

Aspetto fisico Progettazione di reti

La progettazione di una rete LAN richiede di affrontare una serie di problemi che almeno in modo generale sono stati tutti trattati nei precedenti moduli. Si va dalla scelta del mezzo trasmissivo e della tecnologia di trasmissione (*wired* o *wireless*), all'*hardware* dei calcolatori e degli apparati di rete, alla progettazione di connessioni in ambito geografico qualora la rete sia composta di più sezioni geograficamente lontane fra loro, alla scelta dei sistemi operativi, alla definizione degli utenti e delle politiche di autenticazione e autorizzazione all'uso delle risorse del sistema stesso.

In questo modulo si intende riassumere con un esplicito taglio progettuale gli aspetti fondamentali della realizzazione di una rete per applicazioni in ambito locale con particolare riferimento alla definizione della struttura della LAN sia dal punto di vista fisico sia dal punto di vista logico.

Riprenderemo dapprima gli aspetti legati alla realizzazione del sistema di cablaggio, per passare poi all'organizzazione logica di una rete a livello di implementazione tramite opportuni *hardware* di rete, introducendo il concetto di *Virtual LAN*, per poi passare all'organizzazione del sistema di indirizzamento a livello *IP* della rete stessa. Come già detto alcuni dei temi presentati sono già stati trattati in altri moduli e vengono qui ripresi in modo organico in una prospettiva progettuale.

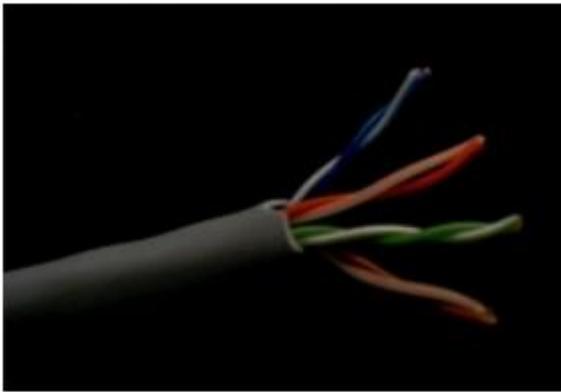
Il cablaggio strutturato - le motivazioni

Il cablaggio strutturato si offre come un moderno sistema di realizzazione delle reti concepito allo scopo di integrare, all'interno di un edificio, i vari apparati di comunicazioni: le reti di calcolatori, i terminali telefonici, gli impianti di videosorveglianza, di controllo degli accessi, per l'apertura delle porte, eccetera. Questi strumenti dispongono normalmente di proprie e separate linee di collegamento. Il cablaggio strutturato si propone di superare questa distinzione (che comporta costose ed inutili ripetizioni dei cablaggi), allo scopo di utilizzare un supporto fisico comune per tutti questi dispositivi.

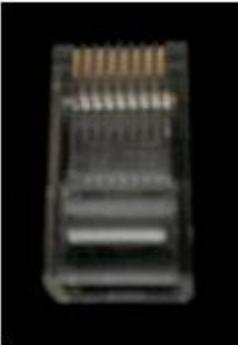
In contesti caratterizzati da possibili modifiche o ampliamenti della rete è altresì sconsigliabile l'adozione di soluzioni di tipo proprietario (cioè adottando schemi di cablaggio proposti da un unico produttore): il reperimento dei materiali necessario per le future modifiche potrebbe risultare difficoltoso o economicamente svantaggioso. Questo tipo di scelta potrebbe anche impedire, in tempi successivi, l'impiego di soluzioni tecnologicamente più evolute. Questa eventualità è tutt'altro che remota: l'esperienza del passato ci insegna come la crescita delle reti sia normalmente molto rapida, contraddistinta da numerose modifiche, afflitta dalla repentina obsolescenza dei prodotti e dalla nascita di nuovi *standard*. È invece opportuno, per colui che si accinge a progettare una rete di comunicazioni, tentare di eliminare o di limitare i costi per le modifiche dell'impianto dovute alle eventuali variazioni d'impiego dell'edificio o all'innovazione tecnologica.

Cos'è un cablaggio

Il cablaggio è un'infrastruttura per la trasmissione di segnali all'interno di un edificio e/o tra più fabbricati di un campus. Si compone di un certo insieme di elementi passivi: cavi, connettori, prese terminali, pannelli di permutazione, cavi di raccordo.



Cavo in rame UTP



Connettore RJ45 per cavo UTP



Pannelli di permutazione (*Patch Panel*)



Prese terminali

Cavi di raccordo (*Patch Cord* UTP)

Esistono elementi che non fanno parte del cablaggio strutturato in senso stretto, ma che contribuiscono a realizzare un'infrastruttura di rete. Si possono citare, a titolo di esempio, gli armadi rack per la collocazione dei permutatori e degli apparati attivi. In figura è rappresentato l'interno di un armadio destinato a ospitare un apparato attivo (lo *switch* visibile in alto) e due permutatori (in basso). Sono inoltre raffigurati diversi fasci di *patch-cord* che interconnettono le porte dell'apparato attivo ai permutatori (e quindi alle porte terminali presso l'utenza). Per una migliore organizzazione dello spazio, i *patch cord* sono raggruppati con delle fascette autobloccanti e corrono all'interno di appositi moduli poggia-cavi (laterali e orizzontali).

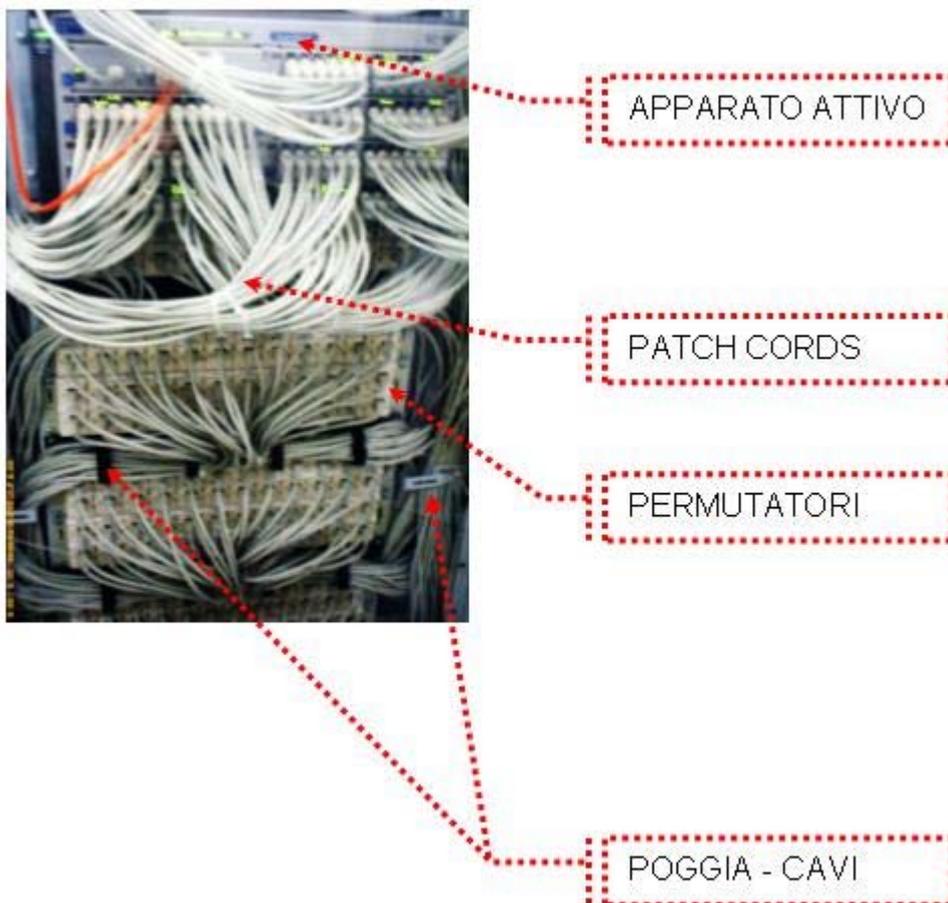
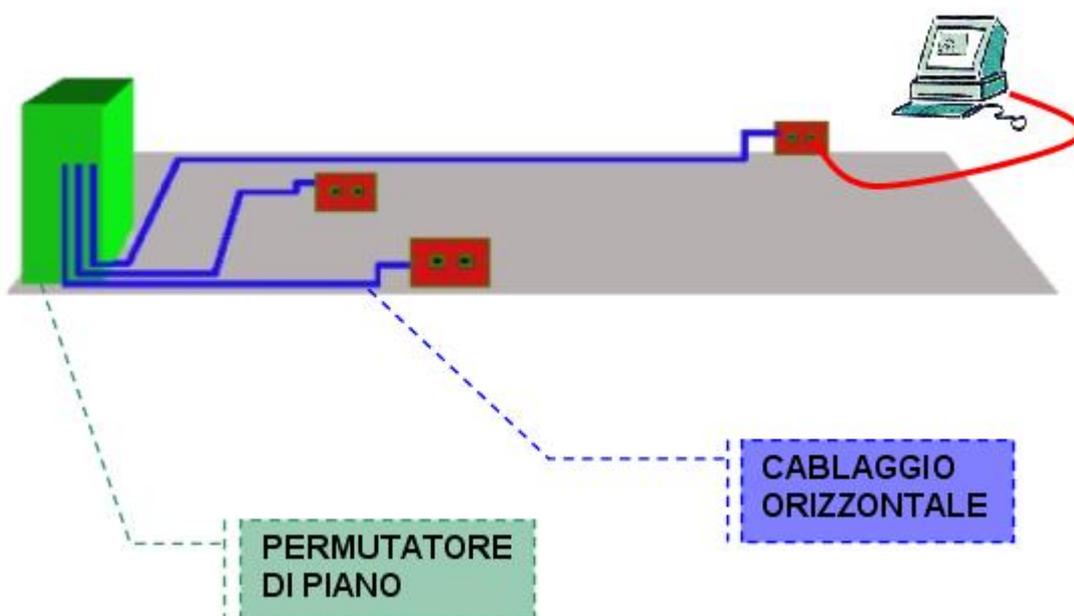


Immagine di un armadio di rete con un apparato attivo e relativi elementi per la connessione

