

## Appendice A - Protocolli

### Introduzione

Affinché una comunicazione tra computer avvenga con successo, questi devono sottostare ad un insieme di regole che ne governano il traffico. Tale insieme di regole prende il nome di **protocollo**.

Poiché l'atto di inviare dati, come spedire un'e-mail, comporta un considerevole numero di azioni da compiere, un comitato di standardizzazione — chiamato International Organization for Standardization (ISO) — ha emesso un elenco di queste funzioni, e le ha suddivise in sette categorie. A tali categorie ci si riferisce comunemente con il nome di modello Open Systems Interconnection (OSI). Il modello OSI rappresenta tutto ciò che deve accadere affinché possano essere inviati (e ricevuti) dei dati. Esso non indica *come* le azioni debbano essere intraprese, ma soltanto *cosa* debba essere fatto (Figura 1).

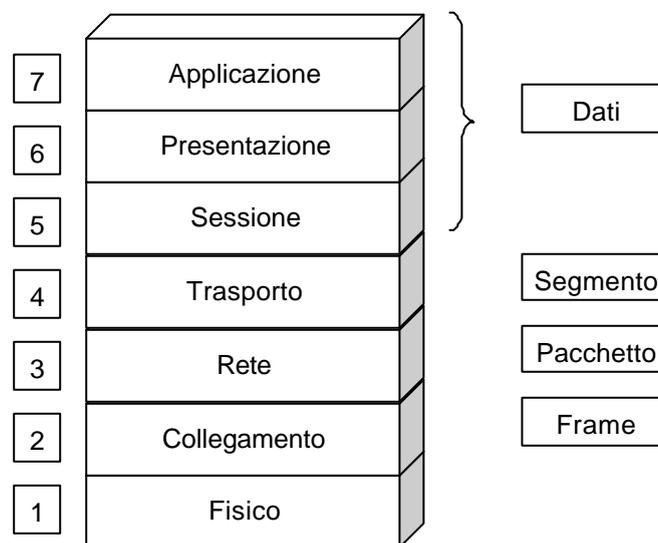


Figura 1 — Ciascuno dei sette livelli del modello OSI rappresenta una funzione necessaria alla comunicazione tra dispositivi

Ognuna delle funzioni sopra indicate verrà realizzata dai venditori con modalità differenti. Per esempio, esistono differenti mezzi fisici (cavi): il rame e la fibra ottica ne rappresentano due tra i più comuni.

Quando i dati sono spediti attraverso le funzioni di ciascuno dei livelli OSI, alcune informazioni vengono aggiunte ad essi per permettere ai dati di fluire attraverso la rete. Si dice che i dati sono *incapsulati* in tali informazioni (contenenti, tra l'altro, indirizzi e controllo di errore).

Al livello 4 (Trasporto), i dati sono incapsulati in un *segmento*.

Al livello 3 (Rete), il segmento è incapsulato in un *pacchetto* o *datagramma*. A tale livello si fa uso dei protocolli di instradamento (*routed protocol*) per inviare i dati attraverso la rete. Esistono diversi tipi di pacchetto a seconda del tipo di protocollo di instradamento: esempi includono pacchetti IP e IPX.

Al livello 2 (Collegamento) il pacchetto è incapsulato in un *frame*. Esistono diversi tipi di frame a seconda del tipo di LAN o WAN. Per esempio, i frame utilizzati da una Ethernet sono diversi da quelli utilizzati da una rete Frame Relay, poiché sono differenti i protocolli a cui obbedire.

Al livello 1 (Fisico), il frame è spedito sul cavo, in bit.

Quando i dati sono ricevuti dall'altro capo della rete, le informazioni aggiuntive devono essere rimosse. I dati vengono così spaccettati fino a quando l'informazione originale non giunge a destinazione.

### **Protocolli LAN**

Una *Local Area Network* (LAN) tipicamente presenta le seguenti caratteristiche:

- Interconnette dispositivi su brevi distanze
- È veloce
- Appartiene a te
- È presente in ogni momento

Esistono numerose tecnologie LAN. La tecnologia Ethernet è la più comune. Ethernet trasporta dati a 10 milioni di bit per secondo (Mbps). Le

nuove versioni, note con i nomi di Fast Ethernet e Gigabit Ethernet, trasportano dati rispettivamente a 100 Mbps e 1 Gbps.

Altre tecnologie LAN includono Token Ring e FDDI. Token Ring è un'invenzione IBM e la si trova prevalentemente nei siti IBM. L'FDDI sfrutta la fibra ottica ed ha una velocità di 100 Mbps.

I protocolli LAN lavorano ai 2 livelli più bassi del modello OSI: il livello fisico e quello di collegamento.

### **Accesso fisico alla LAN**

I protocolli LAN tipicamente utilizzano due metodi per accedere al mezzo fisico:

- Nello schema *CSMA/CD* (*Carrier Sense Multiple Access/Collision Detection*), i dispositivi di rete si contendono l'uso del mezzo fisico. Esempi di LAN che fanno uso di tale schema di accesso sono le reti Ethernet/IEEE 802.3
- Nello schema *Token Passing Media Access*, i dispositivi accedono al mezzo fisico in base al possesso di un "testimone" (*token*). Esempi di LAN che fanno uso di tale schema di accesso sono le reti Token Ring/IEEE 802.5 e quelle FDDI.

### **LAN e tipo di trasmissione dati**

Le modalità con cui i dati possono essere trasmessi su una LAN possono essere così schematizzate:

- In una trasmissione di tipo *unicast*, un singolo pacchetto è spedito sulla rete da una sorgente ad una destinazione. Il nodo sorgente instrada il pacchetto utilizzando l'indirizzo del nodo destinazione. Il pacchetto è spedito sulla rete, e questa lo trasporta a destinazione.
- In una trasmissione di tipo *multicast*, un singolo pacchetto dati viene copiato e spedito ad uno specifico sottoinsieme di nodi della rete. Il nodo sorgente instrada il pacchetto utilizzando un indirizzo multicast. Il pacchetto è quindi spedito sulla rete che ne fa varie

copie e le inoltra a ciascuno dei nodi che fanno parte dell'indirizzo multicast.

- In una trasmissione di tipo *broadcast*, un singolo pacchetto dati viene copiato e spedito a tutti i nodi della rete. In tale tipo di trasmissione il nodo sorgente instrada il pacchetto utilizzando l'indirizzo broadcast. Il pacchetto è quindi spedito sulla rete che ne fa varie copie e le inoltra a ciascuno dei nodi che costituiscono la rete.

### **Protocolli WAN**

Una *Wide Area Network* (WAN) interconnette dispositivi situati in zone geograficamente distinte.

Una WAN tipicamente:

- Interconnette dispositivi posti a grande distanza
- È lenta (in confronto ad una LAN)
- Appartiene a qualcun altro (il "*Service Provider*")
- È presente soltanto quando si desidera spedire qualcosa
- 

I protocolli LAN lavorano ai 2 livelli più bassi del modello OSI: il livello fisico e quello di collegamento (ad eccezione del protocollo X.25, che lavora anche al livello 3).

### **Categorie di WAN**

Le WAN possono essere raggruppate nelle seguenti categorie:

- **Collegamento punto–punto:** il percorso di comunicazione WAN tra l'edificio del cliente e la rete di destinazione è unico e prestabilito. Esso si appoggia ad una rete portante, come quella fornita da una compagnia telefonica. Un collegamento punto–punto è detto anche *linea dedicata* poiché il percorso stabilito è permanente indipendentemente da quale rete remota si debba raggiungere attraverso la rete portante.
- **Commutazione di circuito:** è un metodo di commutazione WAN nel quale, per ogni sessione di comunicazione, viene creata,

mantenuta e terminata una connessione fisica dedicata attraverso una rete portante. Usata intensivamente nelle reti delle compagnie telefoniche, la commutazione di circuito opera in maniera molto simile ad una normale chiamata telefonica. L'*Integrated Services Digital Network* (ISDN) è un esempio di tecnologia WAN a commutazione di circuito.

- **Commutazione di pacchetto:** è un metodo di commutazione WAN nel quale i dispositivi di rete, per trasportare pacchetti da una sorgente ad una destinazione, condividono un unico collegamento punto-punto che poggia una rete portante. Per consentire ai vari dispositivi di condividere tale collegamento si utilizzano tecniche di multiplexing statistico. Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Service (SMDS) e X.25 sono esempi di tecnologie WAN a commutazione di pacchetto.

### ***Le suite di protocolli***

Esistono molte *suite* di protocolli che definiscono i protocolli corrispondenti alle funzioni definite dal modello OSI. Le suite sono così chiamate perché al loro interno contengono i protocolli necessari allo svolgimento di molti e differenti compiti. Le suite di protocolli prendono anche il nome di *stack* di protocolli.

