all'interno del cavo in rame sia pari a $200 \cdot 10^3$Km/s, nello slot time t_s il segnale percorre uno spazio pari a:

$$s = v \cdot t_s = 200 \cdot 10^3 Km/s \cdot 51.2\mu s \cong 10Km$$

In caso di collisione con i dati trasmessi da un altro nodo, i frammenti prodotti dalla propria trasmissione ritornano al mittente in 51.2μs dopo aver percorso 10Km: 5Km in andata e 5Km per il ritorno.

Poiché le prime specifiche Ethernet relative alle reti locali prevedono nodi tra loro distanti per meno di 5Km. si deduce che, in caso di collisione, i frammenti di ritorno raggiungono il trasmettitore prima che questo termini la trasmissione del più piccolo pacchetto di dati consentito dal protocollo Ethernet e cioè 64byte.

Si mostra in fig.3 il flow-chart della tecnica di accesso alla rete CSMA/CD attivato da un nodo. Si osservi che la totalità delle informazioni da trasmettere viene suddivisa in "pacchetti", cioè in sottoinsiemi di dati.

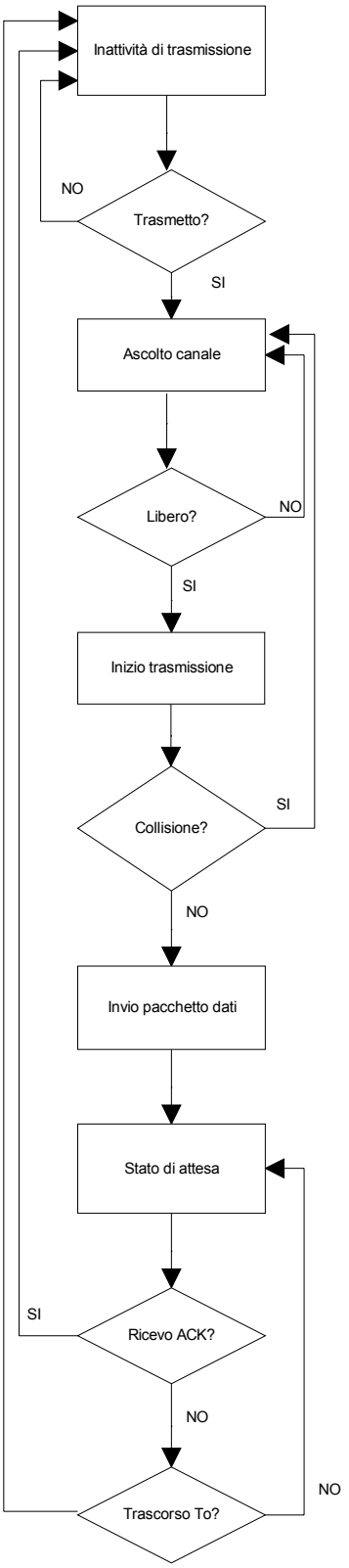


Fig.3. - Flow-chart semplificato relativo alla tecnica di accesso CSMA/CD.

2.2.2. Tecniche di accesso a domanda

Le tecniche di accesso a domanda si possono utilizzare nelle reti locali ad anello e a stella e consistono nell'interrogazione ciclica dei nodi oppure nell'inserire nella rete una stringa (token) che fornisce al nodo che la riceve il consenso o il diniego all'accesso alla rete. Le reti che adottano queste tecniche di accesso non hanno il problema della contesa del mezzo trasmissivo e, di conseguenza, non sono soggette a collisioni.

Tecnica di Polling/Selecting

È utilizzata nelle reti a stella e ad anello in cui un nodo svolge la funzione di controllore.

Nella tecnica di *polling* il controllore effettua una interrogazione ciclica ai nodi della rete: un nodo potrà trasmettere dati al nodo controllore solo quando quest'ultimo glielo consente.

Nella tecnica di *selecting* il controllore chiede al nodo selezionato se è disposto a ricevere dati. In caso affermativo il controllore trasmette i dati al nodo.

Le due tecniche non sono efficienti per due motivi:

- la comunicazione interessa un solo nodo;
- un nodo deve attendere necessariamente il proprio turno anche se deve trasmettere in rete con una certa urgenza.

Tecnica Token-ring

Sviluppata dalla IBM e successivamente pubblicata come standard IEEE802.5, è utilizzata nelle reti ad anello ed è in grado di stabilire l'ordine e il momento in cui un nodo può trasmettere le informazioni.

Il nodo controllore trasmette in rete una particolare configurazione di bit nota col nome di **token** (gettone) che consente, a chi lo riceve, di avviare la trasmissione, ammesso che abbia qualcosa da trasmettere. Se il nodo che ha catturato il token non ha alcun dato da trasmettere, rimette in rete il token che giungerà al successivo nodo.

Il nodo che desidera trasmettere, subito dopo aver catturato il token, avvia la trasmissione dei dati, dell'indirizzo del destinatario ed, infine, del token.

Il pacchetto in trasmissione si propaga di nodo in nodo fino al destinatario.

Il nodo che in un dato istante riceve il pacchetto di dati, confronta il proprio indirizzo con quello inserito nel pacchetto: in caso di coincidenza acquisisce i dati, ne controlla la correttezza e, in caso affermativo, modifica alcuni bit di controllo e rimette i dati in rete. Se gli indirizzi non coincidono, il nodo, senza apportare alcuna modifica, immette il pacchetto in rete che sarà successivamente esaminato dal nodo successivo.

Quando il pacchetto, completando l'anello, ritorna nuovamente al trasmettitore, quest'ultimo riconosce che è stato correttamente acquisito per cui lo rimuove dalla rete e successivamente immette in quest'ultima il token.

Il token, in questa tecnica, soddisfa alcune regole:

- è uno solo in tutta la rete;
- non può essere usato da un nodo due volte consecutivamente.

Tecnica token-bus

Standard IEEE802.4, è utilizzata da reti locali a BUS. Il token percorre un *anello logico* definito a priori: ogni nodo ha un proprio indirizzo e conosce l'indirizzo del nodo che lo precede e di quello che lo segue. In tal modo il token percorre un itinerario ben preciso.

2.3. Gli standard

I costruttori di apparati elettronici hanno da sempre rivolto la loro attenzione all'efficienza e all'ottimizzazione delle loro macchine piuttosto che alla possibilità della comunicazione tra macchine di ditte differenti.

L'incomunicabilità tra le macchine divenne, negli anni '70, un problema troppo serio che impediva il trasferimento automatico delle informazioni per cui nel 1980 l'*Organizzazione Internazionale per Standardizzazione* (ISO) formò un gruppo di studio col compito di formulare un modello di standardizzazione anche per le reti locali.

Fu proposto il modello OSI (Open System Interconnection), descritto nel precedente capitolo, composto di sette livelli, dal livello fisico a quello delle applicazioni.

Ogni livello si avvale di regole e protocolli da rispettare e di relative interfacce, hardware o software, per comunicare con i livelli adiacenti.

Le reti locali non utilizzano tutti e sette i livelli del modello OSI anche perché ciascun costruttore può impiegare protocolli diversi o far svolgere più funzioni ad uno stesso livello. Si riporta in fig.4 il confronto tra i 7 livelli del modello OSI con quelli della rete locale con accesso a contesa CSMA/CD, sicuramente il più utilizzato.

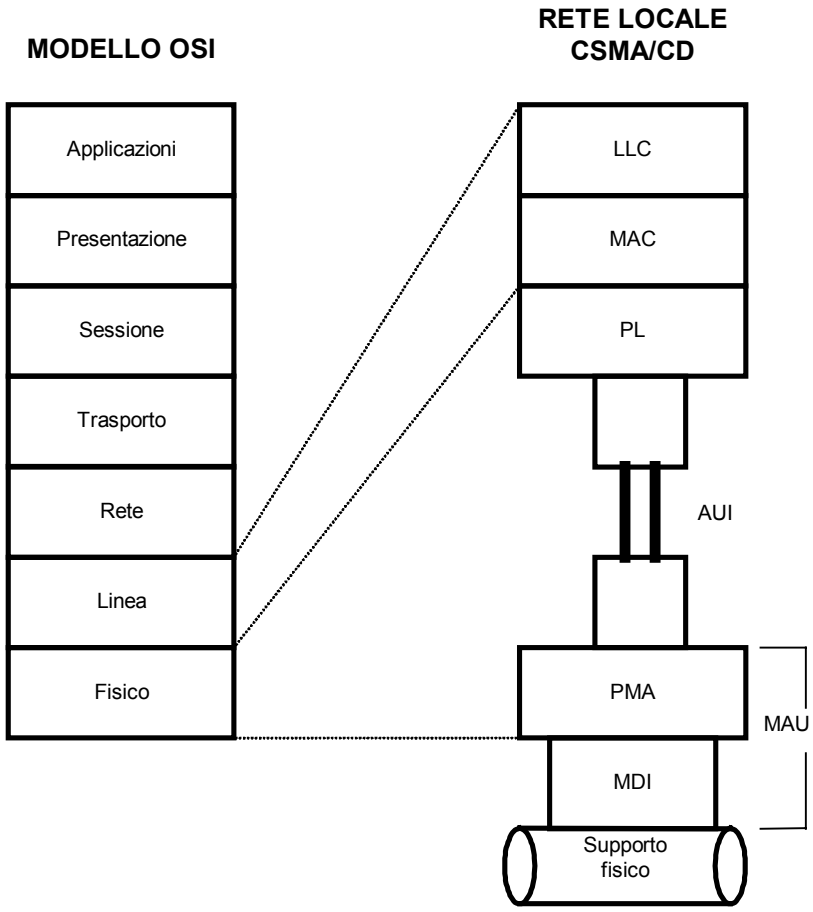


Fig.4. - Confronto tra i livelli del modello ISO/OSI ed i livelli della rete locale CSMA/CD.
Legenda :
LLC : (Logical Link Control = Controllo del collegamento logico);
MAC : (Media Access Control = Controllo dell'accesso ai supporti fisici);
PL : (Physical Layer = Strato fisico);
AUI : (Attachment Unit Interface = Interfaccia per unità di connessione);
PMA : (Physical Medium Attachment = Connessione del supporto fisico);
MDI : (Medium Dependent Interface = Interfaccia dipendente dal supporto fisico);
MAU : (Medium Attachment Unit = Unità di connessione del supporto fisico).

2.3.1. Sottolivello LLC

Il livello di linea del modello ISO/OSI corrisponde, nel modello rete locale CSMA/CD e cioè IEEE802.3, ai due sottolivelli LLC e MAC.

LLC controlla l'accesso al canale condiviso dagli elementi della rete, crea una struttura paritetica tra i vari nodi che rende la rete meno sensibile agli errori ed è indipendente dai metodi di accesso specifici.

Si mostra in fig.5 i sottolivelli LLC e MAC inseriti nel modello ISO/OSI con i vari standard IEEE802 corrispondenti agli standard ISO 8802.

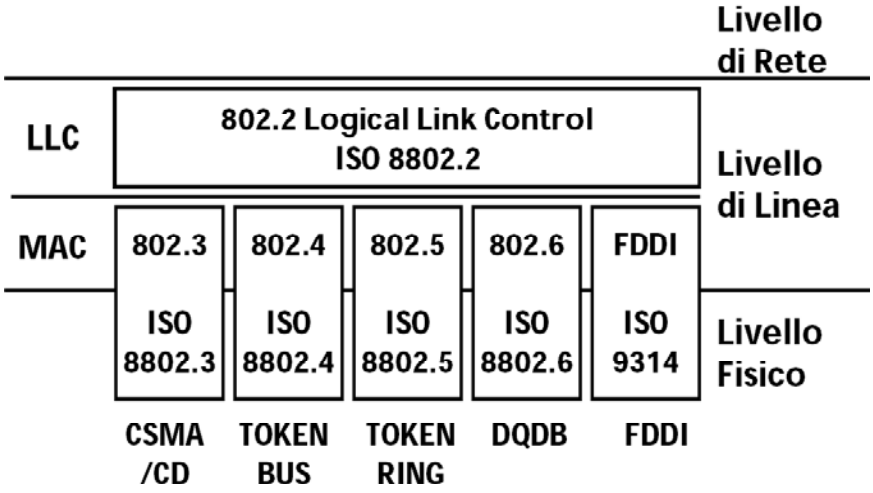


Fig.5. Sottolivelli LLC e MAC.

Gli standard IEEE 802 prevedono quattro tipi di servizio a livello LLC:

1. Servizio senza connessione e senza riconoscimento;
2. Servizio orientato alla connessione;
3. Servizio senza connessione e con riconoscimento;
4. Servizio orientato alla connessione e con riconoscimento.

Un servizio si dice senza connessione se non esiste un collegamento diretto tra due nodi che si scambiano dati ma una rete di connessioni attraverso la quale si possono identificare vari cammini tra i due nodi.

2.3.2. Sottolivello MAC

Lo strato di controllo dell'accesso ai supporti fisici (MAC) è responsabile della gestione del traffico sulla rete locale. Determina l'istante in cui il supporto fisico della LAN può trasmettere i dati, individua le collisioni dei dati e determina quando deve essere effettuata l'eventuale ritrasmissione.

Tutto ciò è praticamente realizzato dalla scheda di rete inserita in un computer.

La scheda di rete è nota col temine NIC (Network Interface Card) e possiede un indirizzo univoco, chiamato *MAC Address*, costituito da 6 byte, espresso in forma esadecimale.

I primi 3 byte individuano la ditta costruttrice, i secondi 3 byte individuano il numero di serie progressivo della ditta che ha prodotto quella scheda.

Ad esempio, il software di indagine delle caratteristiche di un computer fornisce le seguenti informazioni circa il MAC address della scheda di rete montata:

Network Card MAC Address: 82:0A:BD:2F:CF:18

ove 82:0A:BD rappresenta il codice della ditta *Via Tecnologies, Inc.* mentre 2F:CF:18 rappresenta il numero progressivo.

Il MAC address è trasparente all'utente poiché è utilizzato dal software di rete che permette di associare il MAC address al nome convenzionale che l'utente sceglie per il proprio computer.

2.3.3. Standard IEEE802

Le normative sulle reti LAN sono curate, fin dal 1980, principalmente dall'IEEE (Institute of Electrical and Electronics Engineers) che opera con sottocomitati.

I vantaggi che si ottengono dall'utilizzo degli standard si manifestano nella possibilità di collegamento tra risorse informatiche differenti, possibilità di futura espansione del sistema e maggiore ventaglio di scelta dei dispositivi terminali.

Gli standard pubblicati relativi alle reti locali sono noti con la sigla IEEE802. Il numero 802 rappresenta l'anno ed il mese di prima pubblicazione dello standard: anno 80, mese 2 cioè febbraio 1980.

In particolare gli standard relativi alle reti locali, in continuo aggiornamento, sono elaborati da gruppi di lavoro che si occupano della definizione di regole che facilitano il passaggio di dati da una rete all'altra. Si mostra un elenco di alcuni di essi:

802.1 standard per il livello di rete HLI (High Level Interface) che si occupa dell'indirizzamento, individuazione del percorso e controllo della correttezza del flusso dei dati;
802.2 standard per il protocollo Logical Link Control (LLC) (non attivo);
802.3 **standard per LAN CSMA/CD (reti Ethernet);**
802.4 standard per LAN a BUS con Token-Bus (non attivo);
802.5 standard per LAN ad anello con Token-Ring (non attivo);
802.6 standard per MAN (Metropolitan Area Network) (non attivo);
802.7 proposta tecnica broadband (non attivo);
802.8 proposta tecnica a fibre ottiche (gruppo sciolto);
802.9 Servizi LAN Integrati ISLAN (non attivo);
802.10 Interoperable LAN Security (non attivo);
802.11 **standard per LAN senza fili a radiofrequenza (wireless).**

2.4. Rete Ethernet

La rete Ethernet, proposta nel 1973 dal gruppo di aziende Digital-Intel-Xerox (DIX), è utilizzato per brevi distanze. Successivamente le sue specifiche sono convogliate, nell'anno 1980, nello standard IEEE802.3 a sua volta diversificato in varie sottocategorie in funzione della massima velocità di funzionamento e del tipo di supporto utilizzato: cavo coassiale, doppino telefonico, fibra ottica.

Il supporto fisico di base è un cavo coassiale per alta frequenza del tipo RG8 (thick Ethernet) o RG58 (thin Ethernet) con terminale a BNC (British Naval Connector).

Il tipo di rete è a bus o a stella ed utilizza il metodo d'accesso a contesa CSMA/CD.

Il protocollo dei dati supporta il formato HDLC, la massima velocità di trasmissione è di 10Mbps, 100Mbps per la Fast Ethernet e 1Gbps per la Gigabit Ethernet.

I dati sono trasmessi in banda base con codifica Manchester o altre codifiche simili.

La distanza massima tra due nodi adiacenti va da poche decine di metri a 500 metri in funzione della massima velocità di trasferimento dei dati e del supporto fisico utilizzato.

I dati da trasmettere vengono frazionati in pacchetti ognuno dei quali contiene una campo di intestazione di 18 byte e un campo dati di lunghezza compresa tra 46 e 1500 byte. Se il campo dati è vuoto vengono comunque trasmessi 46 byte come riempitivo. La lunghezza complessiva del pacchetto è, quindi, compresa tra 64 e 1518 byte.

Il *formato del pacchetto,* secondo la specifica 802.2*,* prevede otto campi, di seguito elencati:

1. Preambolo. È costituito da 7 byte uguali dal codice binario 10101010 (HEX: AA) e serve per la sincronizzazione dei nodi ricevitori; se la rete funziona a 10Mbps, la durata del preambolo è pari a 5.6μs (7byte · 8bit · 0.1μs).
2. Inizio trama. È costituito dal byte 10101011 (HEX: AB) e segnala la fine del preambolo e quindi l'inizio del pacchetto dati vero e proprio.
3. MAC address del nodo di destinazione. È costituito da 6 byte. Se tutti i bit sono a 1 i dati vengono inviati a tutti i nodi;
4. MAC address del nodo di origine. È costituito anch'esso da 6 byte;
5. Tipo. È costituito da 2 byte. Contiene informazioni di servizio che cambiano di significato in funzione dell'ambiente in cui ci si trova (Novell NetWare, AppleTalk, Internet, ecc.)
6. Campo dati. È costituito da una lunghezza che va da 0 a 1500 byte.
7. Campo riempitivo. È di lunghezza variabile in funzione della quantità di dati del precedente campo dati. Questo campo garantisce che la lunghezza della trama complessiva sia almeno di 64byte anche in assenza di dati da trasmettere. In questo ultimo caso la lunghezza di tale campo è di 46byte.
8. Campo controllo. È costituito da 4 byte. Contiene il codice ciclico di ridondanza (CRC) dei campi indirizzo del nodo di destinazione, di origine e del campo dati. I 18 byte del campo di intestazione sono la somma dei byte occupati nei campi MAC address, tipo e campo di controllo.

n.byte	7	1	6	6	2	0-1500	0-46	4
campo	Preambolo	Inizio trama	MAC address ricevitore	MAC address trasmettitore	Tipo	Dati	Riempitivo	CRC

Fig.6. – Trama Ethernet (specifica 802.2).

Nella rete Ethernet in cavo, l'impedenza caratteristica del cavo coassiale è di 50Ω; per evitare fenomeni di *riflessione* la linea va chiusa su una impedenza resistiva di 50Ω in entrambi gli estremi.

Per evitare *attenuazioni*, la lunghezza massima della linea è stabilita in 500 metri (10Base-5 con cavo coassiale spesso RG8, thick Ethernet) o in 200 metri (10Base-2 con cavo coassiale sottile e più robusto RG58, thin Ethernet).

I segmenti addizionali devono essere collegati con un apparecchio *ripetitore locale* col solo compito di rigenerare il segnale elettrico e filtrare le componenti spurie ma non se ne possono usare più di due, pertanto il numero massimo di segmenti è 3.

I ripetitori remoti hanno il compito di collegare due reti locali fisicamente separate e sono tra loro collegati mediante una connessione punto-punto che non deve superare la lunghezza di 1000 metri.

In fig.7 si mostra una tipica struttura LAN Ethernet costituita da 6 segmenti. I primi 3 segmenti sono collegati tra loro attraverso 2 ripetitori locali. Analogamente, gli altri 3 segmenti sono anch'essi collegati tra loro da 2 ripetitori locali. Le 2 sottoreti sono, invece, connesse tra loro attraverso una coppia di ripetitori remoti tramite collegamento punto-punto.

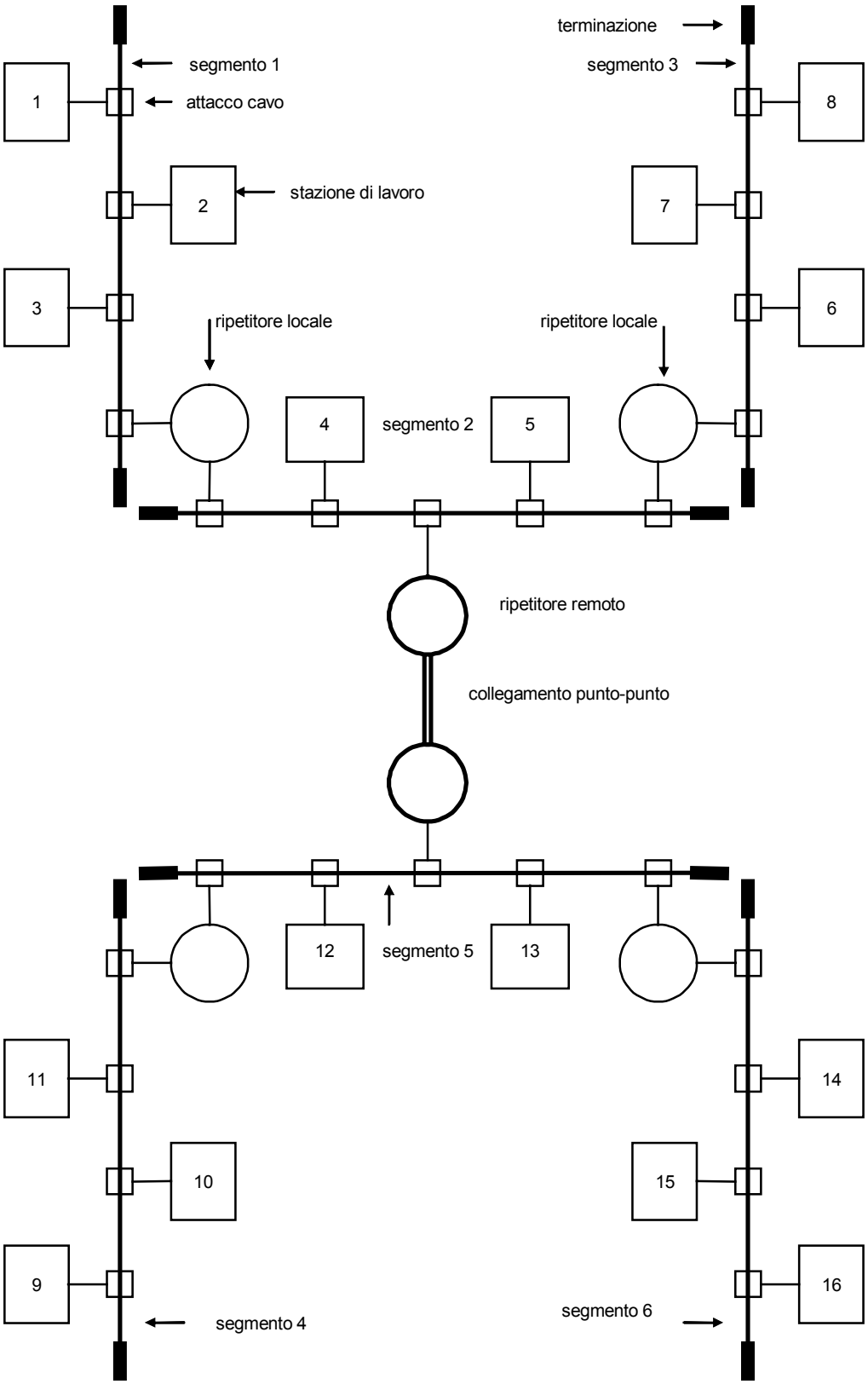


Fig.7. - Esempio di LAN Ethernet in cavo coassiale, ripetitori locali e remoto.

Ciascuna stazione è collegata al cavo coassiale da una scheda di rete denominata *transceiver* con le funzioni di codifica-decodifica dei dati e di stabilire l'accesso al canale. Le funzioni associate alla codifica/decodifica sono:

- generazione/rimozione del preambolo per la sincronizzazione;
- codifica/decodifica col codice Manchester;

Le funzioni svolte per l'accesso al canale sono:

- ascolto della portante in linea per controllare se quest'ultima è libera;
- rivelazione delle collisioni;
- trasmissione e ricezione dei dati codificati.

La soluzione mostrata in fig.7, tuttavia, rappresenta una tipologia di rete ormai superata poiché utilizza il cavo coassiale con i suoi problemi di fragilità e di collegamento di tipo half-duplex.