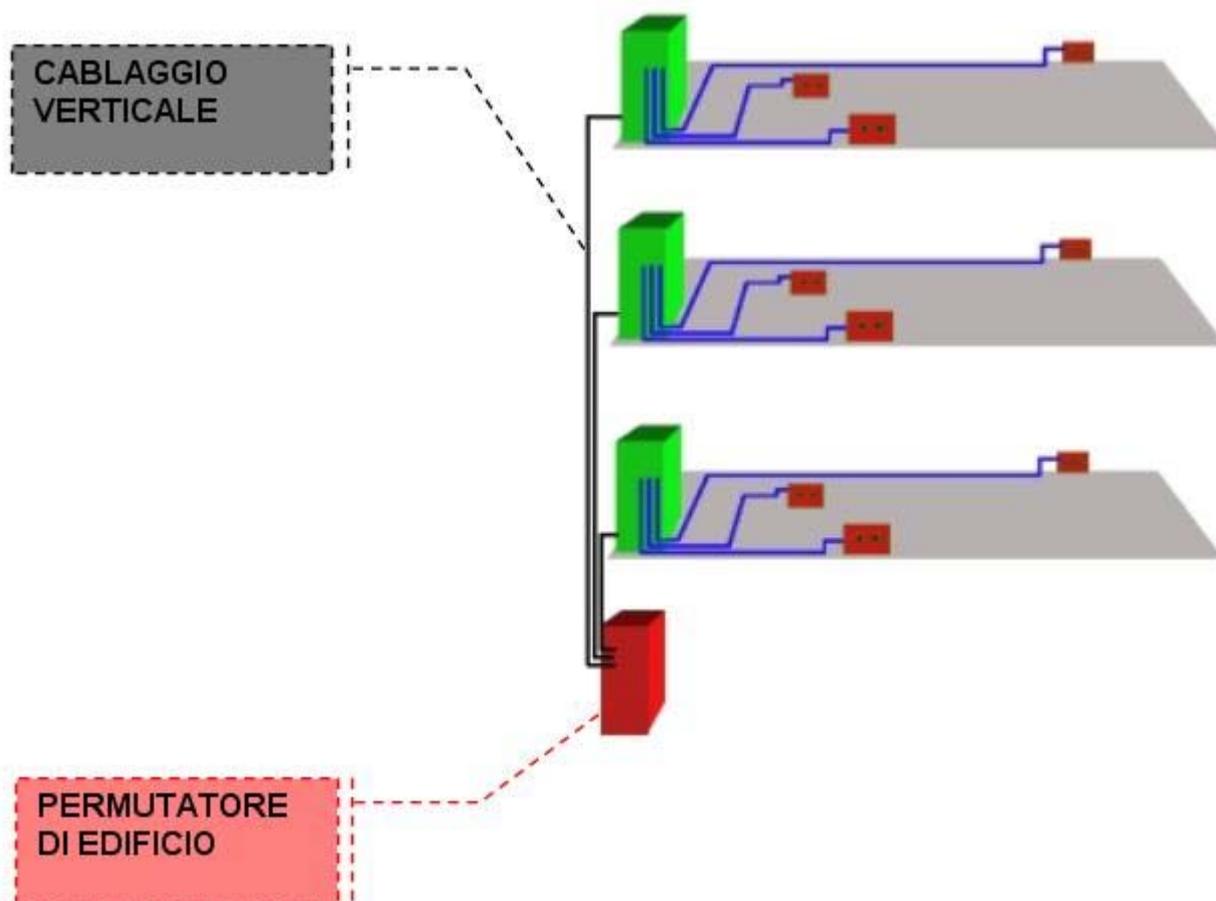
Cablaggio orizzontale

È normalmente riferito ad un singolo piano di un edificio.



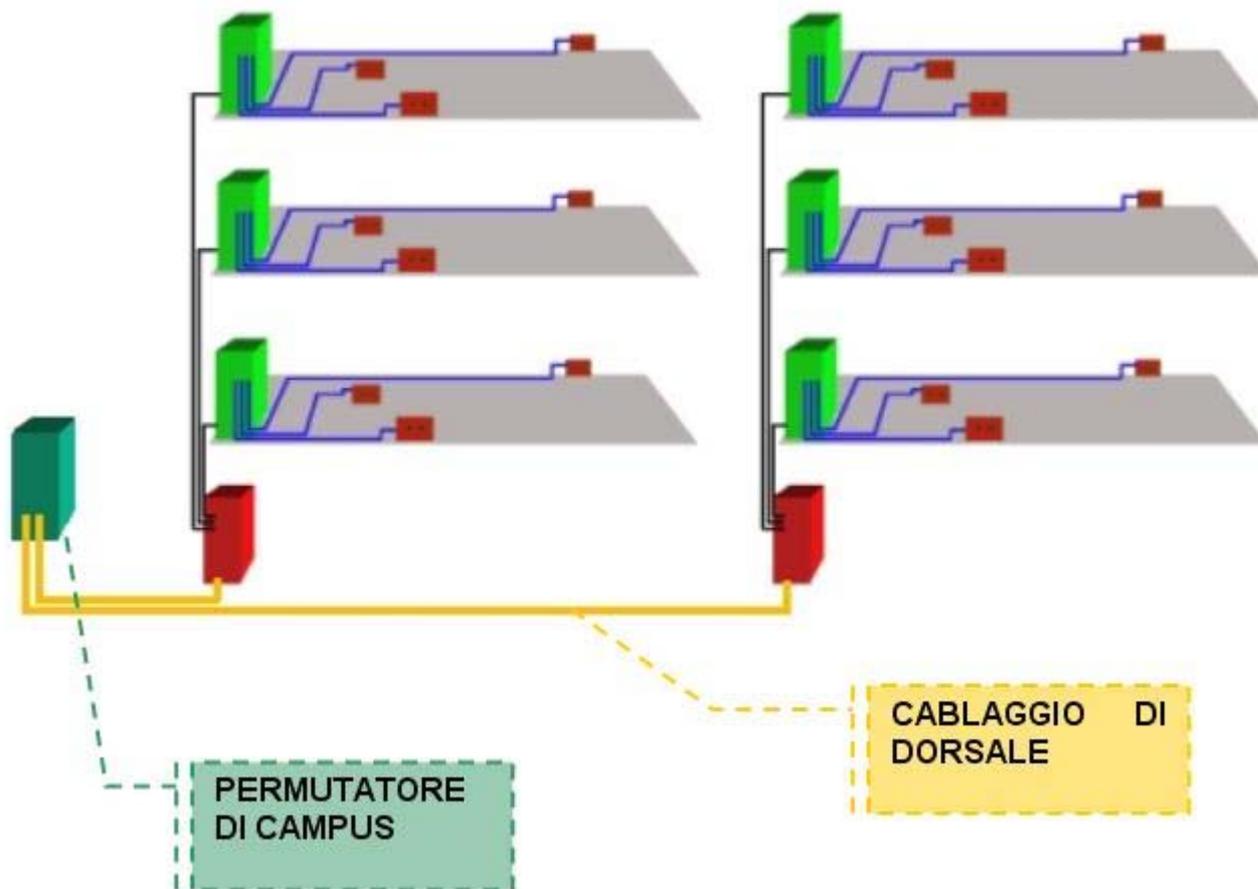
Cablaggio verticale

È normalmente riferito al singolo edificio e interconnette distinti cablaggi orizzontali.



Cablaggio CAMPUS

Interconnette tra loro diversi edifici.



Gli standard attuali

Il rilascio del primo *standard* (EIA/TIA 568) per il cablaggio strutturato risale al 1990: esso fu emesso dall'ente americano EIA e fissò le regole da seguire per la realizzazione di un sistema di cablaggio di tipo generale. Nel 1995 l'EIA pubblicò un primo aggiornamento di questo *standard*, noto con il nome di EIA/TIA 568 A. Questo *standard*, nato per il mercato nordamericano, si diffuse rapidamente in tutto il mondo: a distanza di poco tempo l'ISO (*International Standardization Organization*) pubblicò il primo *standard* per il mercato mondiale, l'ISO/IEC 11801, rifacendosi in gran parte agli *standard* emanati dall'EIA. In seguito, l'Unione Europea, attraverso un proprio comitato, il CENELEC, emanò il proprio *standard* EN 50173, che adottava lo *standard* ISO nel rispetto delle vigenti Direttive europee. È importante notare come questi *standard*, per quanto molto simili, non siano però identici tra loro. Le differenze non riguardano solamente la terminologia adottata, ma anche alcuni vincoli qualitativi sulle prestazioni dei collegamenti. Nella seguente tabella sono illustrate le più importanti specifiche (per i cavi in rame) di ciascuno degli *standard* ora citati.

Standard	EIA/TIA 658 A	ISO 11801	CENELEC EN 50173
Cavi in rame per dorsali o cablaggi orizzontali	Cavo UTP, 4 coppie, 100, guaina in PVC	Cavo UTP, 4 coppie, 100 o 120, guaina a bassa emissione di gas zero-alogeni; Cavo FTP o STP opzionale	Cavo FTP, 4 coppie, 100-120, guaina a bassa emissione di gas zero-alogeni; Cavo STP opzionale
Raggio di curvatura del cavo posato in dorsale	> 10 * (diametro esterno del cavo)	> 6 * (diametro esterno del cavo)	> 6 * (diametro esterno del cavo)

Raggio di curvatura del cavo posato in orizzontale	> 4 * (diametro esterno del cavo)	> 4 * (diametro esterno del cavo)	> 4 * (diametro esterno del cavo)
Prestazioni	Categoria 3 fino a 16MHz Categoria 4 fino a 20MHz Categoria 5 fino a 100MHz	Classe C fino a 16MHz Classe D fino a 100MHz	Classe C fino a 16MHz Classe D fino a 100MHz
<i>Return Loss</i> (perdita per riflessione)	-	10 dB a 100 MHz	10 dB a 100 MHz
Attenuazione massima	23.2 dB a 100 MHz	23.6 dB a 100 MHz	23.6 dB a 100 MHz
ACR minimo	-	4 dB a 100 MHz	4 dB a 100 MHz

Altri *standard* di interesse sono i seguenti:

- CEI 304-14: traduzione in italiano dell'EN50173;
- EIA/TIA569, USA: infrastrutture per il cablaggio;
- EIA/TIA570, USA: cablaggio in ambito residenziale;
- EN50174, europeo: norme per l'installazione;
- ISO/IEC14763, internazionale: gestione e collaudo dei cablaggi.