Questo capitolo fornisce cenni su alcuni di questi stack.

### ***Lo stack TCP/IP***

Il TCP/IP è lo stack di protocolli di gran lunga più usato; è l'unico utilizzato in Internet. TCP/IP è l'acronimo di Transmission Control Protocol/Internet Protocol: questi sono due dei protocolli presenti nello stack. Non è stato inventato da un singolo venditore, e si è evoluto con l'espandersi di Internet.

### ***Il livello di rete TCP/IP***

Il livello di rete (livello 3) include i seguenti protocolli:

- **Internet Protocol (IP):** definisce un insieme di regole per comunicare attraverso una rete. L'IP contiene informazioni di

indirizzamento e di controllo. La consegna dei datagrammi da sorgente a destinazione avviene in modalità *connectionless*<sup>159</sup>.

- **Address resolution Protocol (ARP)**
- **Reverse Address resolution Protocol (RARP)**
- **Internet Control Message Protocol (ICMP)**: utilizzato per segnalare al nodo sorgente errori e altre informazioni riguardanti l'elaborazione del pacchetto IP

### ***Il livello di trasporto TCP/IP***

Al livello di trasporto (livello 4), sono definiti due protocolli:

- **Transmission Control Protocol (TCP)**: fornisce, in ambiente IP, una trasmissione dati *end-to-end*, affidabile e di tipo *connection-oriented*<sup>160</sup>. Lo stabilimento della connessione avviene attraverso l'utilizzo di messaggi di segnalazione, che portano alla sincronizzazione di mittente e destinatario, in modo che il flusso dati tra sorgente e destinazione abbia luogo soltanto una volta che la sessione di trasferimento sia stata stabilita.
- **User Datagram Protocol (UDP)**: protocollo di tipo *connectionless*, funge essenzialmente da interfaccia tra l'IP e i processi di livello superiore. Diversamente dal TCP, l'UDP non aggiunge alcuna caratteristica di affidabilità, controllo di flusso, e controllo di errore al protocollo IP. A causa della sua semplicità, l'UDP necessita di meno banda del TCP.

TCP e UDP utilizzano **porte di protocollo** per distinguere differenti applicazioni in esecuzione su un singolo dispositivo. Esempi di numeri standard di porte protocollo includono i seguenti:

- **File Transfer Protocol (FTP)**: TCP, porte 20 (dati) e 21 (controllo)
- **Telnet**: TCP, porta 23

---

<sup>159</sup> Trasferimento dati che avviene senza l'esistenza di un circuito virtuale, cioè di un circuito logico creato per garantire la comunicazione affidabile tra due dispositivi di rete.

<sup>160</sup> Trasferimento dati che richiede l'esistenza di un circuito virtuale

- **Trivial File Transfer Protocol (TFTP):** UDP, porta 69

### ***Il livello di applicazione TCP/IP***

Nello stack TCP/IP i tre livelli più alti del modello OSI sono uniti insieme in un unico livello, chiamato il livello applicazione. Lo stack TCP/IP include molti protocolli di livello applicazione che rappresentano un'ampia varietà di applicazioni, inclusi i seguenti:

- File Transfer Protocol (FTP) e Trivial File Transfer Protocol (TFTP): muovono dati tra dispositivi
- Simple Network Management Protocol (SNMP): segnala anomalie nel funzionamento della rete e imposta valori di soglia oltre i quali generare uno stato di allarme
- Telnet: protocollo di emulazione terminale
- Simple Mail Transfer Protocol (SMTP): fornisce servizi di posta elettronica
- Domain Name System (DNS): traduce i nomi dei nodi di rete in indirizzi di rete

### ***Lo stack NetWare***

NetWare è un sistema operativo di rete che fornisce accesso remoto a file e numerosi altri servizi di rete distribuiti, inclusi la condivisione di stampanti e il supporto per varie applicazioni, come la posta elettronica e l'accesso a database.

Introdotta nei primi anni '80, NetWare è stata sviluppata da Novell. Deriva dallo Xerox Network Systems (XNS), creato dalla Xerox Corporation alla fine degli anni '70, ed è basato su un'architettura client-server.

L'**Internetwork Packet Exchange (IPX)** è il protocollo originale di livello rete (livello 3) di NetWare, utilizzato per instradare pacchetti attraverso una rete. Basato su datagramma, IPX è un protocollo di tipo connectionless ed è, dunque, simile al protocollo IP presente nelle reti TCP/IP.

Il **Sequenced Packet Exchange (SPX)** è il più comune protocollo di livello trasporto di NetWare. L'SPX è un protocollo affidabile, di tipo connection-oriented, che supplementa il servizio di datagramma fornito dall'IPX.

### ***Lo stack AppleTalk***

L'AppleTalk, uno stack di protocolli sviluppato dall'Apple Computer nei primi anni '80, è stato sviluppato in concomitanza con i computer Macintosh. Lo scopo dell'AppleTalk è quello di consentire a più utenti di condividere risorse, come file e stampanti.

L'AppleTalk è stato disegnato con un'interfaccia di rete "trasparente". In questo senso, l'interazione tra computer client e server di rete richiede poca interazione da parte dell'utente. Inoltre, le operazioni dei protocolli AppleTalk sono invisibili all'utente, che vede solo il risultato di tali operazioni.

Esistono 4 principali implementazioni di accesso al mezzo fisico nella suite AppleTalk: EtherTalk, LocalTalk, TokenTalk e FDDITalk. Queste implementazioni di livello due (livello collegamento) eseguono la trasformazione degli indirizzi ed altre funzioni che permettono ai protocolli proprietari AppleTalk di comunicare su interfacce a standard industriale, che includono l'IEEE 802.3 (usando l'EtherTalk), il TokenRing/IEEE 802.5 (usando il TokenTalk), e l'FDDI (usando l'FDDITalk). Inoltre, l'AppleTalk implementa un'interfaccia di rete proprietaria, nota come LocalTalk.

## Appendice B – Modalità di interconnessione

### *Wired (Fibra ottica, UTP/STP 10/100/1000 Mbps)*

La gran parte delle reti è oggi giorno connessa da cavi; questi costituiscono il mezzo trasmissivo che trasporta il segnale tra computer. Esiste una gran varietà di cavi per soddisfare le diverse necessità e dimensioni delle reti, dalle più piccole alle più estese.

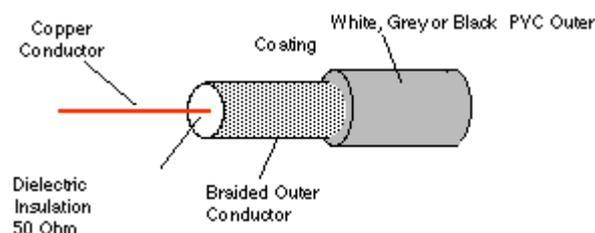
Fortunatamente, nonostante i cataloghi dei produttori elenchino migliaia di tipi di cavi, questi possono essere raggruppati in tre grandi categorie:

- Cavi coassiali
- Cavi *Twisted-Pair* (a coppia ritorta)
- Cavi in fibra ottica

### ***Cavi coassiali***

Un tempo, i cavi coassiali costituivano il tipo di cavo più diffuso. Il motivo della loro popolarità risiedeva nel fatto che essi erano un mezzo leggero, flessibile, facile da utilizzare e relativamente economico.

Nella sua forma più semplice, il cavo coassiale è costituito da un conduttore centrale (solitamente in rame) circondato da un separatore di materiale isolante, a sua volta circondato da un conduttore tubolare. Il tutto è quindi ricoperto da uno strato esterno, protettivo ed isolante.



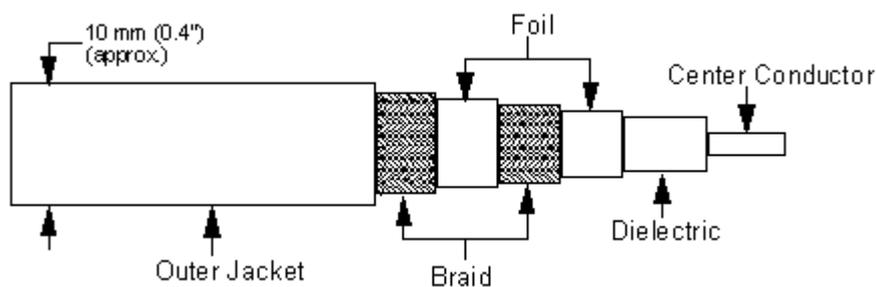
*Figura 1 – Cavo coassiale*

Esistono due tipi di cavi coassiali:

- Thick (thicknet)
- Thin (thinnet)

### **Thicknet**

Thicknet è il cavo coassiale "thick" (spesso) utilizzato nelle reti Ethernet di tipo 10Base5. Il 10Base5 è il sistema originale Ethernet che supporta una trasmissione di 10 Mbps su un segmento di lunghezza massima pari a 500 metri.



