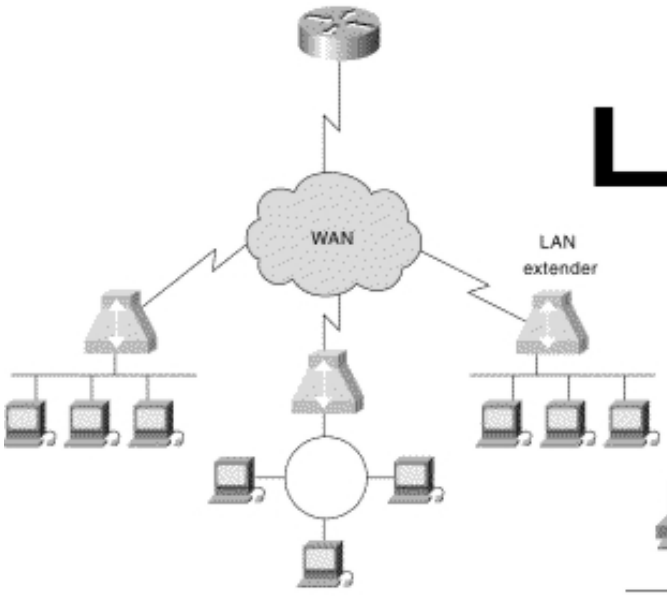
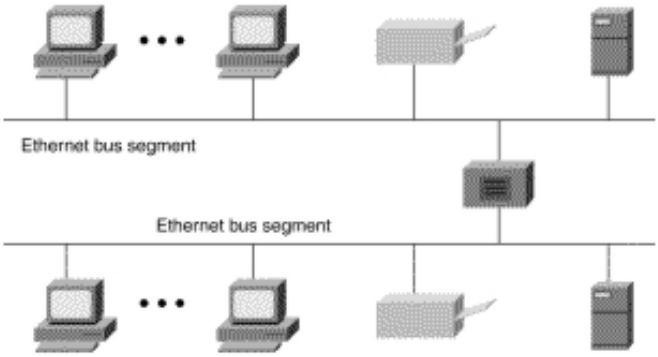
LE RETI



LAN

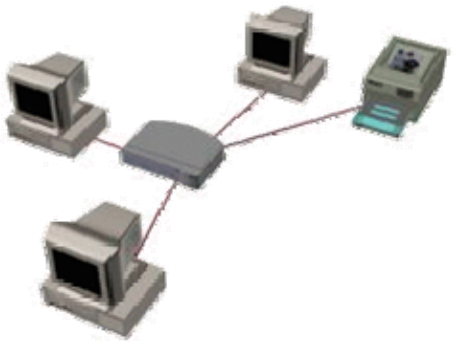


SOMMARIO

Le reti LAN

Definizione e introduzione

Prima di iniziare a definire LAN è opportuno anche se non rilevante fare un breve cenno storico alle LAN.
La diffusione delle LAN negli odierni ambienti di trasmissione era impensabile fino ad una decina di anni fa in quanto prima il fulcro di quasi ogni ambiente di elaborazione era il mainframe a cui erano poi collegati i vari terminali, stampanti, ecc..
Con l'aumento delle esigenze elaborative ci fu l'introduzione delle prime LAN rappresentate da una semplice connettività tra terminale e host.
Successivamente con l'introduzione del pc come lo conosciamo oggi la perfetta combinazione LAN PC portò enormi vantaggi alla struttura aziendale diventando lo strumento fondamentale.
Oggi dopo enormi cambiamenti e sviluppi l'utente può lavorare con il PC e comunicare quando lo necessita con il mainframe condividendo anche i propri dati con gli altri utenti presenti sulla rete.