Si mostra, in fig.8, il collegamento tra il connettore della scheda di rete al bus in cavo coassiale di una rete locale. Un connettore con sagoma a T consente il collegamento alla scheda di rete e a due spezzoni di cavo coassiale con attacco a BNC.

Il connettore a T collegato alla scheda di rete dell'ultimo PC del BUS, come in figura, presenta una terminazione da 50Ω per simulare una linea di lunghezza infinita.

La terminazione presenta un attacco a BNC ed al suo interno contiene una resistenza da 50Ω pari all'impedenza caratteristica del cavo.

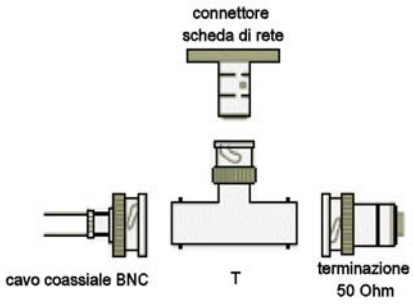


Fig.8

Al giorno d'oggi, però, si preferisce realizzare reti con topologia a stella o misti, come mostrato nella precedente fig.2, con cavo UTP o in fibra ottica a 100Mbps, 1Gbps o 10Gbps che utilizzano apparati di rete di commutazione come gli SWITCH piuttosto che apparati di rete concentratori come gli HUB.

2.5. Evoluzione delle reti Ethernet

In questi ultimi anni si sono succedute numerose versioni dei protocolli di rete tendenti ad ottimizzare questa o quella specifica.

Nella seguente tabella 1 si riassumono le varie tecnologie Ethernet secondo le specifiche IEEE802.3.

Tabella 1. – tipologie delle reti Ethernet

802.3	Ethernet su cavo coassiale spesso e sottile 10Base-5 (Thick Ethernet) 10Base-2 (Thin Ethernet)
802.3i	Ethernet su cavo UTP (doppino intrecciato) 10Base-T
802.3d	Ethernet su fibra ottica FOIRL
802.3j	Ethernet su fibra ottica 10Base-F
802.3u	Fast Ethernet su cavo UTP 100Base-T2 (cavo UTP a 2 coppie) 100Base-T4 (cavo UTP a 4 coppie) 100Base-TX Fast Ethernet su fibra ottica 100Base-FX
802.3ab	Gigabit Ethernet su cavo UTP 1000Base-T
802.3z	Gigabit Ethernet su cavo UTP 1000Base-CX Gigabit Ethernet su fibra ottica 1000Base-SX 1000Base-LX
802.3ae	10 Gigabit Ethernet su fibra ottica 10 GBase-LX per reti locali LAN 10 GBase-R per reti locali LAN 10 GBase-W per reti metropolitane MAN e geografiche WAN

Nel 1985 sono stati approvati gli standard **10Base-5** e **10Base-2**.

Lo standard Ethernet **10Base-2**, in particolare, noto anche come *Thin Ethernet*, consente trasmissioni a 10Mbps in banda base su cavo coassiale sottile con diametro intorno a 5mm. denominato, in sigla, **RG-58**.

La distanza massima è di 200m. La topologia è a BUS e si estende da un nodo all'altro attraverso un collegamento a BNC.

La scheda di rete inserita nel computer presenta una presa a BNC che consente il collegamento al BUS. Affinché quest'ultimo possa estendersi agli altri nodi, si inserisce nella presa a BNC, presente sulla scheda di rete, un adattatore BNC a T, come descritto nella precedente fig.8, in modo da consentire il collegamento di due spezzoni di BUS come si mostra in fig.9.

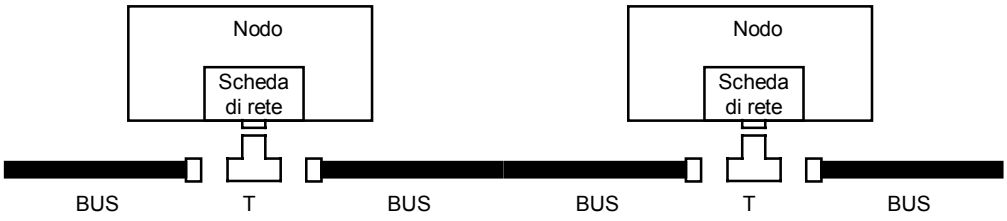


Fig.9. - Collegamento del BUS di rete a due nodi utilizzando adattatore BNC a T.

Agli estremi del BUS si inserisce una resistenza di terminazione del valore di 50Ω col compito di impedire riflessioni del segnale in transito sulla linea.

L'interruzione del cavo in un qualsiasi punto fa "cadere" la rete. È una soluzione economica e flessibile ideale per ambienti di lavoro limitati ad un locale come, ad esempio, un laboratorio scolastico.

Tale rete si presta ad essere utilizzata con gerarchia paritaria (connessione peer-to-peer): ogni macchina può utilizzare le risorse di tutte le altre macchine.

È economica perché non richiede l'utilizzo di HUB, è flessibile perché per l'aggiunta di un nodo è sufficiente aggiungere una tratta di cavo coassiale. Prima di installare il software di rete è opportuno stabilire a priori le risorse che ciascun nodo mette a disposizione della rete, il nome e le password da attribuire a ciascun nodo. Fra gli svantaggi annoveriamo:

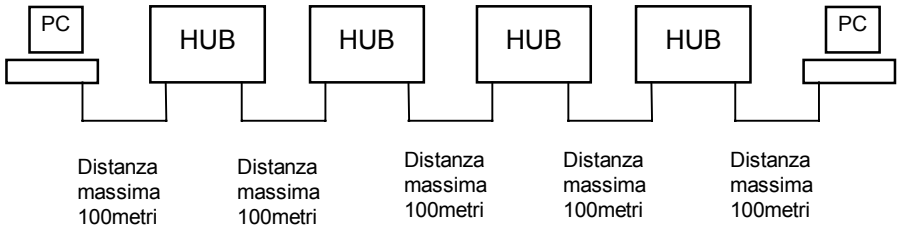
- velocità ridotta ad un massimo di 10Mbps, limite difficilmente raggiungibile;
- connettori BNC non sempre efficienti;
- dorsali volanti esposte a stress fisici;
- difficile manutenzione in caso di guasto per l'impossibilità di isolarlo da una postazione centrale;
- a causa della non elevata qualità del cavo, è bene tenere la lunghezza della linea al di sotto di 100m.

Nel 1990 è stato approvato lo standard **10Base-T** funzionante su doppino telefonico noto con la sigla UTP (Unshield Twisted Pair = Coppia intrecciata non schermata) di categoria 3 – 4, 5 o 5e[2]. I connettori per questo tipo di cavo sono quelli usati nella telefonia americana, conosciuti con la sigla **RJ-45**, molto simili ai *connettori a clip* **RJ11** usati nella telefonia italiana. Il connettore RJ45, però, è ad 8 contatti mentre quello telefonico RJ11 è a 4 contatti. Al primo, pertanto, si possono attestare 4 coppie di cavo intrecciato mentre al secondo solo 2 coppie.

La trasmissione è in banda base a 10 Mbps con topologia a stella. Al centro della stella è ubicato un concentratore, denominato HUB, col compito di smistare, contemporaneamente in tutti i nodi, il flusso dei dati ricevuti. Un altro tipo di centro stella è lo switch. Esso è più intelligente dell'HUB perché esamina il pacchetto ricevuto, individua il nodo di destinazione e trasmette i dati solo al nodo interessato diminuendo, così, il traffico dati nella rete. Il numero di porte di un HUB o di uno SWITCH varia da 4 a 24, tipicamente. Per aumentare la capacità del concentratore è possibile il collegamento in serie tra due di essi. L'interruzione di una tratta isola solo il nodo interessato anziché l'intera rete.

La massima lunghezza della tratta tra un nodo e il concentratore deve essere inferiore a 100m. Si possono collegare fino a 4 HUB e la massima distanza tra i due nodi più lontani è 500m.

Si riporta, in fig.10, lo schema di una rete 10Base-T che utilizza il massimo numero di HUB. Per semplicità di disegno, non sono evidenziati i vari nodi che si attestano sui relativi concentratori.



- Il mezzo trasmissivo è costituito da due delle quattro coppie di doppino non schermato UTP di categoria 3 - 4 o 5 ;
- Due nodi estremi possono essere collegati con non più di 4 HUB ;
- La massima lunghezza della rete è 500m.

Fig.10. - Collegamento Ethernet secondo la specifica 10Base-T.

Ethernet prevede l'uso della fibra ottica a 10Mbps secondo gli standard:
802.3d: FOIRL (Fiber Optic Inter Repeater Link) ormai inutilizzata;
802.3j : 10Base-F, la più lenta tecnologia in fibra ottica, poco utilizzata.

[2] Cavi e connettori per velocità fino a 16Mbps (categoria 3), 20Mbps (categoria 4), 100Mbps (categoria 5), 1000Mbps (categoria 5e).

2.6. Fast Ethernet

Nel 1997 si è affermato lo standard **Fast Ethernet** che consente trasmissioni a 100Mbps. Le schede di rete di questo tipo sono spesso indicate con la sigla 10/100 poiché possono funzionare sia su reti a 10Mbps che su quelle a 100Mbps.

Le principali caratteristiche di tutti i sottostandard Fast Ethernet sono:

- data rate: 100Mbps
- bit time: 10ns
- interpacket gap: 0.96μs
- slot time: 512 bit (64byte) pari a 5.12μs
- diametro della rete: 205m

Le schede di rete Fast Ethernet sono economiche e spesso sono già presenti nei computer appena acquistati.

I sottostandard Fast Ethernet sono: **100Base-T2, 100Base-T4** e **100Base-X**. Quest'ultimo si suddivide in: **100Base-TX** e **100Base-FX**.

Si mostra nella seguente tabella 2 il modello architetturale della Fast Ethernet.

Tabella 2. - Modello architetturale della Fast Ethernet

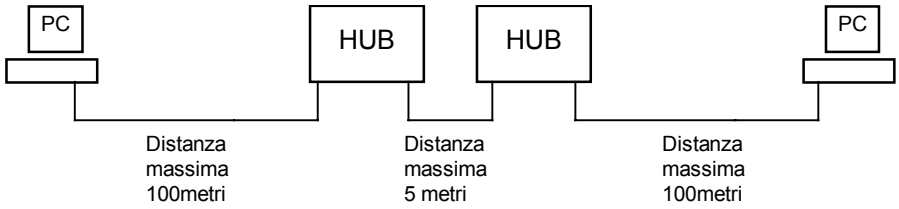
ISO/OSI	IEEE 802.3 – 100 BASE				
LIVELLO DI LINEA	CSMA/CD				MAC
	Sottolivello di autonegoziazione				MII
LIVELLO FISICO	PCS100BASE-T4	PCS100BASE-T2	PCS 100 BASE-X		PHY
	100BASE-T4	100BASE-T2	100BASE-TX	100BASE-FX	

Legenda:
MAC = Media Access Control
MII = Medium Indipendent Interface
PHY = Phisical Layer Device
PCS = Phisical Coding Sublayer

- 100Base-T2. Utilizza due delle quattro coppie del cavo UTP (doppino non schermato) di categoria 3 o superiore. È, praticamente, inutilizzato. La lunghezza massima del collegamento è di 100m ed utilizza la codifica PAM 5x5.
- 100Base-T4. Utilizza le quattro coppie del cavo UTP di categoria 3 o superiore. Anch'esso è praticamente inutilizzato. La lunghezza massima del collegamento è 100m ed utilizza la codifica 8B6T;
- 100Base-TX. Utilizza due delle quattro coppie del cavo UTP o STP di categoria 5. È lo standard più utilizzato. La lunghezza massima del collegamento è 100m, il diametro massimo della rete è di 205m con due ripetitori ed utilizza la codifica FDDI 4B5B-MLT-3 (Multi Level Transmit: +V, 0, -V con transizione ad ogni 1);
- 100Base-FX. Utilizza due fibre ottiche multimodali (62.5μm/125μm) come mezzo trasmissivo. È impiegata per lo più per la realizzazione di dorsali. La lunghezza massima del collegamento è 2Km ed utilizza la codifica FDDI 4B5B-NRZI (Non Ritorno a Zero Invertito).

Con Fast Ethernet TX è possibile utilizzare solo due HUB con distanza massima di 205 metri tra gli estremi di una linea.

Per ottenere le stesse prestazioni in velocità coprendo distanze maggiori si deve ricorrere ad adattatori FX che utilizzano la più costosa fibra ottica. Si riporta, in fig.11, lo schema di una rete 100Base-TX che utilizza il massimo numero di HUB o SWITCH.



- Il mezzo trasmissivo è costituito da due delle quattro coppie di doppino non schermato UTP di categoria 5;
- Due nodi estremi possono essere collegati con non più di 2 HUB;
- La massima lunghezza della rete è 205m.
- La distanza fra gli HUB può essere superiore a 5m purchè il totale sia inferiore a 205m.

Fig.11. - Collegamento Ethernet secondo la specifica 100Base-TX.

Utilizzando SWITCH al posto degli HUB è possibile:

- attivare la modalità di trasmissione full-duplex;
- attivare più comunicazioni simultanee indipendenti ognuna con banda 100Mbps;
- la scomparsa delle collisioni. Eventuali conflitti su trame indirizzate alla stessa stazione sono risolte dallo SWITCH che le memorizza.

La codifica 4B5B consiste nel trasformare 4 bit in un codice a 5 bit per la garanzia di almeno 2 transizioni. Non permette la presenza di 3 zeri consecutivi. La trasmissione è sincrona a 125Mbps. Si mostra in tabella 3 tale codifica.

Tabella 3. – Codifica 4B5B

Dato	Codice 4B	Codice 5B
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

La codifica NRZI, utilizzata nella 100Base-FX a fibre ottiche, consiste nell'effettuare la transizione in presenza di 1. Si riporta un esempio in fig.12 supponendo che lo stato iniziale sia 0.

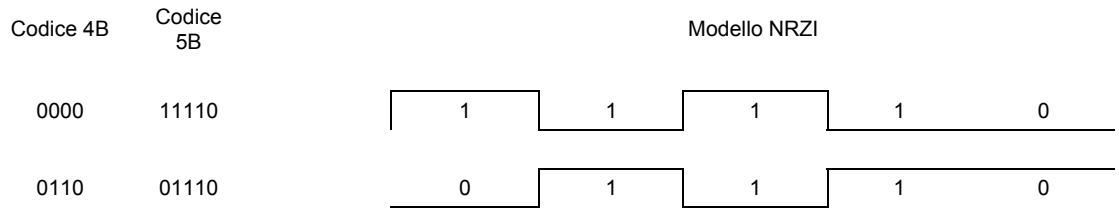


Fig.12. – Codifica dei simboli 0 e 6 dal codice 4B al codice 5B e da questo in NRZI.

La codifica MLT-3, utilizzata nella 100Base-TX con cavo UTP, presenta 3 livelli di tensione (-V, 0 e +V). Si ha una transizione in presenza di un 1. Una transizione avviene in salita passando da –V a 0 e da 0 a +V. Se ci si trova in +V la transizione avviene in discesa passando da +V a 0 e da 0 a –V. Si riporta un esempio in fig.13.

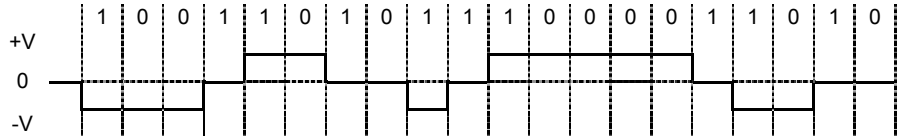


Fig.13. – Codifica MLT-3 per una stringa di 20 bit.

Si riassume, infine, in tabella 4 le caratteristiche principali delle reti Fast Ethernet.

Tabella 4. – Principali caratteristiche delle reti fast Ethernet

Caratteristica	100Base-2	100Base-4	100Base-TX	100Base-FX
Mezzo trasmissivo	2 UTP cat.3	4 UTP cat.3	2 UTP o STP cat.5	2 fibre ottiche
Topologia fisica	Stella	Stella	Stella	Stella
Tecnica di codifica	PAM 5x5	8B6T	4B5B- MLT-3	4B5B-NRZI
Frequenza di simbolo	25MBaud	25MBaud	125MBaud	125MBaud
Full-duplex	Si	No	Si	Si
Lunghezza max di collegamento	100m. (half duplex)	100m. (half duplex)	100m. (half duplex)	100m. (half duplex) 2Km. (full duplex)

2.7. Gigabit Ethernet

Lo standard **Gigabit Ethernet**, compare nel 1998 come standard IEEE802.3z corrispondente al 1000Base-X e nel 1999 come standard IEEE802.3ab corrispondente al 1000Base-T con la caratteristica peculiare di consentire il trasferimento dati alla massima velocità di 1Gbps utilizzando fibra ottica o cavi STP o UTP di categoria 5e e di categoria 6 in 4 coppie. Per poter usufruire di detta velocità tutti gli apparati di rete: HUB, SWITCH, NIC, devono essere certificati per la Gigabit Ethernet e sono compatibili verso il basso: adattano la loro velocità all'apparato di rete più lento. Gli edifici già cablati con cavi UTP di categoria 5e o di categoria 6 possono migrare verso il Gigabit Ethernet sostituendo solamente gli apparati di rete che, però, risultano più costosi di quelli a 100Mbps.

Si mostra nella seguente tabella 5 il modello architetturale della Gigabit Ethernet.

Tabella 5. - Modello architetturale della Gigabit Ethernet

<table>
<tr><th>ISO/OSI</th><th colspan="4">IEEE 802.3 – 1000 BASE</th><th></th></tr>
<tr><td>LIVELLO DI LINEA</td><td colspan="4">CSMA/CD</td><td>MAC</td></tr>
<tr><td rowspan="2">LIVELLO FISICO</td><td colspan="4">Sottolivello di autonegoziazione</td><td>GMII</td></tr>
<tr><td rowspan="2">1000BASE-T</td><td colspan="3">1000BASE-X</td><td rowspan="2">PHY</td></tr>
<tr><td>1000BASE-SX</td><td>1000BASE-LX</td><td>1000BASE-CX</td></tr>
</table>

Legenda:
MAC = Media Access Control
GMII = Gigabit Medium Indipendent Interface
PHY = Phisical Layer Device

Nella Gigabit è possibile negoziare la modalità di funzionamento half e full duplex e, solo per i due standard che utilizzano il cavo UTP e cioè 1000BASE-T e 1000BASE-CX, è possibile negoziare la velocità. Ciò avviene secondo la seguente sequenza:

- 1Gbps full-duplex
- 1Gbps half-duplex
- 100Mbps full-duplex
- 100Mbps half duplex
- 10Mbps full-duplex
- 10Mbps half-duplex

Tra le principali caratteristiche e novità rispetto alla Fast Ethernet troviamo:

- data rate: 1000Mbps
- bit time: 1ns
- interpacket gap: 96ns
- slot time: 4096 bit (512byte) pari a 4.096µs
- diametro della rete: 205m (doppino UTP cat.5e)

Se la trama ha un'estensione inferiore a 512 byte vengono inseriti dei simboli particolari, noti come "extension bit", che rendono la minima lunghezza della trama pari a 512byte.

Altre caratteristiche sono: la stazione trasmittente non rilascia il controllo del mezzo alla fine della trasmissione del pacchetto; la trasmissione dell'extension bit avviene durante l'interpacket gap; la massima trasmissione continua è di 64Kbit.

Nella seguente tabella 6 si indicano il mezzo fisico, l'utilizzo, la massima lunghezza, la frequenza di simbolo e la codifica dei 4 standard Gigabit Ethernet.

Tabella 6

Standard	Mezzo fisico (banda passante per lunghezza)	Utilizzo	Max. lungh.	Frequenza di simbolo	Codifica
1000BASE-SX	MMF 50/125µm (400MHz * Km a 850nm) MMF 50/125µm (500MHz * Km a 850nm) MMF 62.5/125µm (160MHz * Km a 850nm) MMF 62.5/125µm (200MHz * Km a 850nm)	2 fibre	500m 550m 220m 275m	1250Mbps	8B10B
1000BASE-LX	MMF 50/125µm (500MHz * Km a 1300nm) MMF 62.5/125µm (500MHz *Km a 1300nm) SMF 10/125µm	2 fibre	550m 550m 5000m	1250Mbps	8B10B
1000BASE-CX	STP 150Ω	2 coppie	25m	1250Mbps	8B10B
1000BASE-T	UTP cat.5e 100Ω	4 coppie	100m	125Mbaud	4D-PAM5

Legenda:
MMF = Multi Mode Fiber (Fibra ottica multimodale)
SMF = Single Mode Fiber (Fibra ottica monomodale)
STP = Shielded twisted Pair (Coppia di cavo intrecciato schermato)
UTP = Unshielded twisted Pair (Coppia di cavo intrecciato non schermato)

In fig.14 si mostrano le finestre di attenuazione utilizzate dalle fibre ottiche degli standard 1000BASE-SX e 1000BASE-LX.

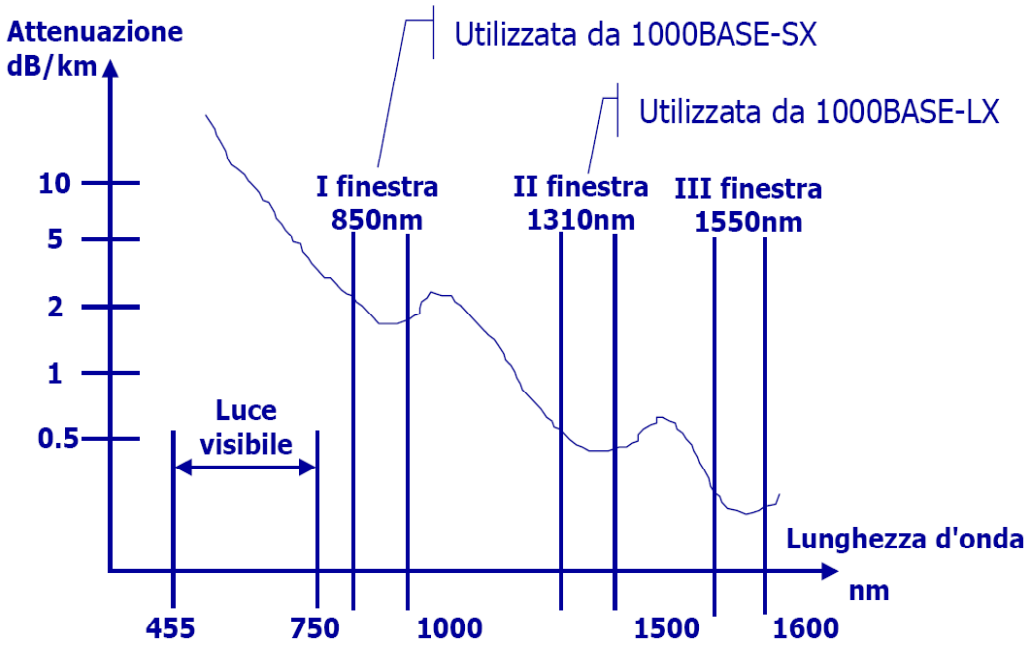
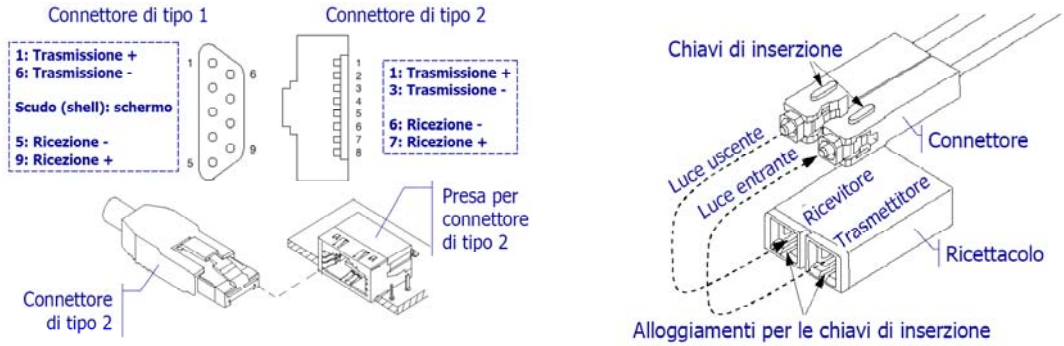


Fig.14. – Finestre utilizzate dalle fibre ottiche multimodali utilizzate nello standard Gigabit Ethernet.

I connettori per la 1000BASE-X sono diversi dal tipo RJ45. Si riportano i vari tipi nella seguente fig.15.



1000BASE-CX **1000BASE-SX e 1000BASE-LX**

Fig.15. – Connettori per la Gigabit Ethernet 1000BASE-X.

La codifica 8B10B si realizza a partire da un byte proveniente dal sottolivello MAC. Di questi 8 bit, 5 subiscono la codifica 5B6B ed i restanti 3 bit subiscono la codifica 3B4B. Vengono, così, generati 10bit.