*Figura 2 – Cavo coassiale Thicknet*

### **Thinnet**

Thinnet è il cavo coassiale "thin" (sottile) utilizzato nelle reti Ethernet di tipo 10Base2. Il 10Base2, sistema Ethernet noto anche con il nome di "Thin Ethernet", supporta una trasmissione di 10 Mbps su un segmento di lunghezza massima pari a 185 metri.

Il cavo thinnet ha il vantaggio di essere più economico, più leggero, più flessibile e più facile da installare del thicknet usato nell'Ethernet 10Base5. Tuttavia, il thinnet presenta lo svantaggio di avere caratteristiche trasmissive peggiori, di supportare segmenti lunghi al massimo 185 metri, con un massimo di 30 stazioni per segmento (contro le 100 del 10Base5).

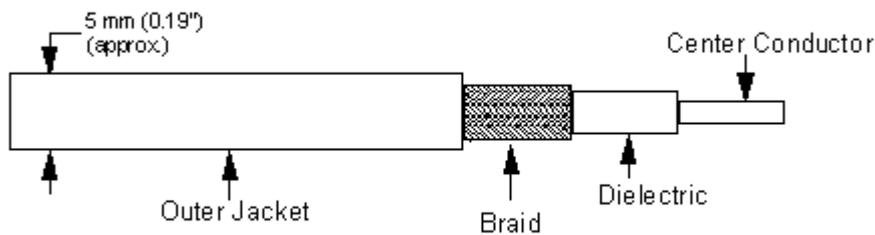


Figura 3 – Cavo coassiale Thinnet

### Connettori per cavi coassiali

Sia thinnet che thicknet utilizzano, per collegare cavi e computer, componenti di connessione chiamati BNC (British Naval Connector).

I molti componenti della famiglia BNC sono indicati in Figura .

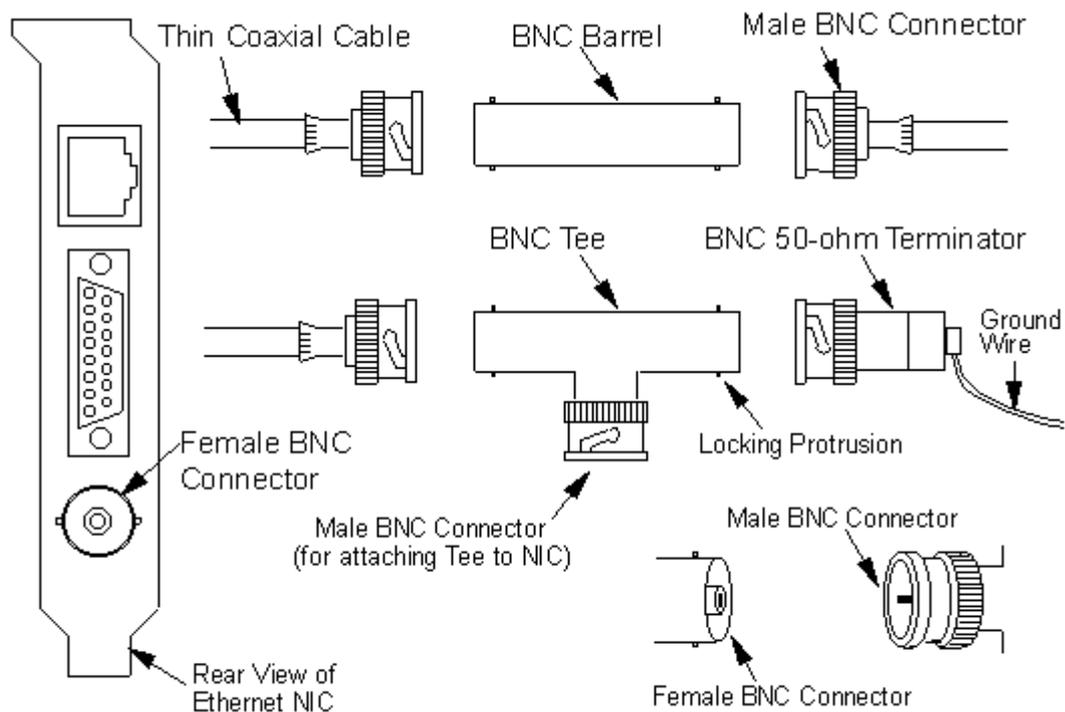


Figura 4 – I componenti della famiglia BNC

### Cavi twisted-pair

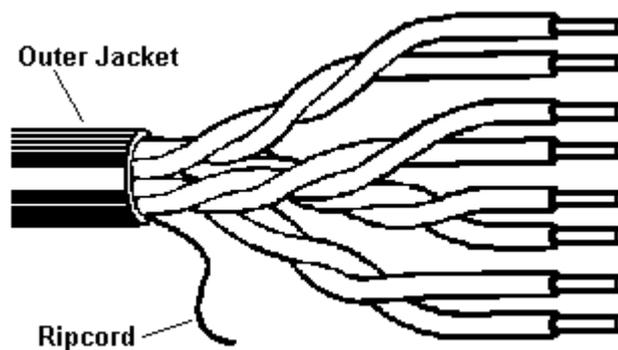
Nella sua forma più semplice, il cavo twisted-pair è costituito da due conduttori di rame isolati avvolti l'uno attorno all'altro. Questa caratteristica aiuta ad aumentare l'immunità del cavo ai disturbi elettrici.

Esistono 3 categorie di cavi twisted-pair:

- UTP (*Unshielded Twisted Pair*)
- ScTP (*Screened Twisted Pair*)
- STP (*Shielded Twisted Pair*)

### **Cavi UTP**

Come implica il nome stesso (Unshielded Twisted Pair si traduce con coppia ritorta senza schermo), il cavo UTP non presenta alcuno schermo. Nelle applicazioni di rete, il termine UTP generalmente si riferisce ai cavi con impedenza 100 Ohm di categoria 3, 4, 5, 5e, 6 e 7.



*Figura 5 – Il cavo UTP (4 coppie)*

Quello che segue è un riepilogo delle categorie dei cavi UTP:

<b>Categoria</b>	<b>Max frequenza di trasmissione</b>	<b>Applicazioni tipiche</b>
1	Meno di 1 MHz	Voce analogica – ISDN
2	4 MHz	Reti IBM Token Ring 4 Mbps
3	16 MHz	Voce e data su Ethernet 10BaseT
4	20 MHz	Token Ring 16 Mbps
5	100 MHz 1000 MHz (4 coppie)	Fast Ethernet Gigabit Ethernet ATM
5e	100 MHz	Fast Ethernet Gigabit Ethernet ATM
6	200–250 MHz	Fast Ethernet Gigabit Ethernet ATM Applicazioni super veloci a larga banda
7	600 MHz	Gigabit Ethernet ATM Applicazioni super veloci a larga banda

### **Connettori per cavi twisted-pair**

I cavi twisted-pair utilizzano connettori di tipo RJ-45 per connettersi ai computer. Il connettore RJ-45 è simile al connettore telefonico RJ-11; tuttavia l' RJ-45 alloggia 8 conduttori, mentre l' RJ-11 soltanto 4.