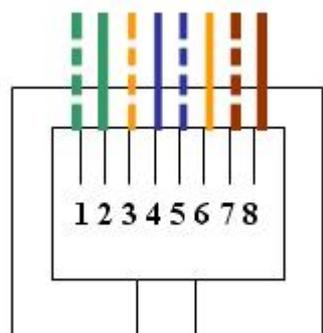
Utilizzo del cablaggio strutturato per i servizi di fonia e dati

La possibilità di utilizzare un cablaggio strutturato per differenti servizi di fonia e dati dipende fondamentalmente dai seguenti elementi:

- utilizzazione dei pins dei connettori;
- rispetto delle lunghezze massime dei collegamenti;
- inserzione di adattatori.

Utilizzazione dei pins dei connettori

In figura è illustrato, a titolo d'esempio, l'utilizzo di un connettore di tipo RJ45 per la connessione di un cavo a quattro coppie intrecciate secondo lo *standard* EIA 568A. Lo *standard* definisce la modalità con cui i fili delle 4 coppie del cavo devono essere associati ai *pin* del connettore (ovviamente in numero di 8).



La corrispondenza di ciascun filo con il relativo *pin* deve essere identica sia sulla presa utente sia

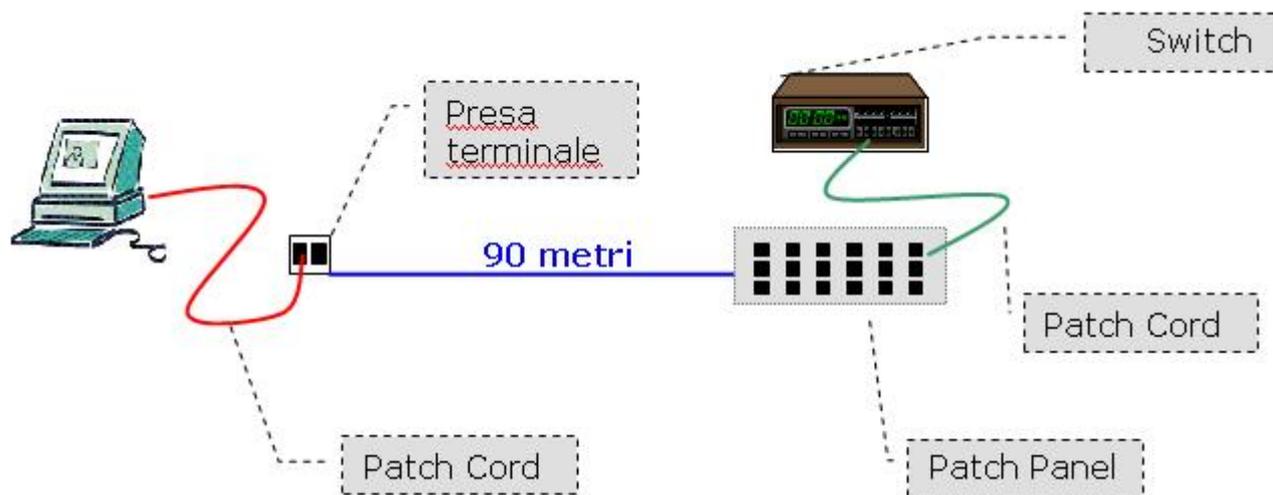
sul pannello di permutazione (detto anche patch panel). Con questo tipo di connettore è possibile utilizzare indifferentemente apparecchi telefonici, terminali *Ethernet*, ISDN, eccetera. Ovviamente la corrispondenza tra fili e *pin* varia di caso in caso.

Per i terminali *Ethernet* (tipicamente i *personal computer*) operanti a frequenze di trasmissione di 10/100 Mbit/s saranno normalmente assegnati i seguenti *pin*:

- *pin* 1: dati in trasmissione (filo caldo);
- *pin* 2: dati in trasmissione (massa);
- *pin* 3: dati in ricezione (filo caldo);
- *pin* 4: non utilizzato;
- *pin* 5: non utilizzato;
- *pin* 6: dati in ricezione (massa);
- *pin* 7: non utilizzato;
- *pin* 8: non utilizzato.

Rispetto delle lunghezze massime dei collegamenti

Per quanto concerne il rispetto delle lunghezze dei collegamenti, lo *standard* ISO 11801 stabilisce che la massima lunghezza del cavo di collegamento tra le prese terminali (ossia disponibili all'utente) e l'armadio di distribuzione deve essere di 90 metri.



A questa lunghezza devono necessariamente essere sommate le lunghezze dei cavi di raccordo (*patch cord*) utilizzati sia per interconnettere il *patch-panel* agli apparati attivi (*switch* e/o *hub*) sia per il collegamento tra terminale utente (tipicamente un *personal computer*) alla presa, per un totale di 10 metri. Complessivamente un collegamento orizzontale in fibra non deve quindi superare i $90 + 10 = 100$ metri. È importante rispettare il vincolo imposto dallo *standard* rispetto alla lunghezza massima di 90 metri. In alcune circostanze, ad esempio per raggiungere una postazione particolarmente distante, si potrebbe valutare di utilizzare un cavo di lunghezza superiore ai 90 metri, utilizzando dei *patch cord* di lunghezza inferiore ai 10 metri complessivi. Questo genere di *escamotage* non solo non rispetta la norma, ma potrebbe pregiudicare la flessibilità del cablaggio: se per qualche ragione (ad esempio un riassetto dei locali) fosse necessario cambiare la collocazione del PC in una posizione tale da richiedere un *patch cord* da 5 metri, il *link* complessivo risulterebbe di lunghezza superiore ai 100 metri. In una situazione di questo genere la trasmissione alla massima velocità (ad esempio a 100 Mbit/s) potrebbe essere impossibile o, peggio ancora, aleatoria.

Inserzione di adattatori

L'inserimento di adattatori consente invece di integrare servizi di comunicazione e mezzi trasmissivi tecnologicamente eterogenei. Una situazione frequente nella pratica è quella in cui il cablaggio strutturato è realizzato con la contemporanea presenza di una tecnologia preesistente. Ad esempio, potrebbe essere utile mantenere attivo presso il proprio edificio un preesistente cablaggio in cavo coassiale *thin-wire*: ad esempio, questa scelta può essere necessaria per permettere una graduale sostituzione delle schede di rete dei PC, compatibilmente con i propri vincoli di tempo e di disponibilità finanziaria. In queste situazioni, l'integrazione del cablaggio preesistente è possibile con l'inserimento di opportuni adattatori, detti *media converter*, in grado di collegare tra loro i diversi mezzi di trasmissione, come una rete coassiale *Ethernet 10Base-2* ad una presa terminale del cablaggio strutturato.

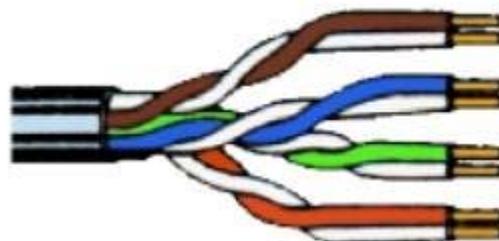
Prestazioni: Cavi in rame

Sono disponibili in commercio vari tipi di cavi *twisted pair* in rame:

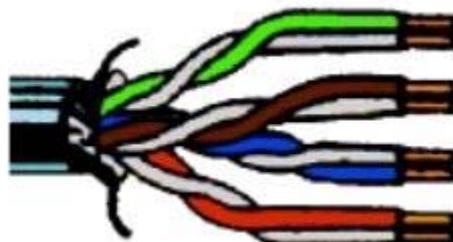
Tipo cavo

Immagine

UTP (*Unshielded Twisted Pair*), cavo a coppie intrecciate non schermato;



FTP (*Foiled Twisted Pair*), cavo a coppie intrecciate, avvolte tutte insieme da una lamina di alluminio schermante;



STP (*Shielded Twisted Pair*), cavo a coppie intrecciate, ciascuna coppia è singolarmente avvolta da una calza schermante in rame, a loro volta tutte insieme schermate da una ulteriore calza in rame.



È importante notare che, per i cavi FTP e STP, è necessario connettere a terra il conduttore schermante. Ciò può porre dei problemi rilevanti nel caso in cui gli impianti elettrici non siano stati realizzati a regola d'arte, pregiudicando le prestazioni offerte dal cablaggio.

Categorie e classi di certificazione

Le categorie definiscono le caratteristiche e le prestazioni offerte da ciascun singolo elemento del cablaggio. I doppini sono distinti in cinque distinte categorie EIA 568 di differenti prestazioni:

- Categoria 1: per la telefonia analogica;

- Categoria 2: per la telefonia digitale e per trasmissioni dati a bassa velocità;
- Categoria 3: per segnali fino a 16 Mhz;
- Categoria 4: per segnali fino a 20 Mhz;
- Categoria 5: per segnali fino a 100 Mhz;
- Categoria 5E (*enhanced*): per segnali fino a 100 Mhz, estensione della categoria cinque per trasmissioni di tipo *Gigabit Ethernet*;
- Categoria 6: per segnali fino a 250 Mhz;
- Categoria 7: per segnali fino a 600 Mhz.

Le classi, introdotte dalla norma ISO 11801, definiscono invece le caratteristiche e le prestazioni offerte da un intero collegamento, inteso come insieme di parti installate. Per ottenere una certa classe di collegamento (ad esempio la classe D), è necessario utilizzare degli elementi appartenenti alla corrispondente categoria (ad esempio la categoria 5E).

Le classi ISO dei collegamenti in rame sono invece quattro:

- classe A: per applicazioni voce e a bassa velocità (fino a 100 khz);
- classe B: per applicazioni a media velocità (fino a 1 Mhz);
- classe C: per applicazioni ad alta velocità (fino a 16 Mhz);
- classe D: per applicazioni ad alta velocità (fino a 100 Mhz);
- classe D2000+ : per applicazioni *Gigabit Ethernet* (fino a 100 Mhz);
- Classe E2000+ (fino a 250 MHz);
- Classe F2000+ (fino a 600 MHz).

Prestazioni dei cavi in rame

Lo *standard* ISO 11801 segna con precisione la qualità dei collegamenti realizzati con cavi in rame. In particolare, attraverso la definizione della classe D, fissa i parametri da tenere in considerazione affinché il cablaggio possa supportare protocolli di trasmissione che richiedono una larghezza di banda fino a 100 MHz. Per quanto riguarda i cavi di tipo *twisted pair*, la valutazione della qualità deve basarsi sulla misurazione delle seguenti grandezze:

- impedenza caratteristica del cavo;
- attenuazione;
- *return loss*;
- NEXT (*Near End Cross Talk*);
- ACR (*Attenuation to Cross talk Ratio*);

già indicate nella precedente tabella.