Una definizione generale di LAN potrebbe essere che *la LAN consente di condividere informazioni ed unità periferiche in maniera efficiente ed economica*.
Ma questa è una delle tante definizioni che si possono dare invece secondo una definizione forgiata dalla IEEE una LAN può essere definita *un sistema comunicativo per connettere fra loro un alto numero di terminali indipendenti distribuito su un'area geografica limitata, utilizzando un canale fisico con elevata velocità di trasmissione e bassissimo tasso di errore.* A prima vista questa definizione potrebbe sembrare semplice e di facile comprensione ma se ci soffermiamo su ogni singola parola dedurremo una gran quantità di valore aggiunto, infatti possiamo rilevare le seguenti caratteristiche:

- Connessione di terminali in un'area geografica limitata;
- Velocità elevate;
- Basso tasso d'errore;
- Costi limitati;
- Infinito numero di terminali collegabili;
- Terminali indipendenti tra di loro e quindi potrebbero essere anche differenti tra loro a patto che le regole comuni di comunicazioni siano rispettate.

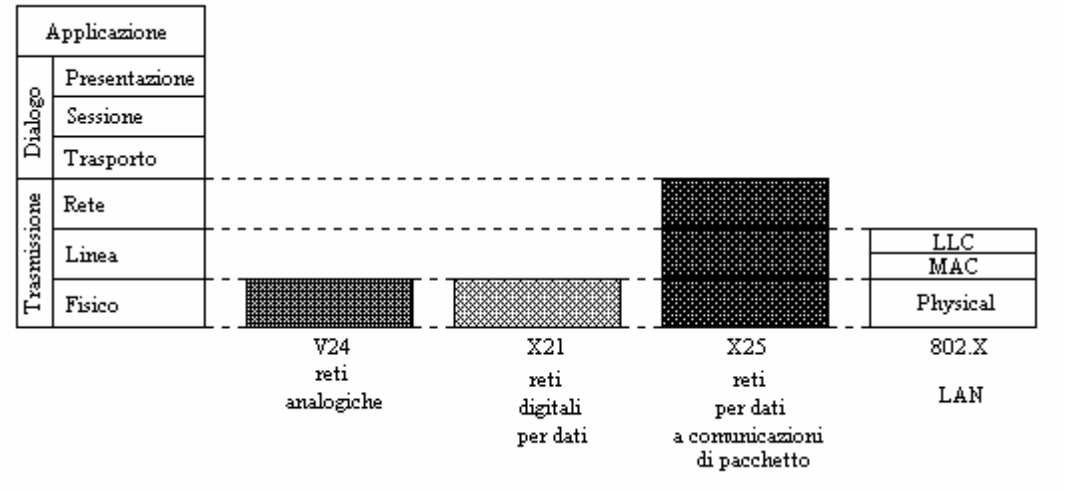
Definizione di pacchetto

Per comprendere il funzionamento e il significato di una rete LAN e utile definire cosa si intende per pacchetto.
Per pacchetto intendiamo una sorta di imbustamento delle informazioni definendo messaggio e destinatario dei dati trasmessi come una sorta di lettera.

L’imbustamento e la dimensione del pacchetto dipende dal tipo di rete fisica che realizza la rete LAN.
I dati possono essere definiti duttili per il semplice fatto che possono essere composti e scomposti in vari modi per formare il pacchetto; quindi parleremo di incapsulamento quando i pacchetti vengono inseriti in altri pacchetti.