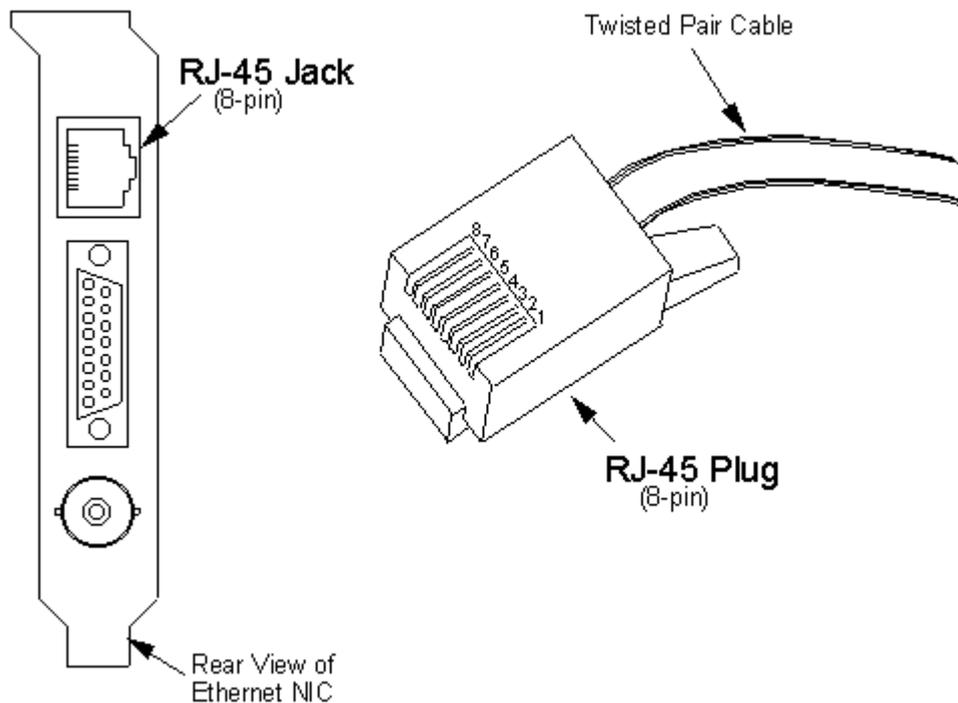


Figura 2 – Il connettore RJ-45

### **Cavi ScTP**

Il cavo Screened Twisted Pair (a coppia ritorta schermata) è formato da 4 coppie di UTP (di impedenza pari a 100 Ohm) con un singolo strato di schermatura che avvolge tutte e 4 le coppie, al fine di minimizzare le interferenze elettromagnetiche e la suscettibilità al rumore esterno.

Il cavo Screened Twisted Pair è noto anche con il nome di **FTP** (*Foiled Twisted Pair*) o **sUTP** (*Screened UTP*).

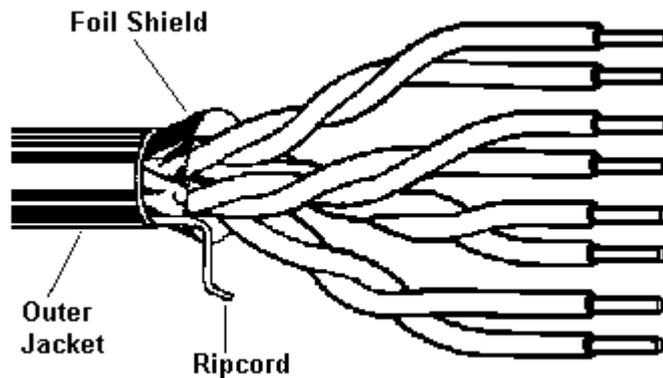


Figura 3 – Il cavo ScTP (4 coppie)

### **Cavi STP**

Sebbene il cavo Screened Twisted Pair sia tecnicamente una forma di coppia *shielded* (schermata), il termine "Shielded Twisted Pair" (STP) molto spesso si riferisce al cablaggio a coppia ritorta con impedenza di 150 Ohm definita nelle specifiche dell'IBM Cabling System, per l'utilizzo in reti di tipo Token-Ring.

Nell'STP, le coppie ritorte sono singolarmente avvolte in uno strato schermante e ulteriormente rivestite da uno schermo esterno.

L'STP 150 Ohm non è generalmente indicato per un utilizzo con reti Ethernet. Tuttavia, lo standard Ethernet fornisce una descrizione di come sia possibile, grazie all'utilizzo di speciali trasformatori chiamati "*Baluns*", adattare l'impedenza di 150 Ohm del cavo con quella di 100 Ohm dei transceiver Ethernet.

### **Cavi in fibra ottica**

Nei cavi in fibra ottica, la fibra trasporta dati numerici sotto forma di impulso modulati di luce. Questa modalità di trasporto è relativamente sicura, poiché nessun impulso elettrico è trasferito sul cavo. Ciò rende impossibile intercettare e rubare i dati trasmessi lungo il percorso, cosa non altrettanto vera per qualsiasi tipo di cavo in rame che trasporti segnali elettrici.

La fibra ottica presenta un'elevatissima capacità di trasmissione, grazie alla scarsa attenuazione del mezzo e alla purezza del segnale condotto.

Il cavo in fibra ottica è costituito da tre strati concentrici. Il nucleo è la regione centrale di una fibra ottica attraverso la quale è trasmesso il segnale luminoso. Lo strato centrale è costituito da un materiale con un indice di rifrazione più basso di quello del nucleo, il che consente di confinare nel nucleo stesso il segnale trasmesso. Lo strato esterno serve come protezione dei due strati sottostanti.

Esistono due tipi fondamentali di cavi in fibra ottica:

- Fibra Multimodale
- Fibra Unimodale

### ***Fibra Multimodale***

La fibra multimodale (*Multi-Mode Fiber* o *MMF*) consente alla luce di propagarsi lungo più percorsi (o modi) all'interno del nucleo. Il nucleo relativamente largo della MMF permette un buon accoppiamento con sorgenti di luce economiche (LED), e con accoppiatori e connettori altrettanto economici.

Le MMF più popolari sono le 62.5/125  $\mu\text{m}$ . Questi numeri indicano che il diametro del nucleo è di 62.5  $\mu\text{m}$ , mentre quello dello strato intermedio è di 125  $\mu\text{m}$ . Altre dimensioni di MMF comunemente utilizzate sono 50/125 e 100/140.

Il vantaggio principale dei cavi in fibra su quelli di tipo twisted-pair è che la fibra supporta segmenti di lunghezza maggiore. La MMF può supportare segmenti di 2000 metri per l'Ethernet 10 e 100 Mbps, e di 550 metri per l'Ethernet 1000 Mbps.

### ***Fibra Unimodale***

La fibra unimodale (*Single-Mode Fiber* o *SMF*) ha un diametro del nucleo così piccolo (dell'ordine dei 10  $\mu\text{m}$ ) che la luce può propagarsi secondo un solo modo. Questo consente di ridurre il principale fattore limitante della banda di trasmissione della fibra, la cosiddetta dispersione modale.

Tuttavia, la ristrettezza del nucleo rende difficoltoso l'accoppiamento della luce nella fibra, richiedendo l'utilizzo di sorgenti di luce (laser) molto dispendiose.

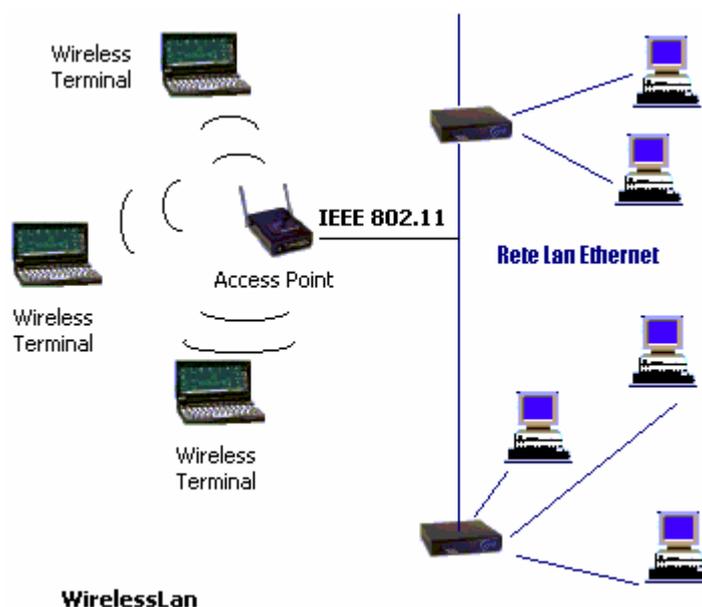
La SMF è capace di supportare segmenti di lunghezza molto superiore a quelli supportati dalla MMF: con l'utilizzo di SMF l'Ethernet 1000 Mbps può sfruttare segmenti fino a 5000 metri, ma il costo di tale tipo di cablaggio è decisamente alto.