L'impedenza caratteristica di un cavo *twisted pair* dipende dalle caratteristiche costruttive del cavo stesso e deve essere pari a 100 Ohm. Questo valore dovrebbe, almeno idealmente, essere costante in tutta la banda di frequenze 0 - 100 Mhz.

L'attenuazione del cavo comporta invece una perdita di potenza del segnale durante la sua propagazione. Essa dipende sia dalla frequenza di trasmissione sia dalla lunghezza del cavo stesso. L'attenuazione di un cavo di lunghezza pari a 100 metri per segnali a 100 Mhz deve essere inferiore a 23.6 dB, mentre nel caso di una trasmissione *Fast Ethernet* (segnali a 31 MHz) l'attenuazione massima di un cavo di lunghezza pari a 100 metri deve invece essere inferiore a 13 dB. Il valore dell'attenuazione determina ovviamente la lunghezza massima di un collegamento.

Nei cavi *twisted pair* di buona qualità devono anche essere limitati eventuali segnali riflessi. In questo senso, il *return loss* misura le perdite delle componenti riflesse del segnale. Un altro effetto indesiderato presente nei cavi *twisted pair* è il trasferimento di potenza del segnale alle coppie di fili

adiacenti (come già accennato il cavo UTP racchiude 4 distinte coppie di fili). Il *NEXT* è il parametro che tiene conto di questo fenomeno ed è definito dal rapporto tra la potenza di segnale indotto e la potenza del segnale trasmesso. È evidente che saranno auspicabili valori del *NEXT* il più possibile ridotti. Il valore massimo del *NEXT*, come vedremo tra breve, è implicitamente definito dal parametro ACR.

La *Attenuation to Cross talk Ratio* o ACR definisce il rapporto che esiste tra la potenza del segnale effettivamente ricevuto (o utile) e la potenza del segnale dissipata su una coppia di fili adiacente. Per questo motivo, l'ACR dovrebbe essere il più possibile elevato. In sostanza:

$$\text{ACR(dB)} = \text{NEXT(dB)} - \text{Attenuazione(dB)}$$

Altri parametri di cui si deve tenere conto sono: ELFEXT, FEXT, velocità di propagazione, resistenza.

In ogni caso, le modalità d'installazione dei cavi contribuiscono notevolmente a modificarne il comportamento: per questo motivo, al termine delle opere di posa, l'installatore deve necessariamente certificarne le effettive prestazioni utilizzando un'apposita strumentazione.

Posa dei cavi in rame

Il mercato offre al presente diverse soluzioni per la posa di cavi in rame. In generale, è possibile trovare tipi di cavi adatti per pose in ambienti interni ed esterni.

I cavi da posare in ambienti esterni devono essere resistenti all'umidità e all'acqua, ai raggi solari (se aerei) e all'azione dei roditori. La protezione è ottenuta ponendo i cavi all'interno di tubi ad alta resistenza meccanica e in grado di isolarli da eventuali sollecitazioni esterne.

Per quanto riguarda i cavi da posare in ambienti chiusi, è importante tenere conto di alcune norme italiane, quali la UNI/CEI 20-37 (i cavi non devono rilasciare gas tossici o corrosivi ad alte temperature - si tratta di cavi LSOH) e la UNI/CEI 20-22 (i cavi non devono contribuire a propagare un incendio). In alcune situazioni il cavo deve attraversare contemporaneamente sia un luogo chiuso sia un ambiente esterno. Sul mercato sono reperibili anche cavi adatti a soddisfare entrambi i requisiti.

Altre norme UNI/CEI da rispettare nella posa dei cavi sono comprese nella sezione dedicata al Capitolato Generale, in particolare al Capo II art.8 di tale documento.

La categoria 5 enhanced: Gigabit Ethernet con cavi in rame

Una rete locale in grado di offrire velocità di trasmissione superiori al 100 Mbit/s deve essere basata su un adeguato sistema di cablaggio. Attualmente la tecnologia Gigabit *Ethernet* consente trasmissioni fino a 1000 Mbit/s utilizzando il cablaggio strutturato in rame. Com'è possibile ciò? Nel caso delle applicazioni *Ethernet* e *Fast-Ethernet* sono utilizzate solamente due delle quattro coppie di fili del cavo UTP. Nel 1999 furono aggiornati gli *standard* EIA 568, ISO 11801 ed EN 50173 contemplando la possibilità di trasmettere a 1000 Mbit/s su un cavo in rame sfruttando tutte le coppie di fili (per un collegamento di lunghezza massima di 100 metri). È però necessario, affinché sia possibile raggiungere queste velocità di trasmissione, che il cavo superi test più restrittivi di quelli normalmente previsti per la categoria 5.

In termini concreti, occorre fissare dei vincoli più rigorosi rispetto ai parametri già esistenti e introdurre alcune nuove grandezze:

- PSNEXT (*powersum NEXT*): è la somma dei *NEXT* di tre coppie di fili sulla quarta;
- PSELFEXT (*powersum ELFEXT*): il FEXT (*Far End Cross Talk*), diversamente dal *NEXT*, rappresenta il disturbo alla terminazione di una coppia causato da un segnale che si propaga in una coppia adiacente. Senza scendere nei dettagli, la differenza tra attenuazione e FEXT definisce l'ELFEXT. Il PSELFEXT è la somma degli ELFEXT di tre coppie sulla quarta;
- DELAY-SKEW: è la differenza tra i ritardi di propagazione di due segnali che si propagano su coppie diverse di fili;
- PSACR (*powersum ACR*): analogamente all'ACR, è la differenza (in dB) tra PSNEXT e Attenuazione.

È evidente che ciò si tradurrà in una migliore tecnologia costruttiva dei cavi (che per questo motivo sono detti di categoria 5 *enhanced*).

I cavi in fibra ottica

I cavi in fibra ottica offrono prestazioni indubbiamente migliori rispetto ai cavi in rame, in particolare per la larghezza di banda disponibile e per la bassa attenuazione delle potenze in gioco. Oltre a ciò, sono immuni alle interferenze elettromagnetiche e non generano disturbi (per questo motivo sono spesso utilizzate in ambienti ospedalieri). Due fattori ne limitano l'utilizzo: il costo e la difficoltà di posa. Per questi motivi, trovano spesso impiego per i collegamenti di dorsale. Come è possibile notare nella seguente tabella, le norme ammettono l'utilizzo sia di fibre monomodali sia multimodali.

Standard	EIA/TIA 658 A	ISO 11801	CENELEC EN 50173
Cavi in fibra ottica per cablaggio orizzontale o per dorsale	Cavo multimodale 62.5/125 microm con connettori SC per le nuove installazioni, connettori ST per installazioni esistenti; Cavo monomodale 8/125 microm opzionale (solo dorsali)	Cavo multimodale 62.5/125 microm o 50/125 microm (opzionale) con connettori SC per le nuove installazioni, connettori ST per installazioni esistenti; Cavo monomodale 8/125 microm opzionale (solo dorsali)	Cavo multimodale 62.5/125 microm o 50/125 microm (opzionale) con connettori SC per le nuove installazioni, connettori ST per installazioni esistenti; Cavo monomodale 8/125 microm opzionale (solo dorsali)

Le fibre multimodali sono attualmente le più diffuse.

Prestazioni delle fibre ottiche

Due parametri fondamentali da considerare per la classificazione di una fibra ottica sono il diametro del nucleo (*core* o *kernel*) e il diametro del rivestimento esterno (mantello o *cladding*). Le prestazioni migliori sono offerte dalle fibre con diametro del *kernel* più ridotto, dal quale dipende la attenuazione della fibra. La norma ISO 11801 richiede il rispetto dei seguenti parametri (misurati alla frequenza di 850 nm):

- Larghezza di Banda > 200 Mhz * Km.
- Attenuazione < 3.5 dB/km.
- Attenuazione dei connettori < 0.75 dB.
- *Return Loss* > 20 dB.
- Perdite per giunzioni < 0.3 dB.

Tipi di fibre ottiche, classi di connessione e connettori

Lo *standard* ISO 11801 definisce quattro tipi di fibre ottiche:

- OM1 (50 o 62.5 /125 microm): multimodale;
- OM2 (50 o 62.5 /125 microm): multimodale;
- OM3 (50/ 125 microm): multimodale;
- OS1 (6/125 microm): monomodale;

e tre distinte classi di connessione:

- OF-300: per coprire una distanza minima di 300 metri;
- OF-500: per coprire una distanza minima di 500 metri;
- OF-2000: per coprire una distanza minima di 2000 metri.

Le fibre ottiche, per essere connesse ai pannelli di permutazione ottici (detti anche cassette ottici), devono essere dotate di un connettore terminale. Le seguenti figure ne illustrano i tipi più comuni. Lo *standard* ISO 11801 raccomanda l'utilizzo di connettori *SC-Duplex*, costituiti da due connettori SC accoppiati; l'attenuazione introdotta non deve superare gli 0.75 dB; eventuali giunzioni tra le fibre non devono introdurre un fattore di ulteriore attenuazione superiore agli 0.3 dB.

Posa delle fibre ottiche

Il mercato offre al presente diverse soluzioni per la posa delle fibre ottiche. In generale, è possibile trovare tipi di cavi adatti per pose in ambienti interni ed esterni.

I cavi da posare in ambienti esterni devono essere resistenti all'umidità e all'acqua, ai raggi solari (se aerei) e all'azione dei roditori. La protezione è ottenuta ponendo la fibra ottica all'interno di tubi ad alta resistenza meccanica e in grado di isolarla da eventuali sollecitazioni esterne.

Per quanto riguarda i cavi da posare in ambienti chiusi, è importante tenere conto di alcune norme italiane, quali la UNI/CEI 20-37 (i cavi non devono rilasciare gas tossici o corrosivi ad alte temperature - si tratta di cavi LSOH) e la UNI/CEI 20-22 (i cavi non devono contribuire a propagare un incendio). In alcune situazioni il cavo deve attraversare contemporaneamente sia un luogo chiuso sia un ambiente esterno. Sul mercato sono reperibili anche cavi adatti a soddisfare entrambi i requisiti.