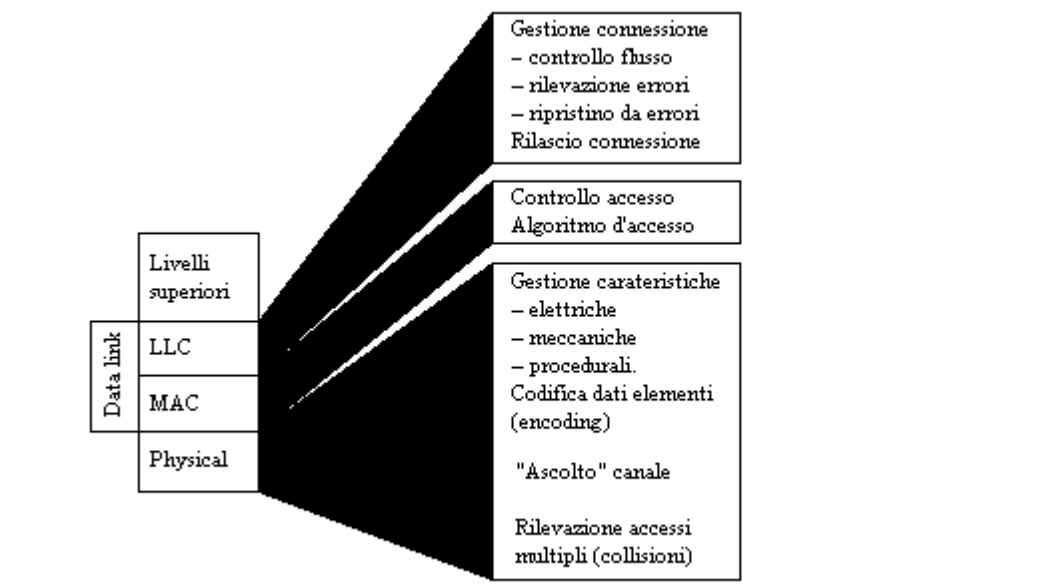
Livelli OSI

Prima di iniziare ad entrare nel vivo delle LAN conviene fare un riferimento ai livelli OSI necessari a connettere computer di diversa manifattura ma anche prodotti di diverse linee produttive pur essendo della stessa azienda. Questi livelli non definiscono uno standard tecnologico, ma un riferimento comune ai concetti che riguardano le reti. Nel nostro caso ci interesseremo del livello 1, del livello 2 e del livello 3, comunque è meglio ridare una breve descrizione degli altri livelli.



- Primo livello (livello fisico): questo livello definisce i metodi usati per trasmettere e ricevere i dati sulla rete. Sono compresi in questo livello i cavi, le unità usate per collegare l’unità di controllo di interfacci rete di una stazione ai cavi. Il cavo o i cavi e le schede Ethernet appartengono a questo primo livello.
- Secondo livello (Livello linea dati): questo livello ha il compito di sincronizzare la trasmissione e di gestire il controllo e la correzione degli errori. Questo livello inoltre definisce i metodi di accesso alla rete.
  Infatti questo livello viene diviso in due parti: (LLC si occupa di aprire la comunicazione e di gestirne il controllo errori e di correggerli eventualmente, ed il MAC per il controllo di

accesso al mezzo).



- Terzo livello (Livello rete): Questo livello è incaricato di controllare l'invio di messaggi tra le stazioni. Utilizzando varie tecniche e algoritmi si preoccupa di *instradare* il messaggio seguendo il percorso più conveniente sia logicamente che fisicamente.
- Livello 4 (Livello Trasporto)
  A questo livello appartengono i protocolli di comunicazione che si occupano di suddividere i dati da inviare in datagramma e di ricomporli all'arrivo. I protocolli principali di questo livello sono TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).
  Il protocollo TCP, oltre alla scomposizione e ricomposizione dei dati, si occupa di verificare e riordinare i dati all'arrivo: i datagramma perduti o errati vengono ritrasmessi e i dati finali vengono ricomposti. Il protocollo UDP, invece, non esegue alcun controllo.
  A questo livello si introduce, a fianco dell'indirizzo IP, il numero di porta, o socket. Il percorso di un datagramma ha un'origine identificata dal numero IP e dalla porta e una destinazione identificata da un altro numero IP e dalla porta. Le porte identificano dei servizi concessi o richiesti e la gestione di questi riguarda il livello successivo.
- Livello 5 (Livello Sessione)
  Ogni servizio di rete (condivisione del filesystem, posta, FTP, ...) ha un proprio protocollo, porte di servizio e un meccanismo di trasporto (quelli definiti nel livello precedente). Ogni sistema può stabilire le proprie regole, anche se in generale è opportuno che i computer che intendono comunicare utilizzino le stesse porte e gli stessi tipi di trasporto.
  Quando si avvia una comunicazione a questo livello, si parla di sessione. Quindi, si apre o si chiude una sessione.
- Livello 6 (Livello Presentazione)
  I dati che vengono inviati utilizzando le sessioni del livello inferiore, devono essere uniformi, indipendentemente dalle caratteristiche fisiche delle macchine che li elaborano. A questo livello si inseriscono normalmente delle librerie in grado di gestire una eventuale conversione dei dati tra l'applicazione e la sessione di comunicazione.
- Livello 7 (Livello Applicazione)
  L'ultimo livello è quello dell'applicazione che utilizza le risorse di rete. Con la suddivisione delle competenze in così tanti livelli, l'applicazione non ha la necessità di occuparsi della comunicazione, e così anche l'utente, in molti casi, può anche non rendersi conto della presenza di questa.