### ***Standard IEEE 802 di riferimento***

- 802.3 (1985) Base standard (10B5)
- 802.3a (1992) 10B2 Ethernet over thin coaxial cable
- 802.3b (1985) Broadband Ethernet (using coaxial TV cable, now seldom used)
- 802.3c (1985) Improved definition of a Repeater
- 802.3d (1987) Definition of Ethernet for Fibre (10BFOIRL) (now seldom used)
- 802.3e (1987) 1Base5 or StarLAN (now seldom used)
- 802.3h (1991) Layer Management
- 802.3i (1990) 10BaseT, Ethernet over CAT-5 Unshielded Twisted Pair (UTP)
- 802.3j (1993) defines Ethernet over Fibre (10BF)
- 802.3p/q (1993) Definition of managed objects
- 802.3u (1995) Definition of Fast Ethernet (100BTX, 100BT4, 100BFX)
- 802.3x (1998) Definition of Full Duplex operation in a switched LAN
- 802.3y (1998) Definition of Fast Ethernet (100BT2 over low quality UTP)
- 802.3z Definition of Gigabit Ethernet (over Fibre)
- 802.3aa Definition of Gigabit Ethernet Maintainance
- 802.3ab Definition of Gigabit Ethernet (over UTP CAT-5)
- 802.3ac Definition of Ethernet VLANs
- 802.3ad Definition of Ethernet VLAN Trunking

### **Wireless (IEEE 802.11, Bluetooth)** [8][9][10][11][12]

Lo standard 802.11 viene pubblicato nel 1999 dell'IEEE (Institute of Electrical and Electronic Engineers)<sup>161</sup>. L'IEEE 802.11 specifica un gruppo di tecnologie che governano la connettività wireless (priva di cablaggio) Ethernet tra dispositivi client – come computer desktop, laptop e PDA (Personal Digital Assistant) – e wireless hub connessi alla rete fisica. Le wireless LAN basate su **tecnologia radio** tipicamente comprendono due componenti fondamentali: una scheda di rete di tipo wireless e un Access Point (AP).



La variante più conosciuta e maggiormente diffusa dello standard IEEE 802.11 è la IEEE 802.11b.

I prodotti conformi allo standard 802.11b sono detti "WiFi" ("Wireless Fidelity"), come deciso dalla Wireless Ethernet Compatibility Alliance<sup>162</sup>.

In condizioni ideali, i prodotti WiFi possono trasmettere e ricevere dati con velocità fino ad 11 Megabit per secondo (Mbps), in modalità *half-duplex*, con un range di copertura di circa 100 metri. Tuttavia, in condizioni tipiche, la maggioranza dei dispositivi WiFi opera a velocità comprese tra

---

<sup>161</sup> <http://www.ieee.org>

<sup>162</sup> <http://www.wi-fi.org>

gli 1 e i 5 Mbps. Ciò è dovuto in parte alla ridondanza di dati di controllo inseriti a livello fisico (overhead), e in parte al fatto che tutte le wireless LAN (WLAN) utilizzano uno spettro di frequenze non riservato, esponendo così i propri dati ad interferenze e ad errori di trasmissione. Questi errori comportano la ritrasmissione dei dati, con conseguente spreco di banda.

Lo standard IEEE 802.11a<sup>163</sup>, sviluppato successivamente, può raggiungere una velocità teorica di 54 Mbps. Esso prevede inoltre una banda di frequenza più alta (5 GHz), più larga e meno affollata della banda 2,4 GHz che lo IEEE 802.11b si trova a dover condividere con telefoni cordless, forni a microonde, e dispositivi Bluetooth. Tuttavia, l'utilizzo di frequenze diverse implica la non compatibilità dei prodotti 802.11a con gli AP 802.11b. Per superare questo ostacolo la IEEE ha sviluppato l'802.11g, che dovrebbe estendere la velocità e il range di copertura dell'802.11b, rimanendo compatibile con i vecchi sistemi. D'altra parte, problemi tecnici e politiche di mercato ne hanno rimandato la ratifica.

Per quello che riguarda l'802.11b e la sicurezza, il criptaggio della trasmissione dati – chiamato WEP (Wired Equivalent Privacy) – è stato incorporato nei prodotti WiFi, con l'obiettivo di fornire un livello di privacy equivalente a quello delle LAN cablate. Tuttavia, le difficoltà di messa in opera e la non completa invulnerabilità del sistema WEP fanno della sicurezza uno dei punti deboli dello standard 802.11b.

Oltre alla tecnologia radio, le wireless LAN possono utilizzare la **tecnologia ad infrarossi**, dove la comunicazione è trasportata da luce nella parte invisibile dello spettro. Questo sistema è utile soprattutto per comunicazioni tra dispositivi posti a distanza ravvicinata (pochi metri), con collegamento a vista (LoS, *Line of Sight*). La luce infrarossa non è in grado di penetrare alcun prodotto solido: persino il vetro della finestre è in grado di attenuare tale segnale. L'elevata larghezza di banda del segnale

---

<sup>163</sup> L'equivalente europeo dell'802.11a prende il nome di HiperLAN2, sistema sviluppato dall'ETSI (European Telecommunication Standard Institute).

infrarosso consente d'altra parte di trasmettere dati fino ad una velocità di 10 Mbps.

### ***Benefici delle wireless LAN***

- Le wireless LAN sono meno costose e meno intrusive da implementare e da mantenere delle LAN cablate.
- I wireless AP possono essere installati sul soffitto, consentendo di variare la disposizione dei client senza alcuno sforzo.
- Le risorse aziendali risultano accessibili da un qualsiasi punto nel raggio di copertura di un AP.

### ***Vulnerabilità e limiti tecnici***

Oltre ai tipici problemi cui una tecnologia relativamente nuova come quella delle wireless LAN deve andare normalmente incontro (standardizzazione, incompatibilità...), le wireless LAN possono esporre il traffico e le risorse di rete ad accessi non autorizzati. L'accesso wireless ad una rete, oltre a consentire la consultazione di dati riservati, può inoltre costituire il punto di partenza per attacchi che possono minare il funzionamento della rete intera.

I segnali radio di una wireless LAN possono estendersi ben oltre i confini fisici di un edificio, e diffondersi nelle strade, nei parcheggi, in altri edifici, rendendo disponibili dati riservati ad utenti malintenzionati che si siano "posti in ascolto".

L'estrema facilità con cui è possibile installare dispositivi WiFi in una rete esistente, potenzialmente costituisce uno stimolo per chi si senta sufficientemente esperto per aggiungere dispositivi wireless senza la preventiva approvazione del personale competente. Questo tipo di comportamento sconsiderato può causare il malfunzionamento dell'intera rete.

Pareti, colonne e altre strutture in muratura presenti all'interno dell'edificio possono ridurre la potenza del segnale tra dispositivi client e AP, limitando severamente portata e qualità di connessione.

### **Bluetooth**

Lo standard Bluetooth è stato annunciato nel 1998 dal Bluetooth Special Interest Group (SIG), un consorzio formato da Ericsson, IBM, Intel, Nokia, Toshiba, ma per il primo documento ufficiale bisogna aspettare il giugno 2002: si tratta dell'802.15.1, emesso dall'IEEE.

Nato con l'idea di soppiantare i prodotti WiFi, il Bluetooth ha presto ridimensionato le proprie ambizioni. Le attuali linee di mercato tendono a proporre Bluetooth e WLAN come due tecnologie complementari, non in competizione l'una con l'altra, anche se tuttora permangono problemi di interferenza, visto che entrambe utilizzano la banda 2,4 GHz.

La vera forza del Bluetooth risiede nelle caratteristiche che lo contraddistinguono: basso consumo, alta sicurezza, supporto integrato del traffico voce. Tali caratteristiche, unite alla bassa velocità di trasmissione dati (circa 700 Kbps) e al limitato range di copertura (circa 10 metri), rendono il Bluetooth ideale per riempire la nicchia delle PAN (Pico Area Network), o *piconet*, ridottissime reti dati che si estendono attorno ad un individuo o ad un dispositivo. Si pensi, per esempio, al rimpiazzo con dispositivi Bluetooth di porte seriali e parallele, dei cavi di connessione tra auricolare e cellulare, tra PDA e PC

L'elevata sicurezza del traffico Bluetooth è garantita dal criptaggio dei dati con un algoritmo chiamato E0, che si è rivelato maggiormente efficiente della tecnologia WEP delle WLAN, anche se non totalmente invulnerabile.

L'802.15.2, standard al quale l'IEEE sta ancora lavorando, dovrebbe adattare il Bluetooth affinché esso non utilizzi le frequenze già occupate dall'802.11b e dall'802.11g. Questo consentirebbe di far convivere nello stesso dispositivo PAN e WLAN.

## Appendice C – Elettronica di rete

### *Repeater*

Il repeater costituisce l'unità base utilizzata nelle reti per connettere segmenti separati. Accetta in ingresso un segnale contenente pacchetti dati, lo amplifica, e lo inoltra a tutte le porte.

Il repeater opera al livello 1 (fisico) del modello OSI: per questo, non ha nessuna visibilità né sui messaggi di tipo broadcast (che, se fuori controllo<sup>164</sup>, possono portare al collasso di una rete), né sul tipo di protocollo di alto livello (IP, IPX, ecc...) che lo sta attraversando.

Affinché un repeater possa funzionare, entrambi i segmenti che esso connette devono basarsi sullo stesso tipo di cablaggio, e devono utilizzare lo stesso protocollo e tecnica di trasmissione.