IEEE 802.3Z: Gigabit Ethernet su fibra ottica

Nel 1998 l'IEEE ha approvato uno *standard* Gigabit Ethernet per trasmissioni su fibra ottica chiamato 802.3z.

Le modalità di trasmissione previste sono due:

- 1000 BASE-SX, per trasmissioni con lunghezze d'onda pari a 850 nm;
- 1000 BASE-LX, per trasmissioni con lunghezze d'onda pari a 1300 nm.

In base al tipo di fibra e alla modalità di trasmissione prescelta, è possibile coprire distanze diverse.

Mezzo trasmissivo	Distanza massima
Fibra multimodale 62.5/125 a 850 nm	220 metri
Fibra multimodale 62.5/125 a 1300 nm	550 metri
Fibra multimodale 50/125 a 850 nm	500 metri
Fibra multimodale 50/125 a 1300 nm	550 metri
Fibra monomodale 6/125 a 1300 nm	5 km

Apparati attivi

Come si è già visto, gli apparati attivi sono dispositivi utili a far transitare i pacchetti di dati nei mezzi trasmissivi. Esempi di questo tipo di apparecchiature sono gli *hub*, gli *switch*, i *router*, i *transceiver* (o *media converter*) e i *bridge*. Gli esemplari di apparati attivi attualmente in commercio sono numerosissimi. Inoltre, la valutazione dei dispositivi più idonei per la propria rete LAN dipende da numerosi elementi. Le apparecchiature d'interesse sono comunemente due: gli *Hub* e gli *Switch*.

Esistono *hub* adatti a diversi generi di mezzi trasmissivi, ad esempio per il cavo coassiale, che permettono di connettere alcuni segmenti di cavo per realizzare tratte estese, oppure *hub* per cavi *twisted* dotati di 8, 12, 16, 24 porte di tipo RJ-45 e che realizzano la interconnessione di un gruppo di stazioni di lavoro. Essendo solo semplici amplificatori di segnali, gli *hub* non svolgono alcuna funzione di separazione dei percorsi sui dati che ritrasmettono. Per semplicità, se un PC collegato sulla porta numero 1 dell'*hub* sta trasmettendo, i dati saranno propagati a tutti gli altri PC connessi alle altre porte dell'*hub*. In ultima analisi, i pacchetti si snoderanno in tutta la rete, tenendola inutilmente occupata ed inibendo la possibilità ad altri PC di spedire i dati nello stesso tempo. Gli *hub* sono tuttavia apparecchiature economiche ed adatte all'interconnessione di un numero limitato (20-30) di PC ed a basso volume di traffico.

Lo *switch* invece arricchisce il modo di funzionare di un *hub*, oltre a rigenerare e amplificare il segnale elettrico, registra il pacchetto in arrivo, lo esamina per individuare attraverso quale porta deve arrivare e lo ritrasmette su quella unica porta. L'operazione di registrazione e ritrasmissione dei pacchetti di dati implica l'introduzione di un lieve ritardo, ma consente di trasferire i pacchetti a diverse velocità, senza apparenti effetti di congestione. Uno *switch* con due sole porte è anche chiamato *bridge*. L'utilizzo di *switch* consente quindi di separare i flussi di traffico e di isolare l'impiego di banda ai soli segmenti di rete che congiungono i calcolatori attivi, ottimizzando le prestazioni della rete. Ovviamente, essendo gli *switch* apparati più evoluti degli *hub* sono anche più costosi.

Alcune possibili classificazioni

Esistono molti modi di classificare gli *switch* (le considerazioni fatte nel seguito valgono anche per gli *hub*). Si cercherà qui di elencare le tipologie più comuni di apparati in commercio in modo strettamente operativo.

Innanzitutto, le apparecchiature possono essere installate in modi diversi. Possiamo quindi distinguere tra apparati:

- da armadio, destinati ad essere collocati all'interno di armadi *rack*;
- da tavolo (o di tipo *desktop*), da appoggiare semplicemente sul proprio tavolo.

Un secondo criterio di classificazione tiene conto dell'espansibilità dei dispositivi, che possono essere:

- *standalone*, ossia in un singolo elemento;
- *stackable*, in grado di essere interconnessi tra loro con un connettore privato ad elevate prestazioni; il pregio di questa tipologia di *switch* è che, pur presentandosi da un punto di vista logico come un unico apparato, sono in realtà espandibili nel tempo a seconda delle esigenze;
- a *chassis*; in questo caso si tratta di un unico dispositivo, dotato di diverse feritoie per l'inserimento di più moduli d'espansione; rispetto ai dispositivi *stackable*, offrono migliori prestazioni (il *bus* di interconnessione dei moduli è interno) e costi complessivamente inferiori ma sono alle volte meno scalabili.

Un ultimo criterio di distinzione degli apparati attivi può riferirsi alla possibilità di gestire questi dispositivi da una postazione remota di controllo. In questo caso è possibile parlare di apparati attivi:

- *unmanaged* (privi di gestione), meno intelligenti, meno costosi ma privi di alcuna possibilità di controllo remoto;
- *manageable* (gestibili), ossia in grado di permettere all'amministratore della rete la configurazione dei parametri di funzionamento e di fornire informazioni sul loro stato, sul traffico di rete che li attraversa, o su eventi critici che li hanno interessati.

In linea generale, è opportuno impiegare gli apparati da tavolo solamente in condizioni sfavorevoli di usufruibilità degli spazi interni; in caso contrario, la collocazione degli *switch* all'interno degli armadi *rack* è sempre consigliabile. Gli apparati *manageable* sono sicuramente da preferire nel caso di LAN estese e con un elevato numero di postazioni collegate.

Parametri di valutazione

La scelta di un apparato di rete è sempre un'attività complessa e di cui è spesso difficile prevedere a priori tutte le ripercussioni.

In generale, è necessario vagliare attentamente le seguenti caratteristiche, oltre al costo.

1. Prestazioni: in linea di principio, i dispositivi dovrebbero poter sostenere il carico immediato di traffico presente in rete ed offrire sufficiente margine di *performance* per fare fronte alle esigenze a medio termine degli utenti. In concreto, per chi si accinge alla progettazione di una nuova rete, questi dati sono ignoti e difficilmente prevedibili. In ogni caso, la scelta dell'apparato dovrebbe tenere conto di alcuni valori normalmente dichiarati dai produttori:
 - *switch fabric speed* (matrice di commutazione interna): offre una misura della capacità massima di traffico che l'apparato è in grado di propagare;
 - *throughput*: numero di pacchetti al secondo che l'apparato è in grado di inoltrare;
 - *latency*: tempo massimo impiegato dall'apparato per far uscire un pacchetto.
2. Affidabilità: molti *switch* in commercio offrono la possibilità di installare un alimentatore secondario in grado di attivarsi automaticamente nel caso di arresto di quello primario.
3. Aderenza agli *standard* ed interoperabilità: la capacità degli *switch* di dialogare con apparati forniti da altri produttori.
4. Facilità d'utilizzo (*management* remoto, *monitoring* e *alerting*): è utile verificare se l'apparato può essere controllato remotamente e attraverso quali protocolli di dialogo (HTTP, Telnet, *Secure Shell*), se può essere configurato in modo da intercettare determinati eventi (ad esempio un picco anomalo di traffico) e segnalarli all'amministratore di rete, se offre il supporto ai protocolli di *management* **SNMP** e **RMON**.
5. Supporto, assistenza e tempi d'intervento tecnico: è bene valutare se il produttore offra un supporto telefonico e/o *Web* e in quali orari, per quale periodo gli apparati saranno coperti da garanzia in caso di guasto, quali siano i tempi d'intervento per la sostituzione delle unità guaste.

Un esempio reale

Nel seguito, a puro scopo esemplificativo, sono elencate le principali risorse offerte da uno *switch* a *chassis* di medie prestazioni:

- Fast path technology: wire-speed switching of intra-module traffic for up to 71.4 Mpps throughput.
- Fast switch fabric: high-performance switch fabric (up to 36.6 Gbps).
- latency: < 10 micros (FIFO).

- Rapid Convergence Spanning Tree Protocol (802.1w): increases network uptime through faster recovery from failed links.
- 802.3ad Link Aggregation Control Protocol (LACP): support up to 6 trunks, each with up to 4 links (ports) per trunk.
- Cisco Fast EtherChannel (FEC): supports Cisco's proprietary FEC trunking protocol.
- VLAN: supports up to 30 port-based VLANs, GVRP, and 802.1Q VLAN tagging.
- Port security: prevents unauthorized access using MAC address lockdown.
- Secure Shell (SSHv2): encrypts all transmitted data for secure remote access over IP networks.
- Traffic prioritization (802.1p): allows real-time traffic classification into 8 priority levels mapped to 3 queues.
- RMON and switch monitoring (SMON): provides monitoring and reporting capabilities for statistics, history, alarms.
- Stacking capability.
- Cisco Discovery Protocol (CDP): enables real-time mapping of nodes to switch ports.
- Find, fix, and inform: finds and fixes common network problems automatically, then informs administrator.
- Layer 3 static routes: enable VLAN-to-VLAN communications and up to 16 external routes - including one default route - in IP networks.
- Lifetime warranty: for as long as you own the product, with next-business-day advance replacement (available in most countries).
- Operating temperature: 32°F to 131°F (0°C to 55°C), relative humidity: 15% to 95% @ 104°F (40°C), non-condensing.
- Dimensions: switch XXXX: 17.4 x 15.3 x 8.75 in (44.2 x 38.9 x 22.23 cm).
- Weight: switch XXXX: 22.9 lb (10.4 kg).

Reti LAN wireless

La necessità di condividere i dati e le risorse tra più utenti, unita ad un sempre più forte bisogno di mobilità, favorisce oggi la crescita del mercato delle reti LAN *wireless* (letteralmente, senza fili). Anche ambienti come le scuole possono trarre vantaggio, per l'accesso ai dati locali e remoti, dall'utilizzazione di queste tecnologie, usufruendo di prestazioni paragonabili a quelle delle LAN cablate. Spesso poi l'impiego delle frequenze radio (*Radio Frequencies* o RF) è realizzato come un ampliamento di una LAN cablata già esistente, allo scopo di incrementarne l'estensione e la flessibilità. In generale, una rete *wireless* deve essere progettata per fornire all'utente un'opportuna copertura geografica, all'interno della quale sia possibile muoversi mantenendosi collegati al resto della rete locale.