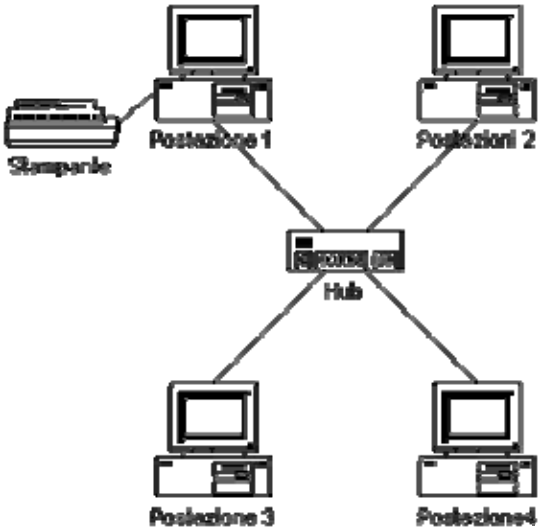
Topologie delle LAN

Quando si vuole analizzare una rete LAN bisogna innanzitutto conoscere le varie topologie esistenti.
Ma prima di tutto dobbiamo sapere che cosa si intende per topologia di una LAN, con topologia di una LAN si intende una struttura architettonica che rappresenta la disposizione fisica e logica dei cavi e dei terminali della LAN.
Le topologie fondamentali sono tre poi esistono vari implementazioni che riguardano la composizione delle tre fondamentali:

- Topologia a stella o star;
- Topologia ad anello o ring;
- Topologia a bus.

Topologia a stella

Questa topologia è una delle più antiche usate nella trasmissione dati; essa fu anche infatti utilizzata con sistemi di commutazione analogici e digitali come i centralini telefonici.
In questa topologia tutte le stazioni sono collegate ad un punto comune.



È bene illustrare i vantaggi e gli svantaggi di questo tipo di LAN in maniera tale da renderci conto dell'efficacia o meno di una soluzione del genere.
Vantaggi:

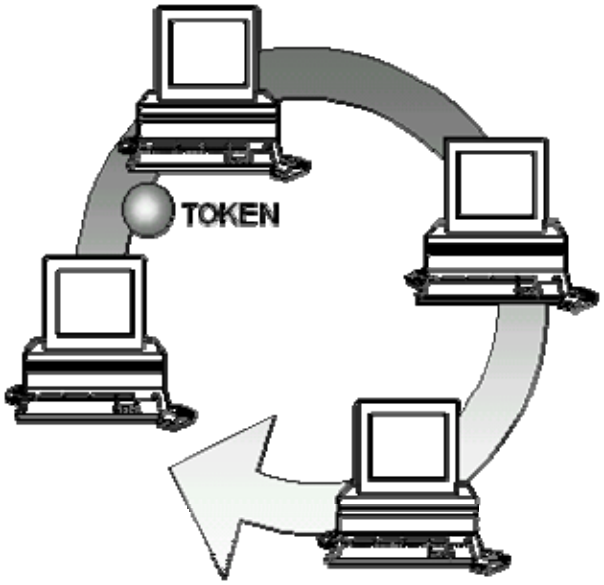
- Prestazioni superiori;
- Maggiore semplicità di protocollo;
- Maggiore facilità di controllo;
- In caso di guasto su un singolo punto non si compromette il funzionamento di tutto il sistema;
- Migliore gestione della rete.

Svantaggi:

- Possibilità di sovraccarico del sistema centrale;
- Dipendenza dell'affidabilità al sistema centrale;
- Notevole lunghezza e complessità dei cavi;
- Nessuna condivisione.