2.8. 10 Gigabit Ethernet

Recentemente si è affermata un altro standard, **10 Gigabit Ethernet**, che può funzionare a 10Gbps ed utilizza esclusivamente una coppia di fibre ottiche. Il gruppo di lavoro è stato creato nel 1999 e nel 2001 ha dato luogo allo standard IEEE802.3ae. Definisce due tipi di livello fisico: uno per reti locali LAN ed uno per reti metropolitane MAN e geografiche WAN.

Si utilizza la fibra multimodale su distanze da 65m a 300m nella I e II finestre e la fibra ottica monomodale su distanze comprese tra 10Km e 40Km nella II e III finestra (vedi figura 14).

Si mostra, nella tabella 7, il modello architetturale della tecnologia 10Gigabit Ethernet.

Tabella 7. - Modello architetturale della 10 Gigabit Ethernet

<table>
<tr><th>ISO/OSI</th><th colspan="7">IEEE 802.3ae – 10G BASE</th><th></th></tr>
<tr><td>LIVELLO DI LINEA</td><td colspan="7">MAC (opzionale)</td><td></td></tr>
<tr><td rowspan="5">LIVELLO FISICO</td><td colspan="7">Sottolivello di autonegoziazione</td><td>XGMII</td></tr>
<tr><td rowspan="2">10G BASE-X (8B10B)</td><td colspan="6">10G BASE-R (64B66B)</td><td>PCS</td></tr>
<tr><td colspan="4"></td><td colspan="2">WAN Interface Sublayer (WIS)</td><td></td></tr>
<tr><td colspan="6">10G BASE-R</td><td>PMA</td></tr>
<tr><td>10G BASE LX-4</td><td>10G BASE SR</td><td>10G BASE LR</td><td>10G BASE ER</td><td>10G BASE SW</td><td>10G BASE LW</td><td>10G BASE EW</td><td>PMD</td></tr>
<tr><td></td><td colspan="3">10G BASE - R</td><td colspan="3">10G BASE - W</td><td></td></tr>
<tr><td colspan="4">LAN PHY</td><td colspan="3">WAN PHY</td><td></td></tr>
</table>

Legenda:
XGMII = 10 Gigabit Medium Independent Interface
PCS = Phisical Coding Sublayer
PMA = Phisical Medium Attachment
PMD = Phisical Medium Dependent
PHY = Phisical Layer Device

Lo standard 10 Gigabit Ethernet funziona solo in modalità full-duplex e quindi utilizza SWITCH e non HUB e non soffre dei problemi di collisione dei dati.

Se l'aumento delle prestazioni di un fattore 10 rispetto al Gigabit Ethernet è sicuramente un vantaggio, non lo è il triplicarsi dei costi di installazione. L'obiettivo principale è quello di affermarsi nel mercato delle reti metropolitane e geografiche in concorrenza con le soluzioni tradizionali e più economiche come il SONET/SDH con cui presenta compatibilità, ATM, Frame Relay.

2.8. FDDI

Lo standard FDDI (Fiber Distributed Data Interface) è stato definito dall'americana ANSI e descrive il funzionamento di reti locali ad alta velocità realizzate in fibra ottica con tecnica di accesso del tipo token-ring evoluta.

Funziona a 100Mbps con fibra lunga fino a 200Km che può collegare fino a 1000 nodi distanti per meno di 2Km. tra di loro.

Sono presenti due anelli che collegano le stazioni di lavoro con direzioni opposte. Il primo anello è quello usato normalmente per la trasmissione dei dati mentre il secondo anello è di riserva e viene utilizzato quando il primo si interrompe per avaria. Il collegamento, in tal caso, si ottiene effettuando l'altro percorso. Per la gestione del token lo standard FDDI si differenzia dal token-ring quando il nodo trasmettitore ha terminato l'invio dei dati: anziché attendere la ricezione del proprio pacchetto trasmesso, rilascia nella rete il "token-free" (particolare stato del token che consente, al nodo che lo riceve, di iniziare una propria trasmissione dati) subito dopo aver terminato la trasmissione. Questa tecnica prende il nome di ETR (Early Token Release).

Un punto a sfavore della tecnica FDDI è l'elevato costo di realizzazione e gestione rispetto alla Ethernet.

2.9. Reti Wireless

Le reti wireless (senza fili) consentono la trasmissione dei dati per reti locali attraverso le onde radio. È una tecnologia ampiamente sperimentata nel tempo da numerose aziende di telecomunicazioni e che sta riscuotendo un successo esponenziale tanto che l'organo mondiale di standardizzazione, l'IEEE, ha istituito gruppi di studio per il rilascio di standard nel campo wireless. I primi risultati rispondono alle specifiche IEEE 802.11 approvate nel 1999.

Gli altri sistemi di trasmissione dati a breve distanza che utilizzano le onde radio sono i collegamenti ad *infrarossi*, sostanzialmente impiegati nei telecomandi, e la tecnologia *Bluetooth* utilizzata principalmente per i bassi costi di trasmissione e soprattutto per la possibilità di far comunicare qualunque tipo di dispositivo wireless attraverso onde radio.

Secondo Nicholas Negroponte, direttore del Media Lab presso il MIT (Massachusetts Institute of Technology) la tecnologia con standard 802.11 è il maggior candidato ad essere il terzo grande evento nella storia delle telecomunicazioni, dopo il passaggio dall'analogico al digitale e dopo il passaggio dal wired (cavo) al wireless.

La frequenza di lavoro è di 2.4GHz nella banda denominata ISM (Industrial, Scientific and Medical) che non richiede specifiche autorizzazioni di impiego.

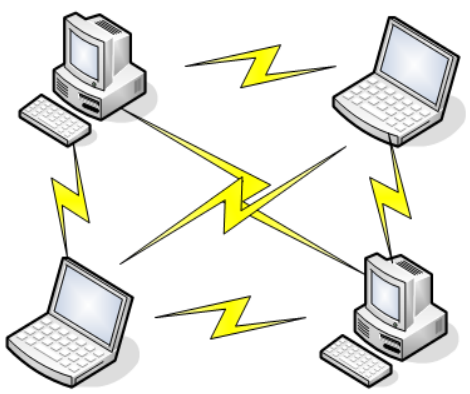
La velocità di funzionamento è di 11Mbps per dispositivi che seguono la specifica IEEE802.11b, attualmente la più diffusa, nota come Wi-Fi (Wireless Fidelity).

La portata va da 30m a 100m in ambienti interni e da 100m a 500m in esterno. I valori dipendono dal dispositivo preso in esame. La presenza di ostacoli come muri, scaffali, tavoli, armadi, piani diversi, limita la portata delle onde radio.

I protocolli wireless sono numerosi ed in continua evoluzione. Ad esempio il protocollo IEEE802.11g, approvato nel 2003, ha una velocità di trasferimento dati di 54MHz, opera alla frequenza di 2.4GHz ed è pienamente compatibile con la più diffusa IEEE802.11b.

Per quanto riguarda la compatibilità elettromagnetica, in Europa sono vigenti le norme ETSI 300328: queste prevedono una potenza massima di trasmissione di 100 mW EIRP (Effective Isotropic Radiated Power - si suppone l'utilizzazione di una antenna isotropica ideale), un guadagno massimo di antenna pari a 3dB e una potenza massima di alimentazione degli apparati di 50mW.

Le reti *wireless* possono essere così strutturate:



1) *host-to-host*, adatte ad ambienti di estensione ridotta e con uno scarso numero di utilizzatori; ciascun PC (tipicamente di tipo *notebook*) è dotato di una propria scheda *wireless* e si collega direttamente ai PC adiacenti, condividendo le proprie risorse o rendendole disponibili agli altri;

Fig.16. – Rete wireless host-to-host

2) con *Access Point* (stazione radio base), offrono un campo d'azione più ampio e possono essere collegate alle LAN cablate. In questo modo gli utenti mobili possono usufruire degli identici servizi di rete normalmente offerti agli utenti fissi. Se necessario, una rete *wireless* può anche essere ampliata semplicemente installando più *access point*.

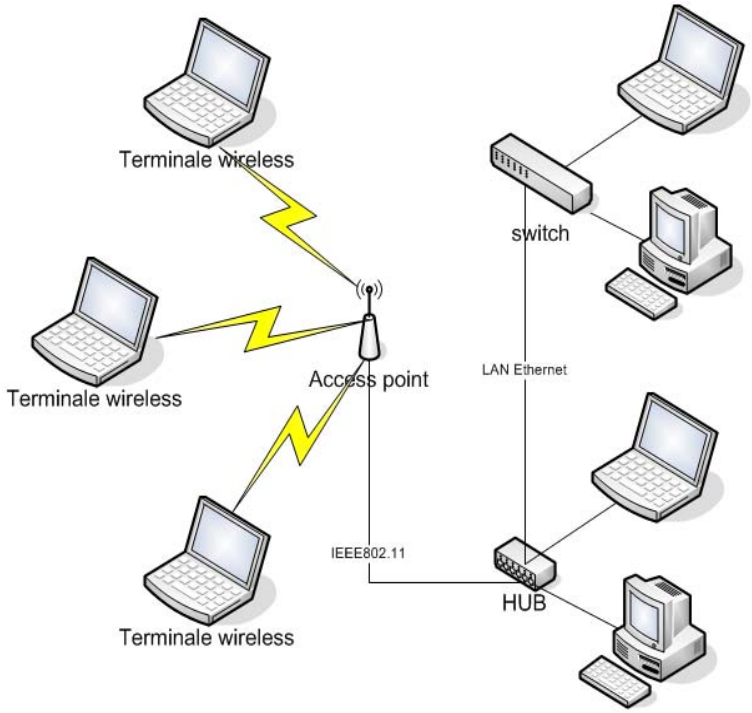


Fig.17. – Rete locale costituita da una sottorete cablata (a destra) ed una sottorete wireless (a sinistra).
L'access point si comporta da ponte (bridge) poiché consente il collegamento tra i due tipi di rete.
L'utilità evidente dei terminali wireless è quella della mobilità non vincolata a cavi di collegamento.
I terminali più indicati per una rete wireless sono senza dubbio i PC portatili.

Ciascuno di questi può fare da riferimento per un certo numero di PC *wireless* all'interno di una determinata zona. Le varie aree di copertura (chiamate celle), si sovrappongono parzialmente, così da offrire una certa continuità di copertura agli utenti mobili. Questi, spostandosi da una cella a quella adiacente, si agganciano all'*access point* con il segnale più elevato. Questa procedura di migrazione inter-cella è anche chiamata *roaming* ed è identica a quella impiegata nella telefonia cellulare.

3) LAN-to-LAN, in grado di collegare via radio due LAN cablate collocate ad una certa distanza e che non sia possibile tecnicamente interconnettere tra loro.

Gli elementi della rete wireless

Gli elementi fondamentali per la realizzazione di una rete wireless sono:

1) adattatore wireless: è una scheda da inserire in uno slot del computer che presenta una antenna ricetrasmittente oppure può essere un dispositivo esterno che si collega al computer attraverso, ad esempio, l'interfaccia USB;
2) Access Point: dispositivo ricetrasmittente di onde radio che si comporta come un HUB nelle reti cablate.

L'Access Point sfrutta il protocollo di accesso al mezzo CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), che utilizza un algoritmo specifico per evitare collisioni, implementando un meccanismo di ascolto virtuale del traffico sulla portante.

L' access point assegna una priorità ad ogni client, in modo da rendere più efficiente la trasmissione dei pacchetti. I dispositivi impiegati effettuano la trasmissione dei dati per mezzo delle onde-radio; il bus logico che realizza la rete è quindi facilmente intercettabile rendendo meno sicuro il sistema.

Per ovviare a questo possibile inconveniente gli standard 802.11 prevedono la possibilità di crittografare i dati con il sistema WEP (Wired Equivalent Privacy, ossia con grado di sicurezza equivalente alla rete cablata).

In realtà sono ancora molte le discussioni sulla reale sicurezza del sistema tuttavia, quando si acquista un Access Point, è fondamentale assicurarsi che questo sia in grado di crittografare con tecnologia WEP.

Un'altra caratteristica importante consiste nella possibilità di filtrare i MAC Address delle interfacce di rete che cercano di collegare l'infrastruttura.

È inoltre opportuno prevedere un sistema di autentica centralizzato, come, ad esempio, RADIUS (Remote Authentication Dial-In User Service), Kerberos o 802.1x, in grado di riconoscere e certificare l'identità della stazione prima di concedere l'accesso alla WLAN nel caso di rete con stazioni wireless molto numerose.

Configurazione dell'access point

Per prima cosa colleghiamo l'Access Point all'HUB o allo SWITCH della rete LAN e procediamo con il setup dell'IP perché sia contattabile dalla rete locale.

La maggior parte degli Access Point dispongono di un'interfaccia di tipo Web per semplificarne la configurazione. Il manuale d'uso specifica l'indirizzo IP di default, cioè l'indirizzo di rete che il dispositivo possiede quando esce della fabbrica.

Spesso esso è: 192.168.0.1 (con netmask 255.255.255.0).

Se la nostra rete Ethernet possiede lo stesso indirizzamento sarà subito possibile contattarlo tramite il browser, altrimenti dovremmo configurare un PC sulla rete 192.168.0.0 con netmask 255.255.255.0 per poter configurare l'Access Point.

Aprendo il browser digiteremo l' indirizzo IP specificato nel manuale di istruzioni del dispositivo. Ad esempio: http://192.168.0.1

A questo punto è possibile configurare il dispositivo attraverso una serie di menu.

È possibile modificare l'indirizzo IP dell'Access Point.

Si procede con il setup della rete wireless. Il parametro standard da impostare è l'SSID (Service Set ID) cioè il nome della nostra rete wireless, senza questo l'apparato utilizzerà quello di default. È importante notare che viene abilitata la crittografia WEP per 3 classi di utenti distinti. Questi parametri dovranno essere configurati allo stesso modo anche sui PC.

Un'altra restrizione di accesso alla rete è possibile grazie alle funzioni di MAC filtering. L'accesso wireless è consentito solo a quei PC di cui si conosce il MAC Address.

Infine per evitare che le configurazioni possano essere manomesse occorre impostare l'accesso tramite password al dispositivo.

Caratteristiche e confronti delle reti wireless

Si mostrano, nella seguente tabella 8, le principali caratteristiche dei protocolli Wireless approvati dall'IEEE 802.11 che sono la frequenza utilizzata per la trasmissione, la banda disponibile sul canale radio ed il tipo di modulazione. È bene sapere che lo standard 802.11a non è compatibile con lo standard 802.11b mentre l'802.11g è compatibile con il diffuso Wi-Fi. L'802.11n è in fase di sviluppo da parte di numerose aziende private e si ritiene che sarà standardizzato dall'IEEE entro il 2006.

Tabella 8. – Principali caratteristiche degli standard wireless

standard	frequenza portante	velocità dei dati	tipo di modulazione
802.11a (Wi-Fi 5)	5.8GHz	54Mbps	OFDM
802.11b (Wi-Fi)	2.4GHz	11Mbps	DSSS
802.11g	2.4GHz	54Mbps	OFDM
802.11n	2.4GHz	108Mbps	

Legenda:
OFDM = Orthogonal Frequency Division Multiplexing
DSSS = Direct Sequence Spread Spectrum
Wi-Fi 5 = Il 5 rappresenta il valore della frequenza portante.

Nella successiva tabella 9, invece, si confrontano la Ethernet cablata con quella senza fili limitatamente all'ingombro, costi, efficienza e sicurezza.

Tabella 9. – Confronti tra la Ethernet cablata e senza fili

	Wired Ethernet	Wireless Ethernet

Ingombro	predisposizione tracce e canalette per la posa dei cavi e punti rete	nessuna predisposizione o tracce e canalette solamente per le dorsali
Costi	costosa predisposizione del cablaggio, costo contenuto dei dispositivi di rete	costo contenuto del cablaggio, costi contenuti dei dispositivi di rete
Efficienza	velocità elevate, poco soggette a disturbi elettrici	velocità contenute, soggette a interferenze elettromagnetiche
Sicurezza	sicurezza maggiore data dalla necessità di possedere accesso fisico alla struttura	livello di sicurezza inferiore (i dati vengono trasmessi in radiofrequenza). Il livello di accesso alla rete può però essere autenticato e crittografato

2.9.1. Tecnologia delle reti Wireless

Anche la tecnologia Wireless, come Internet, ha origini non recentissime: già durante la seconda guerra mondiale le forze Alleate disponevano della tecnologia SST (Spread Spectrum Technology) per evitare che il nemico disturbasse o intercettasse le comunicazioni.

In Europa è stata introdotta di recente e viene utilizzata con frequenza di 2.4 GHz e potenza non superiore ai 100mW.

In America la tecnologia SST per le comunicazioni dei dati è stata impiegata dal 1989 con frequenza di 900 MHz, una minor velocità di trasmissione e maggior potenza rispetto allo standard a 2.4GHz.

Ricordiamo, inoltre, che il canale a 2.4GHz è libero per cui non è necessario alcuna concessione d'uso.

I principali sistemi di comunicazioni sono:

- FHSS = Frequency Hopping Spread Spectrum (divisione di spettro a salto di frequenza)
- DSSS = Direct Sequence Spread Spectrum (divisione di spettro a sequenza diretta)
- OFDM = Orthogonal Frequency Division Multiplexing

La tecnica a salto di frequenza FHSS si basa su un modello pseudocasuale (random pattern) che determina la velocità di salto da una frequenza all'altra (hopping rate).

Il meccanismo è noto solo al ricevitore che dovrà sincronizzarsi col trasmettitore.

La tecnica a divisione di spettro in Sequenza Diretta DSSS consiste nella trasmissione diretta dei bit 1 e 0 ognuno dei quali è seguito da una sequenza ridondante di bit (chiamati chip) per nascondere il contenuto del messaggio. Ovviamente il ricevitore deve conoscere le sequenze ridondanti per poter estrarre correttamente l'informazione.

Questa tecnica permette una buona protezione dei dati trasmessi ed una bassa potenza di trasmissione.

La tecnica OFDM, implementata nei nuovi standard 802.11a e 802.11g, garantisce una migliore protezione alle interferenze elettromagnetiche esterne ed è basata sulla trasmissione di simboli ortogonali.

È una tecnica utilizzata anche per trasportare i dati attraverso la linea elettrica nella tecnologia Powerline che si avvale di 84 frequenze da 4.3MHz a 20.9 MHz.

I sistemi di comunicazioni FHSS e DSSS utilizzano la tecnica di modulazione FSK.

2.9.2. Sicurezza nelle WLAN

Le reti WLAN (Wireless LAN), se da un lato rappresentano una soluzione ideale per ambienti poco adatti alla realizzazione di cablaggi nella infrastruttura e per i PC

portatili, dall'altro soffrono di due inconvenienti a cui devono prestare particolare attenzione sia i costruttori di apparati WLAN che gli utenti:

- interferenze elettromagnetiche e attenuazione del segnale per ostacoli o lunghe distanze;
- impedire ai malintenzionati di agganciarsi nella propria WLAN.

Per quanto concerne il secondo inconveniente, il malintenzionato, ove riuscisse ad inserirsi nella rete WLAN, può sfruttare inopinatamente la connessione ad internet, impossessarsi delle risorse condivise dai server della rete o intercettare pacchetti in transito nella rete.

L'eventuale furto di dati sensibili di clienti, fornitori, dipendenti, ecc., se utilizzati dal malintenzionato, può farci incorrere in eventuali azioni legali nei nostri confronti.

Per aumentare la sicurezza della WLAN conviene ricorrere ai seguenti accorgimenti:

1) assegnare un nome originale alla rete. Conviene, a tale proposito, cambiare il nome di default della SSID (Service Set ID) che, per la maggior parte degli apparati, è il banale "wireless";
2) disabilitare SSID, se possibile. In questo modo si impedisce lo scanning passivo della rete;
3) configurare la connessione a velocità elevata. Poiché l'aumento della velocità comporta un aumento del degrado del segnale in funzione della distanza, il malintenzionato dovrà avvicinarsi di molto all'access point, se può farlo, rischiando di essere facilmente individuato;
4) proteggere la rete intranet con firewall. Il malintenzionato, oltre a superare l'ostacolo della rete wireless, per accedere ai dati contenuti nella rete intranet dovrà superare anche il firewall;
5) bloccare le periferiche sconosciute. Consentire l'accesso alla rete solo ai computer noti dei quali conosciamo l'identificativo universale della scheda di rete: il famoso MAC address. Tale tecnica, tuttavia, rende più difficoltosa la pianificazione e manutenzione della rete.

2.9.3. Caratteristiche di adattatori wireless ed access point commerciali

Gli adattatori wireless, sia interni che esterni, attualmente disponibili in commercio (2005) rispettano lo standard 802.11g a 54Mbps, compatibile con 802.11b. Quelli esterni si interfacciano al computer attraverso la USB2.0 (funzionante alla massima velocità di 480Mbps).

Come è noto, la frequenza di lavoro della 802.11g è di 2.4GHz, la stessa degli apparecchi Bluetooth, e quindi c'è il rischio di interferenze che potrebbero ridurre il *throughtput*, ovvero l'efficienza che si traduce in una minore velocità complessiva.

Il throughtput si riduce aumentando la distanza e soprattutto sistemando l'access-point ad un piano diverso dall'adattatore.

Impostando la negoziazione automatica la velocità spesso scende a 24Mbps al fine di garantire la correttezza dei dati trasmessi. In alternativa è possibile scegliere manualmente la velocità compresa tra 1Mbps e 54Mbps.

Sia l'adattatore che l'access point assicurano una protezione hardware da 64bit a 128bit con crittografia WEP.

Test ripetuti sia in upload che in download effettuati con apparati posti a 5m di distanza e poi ad un piano di distanza hanno dato valori medi, rispettivamente di 16.5Mbps e 4.1Mbps.

Vi sono particolari apparati di rete che conglobano le funzioni di router con 4 porte Switch Ethernet 10/100 Mbps ed Access Point con cifratura WPA. Protocolli proprietari, inoltre, consentono un funzionamento teorico a 108Mbps che si avvale di tecniche di compressione/decompressione dati con algoritmo Lempel-Ziv. Ovviamente il funzionamento a tale velocità è garantito in presenza di adattatori wireless sui PC tutti compatibili con detta tecnologia. La presenza di un solo adattatore 802.11b (a 11Mbps) fa scendere la velocità dei dati su tutta la rete wireless a quella dell'adattatore più lento.

2.9.4. Sistemi di crittografia

Per l'autenticazione lo standard 802.11b prevede l'uso di una chiave "pre-condivisa". Quando l'Access Point riceve una richiesta d'accesso da parte di un terminale wireless, invia un numero casuale. Il terminale wireless firma il numero casuale utilizzando una chiave segreta pre-condivisa e invia la risposta all'Access Point. Questi calcola la firma stessa e confronta il risultato ottenuto con quello ricevuto. Se i due risultati coincidono, il terminale viene autenticato e gli viene garantito l'accesso. Successivamente i dati scambiati vengono crittografati usando il WEP.

Il WEP, chiamato anche stream cipher, opera al livello di linea della struttura ISO/OSI ed è basato sulla specifica RC4.

Il sistema può essere facilmente aggirato da malintenzionati esperti soprattutto perché esso è sicuro finché la chiave è effettivamente segreta. Un altro punto a svantaggio dell'uso della tecnica WEP nella tecnologia wireless è che WEP usa RC4 in modalità sincrona, il che significa che la sicurezza è totalmente compromessa se la chiave è compromessa.

In una trasmissione sincrona, la perdita di un solo bit comporta la perdita di tutti i dati che seguono il bit perduto perché si perde la sincronia del processo.

La perdita dei dati che viaggiano in cavo non è frequente; lo è, invece, quando viaggiano in aria, come accade nelle reti wireless.

L'Access Point e gli adattatori wireless installati sui PC della rete condividono una stessa chiave (shared key) lunga 40 bit e concatenata a un vettore di inizializzazione (IV) lungo 24 bit; si ottiene così una sequenza di 64 bit totali. Vi sono algoritmi di crittografia WEP a 128 bit con chiave a 104 bit e un vettore di inizializzazione a 24bit.

La chiave condivisa viene applicata in XOR (funzione logica OR esclusivo: due bit uguali tra loro applicati all'ingresso dell'XOR producono in uscita un bit uguale a 0 mentre due bit diversi producono in uscita il bit 1) al messaggio da trasmettere.

Il ricevitore decodifica il messaggio criptato riapplicando opportunamente la stessa chiave condivisa in XOR col messaggio criptato.