Scenari di impiego

Le reti *wireless*, secondo lo scenario d'impiego, possono essere:

- *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;
- 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*. 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* (si tratta di una tecnologia ampiamente utilizzata nel caso delle reti radiomobili cellulari);



- 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.

Tecnologie

Le tecnologie impiegate per le reti *wireless* sono essenzialmente tre:

- A banda stretta, la trasmissione e la ricezione dei dati avviene tra i 430 e i 470 MHz (UHF). Poiché la banda disponibile per il canale è abbastanza limitata, questo tipo di tecnologia offre prestazioni ridotte (tipicamente 9.6 Kbit/s). La concessione d'uso delle frequenze deve essere richiesta al Ministero delle Comunicazioni.
- *Spread Spectrum*, è la tecnologia più diffusa. Ne esistono due varianti: *frequency hopping* (salto di frequenza) e *direct sequence* (sequenza diretta). In questi casi, la banda disponibile è molto estesa: ciò consente di distendere la potenza del segnale su una gamma di frequenze molto ampia, arrecando poco disturbo agli altri utenti radio. Per questo motivo, non è necessario richiedere al Ministero la assegnazione delle frequenze, anche se purtroppo resta obbligatorio il pagamento di un canone annuale di utilizzo.
- Infrarossi, scarsamente utilizzata in quanto i campi infrarossi si propagano con difficoltà in aria. Per questo motivo la distanza massima percorribile dai segnali è appena di qualche metro.

Gli standard

A partire dal 1990, il comitato di standardizzazione IEEE 802 ha proposto varie specifiche da rispettare (da parte dei costruttori di apparati *wireless*) allo scopo di garantire il più possibile la interoperabilità dei prodotti. Negli anni seguenti, altre proposte sono state fatte da parte di altri enti, come ETSI o il WLI Forum. Nella seguente tabella sono riassunti i principali *standard* vigenti.

Organizzazione	Standard	Caratteristiche	Banda disponibile
IEEE	802.11	Frequency hopping	2 Mbit/s
IEEE	802.11	Direct Sequence	2 Mbit/s
IEEE	802.11b	Direct Sequence	1, 2, 5.5, 11 Mbit/s
IEEE	802.11 <i>High Speed</i>	Alta capacità	20 Mbit/s
ETSI	<i>HiperLAN</i>	Alta capacità	24 Mbit/s
WLI Forum	<i>OpenAir</i>	Elevata scalabilità	1.6 Mbit/s

Progettazione di reti wireless

Nel predisporre la realizzazione di una rete *wireless* è di fondamentale importanza tenere in considerazione alcuni vincoli che determineranno la scelta degli apparati, quali il numero di utenti, la copertura degli ambienti, la compatibilità elettromagnetica.

Normalmente gli *access point* in commercio possono rispondere alle esigenze di 20-30 utenti

contemporanei.

La copertura radio dipende dalla topologia dei locali. Per questo motivo sarebbe appropriato programmare dei rilievi sul campo utilizzando delle adeguate strumentazioni. Infatti, è assai poco intuibile in quale modo contribuiranno al deterioramento della potenza del segnale gli ostacoli presenti all'interno degli ambienti (muri, scaffali, lampade, tavoli, armadi, eccetera). La portata di un *access point* inoltre può dipendere anche dalla velocità di trasmissione. Nel caso di un *access point* 802.11 a 11 Mbit/s la portata può variare da 25 metri (*indoor*, in ambienti chiusi) a 150 metri (*outdoor*, in campo aperto).

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.

Architettura logica di una LAN

Al di là della pura implementazione fisica per mezzo di un sistema di cablaggio, la progettazione di una LAN richiede anche di effettuare delle scelte relativamente all'architettura della LAN stessa. In un ambiente di rete condiviso da utenti appartenenti a diverse aree amministrative si pone infatti il problema di organizzare la LAN secondo un'architettura che tenga conto di queste divisioni e garantisca la massima funzionalità e sicurezza.

Nelle LAN di prima generazione, tutte le stazioni risultavano connesse alla medesima infrastruttura di comunicazione (cavo) e quindi inevitabilmente le informazioni inviate da una stazione raggiungevano tutte le altre stazioni. Questa caratteristica trasmissione *broadcast* è tipica delle LAN standardizzate in ambito IEEE 802 e viene utilizzata per svolgere varie funzioni di rete (ad esempio il protocollo ARP si basa sulla disponibilità della trasmissione *broadcast*).

A causa della trasmissione *broadcast* nascono però alcuni problemi:

- riservatezza dei dati: in un'unica LAN, utilizzando opportuni programmi di lettura dei dati che transitano in rete (gli *sniffer*) è possibile che per un qualunque utente intercettare i dati di una connessione fra altri utenti;
- efficienza: il traffico *broadcast*, ad esempio i messaggi di ARP *request*, viaggiano per tutta la rete consumando capacità e quindi togliendo risorse alla effettiva trasmissione dei dati, se la LAN è molto vasta la quantità di traffico *broadcast* può risultare molto elevata;
- tolleranza ai guasti: se una interfaccia di rete, a causa di un guasto produce un malfunzionamento sulla LAN (per esempio inizia ad inviare pacchetti senza sosta), questo corrompe il funzionamento dell'intera LAN.

Sulla base di queste considerazioni è quindi desiderabile la separazione fisica della LAN in più di una sezione. Nelle LAN di prima generazione questa separazione si poteva realizzare tramite la posa di diversi mezzi trasmissivi (per esempio diversi spezzoni di cavo coassiale per una *Ethernet* 10BASE5) collegati fra loro tramite uno o più *bridge* capaci di svolgere una funzione di filtro, lasciando passare da una LAN all'altra solamente il traffico strettamente necessario.

Nelle LAN moderne, in particolare *Ethernet*, le stazioni sono connesse alle porte di un apparato attivo, *hub* o *switch*, che si occupa di realizzare l'effettiva comunicazione. La separazione fisica di una LAN in sottoparti distinte può quindi essere realizzata semplicemente utilizzando diversi apparati per diversi insiemi di stazioni. Questo però non è sempre possibile o facilmente praticabile, a causa del fatto che la ripartizione logica della rete solitamente non corrisponde alla disposizione fisica degli utenti, oppure a seguito di spostamenti degli utenti stessi. Può infatti accadere che un piano di un edificio sia condiviso da personale appartenente ad aree logiche diverse, sia che un'area

logica sia ripartita su più piani e/o edifici, eccetera.

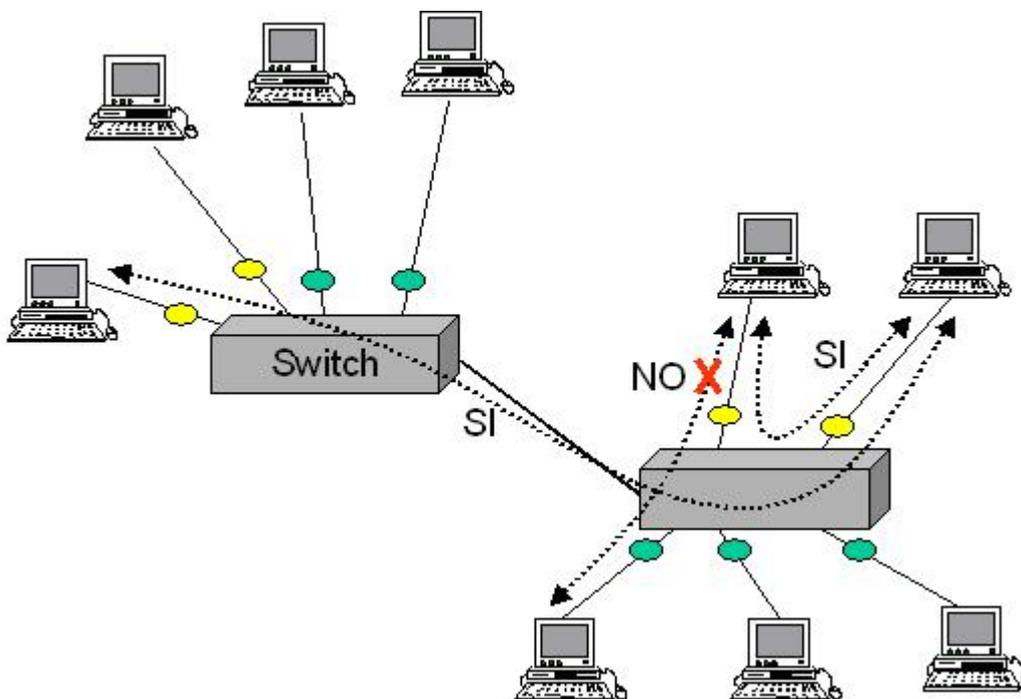
Realizzazione di VLAN

Molti dei moderni apparati di rete permettono di creare delle cosiddette LAN virtuali.

In questo modo è possibile creare con un solo apparato una serie di LAN virtualmente distinte dette appunto LAN virtuali. Sebbene tutti gli *host* delle varie LAN siano connessi tutti al medesimo apparato essi si comportano come se fossero collegati ad apparati distinti e quindi sono virtualmente separati.

La LAN virtuale può essere realizzata utilizzando diverse metodologie che dipendono dal tipo di apparato utilizzato ma anche dalle scelte fatte dal gestore della rete. Di fatto gli apparati che implementano le **VLAN** svolgono un'azione di filtraggio dei *frame* che può essere basata su:

- porta di provenienza;
- indirizzo MAC;
- protocollo di livello 3 o indirizzo *IP*.



Numerazione IP e subnetting

Nel modulo 5 abbiamo visto che gli indirizzi *IP* di 32 *bit* (4 *byte*) sono logicamente suddivisi in due parti; *Net-ID* e *Host-ID*, dove il *Net-ID* identifica la rete, mentre l'*Host-ID* identifica l'*host* all'interno della rete. L'indirizzo con i *bit* relativi alla parte di *host* posti a zero risulta essere l'indirizzo della rete in cui si trova l'*host*, mentre quello con i *bit* di *host* posti tutti a uno indica l'indirizzo *broadcast* di quella rete, cioè quello usato per inviare pacchetti a tutti gli *host* della rete. Quindi il numero di *host* possibili in una certa rete è pari alla dimensione dello spazio di indirizzamento della parte di *host-id* diminuita di 2 unità. Ad esempio:



Inoltre in base al numero di *bit* assegnati a *net-ID* e *host-ID*, gli indirizzi *IP* sono suddivisi in cinque

classi:

- Classe A - Utili per reti che hanno un numero cospicuo di *host*. Il campo *host-ID* è di 24 *bit*, pertanto possono essere identificati circa 16 milioni di *host* per ogni rete di questo tipo. Sette *bit* sono dedicati al *net-ID*, per un massimo di 128 reti di classe A.
- Classe B - Sono utilizzati per reti di dimensioni intermedie. Il *net-ID* è di 14 *bit*, per cui si possono avere al massimo circa 16.000 reti di classe B, ciascuna con una dimensione massima di circa 65.000 indirizzi (*host-ID* da 16 *bit*).
- Classe C - Sono utilizzati per numerose reti con pochi *host*. Le reti di classe C contengono meno di 256 *host* (*host-ID* da 8 *bit*) e sono individuate da 21 *bit* nell'ID di rete.
- Classe D - Sono riservati al *multicasting*, cioè all'indirizzamento di gruppi di *host*.
- Classe E - Sono riservati per usi futuri.