Una regola fondamentale che governa l'utilizzo dei repeater è la cosiddetta "Regola del 5-4-3": il percorso tra due stazioni in una rete può essere al massimo costituito da 5 segmenti con 4 repeater tra essi; di questi 5 segmenti, non più di 3 possono essere popolati.

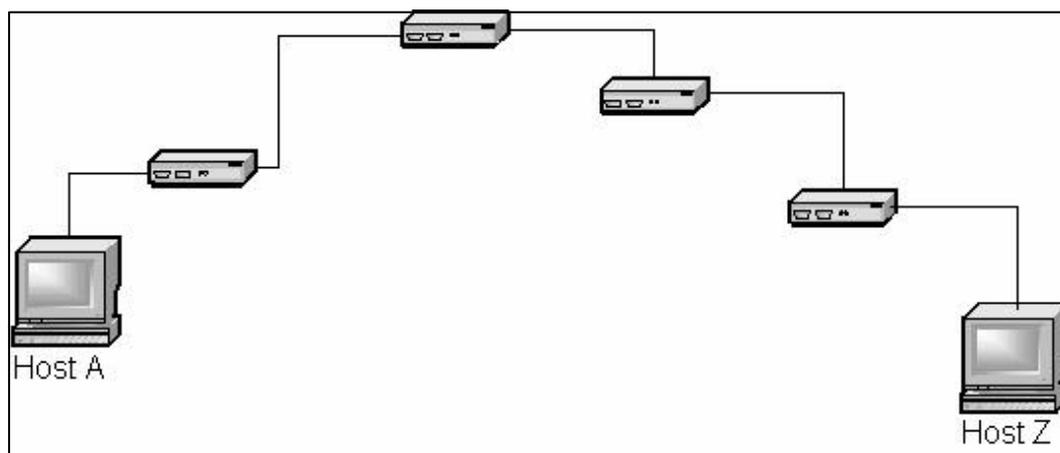


Figura 4

### *Hub*

Opera al livello fisico del modello OSI, e svolge le stesse funzioni dei repeater.

---

<sup>164</sup> Si parla in questo caso di **Broadcast Storm**

### **Bridge**

Il bridge è utilizzato per connettere segmenti separati di una rete. Differisce dal repeater in quanto il bridge è un dispositivo intelligente che opera al livello 2 (Collegamento) del modello OSI.

Il bridge impara l'indirizzo MAC di ogni nodo di ogni segmento e in quale interfaccia essi sono connessi. Per ogni frame in ingresso inoltra il frame solo se l'indirizzo MAC di destinazione è connesso ad un'altra porta o se il bridge non sa dove sia dislocato nella rete. Tuttavia, i frame in ingresso il cui indirizzo MAC appartenga allo stesso segmento dal quale provengono non sono inoltrati ad alcuna porta.

Il bridge è un dispositivo di tipo *store and forward*: memorizza l'intero frame e verifica il CRC prima di inoltrarlo. Se viene individuato un errore CRC, il frame è scartato.

Il bridge ignora il tipo di protocollo di alto livello (IP, IPX, ecc...) che lo sta attraversando, e non opera nessun controllo su messaggi di tipo broadcast.

### **Switch**

Lo switch è l'evoluzione del bridge. Utilizza particolari circuiti integrati che riducono i tempi di latenza introdotti dal bridge nella rete.

Lo switch può funzionare in modalità *cut-through*: non aspetta che l'intero frame abbia riempito il proprio buffer, ma lo inoltra non appena ne ha letto l'indirizzo MAC di destinazione. Poiché la modalità *cut-through* aumenta la probabilità che frame contenenti errori vengano propagati sulla rete, molti switch operano comunque in modalità *store and forward*.

Lo switch ha caratteristiche simili al bridge, ma ha un numero maggiore di porte ed è più veloce. Come il bridge, lavora al livello 2 del modello OSI, mantiene una tabella degli indirizzi MAC per porta e non controlla il traffico broadcast sulla rete.

### **Router**

Il router instrada i pacchetti ricevuti sulla base di criteri che operano al livello 3 (Rete) del modello OSI.

Può condividere le informazioni di instradamento e sullo stato della rete con altri router, e utilizzare queste informazioni per scartare connessioni lente o malfunzionanti.

La tabella di instradamento presente nel router contiene le seguenti informazioni:

- Tutti gli indirizzi di rete conosciuti
- Come connettersi alle altre reti
- I possibili percorsi tra i vari router
- Il "costo" associato all'inoltro dei dati su tali percorsi

Quando un router riceve un frame destinato ad una rete remota, lo inoltra al router che gestisce la rete di destinazione. Questo consente di:

- Segmentare grandi reti in reti di dimensioni ridotte
- Agire come barriera di sicurezza tra segmenti
- Impedire l'insorgere delle *Broadcast Storm*, dato che il traffico di tipo broadcast non è inoltrato.

Eseguendo operazioni complesse su ogni pacchetto, il router è generalmente più lento della maggioranza dei bridge e degli switch. Esso consente di connettere segmenti di rete che utilizzano schemi di accesso al mezzo fisico completamente differenti, come Ethernet e Token Ring.

Da notare che non tutti i protocolli possono lavorare con un router. I protocolli instradabili sono:

- DECnet
- IP
- IPX
- OSI
- XNS
- Apple Talk

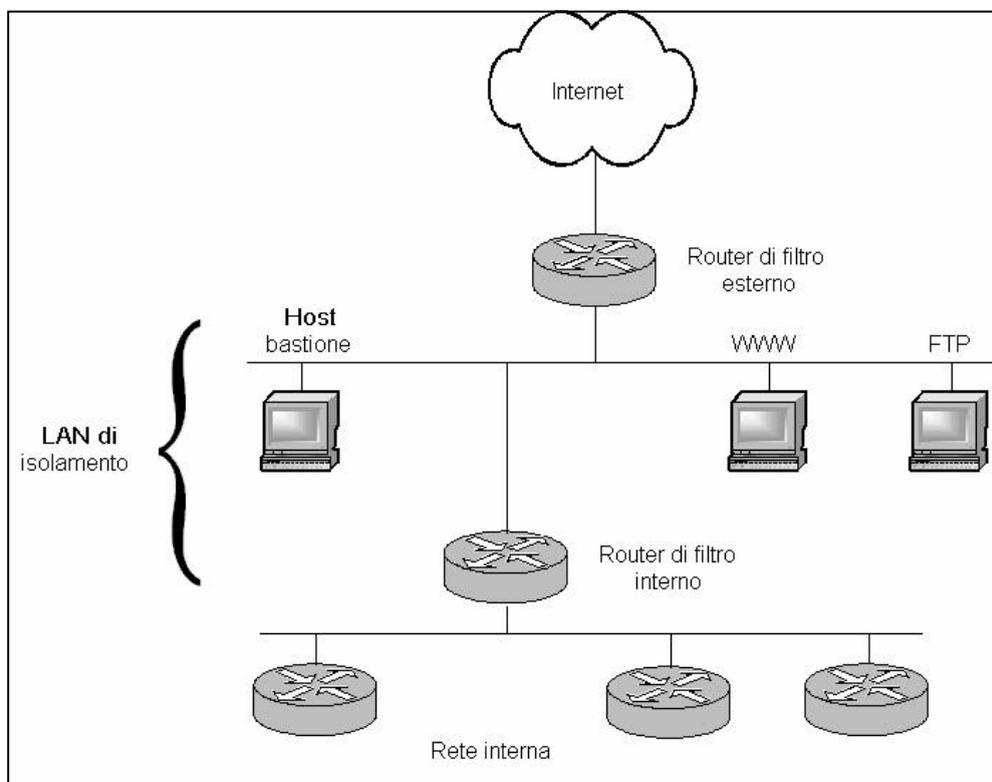
I protocolli non instradabili sono:

- LAT
- NetBEUI

### **Firewall**

Un firewall è un sistema di dispositivi e applicazioni usati per proteggere una rete da un'altra rete potenzialmente non sicura, come Internet. Tipicamente è realizzato utilizzando un progetto a 3 strati (si veda Figura 5). Sul lato esterno della rete viene posto un router di filtro, che consente l'accesso solo agli host presenti nella LAN di isolamento. Nella LAN di isolamento gli host sono installati per fornire servizi tipo Web server, DNS, FTP server, Telnet. Questo tipo di host prendono solitamente il nome di host bastione.

Il router di filtro interno permette l'accesso dalla rete interna alla rete di isolamento. È opportuno che non esistano dispositivi che comunicano direttamente tra la rete interna e il router esterno.