Detto D il generico bit di dati da trasmettere e K il bit della chiave condivisa da applicare in XOR con D, il generico bit crittografato trasmesso T vale:

$$T = D \text{ XOR } K$$

Il ricevitore applica la funzione XOR al bit R ricevuto e al bit K della chiave condivisa ottenendo il bit decrittografato B:

$$B = R \text{ XOR } K$$

Se la trasmissione è avvenuta senza errori si ha: R=T e quindi:

$$B = T \text{ XOR } K = D \text{ XOR } K \text{ XOR } K$$

Essendo K XOR K = 0 (bit uguali) e D XOR 0 = D per definizione di XOR, si ha:

B = D

Quindi il bit B decrittografato dal ricevitore coincide col bit D che il trasmettitore ha successivamente crittografato e trasmesso.

Esempio.
Supponiamo, per semplicità, che la chiave condivisa sia una stringa a 8 bit di valore: K=11110000 e che il dato da trasmettere sia D=10101010.

Risoluzione:
Il trasmettitore esegue bit a bit l'XOR tra D e K ottenendo il messaggio crittografato trasmesso:
T = D XOR K = 10101010 XOR 11110000 = 01011010.

Il ricevitore decrittografa la stringa R ricevuta eseguendo l'XOR tra R = T e K:
B = T XOR K = 01011010 XOR 11110000 = 10101010

WPA

La seconda tecnologia software per la crittografia è il nuovo Wi-Fi Protected Access, WPA, che consente di collegare con uno strato di crittografia maggiore due adattatori wireless o un adattatore wireless e un access point.

È una tecnologia più recente nata per eliminare i difetti di sicurezza della WEP.

2.10. Bluetooth

Lo scopo principale della nascita della tecnologia Bluetooth risiede nella capacità di far dialogare e interagire fra loro dispositivi diversi come stampanti, computer, notebook, TV, impianti Hi-Fi, telefoni cellulari, elettrodomestici, senza la necessità di collegamenti via cavo semplificandone connessione e comunicazione.

Il nome Bluetooth deriva dal soprannome di un famoso condottiero scandinavo, re di Danimarca del medioevo, Harald II Bluetooth che conquistò la Norvegia.

Con la tecnologia Bluetooth si possono creare reti senza fili chiamate *piconet* costituite da due o più periferiche, fino ad un massimo di 8, che condividono un canale di comunicazione utilizzando il Bluetooth sulla frequenza di 2.4 GHz alla velocità di 1Mbps che, nella versione 2.0, consente un incremento di velocità di trasmissione dati fino a 10Mbps con un raggio d'azione fino a 10 metri, supporto simultaneo per slave a bassa e alta velocità, conformità con la versione Bluetooth 1.0.

Bluetooth consente di gestire sia dati che voce utilizzando la trasmissione a commutazione di pacchetto per i dati e una modalità orientata alla connessione per la voce.

La piconet si configura automaticamente quando si inserisce o si elimina un dispositivo. A loro volta più piconet possono interconnettersi tra loro aumentando le possibilità di espansione.

Tutte le apparecchiature bluetooth predisposte in un ambiente di lavoro sono nella condizione di generare piccole reti senza fili.

Il sistema di comunicazione bluetooth è progettato per funzionare correttamente anche in ambienti con forte presenza di interferenze e campi elettromagnetici.

È possibile, ad esempio, ascoltare musica dell' impianto stereo o della TV attraverso la cuffia senza fili anche se ci sono oggetti, ostacoli interposti, cosa ben difficile con le cuffie a raggi infrarossi (tecnologia IRDA).

La velocità di comunicazione è prossima ad 1 Mbps anche con piccole potenze nell'ordine di alcuni milliWatt, mille volte inferiore alla potenza di un cellulare GSM, impiegando la tecnologia TDD (Time Division Duplex).

I dispositivi Bluetooth, in relazione alla potenza emessa, vengono distinti in tre classi di funzionamento.

Un notebook, ad esempio, implementa un terminale bluetooth in classe 2 con raggio d'azione di diversi metri.

Più piconet possono interconnettersi, aumentando le possibilità di espansione fino ad un massimo di 10 piconet. Ciò permette, ad esempio, di sincronizzare i dati di un notebook e un PDA semplicemente avvicinando i due apparecchi, oppure di passare automaticamente al vivavoce quando si entra in auto parlando al cellulare.

Tutto questo è possibile grazie al "service discovery protocol" (SDP) che permette ad un dispositivo Bluetooth di determinare quali sono i servizi che gli altri apparecchi presenti nella piconet mettono a disposizione.

Tale protocollo può fungere sia da server che da client e ogni apparecchio dispone delle informazioni relative ai servizi di cui è capace e dei protocolli supportati: altri apparati potranno fare uso di queste informazioni per determinare le possibilità di interazione con i nodi della piconet.

Questo è necessario perché, naturalmente, una stampante bluetooth non offrirà le stesse possibilità di un PDA o di un auricolare, pertanto occorre che ogni nodo conosca le funzioni e le possibilità di ogni altro nodo della rete. Per fare un esempio concreto, se un telefonino Bluetooth vuole trasferire un messaggio di testo a un PDA, potrà interrogare quest'ultimo per sapere se è dotato di funzionalità e-mail, o se è in grado di ricevere un testo in altro modo.

Un dispositivo inserito per la prima volta in una piconet effettua una "scansione" di tutti i nodi presenti per capire come può interagire con essi.

Tale modalità di interconnessione dinamica consente di sincronizzare i dati tra due apparecchi Bluetooth automaticamente, ad esempio un PDA con un PC portatile, sfruttando il protocollo SDP (Service Discovery Protocol) per distanze comprese tra 10 - 100 metri.

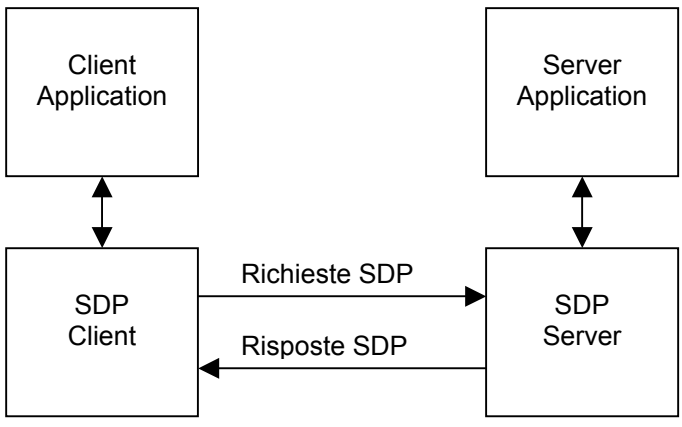


Fig.18.- Schematizzazione del funzionamento del protocollo SDP.

In un collegamento Bluetooth tutti gli apparecchi connessi sono, generalmente, in modalità *standby*, seguendo un ciclo di scansione ad intervalli di tempo di 1.28 secondi al fine di verificare la presenza di eventuali altri dispositivi; in tale modalità tutti i dispositivi bluetooth sono a basso consumo energetico.

La scansione effettuata può essere di due tipi: PS (Page Scan) e IS (Inquiry Scan).

La scansione PS consente la ricerca di un collegamento con un altro apparecchio Bluetooth, che può risultare in modalità *connectable* o *non-connectable*.

La scansione IS, simile alla precedente, permette di identificare la tipologia di apparecchi disponibili nella piconet, *discoverable* o *non-discoverable*, e di approntare i necessari protocolli per il collegamento.

Un comando *inquiry* viene emesso quando l'indirizzo o il numero di identificazione di un dispositivo non è conosciuto, successivamente al riconoscimento seguirà un comando *page* che servirà per risvegliare l'altra unità e stabilire così una connessione completa tra i dispositivi.

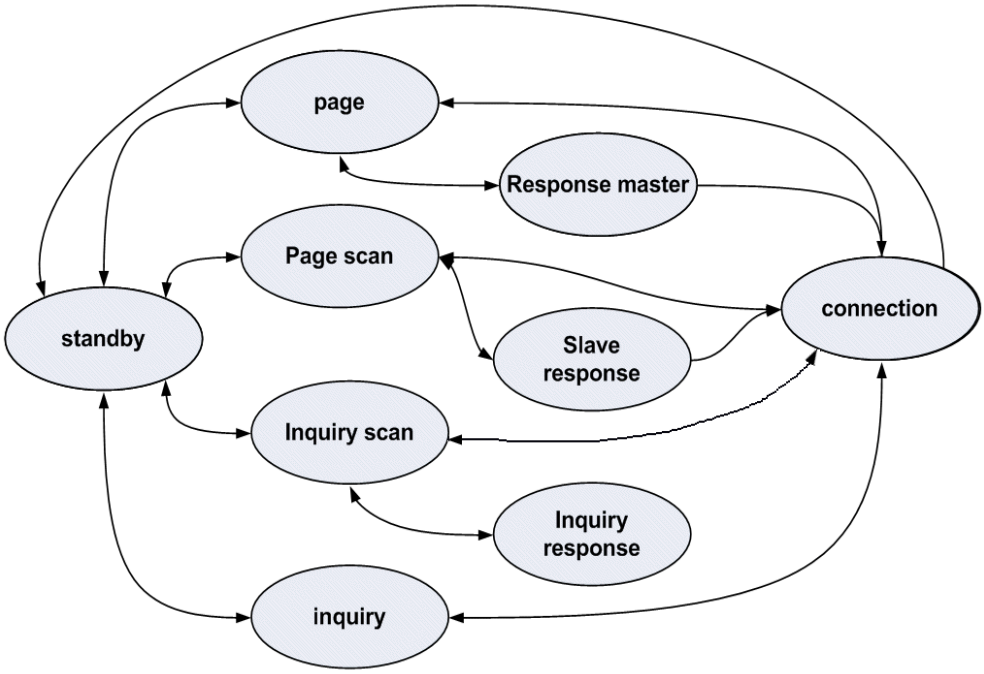


Fig.19. – Modalità di passaggio dallo stato standby a connessione e viceversa.

I risultati di una scansione possono essere:

- A (Active) la connessione è attiva e può avvenire la trasmissione e la ricezione dati, tutte le unità slave sono sincronizzate con il master;
- H (Hold) può svolgere operazioni IS e PS con basso consumo energetico;
- S (Sniff) riduzione del carico di lavoro in modalità di ascolto della piconet con tasso di attesa programmabile;
- P (Park) modalità di attesa rimanendo sincronizzato alla piconet.

La tecnologia Bluetooth opera nella gamma di frequenza da 2.4GHz a 2.483 GHz, suddivisa in canali da 1 MHz impiegando la tecnica FHSS (Frequency Hopping Spread Spectrum), tecnologia che consente a più utenti di condividere lo stesso insieme di frequenze, cambiando automaticamente la frequenza di trasmissione fino a 1600 volte al secondo, al fine di una maggiore stabilità di connessione e di una riduzione delle interferenze tra canali di trasmissione.

Lo *spectrum spreading* consiste in una continua variazione di frequenza utilizzando una modulazione di *frequency hopping*. Gli *hops* corrispondono ai salti di frequenza all'interno della gamma assegnata (complessivamente 79 hops).

Due o più unità che condividono la stessa sequenza di hopping (piconet) vengono ad assumere tale configurazione. Tutti i dispositivi di una piconet condividono lo stesso canale di passaggi di frequenza, determinato dagli slave, sincronizzandosi con l'unità master.

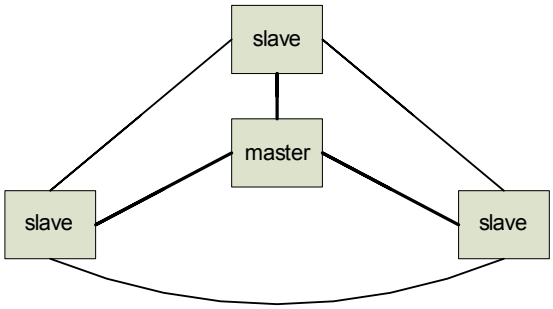


Fig.20. - Collegamento del master agli slave in una piconet.

La comunicazione viene gestita dall'unità master tramite FHSS consentendo la sincronizzazione con le unità slave, fino ad un numero massimo di 7 dispositivi slave attivi. Il master trasmette solo nei *timeslot* pari, mentre lo slave trasmette nei *timeslot* dispari al fine di evitare collisioni. Nella piconet, oltre alle sette unità slave attive, possono rimanere sincronizzate all'unità master altre unità in una modalità di attesa (park).

In ogni piconet un terminale Bluetooth assume la funzione di master scegliendo la sequenza con cui cambiare la frequenza portante radio mentre gli altri, adeguandosi, assumono il ruolo di slave interagendo tra loro secondo protocolli di scambio dati.

La tecnologia Bluetooth consente due principali modalità di collegamento tra unità master e slave, l'ACL e lo SCO.

Il collegamento ACL (Asynchronous ConnectionLess) consente la trasmissione dei dati con una modalità asincrona non orientata alla connessione. La velocità di trasmissione dati nella modalità asimmetrica è 723 Kbps e di 57.6Kbps nell'altra direzione, nella modalità simmetrica invece, è intorno a 434 Kbps.

Il collegamento SCO (Synchronous Connection Oriented) consente la trasmissione radio e la trasmissione Voce. Permette la trasmissione dei dati con una modalità sincrona orientata alla connessione.

La velocità di trasmissione voce è sincrona e bidirezionale e sfrutta una codifica *Continuous Variable Slope Delta Modulation* (CVSD), permettendo un bit rate di 64 Kbps.

Ogni master riesce a gestire un massimo di tre connessioni SCO simultanee verso slave con una cadenza di 64 Kbps, gli ACL agiscono sui time slot liberi gestendo i dati generici. I dati di una piconet vengono trasmessi a pacchetti di 2745 bit e sono composti da tre campi:

- AC (Access Code)

- H (Header)
- P (Payload)

72 bit	54 bit	0 – 2745 bit
ACCESS CODE	HEADER	PAYLOAD (dati)

Fig.21. – Struttura di un pacchetto di una piconet.

Ogni pacchetto può estendersi fino a cinque time slots.

Nel livello immediatamente superiore ISO/OSI i dati vengono gestititi dal protocollo L2CAP (Logical Link Control Adaption Protocol) che si occupa della suddivisione dei file in pacchetti e del loro assemblaggio. Un altro protocollo, di nome IROBEX, permette la gestione delle comunicazioni IRDA.

Le caratteristiche di una scheda Bluetooth di un determinato dispositivo (cellulare, notebook, palmare, stampante,...) dipendono dal costruttore; sarà necessario, quindi, controllare preventivamente la presenza e le modalità di gestione della:

- rete
- posizionamento (GPS)
- informazioni
- audio
- telefonia

La modalità di trasmissione e ricezione dati può cambiare in relazione alle esigenze di comunicazione delle varie unità Bluetooth, passando per esempio da una sola comunicazione voce a una sola comunicazione dati.

Una rete wireless composta da più apparecchi realizza una *piconet*, a sua volta più piconet realizzano un network wireless chiamato *scatternet*.

Due dispositivi Bluetooth vicini tra loro che svolgono un ruolo di master realizzano una scatternet su frequenze diverse, ogni master a sua volta gestisce gli slave della propria piconet. Il limite dei canali radio disponibili è 79.

Una piccola rete Bluetooth può supportare un collegamento punto-punto e multipunto.

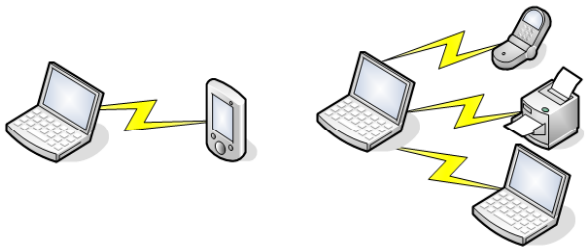


Fig.22. – Esempio di collegamento punto-punto (a sinistra) e multipunto (a destra).

Ogni unità Bluetooth è costituita da:

- unità radio
- unità di controllo del collegamento (link unit)
- unità di gestione e di interfaccia del collegamento

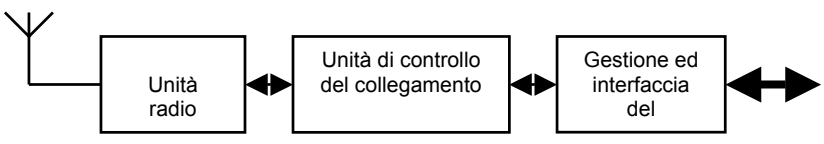


Fig.23. – Costituzione di una unità Bluetooth.

Le connessioni tra dispositivi Bluetooth vengono gestite, autenticate e configurate dall'unità di gestione e di interfaccia del collegamento (Link Manager – LM) attraverso il contatto con un altro Link Manager.

L' unità di controllo del collegamento (Link Controller – LC) gestisce l'invio, la ricezione e le impostazioni dei dati.

Lo scambio delle informazioni di servizio avviene tramite il protocollo LMP (Link Manager Protocol).

Le informazioni del protocollo LMP possono essere di:

- trasmissione e ricezione dati
- di autenticazione
- di scansione (page scan, inquiry scan, park, hold, sniff)
- di identificazione
- di collegamento
- di determinazione canale comunicativo
- di verifica
- compressione dei dati scambiati

Il protocollo LMP controlla, inoltre, le modalità di potenza ed i valori di *duty-cycle* dell'unità radio.

I messaggi inviati si chiamano PDU (Protocol Data Units) e si articolano in 55 tipologie.

Un ulteriore livello di controllo superiore è il protocollo LLCAP (Logical Link Control and Adaptation Protocol) che agisce una volta stabilita la connessione tra dispositivi tramite il protocollo LMP, gestendo la segmentazione/ricompilazione dei pacchetti dati (di max 64 Kbit), il multiplexing, le informazioni QoS (Quality of Service).

Tabella 10

Alcuni protocolli impiegati dal Bluetooth
LMP (Link Manager Protocol)
L2CAP (Logical Link Control and Adaptation Protocol)
SDP (Servive Discovery Protocol)
RFCOMM (protocollo sostituzione cavo, emula segnali RS-232)
TCS-BIN (Telephony Control Specification-Binary
Baseband (connessione fisica RF, sincronizzazione frequenze)
AT-Commands (Audio/Telephony Commands)
PPP (Point to Point Protocol)
TCP/IP/UDP (Transport Control Protocol/Internet Protocol/Datagram Protocol)
IrMC (Infrared Mobile Communication)
WAP (Wireless Application Protocol)
OBEX (Object Exchange Protocol)
WAE (Wireless Application Environment)

2.11. Powerlan

Va sotto il nome di Powerlan una rete locale che utilizza, come mezzo di collegamento tra computer, i cavi della rete elettrica presente in un locale, in un appartamento, in un edificio, in una città. Essa è nota anche come *Broadband over PowerLan* (BPL).

Una'azienda avente uffici attigui, per la realizzazione di una rete LAN che metta in comunicazione il computer del magazzino, dell'ufficio di ragioneria, del marketing, della sala conferenze, ecc., può utilizzare tranquillamente il cablaggio della rete elettrica dell'edificio senza dover ricorrere alla realizzazione di una nuova cablatura.

Come aspetto negativo occorre subito dire che le prestazioni in termini di velocità dei dati degradano all'aumentare dei computer collegati ed è possibile che un vicino dotato di analoga apparecchiatura possa carpire i dati della nostra rete, anche se la probabilità è bassa.

Teoricamente è possibile realizzare, con la tecnologia BPL, reti metropolitane e geografiche. In pratica, la sperimentazione effettuata nel 1997 a Manchester rivelò che i lampioni della pubblica illuminazione irradiavano nello spazio i dati circolanti nei cavi.

In Italia sono state effettuate delle sperimentazioni: quella più significativa, condotta dall'ENEL, si è realizzata a Grosseto nel 2002 su un campione di oltre 2000 utenti per oltre un anno.

I risultati, salvo qualche instabilità e riduzione della velocità nominale lamentata da alcuni utenti, hanno dato esiti incoraggianti in termini di compatibilità del servizio di fornitura di energia elettrica e di trasmissione dati e della competitività del sistema rispetto alla velocità offerta dagli accessi ADSL ad internet.

La tecnologia BPL dà il meglio di se nella realizzazione di reti locali limitate come, ad esempio, una piccola rete locale fino a una rete condominiale.

In questo caso, piuttosto che sottoscrivere un contratto ADSL singolo, è più conveniente realizzare un collegamento ad internet a banda più larga dividendo le spese tra i vari condomini. La rete powerlan per tale soluzione appare la più realizzabile sotto il profilo tecnico ed economico rispetto alla cablatura dell'edificio o all'utilizzo della wireless non in grado di superare certi ostacoli fisici e dislivelli di uno o più piani.

In commercio sono ormai disponibili adattatori powerlan di dimensioni di un pacchetto di sigarette che incorporano una spina di corrente e una presa RJ45 o USB come si mostra in fig.24. Un cavo di rete o USB collegherà l'adattatore al PC.

Fig. 24. – Adattatore powerlan.

Il dispositivo contiene al proprio interno circuiti simili a quelli di un modem.

L'installazione su Windows è semplicissima poiché sono dispositivi plug & play.

Il sistema utilizza la tecnica di trasmissione OFDM (Orthogonal Frequency Division Multiplexing), che con 84 portanti distribuite su un range di frequenze compreso tra 4.5 e 21 MHz, mette al riparo da potenziali interferenze provenienti dagli altri apparati elettrici in rete.

Per realizzare una rete locale tra 3 computer di un appartamento, ad esempio, è sufficiente acquistare 3 di questi adattatori, dal prezzo identico a quello di un adattatore wireless, da inserire ciascuna in una presa di corrente. L'altro capo dell'adattatore va al relativo computer attraverso l'USB o la RJ45. Nella rete elettrica dell'appartamento viaggiano anche i dati tra un computer e l'altro. Volendo collegare ad internet i computer della rete è sufficiente collegare alla RJ45 del router un adattatore powerlan con uscita LAN RJ45. Si mostra un esempio di cablaggio in fig.25.

Alla rete si può collegare una stampante USB utilizzando un adattatore powerlan USB. In questo modo tutti i computer della rete possono utilizzare la stessa stampante.
I valori tipici delle principali caratteristiche di questi adattatori sono:

- Velocità: 10Mbps;
- Distanza: 200m;
- Numero di PC: 10
- Crittografia: a 56bit
- Modulazione: OFDM.

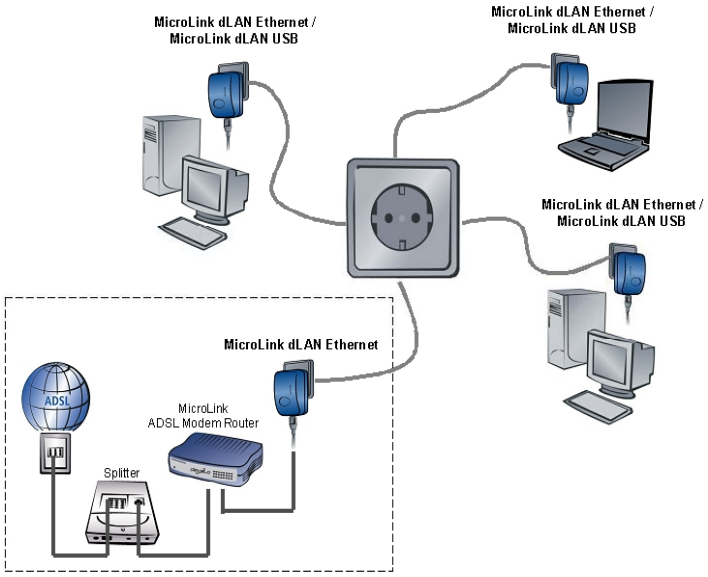


Fig.25. Esempio di rete powerlan costituita da 3 PC connessi ad internet via router ADSL. Servono 4 adattatori powerlan, ad esempio il MicroLink dLAN della "Devolo".

Le aziende che più si sono interessate della tecnologia powerlan sono:

- Devolo: www.devolo.it
- Enel: http://www.enel.it/enelsi/famiglia/f_electrolan.asp
- Lindy: http://www.lindy.com/it/
- SMC: http://www.smc-europe.com/it/index.html

Esistono altri dispositivi di rete di tipo powerlan: switch, router, adattatore wireless.

Utilizzando anche un adattatore powerlan wireless IEEE802.11b si può implementare una rete mista: wireless e cablata con la rete elettrica come si mostra nella fig.26.

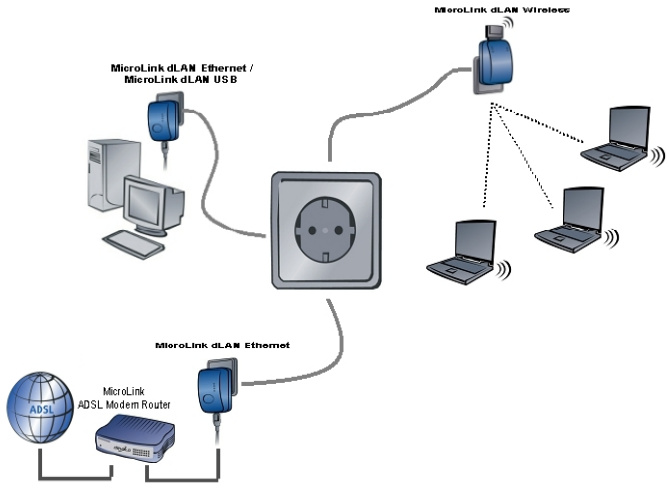


Fig.26. – Con l'utilizzo di adattatori powerlan Ethernet/USB e wireless si può realizzare una rete mista: cablata, via cavi della rete elettrica, e wireless con PC dotati di adattatori wireless, ad esempio il MicroLink dLAN Wireless della "Devolo".