Topologia ad anello

Tutte le stazioni sono considerate attive e quindi dei veri e propri rigeneratori di segnale (possiamo immaginarli come degli amplificatori).
Ciascuna stazione riceve i dati da un'estremità del ripetitore, i dati vengono trasmessi in una sola direzione e ricevuti dal successivo ripetitore dell'anello.



Anche per questa opportuno analizzare vantaggi e svantaggi.
Vantaggi:

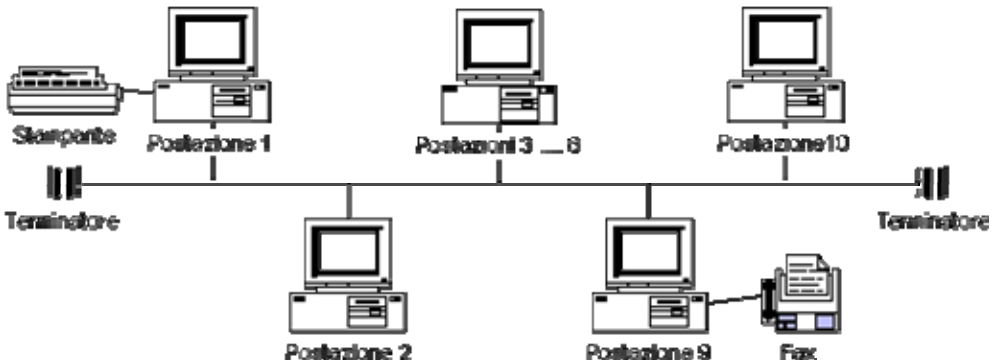
- Velocità elevata;
- Tutte le stazioni sono attive;
- Si possono creare anelli di km purché le stazioni siano vicine perché il segnale viene rigenerato di volta in volta;
- Se implementato con fibra ottica la velocità è enormemente alta.

Svantaggi:

- Ha una limitata flessibilità;
- La lunghezza complessiva del cavo non viene minimizzata;
- L'affidabilità dell'intero sistema è critica in quanto la caduta o il malfunzionamento di una singola stazione può portare alla perdita dell'intera linea;
- L'inserimento di una nuova stazione provoca l'interruzione momentanea dell'intero sistema.

Topologia bus

Ha una struttura semplice e lineare utilizzando un solo tratto di cavo al quale sono collegate le stazioni della rete.
Tutte le stazioni condividono lo stesso cavo e le informazioni vengono ricevute da tutte, le estremità del cavo sono terminate.



Infine anche per questa topologia ci conviene analizzare i suoi vantaggi e svantaggi.
Vantaggi:

- Semplicità;
- Bassi costi di implementazione;
- Affidabilità;
- Se avviene un guasto la rete non viene compromessa;
- Si possono inserire nuove stazioni senza fermare la rete;
- Lunghezza del cavo è minimizzata;
- Sfruttamento delle risorse.

Svantaggi:

- Dipendenza di tutte le stazioni da un unico mezzo trasmissivo condiviso;
- Distanze ridotte perché le stazioni sono passive;
- Metodi di accesso complicati per avere buone prestazioni;
- Velocità limitata.

Riassunto sulle topologie

Adesso che abbiamo analizzato le varie topologie possiamo realizzare una "scheda di valutazione":

CARATTERISTICA	BUS	RING	STAR
AFFIDABILITA'	****	**	**
COMPLESSITA'	****	*	***
ESPANDIBILITA'	****	**	***
SFRUTTAMENTO RISORSE	***	**	***
VELOCITA'	***	****	***
COSTI	****	**	**
DISTANZE	**	****	**
PUNTEGGIO COMPLESSIVO	24	17	18

Come si può ben notare la BUS è la topologia migliore anche se non possiamo dire che è la migliore in assoluto perché bisogna sempre far riferimento a cosa si vuole realizzare, quali sono i mezzi e quali gli strumenti disponibili inoltre bisogna anche analizzare il rapporto prezzo prestazioni e prezzo qualità.