*Figura 5*

Quando il contesto lo richieda, si possono utilizzare dei dispositivi firewall hardware in aggiunta o in sostituzione dei router di filtro (si veda Figura 6). Tali tipi di firewall offrono maggiore sicurezza, maggiore velocità e funzionalità aggiuntive, la descrizione delle quali va oltre lo scopo del presente documento

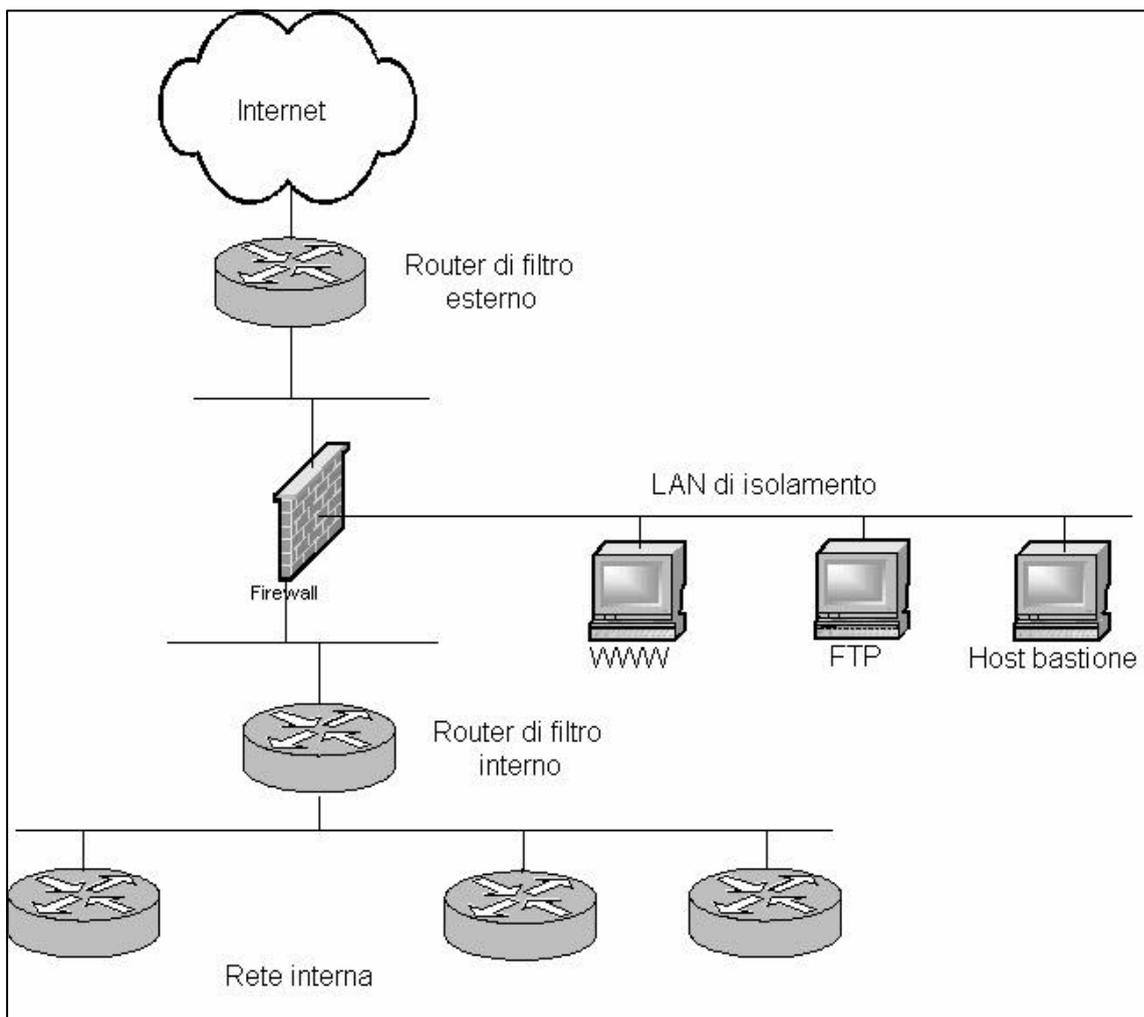


Figura 6

## Appendice D – Accesso a Internet

### **ISDN**

La linea telefonica ISDN opera a 128 Kbps e viene fornita dalle compagnie telefoniche pubbliche. L'ISDN comprende due canali da 64 Kbps (canali B) che operano separatamente, più un canale (chiamato canale D, a 16 Kbps) di servizio per i segnali di controllo. Talvolta, se si dispone di un hardware compatibile, è possibile effettuare il "bonding" (unione) dei due canali B in un unico canale da 128 Kbps. Inoltre, essendo un servizio digitale, l'ISDN non presenta la cosiddetta "interferenza di linea", che rallenta le connessioni analogiche, e garantisce prestazioni molto elevate.

I collegamenti ISDN possono essere effettuati mediante un router predisposto per ISDN o un modem ISDN e una porta seriale sul router. I router, i modem o gli adattatori terminali ISDN possono avere porte analogiche che permettono di collegare telefoni, fax, modem o altri telefoni analogici. Per esempio, un router ISDN con presa telefonica analogica permette di effettuare telefonate e inviare fax e di collegarsi contemporaneamente ad un altro canale ISDN.

Le applicazioni di ISDN sono molteplici. I vari produttori si sono ingegnati per sfruttarne le potenzialità sviluppando hardware e software "ad hoc". Alcuni servizi della rete ISDN garantiti dal gestore del servizio pubblico sono i seguenti:

- Fonia con servizi aggiuntivi, ad esempio:
  - conversazione a tre
  - conversazione intermedia
  - trasferimento di chiamata
- Servizi per monitorare i costi di traffico:
  - disabilitazione a chiave numerica
  - documentazione degli addebiti
  - telelettura del contatore di abbonato
  - indicazione di conteggio in tempo reale

- Servizi di identificazione:
  - identità della linea chiamante sul display del terminale dell'utente chiamato (presentazione e restrizione).
  - identità della linea connessa (presentazione e restrizione)
- Servizi per ottimizzare l'utilizzo della rete:
  - multinúmero: possibilità di assegnare un número diverso a ciascun terminale connesso sul bus S (massimo 8 terminali).
  - sottoindirizzamento: permette di aggiungere altre cifre al número telefonico per individuare un terminale o una specifica applicazione sullo stesso terminale (utilizzabile solo tra utenti ISDN).
  - trasportabilità del terminale. Servizi per la comunicazione intraziendale (Gruppo Chiuso d'Utente).
- Accesso ad altre reti (INTERNET, ITAPAC, RTG, ecc...)
- Videocomunicazione (videotelefonía - videoconferenza), con in più la possibilità di condivisione di ausili grafici (es. telescrittura).
- Backup di linee dedicate.
- Trasferimento file (host-PC, PC-PC, etc...).
- Accesso a banche dati e immagini con associata fonía.
- Teledidattica.
- Telesorveglianza.
- Teleassistenza.
- Telemedicina / teleconsulto.
- Impaginazione di quotidiani a distanza.
- Trasmissione rassegna stampa.
- Stereofonia.

In Italia, secondo lo standard EURO-ISDN, l'utente può collegarsi alla centrale di rete pubblica secondo due modalità:

- **accesso base**: 2 canali B a 64 Kbps + 1 canale D a 16 Kbps, per una capacità totale di 144 Kbps.
- **accesso primario**: 30 canali B a 64Kbps + 1 canale E (chiamato anch'esso D) a 64 Kbps , per una capacità totale di 1984 Kbps

## **ADSL**

ADSL è l'acronimo di Asymmetric Digital Subscriber Line. ADSL trasforma la linea telefonica tradizionale in connessioni digitali per il trasferimento dati. Dunque utilizza il vecchio doppino telefonico (due cavetti in rame arrotolati su sé stessi) per navigare in Internet a velocità 10 volte superiore a linee ISDN e 50 volte superiore a modem 56K. Per rendere possibile queste prestazioni la linea telefonica viene suddivisa in tre canali di frequenze distinte:

- **Downstream:** canale dedicato alla ricezione di dati dalla Rete, con una velocità di trasferimento massima pari a 640 Kbps.
- **Upstream:** canale dedicato alla spedizione di dati verso la Rete, con una velocità di trasferimento massima limitata a 128 Kbps
- **Trasmissione della voce:** canale dedicato alle comunicazioni telefoniche classiche via voce, che sfrutta una minima parte della banda disponibile lasciando il resto al trasferimento ADSL.