2.12. Livelli di reti locali

Le reti locali, a seconda della complessità, possono interessare un numero limitato di nodi ubicati in un'unica stanza o un numero elevato di nodi dislocati in varie stanze di un edificio o di edifici differenti. Se il collegamento avviene tra unità geograficamente lontane si realizza una WAN (Wide Area Network) per la quale sono possibili diverse modalità di connessione. Esaminiamo brevemente i possibili tipi di reti locali.

- *LAN per piccoli uffici.*

Conviene realizzare una rete paritetica su protocollo Fast Ethernet e collegamento a stella. Il centro stella è realizzato da un concentratore HUB o da un apparato di rete di commutazione come lo SWITCH se i nodi sono più di 5. I nodi sono dei computer desktop o portatili. La stampante, connessa ad un PC acceso, può essere utilizzata anche dagli altri computer collegati alla rete. Si potrebbe utilizzare, alternativamente, una stampante di rete, dotata di apposita scheda Ethernet, da collegare al concentratore.

Questa soluzione, più costosa, ha il vantaggio di svincolare la stampante da un PC.

Il cablaggio è su doppino UTP. Si mostra un esempio in fig.27.

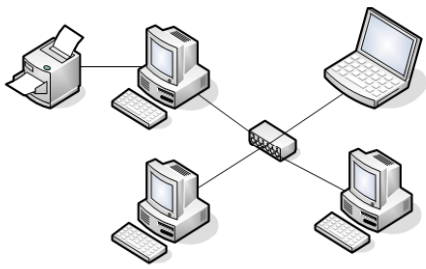


Fig.27. – Piccola rete locale con HUB e stampante collegata ad un PC.

- *LAN per gruppi di lavoro.*

Una possibile configurazione vede un server, con due schede di rete, collegato ad altrettanti HUB o SWITCH ciascuno dei quale svolge la funzione di centro stella.

Il server esegue il sistema operativo di rete e i client eseguono la parte client del sistema operativo di rete. Il cablaggio è su doppino UTP. Si mostra un esempio in fig.28.

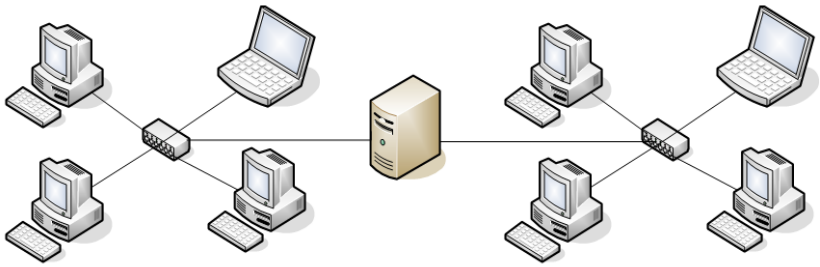


Fig.28. – Server che gestisce due piccole reti locali.

- *LAN aziendale.*

La rete si estende per centinaia di metri e il cablaggio può essere realizzato su fibra ottica che consente il collegamento a distanze anche di alcuni Km. e sopporta un traffico dati molto intenso regolato da appositi router[3].

Il collegamento tra router ed HUB è realizzato tramite doppino UTP. Per applicazioni gestionali conviene disporre di un computer server centralizzato che contiene il database da utilizzare. Si mostra in fig.29 una tipica connessione.

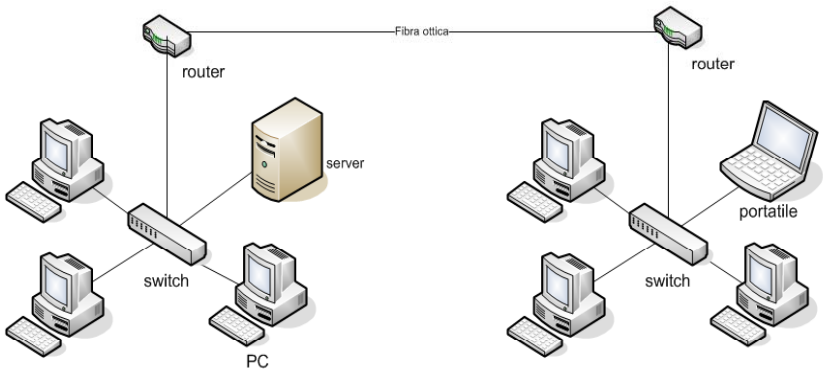


Fig.29. - Rete LAN con router collegati in fibra ottica.

- *Rete aziendale WAN.*

È il caso di aziende che hanno sedi sparse in varie regioni nel mondo. In tal caso i router mostrati in fig.29 saranno collegati tra loro attraverso la rete telefonica commutata o dedicata. Per ottenere elevate velocità si ricorrerà alla ADSL ad almeno 2Mbps oppure alla rete ATM (Asynchronous Transfer Mode) per trasmissioni dati ad alta velocità necessaria, ad esempio, per informazioni audio e video.

[3] Dispositivo che provvede all'instradamento di messaggi tra reti omogenee.

3. Reti geografiche

Le reti geografiche, note col termine WAN (Wide Area Network), sono reti di grandi estensioni utilizzate per la trasmissione dati e possono essere pubbliche e private.

Per quanto riguarda la commutazione, si possono utilizzare quattro tecniche:

1. Commutazione di circuito;
2. Commutazione di messaggio;
3. Commutazione di pacchetto;
4. Commutazione di cella.

La commutazione di pacchetto è la tecnica al giorno d'oggi più utilizzata per le reti di controllo dei sistemi telefonici e per le reti commutate di trasferimento dati.

La commutazione di cella è una nuova tecnica destinata, probabilmente, a sostituire la commutazione di pacchetto nel prossimo futuro.

3.1. Commutazione di circuito

E' una tecnica che consiste nell'attivazione di un collegamento fisico permanente tra l'utente chiamante e l'utente chiamato.

La commutazione di circuito è adottata nelle vecchie centrali elettromeccaniche della rete telefonica commutata.

Un evidente inconveniente è rappresentato dalla impossibilità di ottimizzare il traffico telefonico che potrebbe avere delle tratte di linee sovraccariche ed altre prive di trasmissione.

La commutazione di circuito fornisce solamente un percorso di comunicazione: le problematiche relative al controllo degli errori ed alla scelta dei protocolli è a totale carico dell'utente.

3.2. Commutazione di messaggio

È una tecnica per trasmissione dati che si avvale di un computer che svolge il compito di smistatore delle informazioni provenienti da terminali o elaboratori collegati attraverso la rete telefonica commutata o dedicata.

Il computer smistatore esamina l'indirizzo di destinazione posto nell'intestazione del messaggio e instrada tale messaggio alla stazione ricevente o al commutatore successivo nel percorso.

I dati vengono, solitamente, memorizzati su disco e smistati, successivamente, in funzione del traffico e delle priorità del messaggio.

Questa tecnica non consente, perciò, il tempo reale e l'interattività, inoltre il sovraccarico dei dati o un'avaria al computer smistatore può compromettere la funzionalità della rete.

A ciò si ovvia utilizzando un duplicato del computer smistatore che entra in funzione in caso di guasto del primo.

Un altro svantaggio di tale tecnica è ancora dovuto al computer centralizzato che rappresenta un collo di bottiglia che rallenta le comunicazioni.

3.3. Commutazione di pacchetto

Rappresenta una tecnica di commutazione per le trasmissioni dati che utilizza in modo efficiente le costose linee di comunicazione.

I canali sono ad alta velocità ed interconnettono anche dispositivi che utilizzano codici differenti e che funzionano a velocità diverse.

I dati da trasmettere da un terminale all'altro vengono suddivisi in frammenti più piccoli denominati *pacchetti* e circoscritti da informazioni di servizio costituiti dagli indirizzi del mittente, del destinatario, dal numero d'ordine del pacchetto, ecc.

La rete è costituita da numerosi elaboratori commutatori, denominati *nodi*, del tipo descritto nella rete a commutazione di messaggio, collegati tra loro da linee telefoniche ad alta velocità (oltre 64Kbps).

Tra il terminale e il nodo più vicino, ovviamente, deve esistere una connessione fisica realizzata su rete telefonica commutata o dedicata.

Nel caso di utilizzo della rete telefonica commutata per il collegamento alla rete a commutazione di pacchetto, l'utente deve prima effettuare un *collegamento fisico* di chiamata al nodo più vicino attraverso la classica telefonata e l'uso del modem o di particolari adattatori di rete.

Una volta connesso alla rete, l'utente stesso può chiamare un altro dispositivo connesso alla rete attivando, così, un *collegamento logico*.

Il percorso del pacchetto è stabilito da criteri denominati *routing più economico* che tiene conto delle seguenti situazioni:

- il numero di pacchetti in attesa di trasmissione;
- la capacità del collegamento;
- il livellamento del carico sulla rete;
- sicurezza del collegamento;
- tipo di traffico;
- numero di collegamenti intermedi.

Gli algoritmi adottati per l'instradamento dei pacchetti attraverso la rete possono essere differenti: alcuni vengono impostati da un computer centrale ma, nella maggior parte dei casi, vengono eseguiti in ogni singolo nodo.

Gli algoritmi adattano il percorso del pacchetto ai guasti e alle condizioni del traffico sulle linee.

La rete è in grado di realizzare conversioni di velocità, di codici e protocolli nel caso di utenti dalle caratteristiche diverse.

La lunghezza massima del pacchetto, con riferimento al campo dati, è un numero di byte potenza di 2 e compreso tra 16 e 1024.

L'ultimo pacchetto di un flusso di dati può avere dimensione inferiore alla massima impostata.

I pacchetti sono trasportati in una trama HDLC che ha il vantaggio di consentire il controllo degli errori di trasmissione.

Le linee che collegano i nodi sono utilizzate, durante il collegamento, da pacchetti di altri utenti, rendendo, così, più efficiente l'uso della linea stessa.

Lo scambio dei pacchetti tra due nodi (router) può avvenire con due tecniche:

- datagramma;
- circuito virtuale.

Nei prossimi paragrafi si spiegheranno le due tecniche di trasmissione dei pacchetti.

3.3.1. Datagramma

Nella tecnica a datagramma i vari pacchetti di uno stesso flusso dati possono intraprendere percorsi diversi in tempi diversi per poi essere assemblati nella giusta sequenza dal software del computer ricevitore.

Si mostra, in fig. 30, un esempio di servizio datagramma.

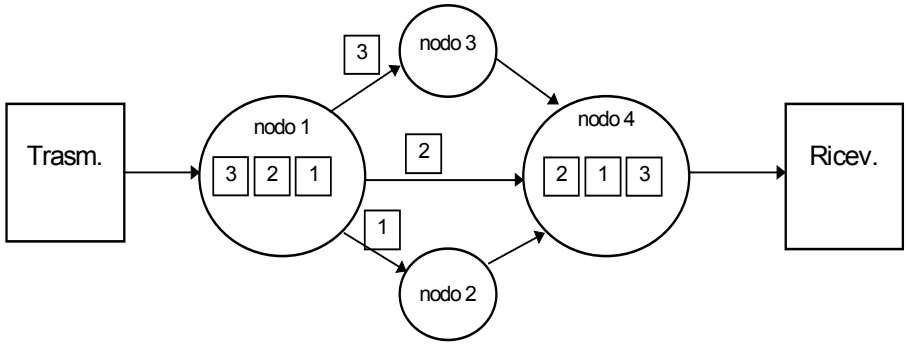


Fig.30. - Datagramma. Esempio di un messaggio suddiviso in tre pacchetti.

Ogni pacchetto viene instradato indipendentemente dagli altri pacchetti della stessa chiamata.

Affinché ciò sia possibile è necessario che ogni pacchetto contenga tutte le informazioni che consentono il corretto spostamento da nodo a nodo fino al raggiungimento del terminale di destinazione.

Il software del computer trasmettitore invia il messaggio al nodo di origine 1 sotto forma di pacchetti 1, 2 e 3. Questi li smista ai nodi 2, 3 e 4 come in figura.

Un nodo prima di accettare un pacchetto esegue un controllo per verificarne la correttezza; in caso di errore chiede la ritrasmissione.

Il nodo sorgente attiva un timer: se alla scadenza non ha ricevuto la conferma della corretta ricezione, inoltra nuovamente il pacchetto. Se la risposta di ricezione arriva a tempo scaduto può capitare che, alla fine, il ricevitore si ritrova con due pacchetti identici duplicati di cui dovrà scartarne uno.

3.3.2. Circuito virtuale

La tecnica a circuito virtuale ricorda il servizio telefonico commutato.

Il DTE che effettua la chiamata inoltra sulla rete una *richiesta di collegamento* che abilita le procedure di collegamento al DTE chiamato.

Il DTE chiamante invia una *richiesta di chiamata*, che rappresenta il primo pacchetto. Questo si propaga da nodo a nodo determinando un percorso che sarà, poi, seguito da tutti gli altri pacchetti.

Il primo pacchetto deve contenere l'indirizzo del mittente, del destinatario e il numero di canale logico.

I pacchetti successivi conterranno solo il numero di canale logico poiché, essendo fisso il percorso, i vari nodi sanno a quale nodo smistare il pacchetto in transito.

Alla fine del trasferimento il DTE chiamante invia una *richiesta di svincolo,* attraverso l'ultimo pacchetto, col compito di chiudere il circuito virtuale.

Si mostra in fig.31 le varie fasi del collegamento.

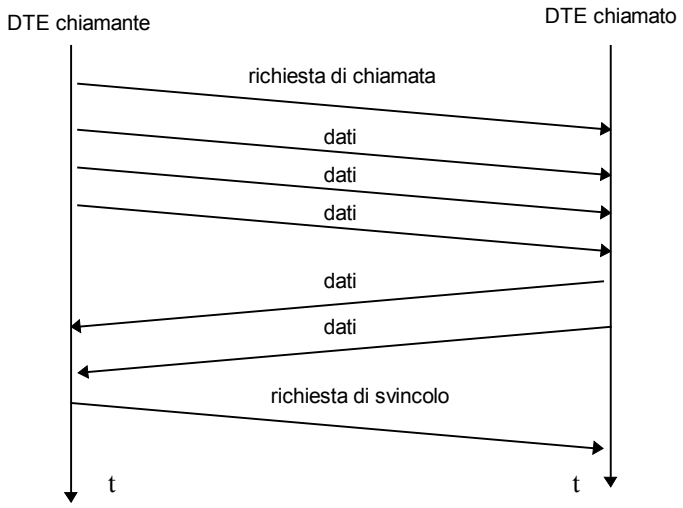


Fig. 31. - Fasi del collegamento.

Il guasto di un nodo blocca lo scambio dei dati causando la chiusura del circuito virtuale. Questo è un aspetto negativo. Nel datagramma, invece, viene cercato un percorso alternativo in grado di bypassare i nodi inattivi o congestionati.

È compito del DTE chiamante o del nodo sorgente, attraverso la funzione di riconnessione automatica, l'attivazione di un nuovo circuito virtuale.

3.4. Commutazione di cella

La commutazione di cella considera segmenti di dati di lunghezza fissa, contrariamente alla commutazione di pacchetto.

Una cella è costituita da un'intestazione di 5 byte e da 48 byte di dati.

Celle con caratteristiche analoghe sono impiegate nelle *Reti Metropolitane* (MAN = Metropolitan Area Network) e nelle moderne e veloci trasmissioni ATM (Asynchronous Transfer Mode).

Il collegamento di celle utilizza etichette ed intestazioni molto brevi per consentire una commutazione rapida. È una tecnologia che si presta ad essere applicata sia per reti locali che geografiche.

4. Protocolli di rete

I protocolli di rete, posti al terzo livello nella gerarchia ISO/OSI, mirano a fornire le caratteristiche che consentono il trasferimento dei dati indipendentemente dalla natura del DTE.

Le raccomandazioni dell'ITU-T relativi alla commutazione di pacchetto sono: X.25, X.28 e X.75.

La conversione dei dati dal formato nativo nel formato a commutazione di pacchetto è realizzata dal software residente nel computer del terminale o nel nodo di commutazione o da particolari apparecchiature PAD (Packet Assembler / Disassembler) poste tra l'utente e il nodo di commutazione.

4.1. Raccomandazione X.25

La raccomandazione ITU-T X.25, emessa nel 1976 e successivamente aggiornata, stabilisce le modalità di interfaccia tra un dispositivo terminale DTE di tipo X.25 al dispositivo di comunicazione DCE appartenente alla rete.

Il protocollo X.25 è suddiviso in tre livelli funzionali, tra loro indipendenti, che corrispondono ai tre livelli più bassi dell'architettura ISO/OSI.

- Livello 1 : Interfaccia a livello fisico.
  Definisce le caratteristiche elettriche e meccaniche dell'interfaccia tra DTE e DCE.

- Livello 2 : Interfaccia a livello di trama.
  Definisce le caratteristiche funzionali dell'interfaccia logica tra DTE e DCE e le procedure di controllo e correzione dei dati in trasmissione.

- Livello 3 : Interfaccia a livello di pacchetto.
  Definisce il formato dei pacchetti e le procedure di scambio di questi tra DTE e DCE.

In fig.32 si mostra lo schema a blocchi, secondo i livelli, del collegamento X.25 tra un DTE e un DCE.

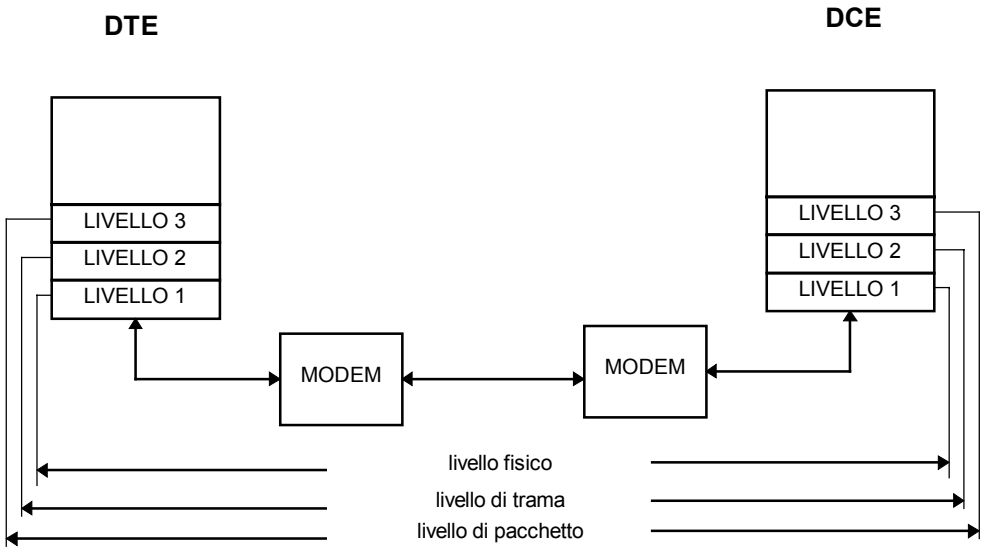


Fig.32. - I tre livelli ISO/OSI del protocollo X.25.

4.1.1. Livello 1

La raccomandazione X.25 stabilisce che la trasmissione è seriale sincrona full-duplex e l'accesso alla rete a commutazione di pacchetto può avvenire su rete commutata o dedicata. In entrambi i casi si utilizzano le interfacce X.21 o la X.21bis.

La raccomandazione X.21 descrive l'interfaccia tra DTE e DCE per operazioni sincrone su reti pubbliche per trasmissione dati.

La X.21 bis descrive l'interfaccia del DTE verso i modem sincroni della serie V. Quest'ultima è analoga alla V.24 corrispondente alla RS-232C.

Per velocità fino a 19.6Kbps si utilizza un connettore a 25 pin con caratteristiche elettriche V.28; per velocità superiori si utilizza un connettore a 34 poli con caratteristiche V.35. In tabella 11 si riportano le linee utilizzate nella raccomandazione X.21bis.

Tabella 11. - Linee di interfaccia X.21 bis

Nome	Funzione
C102	Massa dei segnali
C103	Dati in trasmissione
C104	Dati in ricezione
C105	Richiesta di trasmissione
C106	Pronto a trasmettere
C107	DCE pronto
C108/2	DTE pronto
C109	Rivelatore portante
C114	Clock di trasmissione
C115	Clock di ricezione
C140	Loop remoto
C141	Loop locale
C142	Indicatore di loop

4.1.2. Livello 2

La raccomandazione X.25, circa il livello 2, stabilisce che il protocollo utilizzato è l'HDLC la cui struttura è riportata in fig.33.

1 byte	1byte	1-2byte	0-1Kbyte	2byte	1byte
Flag	Indirizzo	Controllo	Dati	FCS	Flag

Fig.33. - Trama HDLC

Il campo *Flag*, presente sia all'inizio che alla fine del pacchetto, è un byte di valore $7E_{16}$ = 0111 1110, utilizzato per delimitare il pacchetto e come byte di sincronismo.
Il campo *Indirizzo*, della capienza di un byte, ci consente di distinguere i comandi dalle risposte sia nella direzione DTE → DCE che viceversa secondo la tabella 12.

Tabella 12

Direzione	Comandi	Risposte
DTE → DCE	0000 0001	0000 0011
DCE → DTE	0000 0011	0000 0001

Il campo *Controllo*, di ampiezza di uno o due byte, individua il tipo di trama che può essere :

- Informativa;
- di supervisione;
- non numerata.

La *trama informativa* è utilizzata per effettuare il trasferimento dei dati dell'utente.

La *trama di supervisione* è utilizzata per fornire la conferma di corretta ricezione o per la temporanea sospensione delle trame informative.

La *trama non numerata* è utilizzata per l'apertura o l'abbattimento del collegamento.

Il campo *Dati* contiene le informazioni da trasmettere e può essere ampio fino a 1Kbyte.

Il campo *FCS* (Frame Check Sequence - Sequenza di Controllo della Trama) è costituito da due byte ed è utilizzato per la rivelazione degli errori.

Esso è, in sostanza, il CRC ottenuto dai campi indirizzo, controllo e dati (quando quest'ultimo esiste). Il polinomio generatore è il CRC-CCITT di valore:

$$\mathbf{X^{16} + X^{12} + X^5 + 1}$$

Come è noto, il CRC è il resto della divisione tra la stringa dati (campi indirizzo, controllo e dati) e il polinomio generatore.

Tale resto, al più a 16 bit, ha una lunghezza massima pari al grado del polinomio generatore. Il protocollo HDLC ha due varianti:

- LAP (Link Access Procedure);
- LAP B (Link Access Procedure Bilances).

Le procedure LAP e LAP B sono entrambe *asincrone*, nel senso che la stazione secondaria può iniziare a trasmettere in qualsiasi istante senza il consenso della stazione primaria.

La procedura LAP è di tipo *sbilanciata* nel senso che la comunicazione può essere attivata solo dalla stazione primaria.

La procedura LAP B è di tipo *bilanciata* nel senso che la comunicazione può essere attivata sia dalla stazione primaria che dalla secondaria.

La procedura LAP B, avendo le caratteristiche consigliate dalle norme ISO/OSI, è quella utilizzata nelle nuove reti geografiche a commutazione di pacchetto.

4.1.3. Livello 3

Il livello 3 della raccomandazione X.25 descrive i formati e le procedure di scambio dei pacchetti tra un dispositivo terminale e la rete. Le procedure permesse sono:

- datagramma;
- chiamata virtuale;
- chiamata virtuale permanente.

La chiamata virtuale permanente, a differenza della chiamata virtuale, è priva delle fasi di richiesta di chiamata e richiesta di svincolo ed è, quindi, paragonabile ad un collegamento telefonico dedicato.

Il canale fisico che collega il dispositivo terminale alla rete contiene 4096 canali logici suddivisi in 16 gruppi (GCL) ciascuno costituito da 256 canali logici (CL).

Il canale logico rappresentato da tutti 0 è impiegato nei pacchetti di "restart" e di "diagnostica" per cui restano disponibili all'utente 4095.

Di ogni canale logico può essere definita la direzione: bidirezionale o monodirezionale.

Nella chiamata virtuale ogni canale logico è individuato da un numero stabilito all'atto della formazione del collegamento, nella chiamata virtuale permanente il numero che individua un canale logico è fisso.

Il campo "dati" del livello 2 rappresenta il pacchetto del livello 3. Quest'ultimo, a sua volta, contiene una sezione di intestazione ed una sezione di dati veri e propri.

La fisionomia del pacchetto dipende dalla particolare fase di appartenenza del pacchetto che qui ricordiamo:

- fase di chiamata;
- fase dati;
- fase di chiusura.