Lo spazio di indirizzamento va partizionato tra le varie classi di indirizzi, in modo che non vi siano sovrapposizioni tra classi diverse. Questo si ottiene fissando, per ogni classe, particolari configurazioni nel primo *byte*.

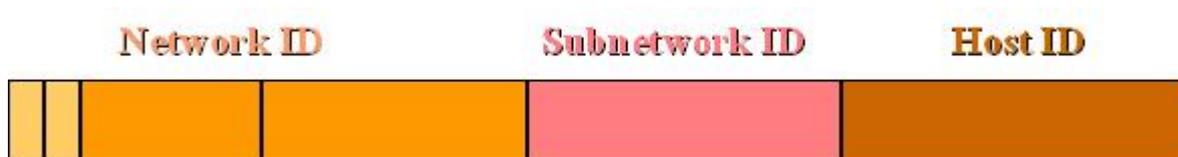
Classe A		(0 . 0 . 0 . 0 + 127 . 255 . 255 . 255)
		127 . 0 . 0 . 0 è riservato al localhost
0	7 bit net ID	24 bit host ID
Classe B		(128 . 0 . 0 . 0 + 191 . 255 . 255 . 255)
1 0	14 bit net ID	16 bit host ID
Classe C		(192 . 0 . 0 . 0 + 223 . 255 . 255 . 255)
1 1 0	21 bit net ID	8 bit host ID
Classe D		(224 . 0 . 0 . 0 + 239 . 255 . 255 . 255)
1 1 1 0	28 bit multicast group ID	
Classe E		(240 . 0 . 0 . 0 + 255 . 255 . 255 . 254)
1 1 1 1 1	27 bit reserved	

Subnetting

Una rete *IP* può essere logicamente partizionata in più sottoreti o *subnet*. In pratica questa operazione permette al gestore di una rete *IP* di suddividerla in sezioni logicamente distinte.

Il *subnetting* viene realizzato ripartendo l'*Host-ID* in due parti, una che identifica la sottorete ed una che identifica univocamente gli *host* della sottorete stessa.

Nell'esempio che segue viene mostrato come i 16 *bit* di *Host-ID* di un indirizzo di classe B possano essere ripartiti in 8 *bit* di *Subnet-ID* e 8 *bit* di *Host-ID*. Per convenzione il *Subnet-ID* deve essere contiguo al *Net-ID* mentre l'*Host-ID* deve occupare la parte più a destra dell'indirizzo *IP*.



L'operazione di *subnetting* è locale alla rete *IP* considerata per cui non viene vista al di fuori della rete stessa. Per realizzarla è necessario configurare correttamente il parametro *Netmask* delle interfacce *IP*. La *Netmask* è una sequenza di 32 *bit*. I *bit* aventi valore 1 nella *Netmask* indicano che

i corrispondenti *bit* dell'indirizzo *IP* fanno parte del *Net-ID* o del *Subnet-ID*, mentre i *bit* a 0 nella *Netmask* indicano che i *bit* in posizione corrispondente nell'indirizzo *IP* dell'*host* fanno parte dell'*Host-ID*.

Ad esempio per un *host* della rete di classe B 137.204.0.0, che sia suddivisa in sottoreti identificate da 8 *bit* avrà una configurazione dell'interfaccia di rete del tipo:

Numero *IP*: 137.204.60.230 (137.204 *Net-ID*, 60 *Subnet-ID*, 230 *Host-ID*)

Netmask:

in formato binario: 11111111 11111111 11111111 00000000

in formato decimale: 255.255.255.0

Oggi è consuetudine riassumere queste informazioni in modo unitario come segue:

- Numero *IP* e *netmask*: 137.204.60.230/24

ad indicare che 24 *bit* dell'indirizzo sono utilizzati per indirizzi di rete o sottorete mentre 8 sono utilizzati per indirizzo di *host*.

È importante notare che l'operazione di *subnetting* in rete *IP* è solamente logica:

- *host* di diverse *subnet* possono essere sulla medesima rete fisica (LAN);
- *host* della medesima *subnet* possono essere su diverse reti fisiche (LAN).

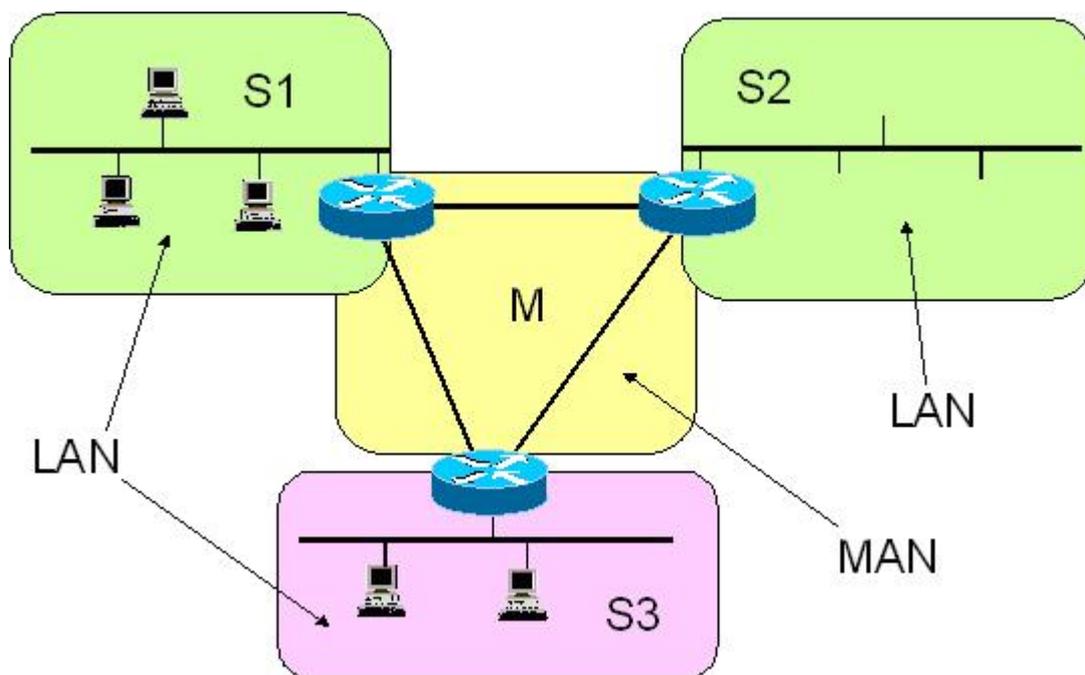
Esempio di subnetting

Un'azienda di grandi dimensioni possiede tre siti distribuiti su una grande area urbana: S1, S2, S3. Ciascun sito aziendale è dotato di infrastrutture informatiche comprendenti, tra l'altro, una LAN ed un *router* di uscita verso il mondo esterno. Tutti i siti devono essere interconnessi tra loro con una rete *MAN* a maglia completa M. Il protocollo usato è il *TCP-IP*.

I siti sono così divisi:

- S1, S2: 50 *host*;
- S3: 20 *host*.

Si richiede di progettare il piano di numerazione *IP* della rete utilizzando una rete di classe C a cui viene assegnato l'indirizzo 196.200.96.0 comprensiva della numerazione dei *router*, definendo le relative *netmask*.



Al progettista, dovendo utilizzare una rete di classe C, vengono messi a disposizione 8 *bit*, su cui creare delle eventuali *subnetwork*. Una possibile scelta della *netmask* è la seguente illustrata in una tabella che mostra il risultato in termini di *netmask*, numero di *subnet* e di *host* per tutte le possibili suddivisioni degli ultimi 8 *bit* dell'indirizzo in *Subnet-ID* e *Host-ID*:

Ultimo byte netmask	#host	#subnets
00000000	254	1
10000000	126	2
11000000	62	4
11100000	30	8
11110000	14	16
11111000	6	32
11111100	2	64

Una possibile soluzione al problema di progetto potrebbe quindi essere la seguente:

Subnets:

196.200.96.0 (S1)
 196.200.96.64 (S2)
 196.200.96.128 (S3)
 196.200.96.192 (M)

Netmask: 255.255.255.192

Broadcast:

196.200.96.63 (S1)
 196.200.96.127 (S2)
 196.200.96.191 (S3)
 196.200.96.255 (M)

Per cui la configurazione degli indirizzi *IP* di *hosts* e *router* verrà fatta seguendo lo schema che

segue:

Routers LAN:

196.200.96.62 (S1)
196.200.96.126 (S2)
196.200.96.190 (S3)

Routers MAN:

qualunque indirizzo tra: 196.200.96.193 e .254 (M)

IP Hosts: qualunque indirizzo tra:

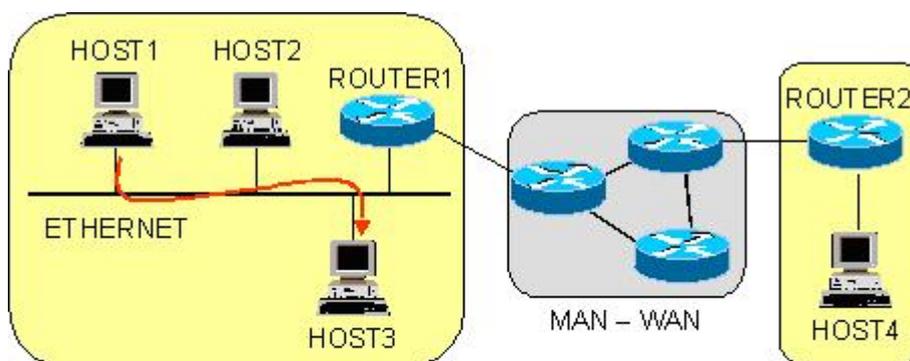
196.200.96.1 e .61 per la LAN S1
196.200.96.65 e .125 per la LAN S2
196.200.96.129 e .189 per la LAN S3

In questo esempio si è seguita una convenzione non strettamente necessaria ma molto diffusa che vuole che quando ad una LAN è collegato un solo *router* che rappresenta il punto di accesso al di fuori della LAN, all'interfaccia di quest'ultimo si associ il massimo numero *IP* disponibile, ossia quello che nella parte di *Host-ID* contiene la configurazione di *bit* immediatamente precedente a quella di *broadcast* (tutti i *bit* a 1).