La suddivisione in canali con diversa frequenza permette, da un lato, di aumentare la velocità di collegamento, dall'altro di non occupare la linea telefonica tradizionale quando si è connessi ad Internet. In altri termini si può navigare e contemporaneamente parlare al telefono, senza per questo dover installare una nuova linea telefonica (come per ISDN). Il valore di 640 Kbps in entrata non è il limite massimo consentito dalla tecnologia DSL, che in realtà può raggiungere la velocità di 1,5 Mbps. Si tratta di un limite massimo possibile dall'attuale sistema delle telecomunicazioni nazionali, che comunque non viene garantito dai fornitori di accesso.

Nessun provider garantisce una velocità minima di upstream e downstream, ed è possibile che i 640 Kbps teorici non vengano mai raggiunti. Anzi, molti paventano il dubbio che quando il numero di utenti crescerà le prestazioni scadranno notevolmente. In effetti la velocità di connessione dipende da fattori che ADSL non può prevedere: numero di utenti connessi al provider; traffico sul server remoto; distanza fisica del modem ADSL dal provider (la propria postazione non deve superare 5 Km

dalla centrale Telecom affinché il collegamento ADSL funzioni alla perfezione)

Per trasformare la propria linea telefonica in una linea ADSL è necessario installare un modem che trasforma il segnale analogico della linea in digitale, e separa i tre canali visti in precedenza.

La connessione ADSL è permanente; questo significa che non è più necessario collegarsi ad Internet, perché in realtà si è sempre connessi attraverso un indirizzo IP assegnato dal provider. Per questo motivo ADSL elimina i costi degli scatti telefonici in favore di un canone fisso pagato al provider. Il collegamento permanente porta con sé, oltre ad evidenti vantaggi, dei seri problemi di sicurezza. Una connessione permanente è teoricamente vulnerabile ad attacchi hacker, con tutti i rischi che questo comporta. In termini pratici, ogni utente ADSL corre gli stessi rischi di un'azienda proprietaria di connessioni dedicate, con la differenza che questi spesso non possiede i mezzi tecnici ed economici per difendersi.

Affermare che ADSL rappresenta una vera e propria rivoluzione nell'accesso diffuso ad Internet non è retorica. Il collegamento permanente e super-veloce rende possibile la visione di filmati fluidi, il download di file musicali in pochi secondi; ma soprattutto trasforma il Web in uno strumento veloce da consultare e continuamente disponibile. Alla stregua di un televisore o di una radio, Internet sarà immediatamente accessibile senza il timore di vedersi recapitare bollette astronomiche.

### ***HDSL***

La DSL (x Digital Subscriber Line) è, l'insieme di tecnologie per trasmissione dati ad alta velocità, che riesce ad utilizzare, come supporto fisico, il vecchio "doppino" telefonico di rame.

Nasce negli anni ottanta negli Stati Uniti, ma solo con Internet trova la sua reale applicazione. Attualmente sono disponibili varie forme di tale tecnologia, ciascuna caratterizzata da prestazioni e caratteristiche diverse:

- **Adsl** (A sta per Asymmetric)

- **R-Adsl** (R sta per Rate adaptive), in grado di modificare in tempo reale la velocità di trasmissione per adattarla alle condizioni di traffico esistenti al momento del collegamento. Questa tecnologia consente prestazioni in velocità comprese tra 16 e 64 Kbps in un upstream e tra 1,5 e 8 Mbps in downstream.
- **Hdsl** (H sta per High bit rate), sfrutta i 4 fili delle connessioni T1/E1, dove consente un'installazione economica e prestazioni valide, le velocità raggiunte rispettivamente 1,544 e 2,048 Mbps e lavora in modo simmetrico, con la medesima banda per upstream e downstream.
- **Sdsl** (S sta per Single-line), è una versione ridotta dell'HDSL in grado di lavorare su un solo doppino, in modo simmetrico e con velocità massima di 768 Kbps per upstream e downstream.
- **Vdsl** (V sta per Very high bit-rate), a struttura asimmetrica variabile, che permetterà, in futuro, velocità comprese tra 13 e 52 Mbps in downstream e tra 1.6 e 26 Mbps in upstream, in funzione delle condizioni di traffico presenti nella rete. VDSL sarà capace di sfruttare anche mezzi diversi dai doppini, come le fibre ottiche e i cavi coassiali.
- **MDSL** (M sta per Multi-Rate), rappresenta una soluzione efficace e molto promettente, in grado di trasmettere, attraverso il normale doppino telefonico, con velocità variabili tra 272 a 1168 Kbps in upstream e downstream. A differenza dell'ADSL che, una volta installato, mantiene stabilmente fisse le due larghezze di banda, in questo caso è possibile modificarle a piacere.
- **HDSL2**, evoluzione del precedente HDSL, è in grado di lavorare anche su un solo doppino con prestazioni che offrono 1,5 Mbps di velocità in in upstream e downstream

Il vantaggio principale di questa tecnologia è la possibilità di realizzare servizi che necessitano di banda molto larga senza dover stendere nuovi cavi, risolvendo così il cosiddetto "problema dell'ultimo miglio".

L'HDSL è la miglior espressione di una tecnologia denominata xDSL (Digital Subscriber Line) che utilizza la larghezza di banda disponibile sui collegamenti diretti analogici con supporto in rame (CDA) tra utente-utente o utente-centrale.

Le linee HDSL permettono connessioni full duplex fino alla velocità di 2 Mbps su collegamenti lunghi fino a qualche chilometro con un tasso di errore comparabile a trasmissioni su fibra ottica.

Uno dei limiti alla tecnologia HDSL risulta essere la distanza tra i due estremi: la lunghezza dei collegamenti produce una attenuazione del segnale direttamente proporzionale alla lunghezza della linea.

Su distanze di 2-3Km, usando due "coppie" (una CDA a 4 fili) si raggiungono i 2 Mbps, mentre, limitandosi a 64, 128 e 256 Kbps, anche con una sola coppia si superano agevolmente i 10-12 Km. L'HDSL è caratterizzata da una connessione simmetrica, ovvero permette di scaricare dati (download) e di trasmetterli (upload) alla stessa velocità con notevoli vantaggi in termini di connettività.

Come per ogni altra tecnologia a banda larga, l'utente è permanentemente connesso ad Internet, e non ha perciò la necessità di attivare ogni volta la connessione via modem

Per rendere propria una connessione HDSL, devono essere utilizzati dei modem specifici che funzionano su circuiti dedicati a due o quattro fili caratterizzati dalla continuità elettrica della connessione tra i due estremi.

Diversamente dai modem tradizionali (che hanno un'interfaccia seriale asincrona), i modem HDSL dispongono di un'interfaccia seriale sincrona (V35 o V24); questo comporta l'impossibilità di collegarli direttamente ad un computer, e la necessità di connetterli ad un router.

A differenza di altre tecnologie, l'HDSL non consente il transito della normale fonia, (per cui risultano assenti i filtri).

## Appendice E – Standard di progettazione

### *Cablaggio strutturato*

La tabella che segue rappresenta un elenco degli standard più utilizzati nell'ambito del cablaggio strutturato.

Per ognuno di essi è riportato l'ente ratificante e la descrizione del campo di applicazione

Standard	Ente di ratificazione	Descrizione
EN50173:1995	CENELEC (europeo)	Usata per la progettazione di cablaggi strutturati.
EN50173A1:2000	CENELEC	Estende la EN50173:1995 al Gigabit e ATM155.
EN50173:2001	CENELEC	Estende la EN50173:2000 alle nuove classi E e F.
EN50174-Parte 1	CENELEC	Usata per pianificare, installare e operare sulle installazioni. Comprende aspetti relativi a: redazione di specifiche; qualità, documentazione, amministrazione, riparazione e manutenzione.
EN50174-Parte 2	CENELEC	Usata per pianificare e installare all'interno degli edifici.
EN50174-Parte 3	CENELEC	Usata per pianificare e installare all'esterno degli edifici.
568A – A5	TIA/EIA (americano)	Usata per la progettazione di cablaggi strutturati fino alla cat. 5e. Non si occupa di installazione e documentazione.
568B1 – B2	TIA/EIA	Rimpiazza le specifiche dalla 568A alla 568A5.
568B2.1	TIA/EIA	Estende la 568B2 alla cat. 6.
568B3	TIA/EIA	Specifica i requisiti per i sistemi ottici.
11801	ISO/IEC (Internazionale)	Adatta al mercato europeo le specifiche introdotte dalle TIA/EIA 568

11801:2000 (FDAM2)	ISO/IEC	Estende la 11801 alle nuove classi E e F.
-----------------------	---------	---

A titolo esemplificativo, sulla base delle normative CENELEC (in ambito europeo), si può considerare il seguente prospetto di applicazione degli standard:

Progetto	EN50173
Pianificazione	EN50174-1
	EN50174-2
	EN50174-3
Installazione	EN50174-1
	EN50174-2
	EN50174-3
Intervento	EN50174-1