In fig.34 si riporta il formato generale del pacchetto della raccomandazione X.25 relativamente al livello 3.

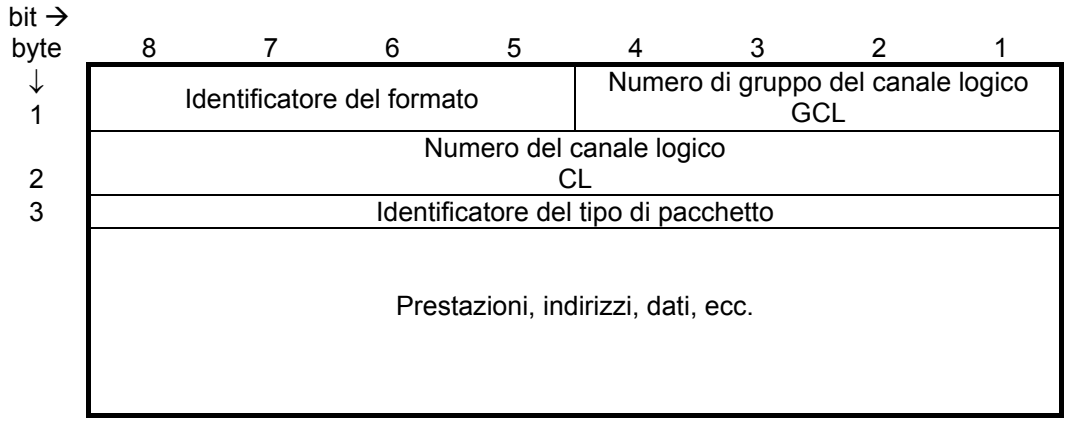


Fig.34. - Formato del pacchetto X.25.

I quattro bit dedicati all'identificatore del formato individuano il tipo di pacchetto:

`XX01`: Pacchetto dati (purché XX≠00);
`0001`: Pacchetti di impegno, svincolo, controllo flusso, interrupt, reset e restart.

Il terzo byte individua il tipo di pacchetto secondo la tabella 13.

Tabella 13

DCE → DTE	DTE → DCE	8 7 6 5 4 3 2 1
Call setup e svincolo		
Chiamata entrante	Richiesta di chiamata	0 0 0 0 1 0 1 1
Chiamata connessa	Chiamata accettata	0 0 0 0 1 1 1 1
Indicazione di svincolo	Richiesta di svincolo	0 0 0 1 0 0 1 1
Conferma di svincolo	Conferma di svincolo	0 0 0 1 0 1 1 1
Dati e interrupt		
Dati DCE	Dati DTE	x x x x x x x 0
Interrupt dal DCE	Interrupt dal DTE	0 0 1 0 0 0 1 1
Conferma interrupt DCE	Conferma interrupt dal DTE	0 0 1 0 0 1 1 1
Controllo di flusso e reset		
DCE RR	DTE RR	x x x 0 0 0 0 1
DCE RNR	DTE RNR	x x x 0 0 1 0 1
	DTE REJ	x x x 0 1 0 0 1
Indicazione di reset	Richiesta di reset	0 0 0 1 1 0 1 1
Conferma al reset	Conferma al reset	0 0 0 1 1 1 1 1
Restart		
Indicazione di restart	Richiesta di restart	1 1 1 1 1 0 1 1
Conferma di restart	Conferma al restart	1 1 1 1 1 1 1 1

Legenda :
RR = Receiver Ready: pronto a ricevere.
RNR = Receiver Not Ready: non pronto a ricevere
REJ = REJect: rifiuto di una trama.

Siamo ora in grado di dettagliare il diagramma delle connessioni tra due DTE collegati alla rete a commutazione di pacchetto con la procedura di chiamata virtuale secondo la raccomandazione X.25.

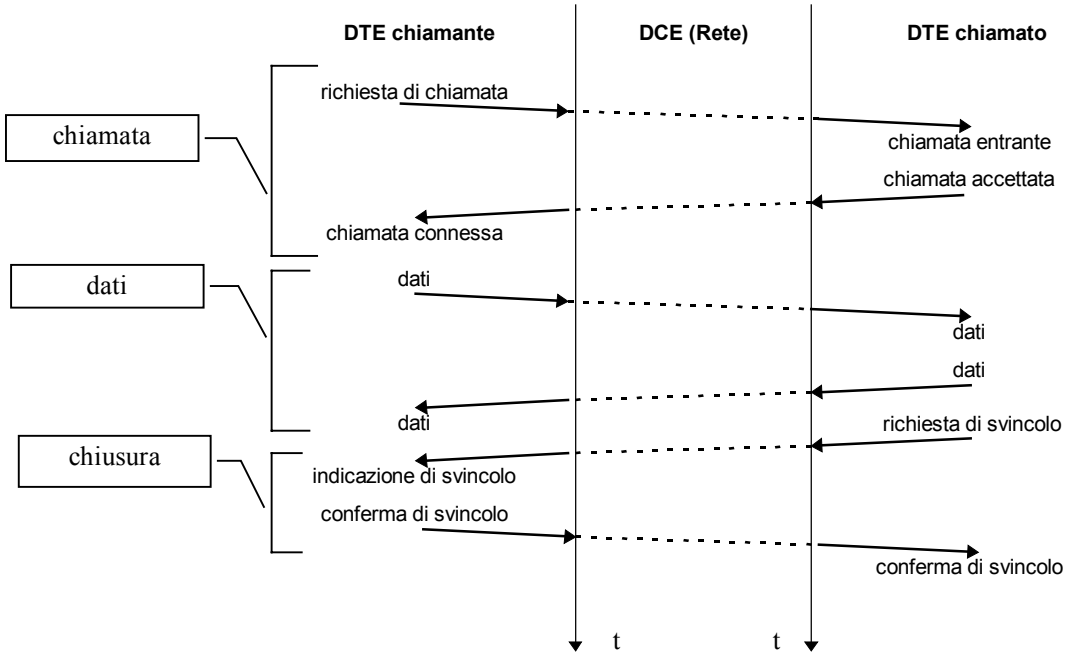


Fig. 35. - Diagramma delle connessioni relativa ad una chiamata virtuale X.25.

4.2. Raccomandazione X.75

La raccomandazione X.75 stabilisce le norme di collegamento su circuiti internazionali funzionanti a commutazione di pacchetto a circuito virtuale o datagramma.

Le funzioni dei livelli 1 e 2 coincidono, sostanzialmente, con quelle della raccomandazione X.25.

La differenza tra le due raccomandazioni riguarda il livello 3, cioè il protocollo di rete. Infatti, in alcuni tipi di pacchetti sono inseriti dei campi aggiuntivi che contengono informazioni per la gestione della rete come, ad esempio, l'aggiornamento delle tabelle di instradamento, formulazione di statistiche, dati per la tariffazione, ecc.

4.3. Raccomandazione X.28

I terminali che non rispettano lo standard X.25 possono collegarsi ad una rete X.25 attraverso un dispositivo PAD dislocato presso l'utente o nella rete stessa (Packet Assembler Disassembler) che ha lo scopo di trasformare i dati del terminale in un pacchetto di dati che soddisfa lo standard X.25.

Le caratteristiche dei PAD e le relative funzioni svolte nella rete sono descritte dalla raccomandazione X.3.

Ovviamente se il terminale riceve i dati, questi vengono disassemblati dal PAD dal formato di rete X.25 al formato Start/Stop tipico del terminale considerato.

La raccomandazione X.28 descrive le procedure di interfaccia tra il terminale e il PAD.

La raccomandazione X.29, infine, descrive le procedure di comunicazioni tra PAD e tra PAD e terminali X.25.

4.4. Raccomandazione X.32

La raccomandazione X.32, ultima modifica emessa nel marzo del 1993, descrive l'interfaccia tra un dispositivo terminale DTE e uno di comunicazione DCE per terminali che lavorano a pacchetto ed accedono ad una rete pubblica a commutazione di pacchetto tramite la rete telefonica commutata.

4.5. Itapac

Itapac è una rete publica a commutazione di pacchetto che supporta la chiamata virtuale e il circuito virtuale permanente e rispetta la raccomandazione X.25.

Realizzata nel 1972 attraverso un accordo tra la SIP (il gestore della rete telefonica pubblica nazionale fino al 1994, ora TELECOM Italia) e il Ministero delle Poste e Telecomunicazioni con lo scopo di consentire all'utenza la fruizione di una rete ad alta velocità fino a 9600 bps (per quei tempi) per le trasmissioni dati, è attualmente una rete scarsamente utilizzata visto che la maggior parte dei clienti preferisce lo scambio dei dati attraverso le tecnologie fornite da internet che consentono, tramite la suite di protocolli TCP/IP (Transmission Control Protocol/Internet Protocol), di attivare collegamenti tra un DTE intelligente, come un personal computer dotato di un opportuno software per la trasmissione dei dati, e un altro DTE intelligente, locato in un qualsiasi punto del pianeta. La trasmissione internet può concretizzarsi in una serie di servizi a basso costo che spaziano dalla trasmissione di file, alla posta elettronica, alla consultazione di pagine Web pubblicate da inserzionisti come enti sociali, militari, scolastici, universitari e commerciali.

5. Protocolli TCP/IP

Va sotto il nome di TCP/IP (Transmission Control Protocol/Internet Protocol) un insieme di circa 100 protocolli che consentono di dar vita ad *internet*, la rete delle reti.

L'obiettivo di internet è quello di assicurare la comunicazione di dati digitali dalla postazione di una rete locale alla postazione di un'altra rete, anche tecnologicamente diversa dalla prima, attraverso collegamenti che danno vita ad una particolarissima e sconfinata rete geografica. Vi sono, pertanto, particolari dispositivi di rete, di nome *gateway*, che hanno appunto il compito di stabilire il percorso che devono compiere i dati nel transitare da una rete locale all'altra.

La tecnica di trasmissione utilizzata da internet è a *commutazione di pacchetto* con servizio a datagramma (vedi paragrafo 3.3).

Il file da trasmettere viene suddiviso in frammenti ognuno dei quali prende il nome di *pacchetto*. Ogni pacchetto è autonomo poiché contiene tutte le informazioni necessarie: indirizzo IP del mittente e del destinatario, numero di sequenza, tipo di applicazione, ecc. Ogni pacchetto, per raggiungere la destinazione, prende un percorso autonomo che può essere diverso da quello attraversato da altri pacchetti.

Anche l'ordine di arrivo può essere differente per cui il protocollo TCP/IP del destinatario deve poter mettere "nella giusta sequenza" i pacchetti pervenuti.

Al TCP/IP appartengono, separatamente, anche il protocollo TCP e il protocollo IP.

Il TCP/IP è organizzato a livelli; in ciascuno di questi vengono svolti compiti specifici correlati a quelli dei livelli adiacenti attraverso interfacce.

I livelli del TCP/IP sono 4 e corrispondono in parte a quelli del modello ISO/OSI.

Tabella 14

ISO/OSI	TCP/IP	
Applicazione	Applicazione	HTTP, FTP, SMTP, TELNET
Presentazione		
Sessione		
Trasporto	Trasporto	TCP, UDP
Rete	Rete	IP, ICMP, ARP, RARP
Linea	Linea + Fisico	IEEE 802, EIA232, X21, ISDN, ecc.
Fisico		

Il *quarto livello*, il più alto, è quello nel quale gira la specifica applicazione (TELNET, FTP, SMTP, HTTP, ecc.).

Il *terzo livello*, corrispondente al quarto livello del modello OSI (trasporto), è utilizzato dal protocollo TCP che ha il compito di garantire che i pacchetti giungano a destinazione e che vengano opportunamente e ulteriormente suddivisi per consentire il passaggio su particolari rami della rete.

Il *secondo livello*, corrispondente al livello di rete del modello OSI, è utilizzato dal protocollo IP che ha il compito di instradare le informazioni al ricevitore.

Il *primo livello*, corrispondente ai primi due livelli del modello OSI, è relativo alle interfacce fisiche che consentono il reale trasferimento dei segnali elettrici.

In fig. 36 si mostrano i livelli o strati dei protocolli TCP/IP.

strato 4	FTP	TELNET	SMTP	RCP	SNMP	ecc.
strato 3	TCP		UDP			
strato 2	Protocolli dei gateway		IP e ICMP		ARP, RARP	
	IEEE802, Ethernet, DDCMP, LAPB/D/M/X, SDLC, ecc.					
strato 1	IEEE802, Ethernet, EIA-232, X.21, X.21bis, V.24, V.28, ISDN, ecc.					

Fig.36. - Stack dei protocolli TCP/IP.

5.1. Indirizzi IP

Le reti collegate ad internet attraverso i protocolli TCP/IP utilizzano un indirizzo a 32 bit (oltre 4 miliardi di configurazioni numeriche), secondo lo standard RFC 791 (Request For Comments) http://www.faqs.org/rfcs/rfc791.html per individuare un computer e la rete nella quale è inserito il computer. Il formato di tale indirizzo è:

Indirizzo IP = Indirizzo di rete + Indirizzo di host

L'indirizzo è rappresentato da 4 byte ognuno dei quali espresso in forma decimale da 0 a 255 e separato dagli altri con un punto.

Ad esempio, un tipico indirizzo IP è: 195.32.115.9.

Sono consentiti quattro tipi di formati di indirizzo IP indicati con classe A, classe B, classe C e classe D.

È previsto un ulteriore formato per usi futuri indicato con classe E.

Si escludono quegli indirizzi IP che hanno indirizzo di rete costituito da tutti 0 e da tutti 1 e, analogamente, si escludono quelli con indirizzo di host costituito da tutti 0 e da tutti 1. Quando l'indirizzo di host è costituito da tutti 0 l'indirizzo IP esprime l'indirizzo di rete. Quando l'indirizzo di host è costituito da tutti 1 si ha il broadcast a tutti i PC della rete.

L'ente che ha il compito di assegnare gli indirizzi di rete è il NIC (Network Information Center). La rete provvede ad assegnare a ciascun suo host la parte rimanente dell'indirizzo.

Si mostra, in tabella 15, il formato degli indirizzi IP in funzione della classe di appartenenza.

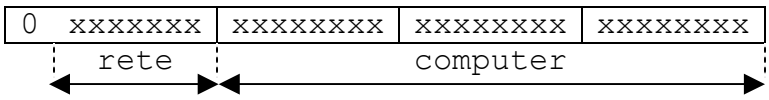
Tabella 15

Classe	bit iniziali	indirizzo rete (in bit)	indirizzo host (in bit)	reti individuabili	host disponibili
A	0	7	24	128	16.777.216
B	10	14	16	16.384	65.536
C	110	21	8	2.097.152	254
D	1110	Indirizzo Multicast a 28 bit (268.435.456 indirizzi)			
E	11110	Riservato per usi futuri a 27 bit (134.217.728 indirizzi)			

Classe A

È il formato di indirizzo per reti aventi un numero elevatissimo di host. Le reti disponibili sono 126 (da 1 a 126; i numeri 0 e 127 sono riservati). Il campo per individuare un host è di 24 bit corrispondente ad un numero massimo superiore a 16 milioni. Il primo numero dell'indirizzo IP va da 1 a 126 ed individua la rete; i restanti 3 numeri (24 bit) individuano l'host all'interno della rete. Gli host individuati da tutti 0 e da tutti 1 non sono utilizzabili.

L'intervallo dei valori consentiti va da 1.0.0.1 a 126.255.255.254.

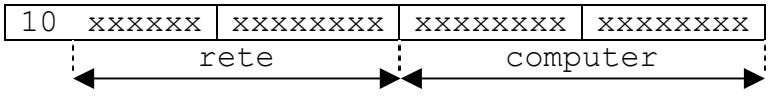


Si riportano alcune società che hanno indirizzi IP in classe A:
Hewlett Packard (15.0.0.0), Apple Computer (17.0.0.0), Stanford University (36.0.0.0), Posta Americana (56.0.0.0).

Classe B

Gli indirizzi di classe B sono utilizzati dalle reti di dimensioni intermedie. Le reti individuabili sono oltre 16000 (14 bit) e il numero massimo di host di ciascuna rete è superiore a 64000 (16 bit). I primi due numeri dell'indirizzo IP vanno da 128.1 a 191.254 ed individuano la rete (al solito si escludono il primo e l'ultimo indirizzo cioè 128.0 e 191.255); i restanti due numeri individuano l'host all'interno della rete. Gli host individuati da tutti 0 e da tutti 1 non sono utilizzabili.

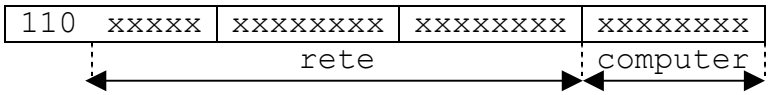
L'intervallo dei valori consentiti va da 128.1.0.1 a 191.254.255.254.



Classe C

Gli indirizzi di classe C sono utilizzati da reti molto piccole. Le reti individuabili sono oltre due milioni (21 bit) ed il numero massimo di host di ciascuna rete è di 254 (si escludono 0 e 255). I primi tre numeri dell'indirizzo IP vanno da 192.0.1 a 223.255.254 ed individuano la rete; l'ultimo numero, da 1 a 254, individua l'host all'interno della rete.

L'intervallo dei valori consentiti va da 192.0.1.1 a 223.255.254.254.



Classe D

Gli indirizzi di classe D sono utilizzati dagli host che costituiscono un gruppo di Multicast. Poiché i primi 4 bit dell'indirizzo IP valgono 1110, l'intervallo dei valori consentiti va da 224.0.0.0 fino a 239.255.255.255. L'indirizzo 224.0.0.0 non è consentito da internet e l'indirizzo 224.0.0.1 individua un gruppo di tutti host che partecipano ad una operazione di *multicast IP internet*.

Esempio

Individuare il tipo di rete, l'indirizzo di rete e di host per il seguente indirizzo IP:

195.32.115.9 (1)

Risoluzione

L'indirizzo IP assegnato corrisponde al seguente numero binario a 32 bit:

11000011 00100000 01110011 00001001

L'indirizzo di rete si ottiene dalla (1) eliminando i bit che individuano la classe (110 per la classe C) e gli ultimi 8 bit che rappresentano l'indirizzo di host.

$$00011\ 00100000\ 01110011_2 = 204915_{10}\ .$$

L'indirizzo interno dell'host è: $00001001_2 = 9_{10}$.

5.1.1. Indirizzi IP privati

Una rete locale può utilizzare il protocollo TCP/IP per lo scambio dei dati tra gli elementi della LAN. In tal caso ciascun nodo deve possedere un indirizzo IP che può essere fisso oppure assegnato dinamicamente come, ad esempio, viene attribuito dal servizio DHCP, se attivato, del sistema operativo di rete Windows Server.

Esistono particolari intervalli di indirizzi IP destinati ai nodi delle reti locali e non accessibili da internet. Ciò consente una certa protezione dei dati che circolano all'interno della LAN lontano da occhi indiscreti.

Nella seguente tabella 16 si forniscono gli intervalli di indirizzi privati utilizzabili dalle postazioni LAN. Essi possono essere di classe A, di classe B e di classe C. La scelta che l'amministratore di rete dovrà compiere è funzione della dimensione della rete locale.

Tabella 16. – Indirizzi IP privati utilizzabili nelle reti LAN

Classe	Intervallo di indirizzi
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

In genere si preferiscono gli indirizzi di classe C poiché quasi tutte le reti locali sono costituite da meno di 254 nodi. In particolare si sceglie la rete con indirizzo 192.168.0.0.

Il computer server normalmente ha indirizzo 192.168.0.1 e nella rete si possono individuare fino a 254 nodi. Quello con indirizzo IP più alto è 192.168.0.254.

Un altro indirizzo IP particolare è 127.0.0.1 che individua il computer locale, la macchina, cioè, su cui si sta lavorando. Tale indirizzo è particolarmente utile quando si vuole testare la funzionalità di un'applicazione in rete residente sulla propria macchina senza doversi spostare su un'altra macchina della rete. Ad esempio nel PC sul quale si sta lavorando è installato ed attivato un web server. Tale PC è in rete locale con indirizzo 192.168.0.1. Supponiamo che il nome del PC sia "PCserver".

Per visualizzare la home page senza dover eseguire la prova da un altro PC della rete è sufficiente digitare, all'interno del proprio browser: http://127.0.0.1 .

Questo comando è equivalente ai seguenti altri comandi:
http://localhost , http://192.168.0.1 , http://PCserver .

5.1.2. Sottoreti

Una rete locale fisica può suddividersi in una o più sottoreti locali logiche. Per far questo si utilizza una particolare maschera costituita da 32 bit, suddivisa in 4 numeri separati da punti, come l'indirizzo IP, nota come *subnet mask* (maschera di sottorete).

I computer con stessa subnet mask appartengono alla stessa sottorete.

La subnet mask individua la sottorete. Il computer con subnet mask 255.255.255.0 ed indirizzo IP 192.168.0.5 appartiene alla rete di classe C 192.168.0.0. Qualsiasi computer i cui primi tre numeri dell'indirizzo IP sono pari a 192.168.0 appartiene alla rete. Per individuare una sottorete si utilizzano due o più bit da sottrarre all'indirizzo di host. Nella subnet mask devono essere posti ad uno i bit omologhi ai seguenti campi:
bit iniziali, indirizzo di rete, indirizzo di sottorete.

In pratica l'indirizzo IP di un nodo della rete è costituito da 4 campi:

bit iniziali	indirizzo di rete	indirizzo di sottorete	indirizzo di host

Volendo realizzare due o più sottoreti della rete locale in classe C 192.168.0.0, il quarto numero della subnet mask dovrà essere diverso da 0.

Esempio 1

Ponendo a 1 i primi due bit del quarto numero della subnet mask, si individuano 4 sottoreti (4 combinazioni degli omologhi bit degli indirizzi IP dei computer della rete: 00, 01, 10, 11).
Subnet mask: $255.255.255.192_{10}$ = $11111111.11111111.11111111.11000000_2$
Indirizzo della rete fisica: 192.168.0.0
Sottorete 0: da 192.168.0.0 a 192.168.0.63
Sottorete 1: da 192.168.0.64 a 192.168.0.127
Sottorete 2: da 192.168.0.128 a 192.168.0.191
Sottorete 3: da 192.168.0.192 a 192.168.0.255

Le sottoreti 0 e 3 non sono utilizzabili. Ogni sottorete dispone di 64 indirizzi IP di cui solo 62 sono utilizzabili (si escludono il primo e l'ultimo di valore 0 e 63, come al solito). Infatti, potendo gestire 6 bit di indirizzo di host si possono individuare un massimo di 2^6=64 host da cui sottrarre il primo e l'ultimo (64-2=62).

Esempio 2

Ponendo a 1 i primi 3 bit del quarto numero della subnet mask, posso individuare 8 sottoreti di cui solo 6 utilizzabili (le sottoreti 0 e 7 non sono utilizzabili cioè la prima e l'ultima della lista).

La subnet mask vale: 255.255.255.224 e le sottoreti sono:
Sottorete 0: 192.168.0.0 - 192.168.0.31
Sottorete 1: 192.168.0.32 - 192.168.0.63
Sottorete 2: 192.168.0.64 - 192.168.0.95
Sottorete 3: 192.168.0.96 - 192.168.0.127
Sottorete 4: 192.168.0.128 - 192.168.0.159
Sottorete 5: 192.168.0.160 - 192.168.0.191

Sottorete 6: 192.168.0.192 - 192.168.0.223
Sottorete 7: 192.168.0.224 - 192.168.0.255

Ogni sottorete dispone di 32 indirizzi IP di cui solo 30 sono utilizzabili (si escludono il primo e l'ultimo). Infatti, potendo gestire 5 bit di indirizzo di host si possono individuare un massimo di 2^5=32 host da cui sottrarre il primo e l'ultimo (32-2=30).

Si mostra in fig. 37 una rete fisica suddivisa in 2 sottoreti logiche. Il quarto numero della subnet mask di ciascun PC vale 192 che, in binario, corrisponde a 1100000. Si possono individuare 4 sottoreti, come nell'esempio 1. Alla sottorete 1 appartengono i PC con indirizzi di host 100 e 101; alla sottorete 2 appartengono i rimanenti 3 PC con indirizzi di host 130, 131 e 132.

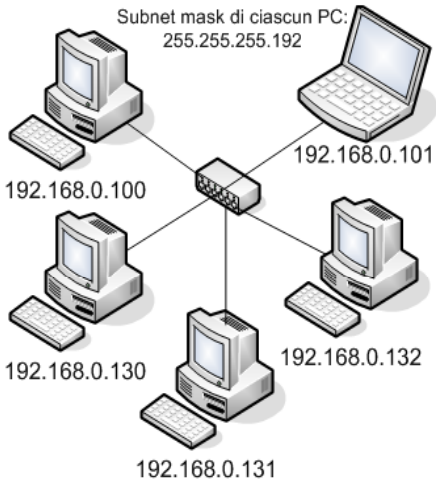


Fig.37. – Rete fisica suddivisa in due sottoreti logiche.