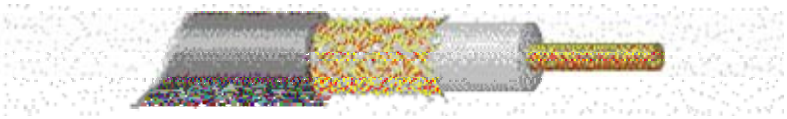
Cablaggio della rete

Una delle caratteristiche fondamentali di una rete è rappresentata dal mezzo trasmissivo impiegato per il trasferimento dell'informazione. Molti sono i tipi di mezzo trasmissivo utilizzato in una LAN. In alcuni casi una rete utilizzerà un solo tipo di cavo, in altri casi vengono usati diversi tipi di cavo. La scelta del cavo è correlata alla topologia, al protocollo e all'estensione della rete.
Ecco una lista di cablaggi esistenti per una rete LAN:

Cavo THINNET Coassiale

Diametro: 1/4 di pollice
Massima lunghezza (prima dell'attenuazione): 185 metri.
Tipo: Famiglia degli RG-58
Impedenza: 50 ohm

Il cavo coassiale ha al suo centro un singolo conduttore di rame. Poi troviamo uno strato di plastica per garantisce l'isolamento tra il centro del conduttore ed uno schermo di metallo intrecciato. Lo schermo di metallo aiuta a bloccare qualsiasi interferenza esterna.



Il cavo coassiale, simile al cavo che trasporta i segnali radio e TV su lunghe distanze, fu adattato alla comunicazione di dati digitali. I dati digitali sono molto più suscettibili rispetto ai dati analogici al rumore e alle distorsioni di segnale che vengono introdotte quando i segnali viaggiano su grandi distanze. A causa di questo fatto le reti che usano come mezzo trasmissivo il cavo coassiale possono estendersi solo per distanze limitate a meno che non vengano utilizzati dei ripetitori di segnale che rigenerano il segnale periodicamente (repeater) altrimenti il segnale influenzato da perdite e rumore risulterebbe abbastanza alterato al ricevitore. Semplici amplificatori non sarebbero sufficienti perché questi amplificherebbero il rumore e la distorsione che il segnale raccoglie mentre viaggia sul mezzo.

Per molto tempo il cavo coassiale è stata la sola scelta economica da usare nella cablatura di reti locali ad alta velocità. Gli svantaggi di installare e mantenere un sistema in cavo coassiale includono il fatto che il cavo è difficile e costoso da fabbricare, è difficile da utilizzare in spazi confinati, in quanto non può essere piegato troppo intorno ad angoli stretti, ed è soggetto a frequenti rotture meccaniche ai connettori. Va però segnalato che è altamente resistente all'interferenza del segnale.

Esiste più di un tipo di Thinnet:

Tipo di Thinnet	**Descrizione / Utilizzo**
RG-58 /U	Cavo in Rame pieno
RG-58 A/U	Cavo a Fili Intrecciati
RG-58 C/U	Specifica Militare del RG-58 A/U
RG-59	Cavo per trasmissioni a Banda Larga, usato anche per antenna TV
RG-62	Cablaggio per reti ArcNet
RG-6	Come l'RG-59 ma con un diametro superiore.

Cavo THICKNET Coassiale

Diametro: 1/2 di pollice
Massima lunghezza (prima dell'attenuazione): 500 metri.

Il cavo thicknet coassiale funziona in modo identico al fratello thinnet varia solo nella dimensione.

UTP (Unshielded Twisted Pair)

Tipo di cavo che può trasmettere fino a 100 metri. E' unshielded, cioè non protetto dalle interferenze elettro-magnetiche.

Il twisted pair è un doppino telefonico particolare (di categoria 5). Il doppino telefonico puro, utilizzato in passato, non è più adatto per le nuove tecnologie: ora esiste il doppino TP, testato fino a 100 Mhz, che garantisce velocità dell'ordine dei 100 Mbps (se di categoria 5). Il twisted pair può essere schermato (STP, Shielded Twisted Pair) o non schermato (UTP, Unshielded Twisted Pair).

Il TP è un mezzo trasmissivo generalizzato: su questo mezzo passa infatti sia traffico digitale che traffico telefonico classico (analogico).