Instradamento diretto ed indiretto

Un datagramma può essere consegnato in due modi:

- *Direct delivery:* *host* sorgente e destinatario sulla stessa rete fisica; l'*host* sorgente associa l'indirizzo *IP* dell'*host* destinatario al suo indirizzo fisico (*MAC*) utilizzando il protocollo ARP, incapsula il *datagram* in un *frame*, e lo spedisce direttamente al destinatario utilizzando la LAN.
- *Indirect delivery:* *host* sorgente e destinatario non sulla stessa rete fisica; in questo caso l'*host* sorgente invia ad un *router* i pacchetti da consegnare, sarà poi responsabilità del *router* fare sì che il datagramma raggiunga l'*host* destinazione. Il *router* deve essere collegato alla stessa rete fisica dell'*host* sorgente, per l'invio del datagramma al *router* l'*host* sorgente usa *direct delivery*.

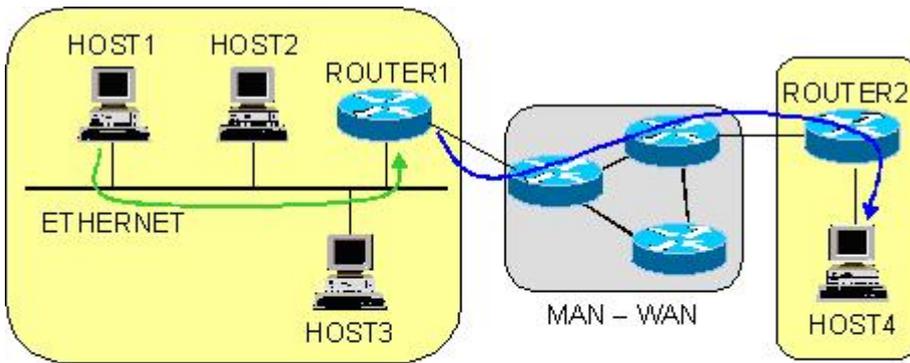


ARP request HOST1 chiede l'indirizzo MAC di HOST3
ARP reply HOST3 risponde direttamente a HOST1

MAC ADDRESS: HOST3

IP ADDRESS: HOST3

DATI



ARP request HOST1 chiede l'indirizzo MAC di ROUTER1
ARP reply ROUTER1 risponde a HOST1

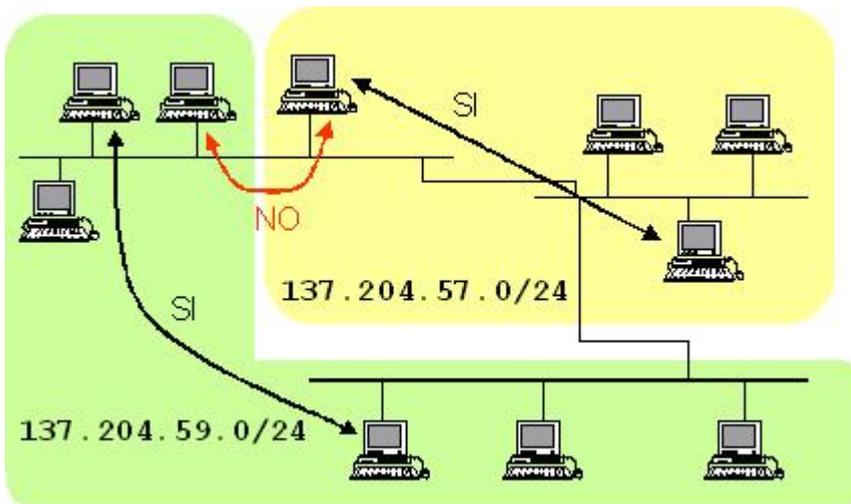


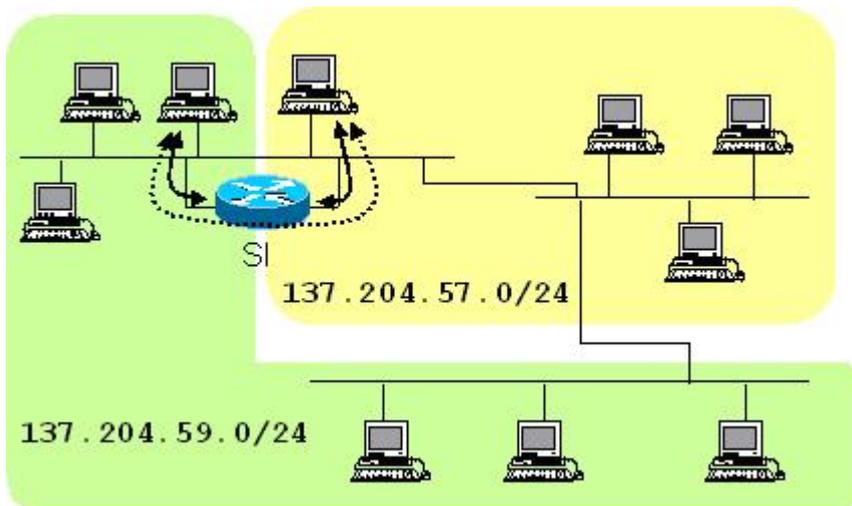
Interconnessione di sottoreti IP sulla stessa LAN

In generale fra calcolatori appartenenti alla medesima *Subnet IP* la consegna dei datagrammi avviene in modo diretto. Quando due *host* appartengono a due *Subnet* diverse invece, la consegna dei datagrammi deve avvalersi di un *router* anche se gli *host* sono connessi alla medesima LAN (e quindi sarebbe teoricamente possibile operare con instradamento diretto).

Quindi *host* di diverse *Subnet* non possono dialogare fra loro a meno che non vengano presi opportuni accorgimenti (ad esempio inserendo un *router* sulla LAN), indipendente dal collegamento fisico alla LAN.

La soluzione più usuale per interconnettere della *Subnet* è quella di utilizzare un *router* che faccia da ponte fra le *subnet*, in modo del tutto analogo ai compiti che svolge per interconnettere due LAN separate.





Perché il subnetting

La ripartizione di una rete *IP* in più sottoreti viene molto utilizzata in particolare quando si devono gestire reti di grandi dimensioni.

La ragione è prettamente di tipo logico/organizzativo e si giustifica per le stesse ragioni che portano alla realizzazione di strutture gerarchiche in presenza di grandi organizzazioni. Con il *subnetting* si crea una struttura gerarchica in grado di semplificare compiti di tipo gestionale/amministrativo:

- gli *host* di aree logiche distinte non sono in grado di dialogare in condizioni normali a meno che non sia stato opportunamente configurato un *router* per l'interconnessione, questo può essere importante per ragioni di sicurezza (ad esempio gli *host* di un laboratorio didattico sono separati dagli *host* degli uffici amministrativi);
- la gestione della numerazione può essere demandata a responsabili locali per le varie aree della rete, senza bisogno di coinvolgere l'amministratore;
- il mantenimento delle informazioni relative al piano di numerazione della rete risulta più organico ed ordinato, al fine di evitare errori di doppia assegnazione o perdita di informazioni.

Se da un lato porta questi indiscutibili vantaggi la creazione di sottoreti richiede una attenta e preventiva progettazione del piano di numerazione. Infatti una volta creato uno spazio di 64 indirizzi per una sottorete, risulterebbe problematico scoprire a posteriori che la sottorete deve poter ospitare 80 *host* e quindi non dispone di un numero di indirizzi sufficienti. Questo richiederebbe la creazione di una nuova sottorete, utilizzando indirizzi che potrebbero già essere stati dedicati ad un'altra area logica e determinando quindi dei problemi di carattere gestionale.

È quindi importante:

- Dedicare attenzione all'identificazione delle aree logiche in cui suddividere la rete.
- Censire gli *host* appartenenti alle aree logiche per valutarne la numerosità.
- Prevedere il potenziale tasso di crescita di tale numero di *host*, al fine di progettare le sottoreti lasciando un certo margine per il loro sviluppo.

A fronte dei vantaggi suddetti è bene comunque anche tenere presente che l'organizzazione di una rete *IP* in sottoreti comporta dei costi, da un lato di tipo logico per la realizzazione del piano di numerazione, e dall'altro di tipo fisico in quanto per garantire l'interconnessione è necessario dotarsi di almeno un *router*.

Supernetting e CIDR

Con l'aumentare delle dimensioni e della complessità di *Internet* ci si è reso conto che l'indirizzamento *IP* sarebbe più flessibile senza l'uso delle classi. In particolare due sono i problemi che si pongono. Si è quindi modificato lo *standard* (e anche l'implementazione del *software* dei *router*), per poter supportare un indirizzamento che non sia rigidamente rispondente alla suddivisioni in classi. È il cosiddetto CIDR o *Classless Inter-Domain Routing*.

Il CIDR permette di creare, oltre alle sottoreti già viste in precedenza delle Super-reti, come aggregazioni di reti *IP*.

Ad esempio per un ente che ha bisogno di circa 2000 indirizzi *IP* una rete di classe B è troppo grande (64000 indirizzi) per cui è più opportuno assegnarli 8 reti di classe C (8 x 256 = 2048 indirizzi). Supponiamo si tratti delle reti dalla 194.24.0.0 alla 194.24.7.0.

Queste 8 reti di classe C possono essere accorpate in un'unica super-rete:

Identificativo: 194.24.0.0/21

Supernet mask: 255.255.248.0

Indirizzi: 194.24.0.1 - 194.24.7.254

Broadcast: 194.24.7.255

Il CIDR permette di:

- distribuire i numeri *IP* in modo più efficiente e conforme con le effettive necessità;
- semplificare le informazioni da memorizzare nei *router*.