5.2. DNS

Poiché non è facile ricordare a memoria l'indirizzo IP numerico del server al quale ci si desidera collegare, si è pensato di utilizzare un indirizzo mnemonico da porre in corrispondenza biunivoca con l'indirizzo numerico IP attraverso una tabella.

L'insieme degli indirizzi mnemonici è denominato DNS (Domain Name System).

La scelta dell'indirizzo mnemonico non è del tutto arbitraria perché deve seguire una logica che consente, seppur in minima misura, di riconoscere la natura del sito: università (edu), militare (mil), governativo (gov), commerciale (com), italiano (it), inglese (uk), svizzero (ch), francese (fr), europeo (eu), ecc. e il tipo di protocollo: ftp, www, mail, news, ecc. I vari nomi che compongono l'indirizzo sono separati tra loro da un punto. La documentazione è disponibile nella RFC 1034 (http://www.faqs.org/rfcs/rfc1034.html).

Ad esempio, i seguenti DNS individuano, rispettivamente:
http://www.tiscali.it un server *Wide World Web italiano* di nome *tiscali*.
http://www.sony.com un server *Wide World Web commerciale* di nome *sony*.
ftp://ftp.libero.it/pub/ la sottodirectory *pub* del server *ftp italiano* di nome *libero*.

I prefissi http (HyperText Transfer Protocol) ed ftp (File Transfer Protocol) individuano il tipo di applicazione da utilizzare.

Il protocollo per la gestione del DNS funziona nel seguente modo:

- Quando una applicazione deve collegarsi ad una risorsa di cui conosce l'indirizzo mnemonico, invia una richiesta al DNS server locale;
- Il DNS server locale, se conosce la risposta, la invia direttamente al richiedente altrimenti interroga un DNS server di livello superiore e così via;

- L'applicazione, ottenuta la risposta, attiva una connessione TCP usando, come indirizzo di destinazione, l'indirizzo IP ricevuto.

Il coordinamento di questo complesso sistema è stato affidato ad un organismo internazionale di nome ICANN (Internet Corporation for Assigned Names and Numbers) http://www.icann.org che, a sua, volta, ha affidato il coordinamento nelle singole nazioni ad organismi nazionali. In Italia tale organismo è l'Istituto di Informatica e Telematica del CNR di Pisa che si avvale del sito con indirizzo: http://www.nic.it/RA (RA=Registration Authority).

5.3. Protocolli per la risoluzione degli indirizzi

Il protocollo ARP (Address Resolution Protocol, RFC 826, reperibile sul sito http://www.faqs.org/rfcs/rfc826.html) consente di determinare l'indirizzo univoco di scheda di rete (MAC address) a partire dall'indirizzo IP del destinatario del pacchetto. Il protocollo funziona nel seguente modo: viene inviata a tutti i nodi della rete LAN una richiesta del tipo "a chi appartiene questo indirizzo IP?"; risponde solo il nodo che ha tale indirizzo fornendo anche il MAC address (fig.38).

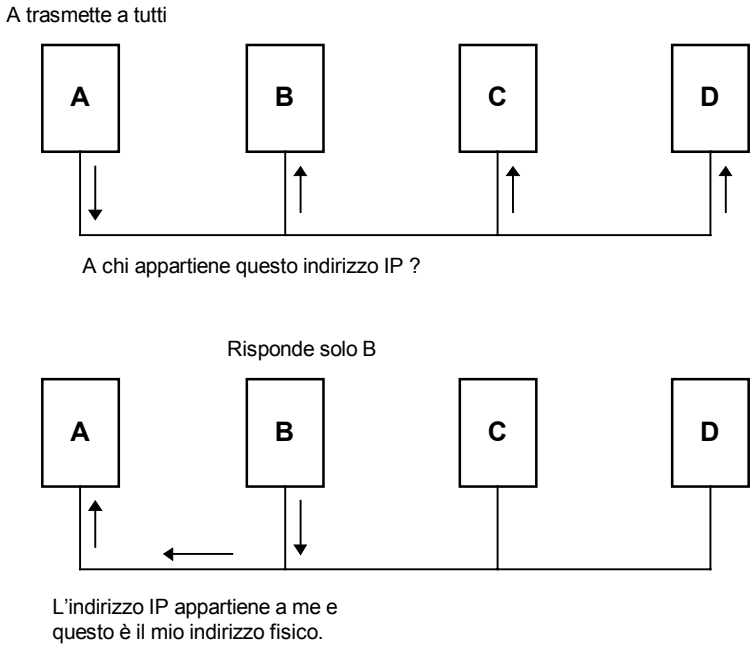


Fig.38. - Protocollo ARP: richiesta e risposta.

Vi sono alcune stazioni di lavoro senza disco fisso che non conoscono il proprio indirizzo IP. Per ottenere l'indirizzo IP la stazione invia a tutti il proprio MAC address e solo il server RARP (Reverse Address Resolution Protocol) è in grado di trasmettere l'indirizzo IP conoscendo quello fisico. Il server RARP, quindi, esegue l'operazione inversa rispetto al protocollo ARP. In fig.39 si mostra la metodologia per risalire al proprio indirizzo IP.

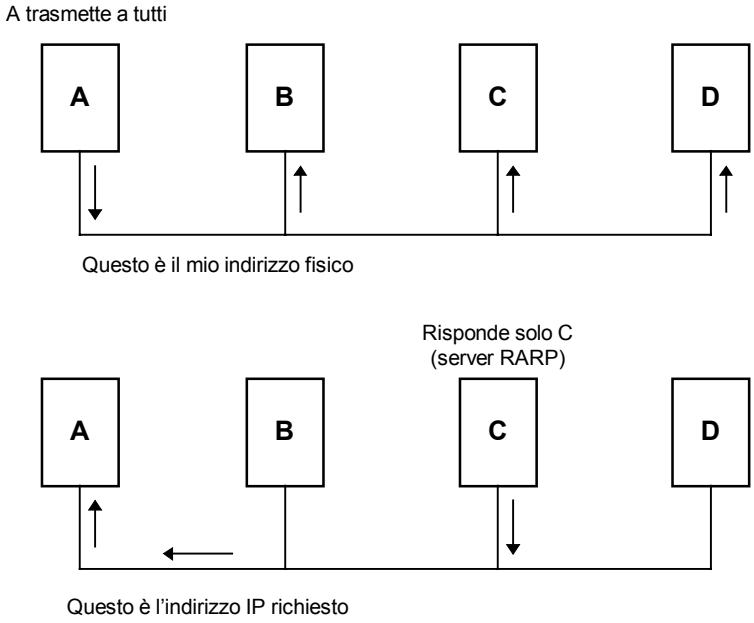


Fig.39. - Metodo per ottenere il proprio indirizzo IP.

5.4. Protocollo Internet IP

Il Protocollo di rete IP (Internet Protocol), elaborato dal Dipartimento della Difesa degli Stati Uniti, abbastanza simile alla specifica ISO 8473 relativa al protocollo senza connessione CLNP, consente lo scambio di dati tra due computer host senza alcuna impostazione preliminare della chiamata. Poiché IP è un protocollo senza connessione è possibile che i datagrammi vadano persi prima di completare l'intero tragitto.

IP non è dotato di meccanismi di sicurezza: non prevede la correzione degli errori né il controllo se i datagrammi sono persi, duplicati o giunti in ordine errato.

Tutti questi inconvenienti vengono risolti dal protocollo TCP appartenente allo strato superiore, il livello di trasporto.

Il protocollo IP supporta l'operazione di frammentazione che consiste nella suddivisione di una **PDU**[4] in unità più piccole poiché non tutte le reti adottano la stessa dimensione per la PDU. La dimensione di una PDU va da 128byte (X.25) a 1500byte (Ethernet).

Tutte le reti prevedono una dimensione massima per la PDU *denominata Unità di Trasmissione Massima* **MTU**.

Si mostra, nella tabella 17, il datagramma IP. Fra parentesi è indicato il numero di bit impiegato dal relativo campo.

Tabella 17. – Datagramma IP

[4] PDU=Protocol Data Unit. Corrisponde al pacchetto nel protocollo X.25.

Versione (4)	Lunghezza intestazione (4)
Tipo di servizio (8)	
Lunghezza totale (16)	
Identificatore (16)	
Flag (3)	Scostamento del frammento (13)
Tempo di durata (8)	
Protocollo (8)	
Checksum dell'intestazione (16)	
Indirizzo di origine (32)	
Indirizzo di destinazione (32)	
Opzioni e riempimento (variabili)	
Dati (variabili)	

Si descrivono i campi del protocollo IP:

1. La *versione* identifica il tipo di IP. Attualmente la versione è la 4 (IPV4). In futuro si avrà la IPV6.
2. Occorre specificare la *lunghezza dell'intestazione* poiché i campi opzioni e riempimento sono di lunghezza variabile.
3. Il *tipo di servizio* consente di impostare le funzioni di qualità del servizio; è composto da 4 sottocampi: precedenza (3bit) che indica l'importanza del datagramma, ritardo (1bit), efficienza (1bit), attendibilità (1bit). Normalmente questi ultimi 3 bit sono impostati a 0. Se sono impostati a 1 si richiede un basso ritardo ed una elevata efficienza ed attendibilità.
4. La *lunghezza totale* si riferisce al datagramma comprensivo dell'intestazione.
5. *L'identificatore* viene utilizzato con i campi degli indirizzi per identificare in modo univoco la PDU da frammentare.
6. Il *flag* è utilizzato nelle operazioni di frammentazione. Il primo bit è inutilizzato. Il secondo bit è Don't Fragment (DF) ed il terzo è More Fragment (MF). Se DF=1 il datagramma non può essere frammentato.
7. Lo *scostamento del frammento* indica a quale frammento della PDU appartiene il datagramma.
8. Il *tempo di durata* (TTL=Time To Live) indica quanto tempo un datagramma può vivere in Internet. Quando un datagramma attraversa un router il campo TTL viene decrementato di 1. Quando TTL=0 il router scarta il datagramma ed invia al mittente, tramite protocollo ICMP, un messaggio di invito a ritrasmettere il datagramma.
9. Il campo *protocollo* individua il protocollo dello strato superiore del ricevitore che deve elaborare il datagramma. Ogni protocollo ha un suo codice ben definito, ad esempio: ICMP è il protocollo 1, TCP è il protocollo 6.
10. Il *checksum* dell'intestazione serve ad effettuare il controllo degli errori nell'intestazione. Ogni router attraversato dal datagramma deve ricalcolare questo campo poiché decrementa di 1 il TTL.
11. *Indirizzo di origine* e di *destinazione* identificano i relativi computer e le reti collegate direttamente ad essi. In pratica rappresentano gli indirizzi IP.
12. Il campo *opzioni* viene utilizzato per richiedere servizi supplementari.
13. Il campo *riempimento* viene utilizzato per dare al datagramma un allineamento a 32 bit.
14. Il campo *dati* contiene i dati dell'utente.

IP è un protocollo di strato di rete che svolge le funzioni di:

- indirizzamento;

- instradamento;
- frammentazione;
- aggregazione.

Il principale servizio di IP è il trasferimento delle unità informative PDU.

Esso è inaffidabile poiché la consegna della PDU non è garantita: il pacchetto può essere perso, non consegnato o fuori sequenza.

Il datagramma, trasferendosi di rete in rete, può essere frammentato, cioè ulteriormente suddivido, per poi essere ricomposto quando giunge a destinazione.

Le procedure di frammentazione e di aggregazione da parte di IP devono essere in grado di segmentare il pacchetto in un numero arbitrario di unità che, giunte a destinazione, devono poter essere ricomposte nella forma originaria.

L'instradamento può essere diretto o indiretto. Nel primo caso il mittente e il destinatario del pacchetto appartengono alla stessa sottorete; non viene coinvolto alcun gateway, punto di accesso ad una sottorete. Nel secondo caso il mittente e il destinatario del pacchetto appartengono a sottoreti diverse.

I gateway delle varie sottoreti fanno da ponte al pacchetto che si muove dal mittente al destinatario.

5.4.1. IPV6

La quantità di indirizzi IP ancora disponibili nella rete internet va rapidamente diminuendo per cui si è pensato di elevare da 32 a 128 il numero di bit che individua un indirizzo IP. In tal modo si metterebbe a disposizione un numero sconfinato di possibili indirizzi IP (2^{128}). Questo è il principale motivo per cui il gruppo di lavoro IETF (Internet Engineering Task Force) ha messo a punto la versione 6 del protocollo IP coniando il termine IPV6. Gli altri vantaggi rispetto all'attuale versione di IP (IPV4) sono: maggior efficienza nei router in quanto permette di minimizzare le tabelle di routing grazie ad un'organizzazione più flessibile degli indirizzi, miglior supporto del traffico dati "real time", maggior sicurezza nei confronti dei dati riservati, 8 campi anziché 13 nelle intestazioni, funzioni di autentificazione e privacy basate su crittografia. I pacchetti non possono più essere frammentati lungo il percorso ma solo da chi trasmette e riceve.

L'utilizzo di IPV6 su sistemi Windows XP e 2003 è immediato: è sufficiente eseguire, dal prompt del DOS, il comando **ipv6 – install.** Su Windows 2000 SP1 è necessario applicare una opportuna patch scaricabile da internet.

Nell'attuale periodo di transizione da IPV4 a IPV6, una volta installato IPV6, per poter comunicare con un PC che implementa il vecchio IPV4 è necessario collegarsi ad un "tunnel broker". Microsoft consente il collegamento automatico ad un proprio server di tunnelling. Volendo scegliere un diverso "tunnel broker" si possono ottenere informazioni al sito http://ipv6.he.net/. Il datagramma di IPV6 è così costituito:

1) Versione (4 bit): versione del protocollo usato;
2) Priorità (4 bit);
3) Flow label (24 bit): indicatore di flusso;
4) Payload lenght (16 bit): lunghezza del pacchetto;
5) Next Header (8 bit): indica l'extension header;
6) Hop limit (8 bit): numero di nodi attraversati prima dell'abbattimento del pacchetto;
7) Source Address (128 bit): indirizzo di origine;
8) Destination Address (128 bit): indirizzo di destinazione.

La vecchia notazione a 4 cifre decimali per l'individuazione dell'indirizzo IP è sostituita, nella versione IPV6, da 8 numeri esadecimali ciascuno a 4 cifre. Un esempio di indirizzo IPV6 è il seguente:

5B3E:00A0:0000:0000:A502:753B:0000:0007

Si ritiene che ogni essere umano possa disporre di 256 indirizzi IPV6.

È possibile semplificare la notazione IP omettendo gli zeri in testa ad ogni blocco di 4 cifre esadecimali ed omettendo i blocchi consecutivi costituiti da tutti 0, operazione che può essere svolta una sola volta. L'indirizzo IP precedente, pertanto, si può così semplificare:

5B3E:A0::A502:753B:0:7

L'indirizzo di localhost 127.0.0.1 in IPV4, è costituito, in IPV6, da tutti i bit uguali a zero tranne l'ultimo che, ovviamente, vale 1. In esadecimale:

0000.0000.0000.0000.0000.0000.0000.0001

In notazione esadecimale semplificata l'indirizzo di localhost vale **::1**.

5.5. Protocollo ICMP

Il protocollo IP non è in grado di individuare o correggere gli errori ma si affida al *Protocollo dei Messaggi di Controllo di Internet* avente sigla ICMP, residente nel computer host o nel gateway.

Tale protocollo viene utilizzato per fornire messaggi di errore, di stato e amministrativi.

ICMP, protocollo di rete, è impiegato tra gli host o i gateway quando i datagrammi non possono essere consegnati, quando un gateway dirige il traffico su percorsi più brevi o quando un gateway non ha sufficiente memoria per conservare ed inoltrare dati.

ICMP comunica all'host se una destinazione è irraggiungibile, crea e gestisce messaggi per segnalare il superamento del tempo massimo TTL ed esegue delle funzioni di modifica per determinare se l'intestazione IP è errata.

Ping

Una delle funzioni, denominata PING, consiste nella richiesta di eco inviata a un qualsiasi indirizzo IP; l'host o il gateway sollecitato risponde all'unità richiedente.

Questo servizio consente di verificare se ci sono problemi sulla rete, se la destinazione è attiva e disponibile senza effettuare alcun trasferimento dati.

Per verificare, ad esempio, che la scheda di rete sul proprio computer è correttamente configurata e funzionante è sufficiente digitare dal prompt DOS il comando:

```
c:\>ping 127.0.0.1
```

Si ottiene come risposta:

```
Esecuzione di Ping 127.0.0.1 con 32 byte di dati:
Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128
Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128
Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128
Risposta da 127.0.0.1: byte=32 durata<1ms TTL=128

Statistiche Ping per 127.0.0.1:
Pacchetti: Trasmessi=4, Ricevuti=4, Persi=0 (0% persi),
```

```
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo=0ms, Massimo=0ms, Medio=0ms
```

Si ottiene lo stesso risultato digitando uno qualsiasi dei tre seguenti comandi ping ove 10.5.1.6 è l'indirizzo IP del computer di nome P4:

```
C:\>ping localhost    c:\>ping 10.5.1.6    c:\>ping P4
```

Eseguendo, invece, un ping ad un indirizzo IP non raggiungibile (computer remoto spento, scheda di rete del computer remoto guasta, rete bloccata, IP inesistente, ecc.) si ottiene:

```
c:\>ping 10.5.1.7
Esecuzione di Ping 10.5.1.7 con 32 byte di dati:
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.

Statistiche Ping per 10.5.1.7:
Pacchetti: Trasmessi=4, Ricevuti=0, Persi=4 (100% persi),
```

Per avere la sintassi e lista delle opzioni possibili col comando ping è sufficiente digitare solamente **ping** al prompt dei comandi senza specificare alcun nome o indirizzo IP.

Se si esegue un ping ad un computer collegato ad internet non è certo che la funzione vada a buon fine poiché l'host che riceve il comando ping potrebbe essere protetto da un *firewall* che rifiuta il comando ping.

Si esegua, a tale proposito il comando ping ai siti www.deltabeta.it e www.libero.it . Il comando ping, nei due casi, restituisce anche il numero di IP.

Si mostra in fig.40 l'esito del comando ping nei due casi.

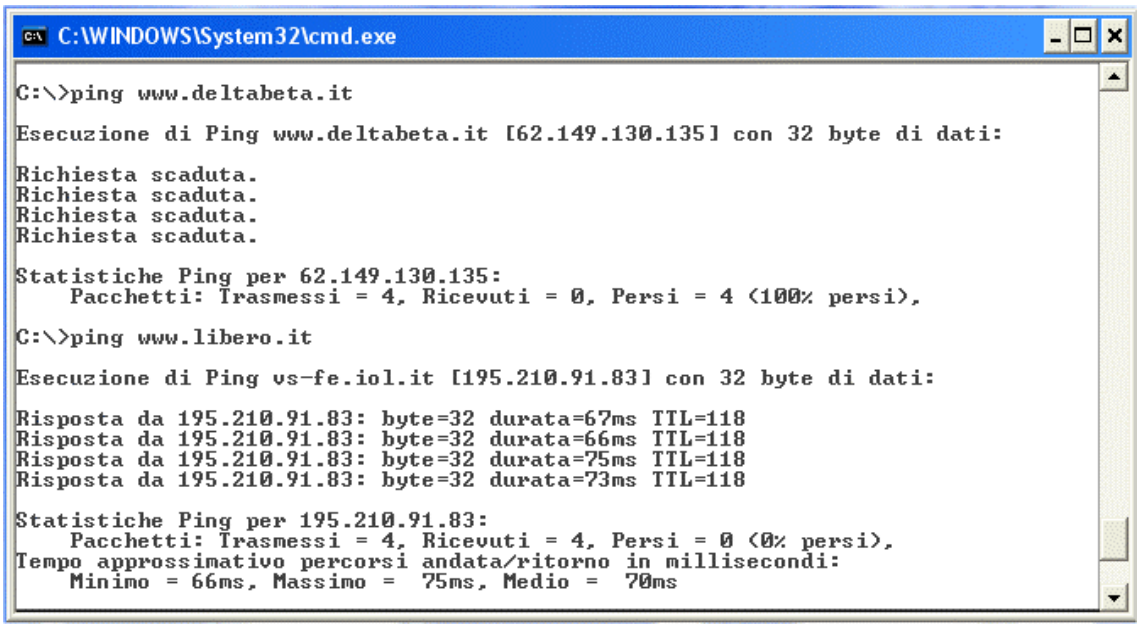


Fig.40. – Esecuzione del comando ping a due siti internet.

Si noti che la risposta, nel secondo caso, fornisce una durata significativa della vita di un pacchetto compresa tra 66ms e 75ms e un TTL=118 ad indicare che il pacchetto, tra andata e ritorno, ha attraversato 10 nodi (128-10=118).

5.6. Protocollo TCP

Il protocollo TCP (Transmission Control Protocol) è molto simile al protocollo di trasporto di quarto livello OSI. La documentazione è disponibile nella RFC 1122 e nell'aggiornamento RFC1323 disponibili sul sito: http://www.faqs.org/rfcs/

In fig.41 si mostra la collocazione del protocollo TCP tra i diversi strati e gli strati interessati nella comunicazione dei dati da un host della rete A ad un host della rete C attraverso i router 1 e 2 (o gateway).

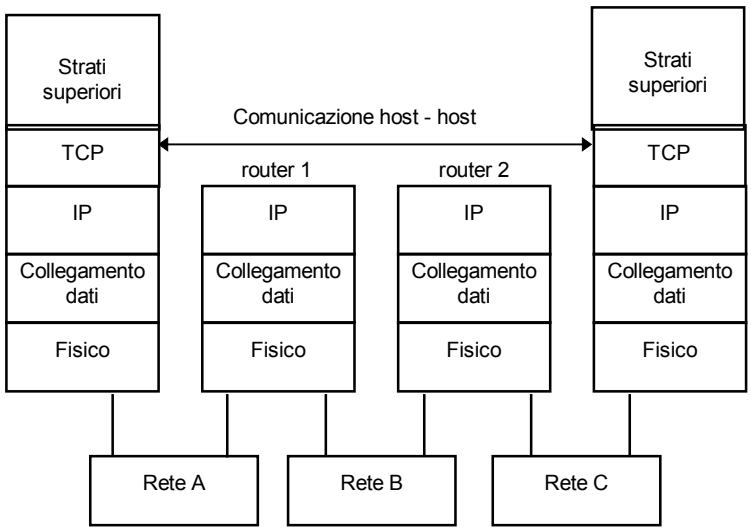


Fig.41. - Strati interessati nella comunicazione host-host.

Il protocollo TCP risiede nel computer host e non nel router ed è progettato per funzionare sopra il protocollo IP.

Quest'ultimo non prevede il sequenziamento e il riconoscimento dei dati per cui spetta al protocollo TCP le operazioni di affidabilità dei dati, il controllo di flusso e il sequenziamento delle sessioni delle applicazioni.

I protocolli di livello superiore come HTTP per il trasferimento di ipertesti, l'FTP per il trasferimento dei file e l'SMTP (Simple Mail Transfer Protocol) per il trasferimento semplice della posta elettronica si basano sui servizi TCP.

Molte delle funzioni svolte da TCP possono essere eseguite dall'interno del software applicativo; in realtà, però, si preferisce affidare tutte le funzioni ad un programma specifico richiamabile dal software applicativo.

Si ricordi, a tale proposito, il programma Winsock che attiva lo stack TCP/IP e gli applicativi in grado di gestire la posta elettronica (Outlook Express), gli ipertesti (Internet Explorer), le news di Usenet (Free Agent), FTP (Filezilla), ecc.

5.6.1. Caratteristiche del TCP

I servizi garantiti dal protocollo TCP ai livelli superiori si possono elencare nei seguenti:

- Gestione dei dati orientati alla connessione;
- Trasferimento affidabile dei dati;
- Trasferimento dei dati organizzato a flussi;
- Funzioni di impilaggio;
- Risequenziamento;

- Controllo del flusso;
- Multiplexing;
- Trasmissione full-duplex;
- Precedenza e sicurezza;
- Chiusura garbata.

Il protocollo TPC è *orientato alla connessione* nel senso che conserva le informazioni relative allo stato del flusso dati che l'ha attraversato.

Il TCP ricevente adotta la tecnica del checksum per il *controllo degli errori*: una PDU errata viene scartata e, in base al numero di sequenza, il TCP ricevente comunica al trasmittente quale PDU ritrasmettere; se la PDU è verosimilmente corretta il TCP ricevente risponde con un messaggio di riconoscimento **ACK**.

Il TCP trasmittente invia altri segmenti prima di ricevere il messaggio ACK.

La funzione di *impilaggio* consente ad un'applicazione di verificare che sono stati trasmessi i dati trasferiti al protocollo di strato inferiore.

Se per qualche motivo il TCP trasmittente inoltra uno stesso segmento, il ricevente *scarta i duplicati*.

Per questi motivi le PDU possono giungere a destinazione in ordine non corretto e il TCP ricevente utilizza il numero di sequenza per il *risequenziamento* dei segmenti.

Il protocollo TCP riceve i dati dallo strato superiore a *flussi*, cioè un byte per volta; è suo compito organizzarli in *segmenti* TCP che vengono passati a IP o ad un altro protocollo di strato inferiore.

Un'altra funzione assicurata dal TCP è il *controllo di flusso* dei dati del mittente: essa si basa sull'emissione di un valore, definito *finestra*, alla stazione trasmittente; quest'ultima deve interrompere la trasmissione quando il numero di byte raggiunge quello specificato in finestra.

Il servizio di *multiplexing* supportato da TCP consiste nel far coesistere più sessioni contemporaneamente nello stesso PC semplicemente assegnando un numero di porta alle varie applicazioni.

Col *full-duplex* TCP consente contemporaneamente la trasmissione e la ricezione senza attendere un segnale di inversione come avviene nella half-duplex.

La *chiusura garbata* consiste nell'attesa del riconoscimento di tutti i dati prima di interrompere la connessione tra due host.

5.6.2. Segmento di TCP

Nella tabella 18 si mostra il tipico segmento del protocollo TCP. In parentesi si indica il numero di bit del campo relativo.

Tabella 18. - Segmento del TCP.

<table>
<tr><td colspan="5">Porta d'origine (16)</td><td colspan="5">Porta di destinazione (16)</td></tr>
<tr><td colspan="10">Numero di sequenza (32)</td></tr>
<tr><td colspan="10">Numero di riconoscimento (32)</td></tr>
<tr><td>Scosta-mento dei dati (4)</td><td>Riservato (6)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">Finestra (16)</td></tr>
<tr><td colspan="5">Checksum (16)</td><td colspan="5">Puntatore d'urgenza (16)</td></tr>
<tr><td colspan="5">Opzioni (variabile)</td><td colspan="5">Riempimento</td></tr>
<tr><td colspan="10">Dati (variabile)</td></tr>
</table>

Il segmento si compone di due parti: il campo intestazione (24 byte) e il campo dati.

I primi due campi sono la *porta d'origine* e quella di *destinazione*: essi servono per identificare i programmi applicativi dello strato superiore.

Il campo *numero di sequenza* (ISS = Initial Send Sequence = Sequenza di trasmissione iniziale) si riferisce al primo byte del campo dati e specifica la posizione del flusso di byte del modulo trasmittente.

Il *numero di riconoscimento* contiene il numero d'ordine, all'interno del file in trasmissione, del primo byte del prossimo segmento che ci si aspetta di ricevere dal TCP trasmettitore. In pratica il TCP ricevitore ha incassato e riconosciuto correttamente una quantità di byte pari a: *numero di riconoscimento* – 1.

Il campo *scostamento dei dati* contiene il numero di parole a 32 bit utilizzate per l'intestazione. In questo modo è possibile individuare il punto da cui iniziano i dati.

I sei bit, dopo il campo *Riservato*, sono dei flag utilizzati da TCP per controlli:

- URG: campo puntatore d'urgenza;
- ACK: riconoscimento;
- PSH: funzione di impilaggio (push);
- RST: connessione da reinizializzare;
- SYN: numeri di sequenza da sincronizzare;
- FIN: il mittente non ha più dati da trasmettere.

Il campo *finestra* indica quanti byte il ricevitore è disposto ad accettare.

Il campo *checksum* è il codice di controllo a 16 bit effettuato sull'intero segmento, comprendente intestazione e dati, organizzato come parole a 16 bit.

Il campo *puntatore d'urgenza* è utilizzato solo se il flag URG è settato ed indica i byte urgenti, definiti *dati fuori banda*. I dati urgenti possono essere segnali di controllo come interrupt, punti di arresto, ecc.

Il campo *opzioni* è previsto per ampliamenti futuri.

Il campo *riempimento* permette all'intestazione di essere un multiplo intero di 32.

L'ultimo campo contiene i *dati*.

5.6.3. Operazioni di gestione di TCP

Le operazioni fondamentali per una connessione gestita dal protocollo TCP consistono nelle seguenti tre fasi fondamentali:

- apertura;
- trasferimento dati;
- chiusura.

In realtà la situazione è più complessa di quanto si creda perché TCP può essere utilizzato contemporaneamente da più processi di utente per cui TCP deve conservare le informazioni riguardanti ciascun processo.

Apertura di TCP

Esaminiamo le principali operazioni che avvengono tra due TCP per realizzare l'apertura di una comunicazione facendo riferimento alla fig.42 nella quale si indica con ULP (Upper Layer Protocol) il protocollo dello strato superiore.

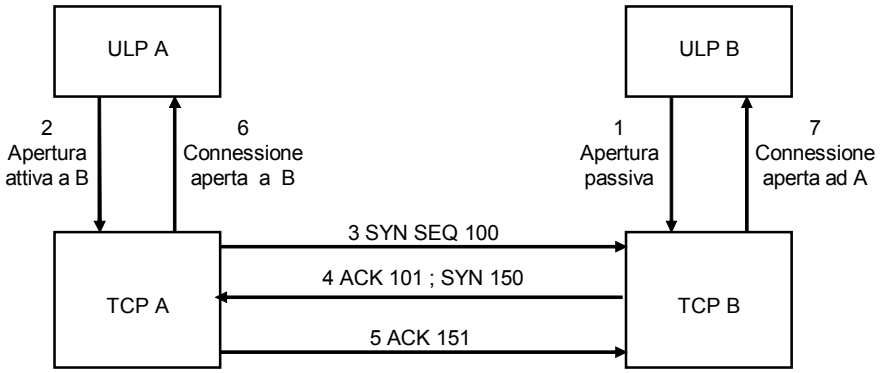


Fig. 42. - Apertura di TCP.

L'utente A invia una apertura attiva a B al suo TCP A indicata dalla freccia 2; il TCP A prepara un segmento con il flag SYN posto ad 1 che invia a TCP B, come si vede in figura dalla freccia numero 3, codificato come SYN SEQ 100. La comparsa della parola SYN significa che il relativo flag è posto ad 1 mentre il numero di sequenza ISS, indicato con SEQ 100, potrebbe avere anche un altro valore.

Il TCP B riconosce il segmento SYN e risponde settando il flag ACK col numero di sequenza 101 come indicato dalla freccia 4; inoltre trasmette il segmento SYN col numero di sequenza 150. Il TCP A riconosce il segmento SYN e risponde col segmento ACK avente numero di sequenza 151 come indicato dalla freccia 5.

Dopo queste operazioni, note come *sincronizzazione tridirezionale*, i TCP effettuano le aperture ai relativi utenti.

La freccia numero 1 indica una apertura passiva che è quella che normalmente compie un server che attende l'arrivo di una richiesta di connessione da parte di un utente remoto. Ciò consente di evitare il tempo necessario all'apertura attiva.

Trasferimento dati di TCP

Esaminiamo le principali operazioni svolte per effettuare un trasferimento dati facendo riferimento alla fig.43.

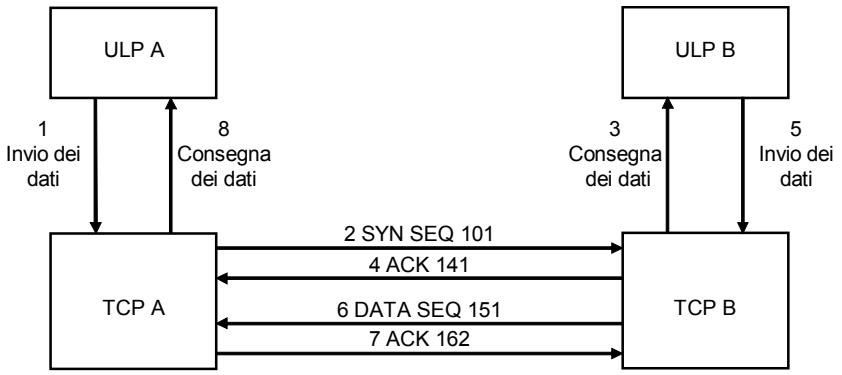


Fig. 43. - Trasferimento dati di TCP.

A titolo di esempio supponiamo che l'utente A vuole trasmettere 40 byte, a partire dal byte n.101, all'utente B e, viceversa, l'utente B desidera rispondere con un messaggio di 11 byte a partire dal byte n.151.

L'utente A, nella fase 1, invia i dati al protocollo TCP A che incapsula 40 byte in un segmento che invia a TCP B durante la successiva fase 2 con numero di sequenza 101 che identifica il primo byte dei dati da trasmettere.

I dati vengono consegnati all'utente B nella fase 3 e nella fase 4 il protocollo TCP B risponde col messaggio di riconoscimento ACK avente numero di sequenza 141. Tale numero conferma il riconoscimento dei 40 byte trasmessi durante la fase 2.

L'utente B invia dati durante la fase 5: questi vengono incapsulati da TCP B ed inviati a TCP A durante la fase 6 con numero di sequenza 151. Nella fase 7 TCP A accusa la ricevuta di 11 byte poiché risponde con ACK 162. Nella fase 8 i dati vengono consegnati all'utente A.

Chiusura di TCP

Esaminiamo le principali operazioni che avvengono tra due TCP per realizzare la chiusura di una comunicazione facendo riferimento alla fig.44.

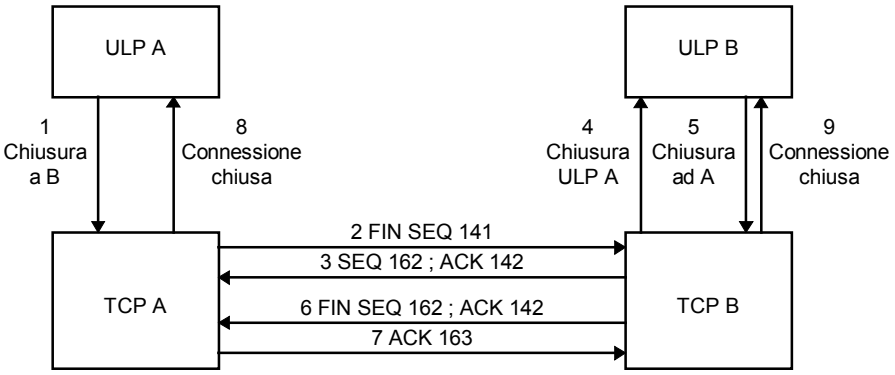


Fig. 44. - Chiusura di TCP.

Nella fase 1 l'utente A manifesta la volontà di chiudere il collegamento con l'utente B. L'effetto di ciò è l'inoltro di un segmento col flag FIN settato durante la fase 2.

Il numero di sequenza 141 è la continuazione della operazione di trasferimento dati.

Nella fase 3 il TCP B emette un segmento con numero di sequenza pari a 162 e di riconoscimento pari a 142, successivo a 141.

TCP B, nella fase 4, invia un comando di chiusura a ULP B.

Nella fase 5 ULP B riconosce e concede la chiusura ad A.

Nella fase 6 si ha il segmento finale emesso da TCP B che consiste nel flag FIN settato ad 1 e il numero di sequenza pari a 162 e di riconoscimento pari a 142.

Il TCP A riconosce questo segmento finale emettendo un numero di riconoscimento pari a 163 durante la fase 7.

Nella fase 8 TCP A chiude la connessione all'utente A e nella fase 9 TCP B chiude la connessione all'utente B.

5.6.4. Finestre di scorrimento

Il semplice meccanismo della conferma di ricezione con ritrasmissione in caso di mancata ricezione ha un grosso svantaggio. Anche se i tempi di attesa sono scelti in modo ottimale, esso causa un notevole sottoutilizzo della rete.

Infatti, indipendentemente dalla capacità della rete, i due TCP passano la maggior parte del tempo attendendo le varie conferme.

Una tecnica di ottimizzazione usata dal TCP per rendere più efficiente il trasferimento dei dati è quella delle finestre di scorrimento (sliding window).

Supponiamo che la finestra sia ampia 10 pacchetti. Si avvia, senza attendere conferme di ricezione, la trasmissione a raffica dei primi 10 pacchetti e poi si attendono le conferme di ricezione.

Quando giunge a destinazione il primo pacchetto il ricevitore accusa conferma ed il trasmettitore aggiunge un undicesimo pacchetto, poi un dodicesimo e così via. Se un

pacchetto non viene ricevuto il trasmettitore ripete l'invio e lo reinserisce nella finestra con lo stesso numero di quello che non è arrivato, tanto il destinatario può comunque riordinare i pacchetti utilizzando i numeri di sequenza.

Se si scegliesse una dimensione della finestra tale da impegnare continuamente il canale trasmissivo si sfrutterebbe al massimo la capacità dello stesso.

In pratica questo sistema divide la sequenza di pacchetti in tre fasce.

La prima è rappresentata dai pacchetti spediti e di cui si è avuta la conferma di ricezione. La seconda è formata dai pacchetti spediti ma dei quali non si sa ancora niente.

La terza è formata dai pacchetti ancora da spedire.

Con questa tecnica il TCP mantiene un timer per ogni singolo pacchetto che appartiene alla seconda fascia. Il nome "Finestra di scorrimento" deriva dal fatto che è come se ci fosse una finestra ampia quanto l'insieme di pacchetti che possono essere spediti senza attendere la conferma dell'avvenuta ricezione e che scorre in avanti un pacchetto alla volta ogni qual volta arriva una conferma.

Anche in questo caso, come in quello del tempo di attesa prima di ritrasmettere un pacchetto, le dimensioni della finestra di scorrimento rappresentano un fattore critico per determinare l'efficienza del sistema. In generale, se le dimensioni della finestra sono maggiori del tempo di attesa per il singolo pacchetto, allora la finestra continua a scorrere regolarmente senza interruzioni, salvo nel caso di ritrasmissioni, e la capacità di carico della rete viene sfruttata al massimo.

Le dimensioni della finestra di scorrimento non sono fisse ma variano nel tempo in funzione della capacità di ricezione del destinatario. Ogni conferma di ricezione che ritorna al mittente contiene una soglia di capacità (window advertisement) che contiene il numero di ulteriori ottetti che il destinatario è in grado di ricevere.

In pratica questo meccanismo permette di adattare la finestra di spedizione alle dimensioni del buffer di ricezione.

È un meccanismo di controllo del flusso dei dati che limita il numero dei dati in ingresso man mano che il buffer di ricezione si riempie fino a poter interrompere temporaneamente la trasmissione nel caso che si sia raggiunta la massima capacità di ricezione del destinatario.

Il campo finestra nella trama TCP è di 16 bit per cui la dimensione massima della finestra è di 65536byte.

Poiché la trasmissione è full-duplex si devono considerare due finestre di scorrimento: una per i dati in ricezione ed una per quelli in trasmissione. I due protocolli TCP dei due host che scambiano dati dovranno tener conto sia dei contatori della finestra in ricezione che di quella in trasmissione.

Per trasmissioni velocissime il limite della finestra ampia non più di 64Kbyte è un serio problema. Infatti nel caso di trasmissioni satellitari il tempo di attesa di ACK è dell'ordine di 200-300ms e l'intera finestra è stata ricevuta in un tempo assai inferiore. Il mittente resta inattivo per oltre l'80-90% del tempo. Una finestra più lunga consentirebbe al trasmettitore di inviare più dati aumentando l'efficienza del canale di comunicazione. La RFC 1323 consente di utilizzare, nella trama TCP, il campo *opzioni* nel quale definire il campo *windows scale* che permette di negoziare un fattore di scala che consente di definire la larghezza della finestra di scorrimento fino ad un massimo di 2^{32} byte.

5.6.5. Tabella delle connessioni TCP

La tabella delle connessioni TCP fornisce informazioni relative alle connessioni TCP esistenti. Di ogni connessione vengono fornite le seguenti informazioni:

- Stato della connessione (chiusa, in ascolto, in attesa di FIN, ecc.);
- Indirizzo locale: contiene l'indirizzo IP locale di ciascuna connessione TCP; nello stato di ascolto questo valore è 0.0.0.0;
- Porta locale: contiene il numero della porta locale di ciascuna connessione TCP;
- Indirizzo remoto: contiene l'indirizzo IP remoto di ciascuna connessione TCP;
- Porta remota: contiene il numero della porta remota di ciascuna connessione TCP.

Tabella 19. – Tabella delle connessioni TCP

	Stato della connessione	Indirizzo locale	Porta locale	Indirizzo remoto	Porta remota
Connessione 1					
Connessione 2					
Connessione 3					
Connessione n					

5.6.6. Numero di porte

Quando il protocollo TCP crea una connessione identifica una coppia di punti di accesso definita *socket*.

I due elementi del socket sono *l'indirizzo IP* ed il numero di *porta*.

Quest'ultimo è un campo numerico lungo 16 bit e corrisponde, per analogia, ad un indirizzo di I/O del computer. È possibile definire un numero di porte fino a 65536 (2^{16}).

Le porte riservate ai servizi standard hanno una numerazione inferiore a 256.

Si riportano nella seguente tabella 20 i numeri di porte relativi ai più importanti servizi internet. Maggiori informazioni sono reperibili sul sito:
http://www.faqs.org/rfcs/rfc1060.html

Tabella 20

Numero di porta	Servizio
7	Echo
20	FTP (dati)
21	FTP (controlli)
23	Telnet
25	SMTP
80	HTTP
110	POP3
119	NNTP

5.7. Protocollo UDP

Il Protocollo UDP (User Datagram Protocol) è classificato come protocollo senza connessione. La documentazione è disponibile nella RFC768 sul sito http://www.faqs.org/rfcs/rfc768.html

Talvolta UDP sostituisce TCP quando i servizi di quest'ultimo non sono necessari.

Questo accade per i protocolli dello strato superiore di trasferimento file triviale TFTP (Trivial File Tranfer Protocol), il protocollo semplice per la gestione di rete SNMP (Simple Network Management Protocol) e la chiamata di procedure remote RPC (Remote Procedure Call).

UDP non possiede funzioni di sicurezza, controllo di flusso e correzione di errori ma cura sostanzialmente la ricetrasmissione di dati IP come multiplatore/demultiplatore.

Si riporta nella tabella 21 il formato di un datagramma UDP. In parentesi si indica il numero di bit del campo in esame.

Tabella 21. - Formato del datagrama UDP.

Porta di origine (16)	Porta di destinazione (16)
Lunghezza (16)	Checksum (16)
Dati (variabile)	

Il numero inserito nel campo porta di origine specifica la porta del processo applicativo emittente; quello inserito nel campo porta di destinazione individua il processo ricevente sulla macchina di destinazione; la lunghezza si riferisce al datagramma che, comunque non può essere inferiore a 8.

Il campo checksum, facoltativo, effettua il controllo degli errori di trasmissione.

5.8. Considerazioni finali

Nei precedenti paragrafi sono stati descritti i protocolli più importanti dello stack TCP/IP.

Esistono numerosi altri protocolli, ognuno dei quali abilitato a svolgere specifiche funzioni quali, ad esempio: protocolli per la scoperta del percorso, dello strato delle applicazioni (TELNET, FTP, SMTP, POP3, HTTP) e protocolli vari come PPP, NTP, Finger, Ping, BOOTP, NFS.

Questionari

Quesiti a risposta singola
Rispondere a ciascuna domanda in 10 righi al massimo.

1. Descrivi il funzionamento della tecnica di accesso a contesa CSMA (Carrier Sense Multiple Access)

2. Il MAC (Media Access Control) address della scheda di rete.

3. Descrivi i campi del pacchetto Ethernet.

4. Descrivi le principali caratteristiche della rete locale Fast Ethernet.

5. Descrivi le principali caratteristiche della rete locale Gigabit Ethernet.

6. Descrivi le principali caratteristiche delle reti locali wireless IEEE802.11.

7. Accorgimenti per elevare il grado di sicurezza delle reti wireless.

8. Principio di funzionamento di almeno uno dei seguenti sistemi di comunicazione wireless: FHSS, DSSS, OFDM.

9. Descrivi le principali caratteristiche della tecnologia Bluetooth.

10. La costituzione del pacchetto dati di una piconet in tecnologia Bluetooth.

11. Descrizione dei blocchi costitutivi di una unità Bluetooth.

12. Descrivi il principio di funzionamento della trasmissione dati a commutazione di pacchetto.

13. Descrivi la costituzione di un indirizzo IP e la suddivisione in classi.

14. Descrivi gli indirizzi IP privati utilizzabili nelle reti locali.

15. Maschera di sottorete (Subnet mask) per la suddivisione di una LAN in sottoreti.

16. Il DNS (Domain Name System) per l'individuazione mnemonica di un indirizzo IP.

17. Descrivi le principali caratteristiche del protocollo IP (Internet Protocol).

18. Utilizzo della funzione PING per la verifica della disponibilità del collegamento di un dispositivo con indirizzo IP.

19. Descrivi le principali caratteristiche del protocollo TCP (Transmission Control Protocol).

20. Finestre di scorrimento: tecnica utilizzata dal TCP per rendere più efficiente il trasferimento dei dati.

Quesiti a risposta vero/falso

Barrare la casella relativa alla risposta che si ritiene esatta.

1. [V] [F] La rete geografica interconnette sistemi distanti anche migliaia di chilometri.

2. [V] [F] Il doppino intrecciato non consente velocità di trasmissione superiore a 100Mbps.

3. [V] [F] In una rete a stella il centro stella può essere uno switch.

4. [V] [F] La circolazione del token avviene in una rete a BUS.

5. [V] [F] Nella tecnica di accesso a contesa CSMA, se il canale è occupato, si aspetta che esso si liberi prima di trasmettere.

6. [V] [F] Il livello di linea del modello OSI corrisponde ai livelli LLC e MAC delle reti locali CSMA/CD.

7. [V] [F] Il MAC address è un indirizzo univoco della scheda di rete costituito da 6 byte.

8. [V] [F] Le reti locali Ethernet sono standardizzate dall'IEEE con la sigla 802.11.

9. [V] [F] Il campo dati del pacchetto Ethernet non può superare i 2500byte.

10. [V] [F] Il thin Ethernet utilizza cavi coassiali RG58.

11. [V] [F] La massima velocità consentita dalla Fast Ethernet è 100Mbps.

12. [V] [F] Nella Fast Ethernet è possibile utilizzare cavo UTP (Unshielded twisted Pair) di cat.4 o superiore.

13. [V] [F] Nella Fast Ethernet 100Base-TX la lunghezza massima di un collegamento è 100m. ed il diametro massimo della rete è 205m.

14. [V] [F] La tecnologia Fast Ethernet 100Base-FX utilizza la codifica FDDI 4B5B MLT-3.

15. [V] [F] L'utilizzo dello switch nella Fast Ethernet consente il full-duplex e la scomparsa delle collisioni.

16. [V] [F] Gli apparati di rete della Gigabit Ethernet funzionano a 1GBps ma non sono compatibili verso il basso.

17. [V] [F] Lo standard 10 Gigabit Ethernet utilizza esclusivamente una coppia di fibre ottiche.

18. V F La rete wireless che segue lo standard IEEE 802.11b è denominata wi-fi.

19. V F La rete wireless IEEE 802.11g può funzionare fino a 11Mbps.

20. V F La rete wireless host-to-host non prevede l'utilizzo dell'access point.

21. V F L'access point, se collegato alla rete cablata, funge da bridge.

22. V F Le reti wireless utilizzano il sistema WEP di crittografia.

23. V F La tipica frequenza portante del wireless 802.11 vale 54GHz.

24. V F Uno dei principali sistemi di comunicazione wireless è OTDM (Orthogonal Time Division Multiplexing).

25. V F Le reti senza fili Bluetooth sono denominate micronet.

26. V F La frequenza portante del sistema Bluetooth è di 2.4GHz.

27. V F Nella tecnica a datagramma i pacchetti possono transitare nella rete seguendo un tragitti diversi.

28. V F I livelli del TCP/IP sono gli stessi del modello ISO/OSI.

29. V F Un indirizzo IPV6 è costituito da 48 bit.

30. V F Gli indirizzi di classe C sono utilizzati da reti di grandi dimensioni.

31. V F L'indirizzo IP 10.50.100.1 appartiene ad una rete locale e non può essere utilizzato in internet.

32. V F L'indirizzo mnemonico http://127.0.0.0 equivale all'indirizzo di localhost http://localhost.

33. V F La subnet mask 255.255.255.224 individua 8 sottoreti di cui solo 4 utilizzabili.

34. V F Il protocollo IPV6 utilizza 128 bit per l'indirizzamento IP.

35. V F Il coordinamento del DNS è affidato all'ICANN.

36. V F Il protocollo ARP (Address Resolution Protocol) consente di determinare l'indirizzo IP del destinatario noto il suo MAC address.

37. V F Il protocollo IP prevede la correzione degli errori mediante il checksum.

38. V F Quando un datagramma IP attraversa un router il campo TTL (Time To Live) viene decrementato di 1.

39. [V] [F] Il comando PING 127.0.0.1 permette di controllare se la scheda di rete montata sul proprio computer funziona correttamente.

40. [V] [F] TCP è un protocollo orientato alla connessione.