Mentre il cavo coassiale permette cablaggi a catena con il TP sono possibili solo situazioni punto a punto; infatti la topologia di rete che utilizza come mezzo trasmissivo il TP è la topologia a stella.

L'UTP è oggi il più popolare tipo di cablatura usato nelle reti locali, viene infatti usato nella maggioranza delle reti Ethernet come pure nelle Token Ring.

Il cavo UTP è composto da quattro coppie di fili contenuti in un rivestimento isolante. Ogni coppia è intrecciata per eliminare l'interferenza proveniente dalle altre coppie e da altre apparecchiature elettriche.

STP (Shielded Twisted Pair)

Ha le stesse caratteristiche dell'UTP con la sola differenza che l'STP è protetto (shielded) da interferenze elettro-magnetiche.

La tabella seguente mostra le velocità dei cavi UTP / STP

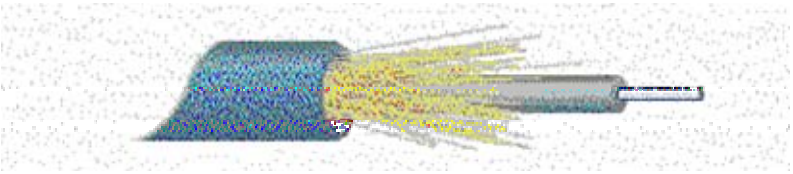
Categoria Velocità massima di trasmissione dati

Categoria	**Velocità**
Categoria 1	Solo per uso telefonico. (Doppino a 4 fili)
Categoria 2	4 mbps
Categoria 3	10 mbps
Categoria 4	16 mbps
Categoria 5	100 mbps

Fibra-Ottica

E' formato da una coppia di cavi, uno trasmette e l'altro riceve. Il tutto attraverso segnali luminosi al suo interno. La sua velocità varia tra i 100Mbps ai 200.000Mbps. Attualmente è il cavo di connessione più veloce.

Il cavo in fibra ottica per trasportare i dati utilizza segnali luminosi trasmessi sopra una sottile fibra in vetro. Il cavo in fibra ottica consiste infatti di una parte centrale in vetro circondata da parecchi strati di materiali protettivi. Questo cavo trasmette luce anziché segnali elettrici, eliminando così il problema dell'interferenza elettrica; questo lo rende il mezzo trasmissivo ideale in ambienti che hanno un'elevata interferenza elettrica. Il cavo in fibra ottica ha la capacità di trasmettere segnali su distanze maggiori rispetto al cavo coassiale e al twisted pair, ed inoltre consente di trasferire l'informazione a velocità più elevate.



Riassumendo i cavi in fibra ottica offrono rispetto agli altri mezzi una velocità di trasmissione più elevata, una maggiore affidabilità e si estendono su più grandi distanze.

La fibra ottica viene utilizzata come dorsale perché è un mezzo trasmissivo che offre velocità superiori al TP; pertanto anche se si utilizza come mezzo trasmissivo predominante il twisted pair le dorsali (per esempio il collegamento tra un Hub e un router) si continuerà a farle in fibra ottica.

Il collegamento in fibra ottica va sempre fatto punto a punto per cui una rete locale in fibra ottica è fatta in configurazione stellata.

Wireless LAN (WLAN)

Oggi inoltre esiste un nuovo tipo di LAN: la LAN wireless utilizzate generalmente per far comunicare i computer usando segnali radio ad alta frequenza o raggi di luce infrarossa.
Ogni computer deve avere un dispositivo che permette di spedire e ricevere i dati.
Le reti wireless sono adatte per consentire a computer portatili o a computer remoti di connettersi alla LAN. Sono inoltre utili negli edifici più vecchi dove può essere difficoltoso o impossibile installare i cavi. Le reti wireless hanno però alcuni svantaggi: sono molto costose, garantiscono poca sicurezza, sono suscettibili all'interferenza elettrica della luce e delle onde radio e sono più lente delle LAN che utilizzano la cablatura.

Ma nello specifico che cos'è una rete WLAN?
La WLAN è un tipo di rete locale basata su trasmissioni radio ad alte frequenze, che permette di evitare l'utilizzo dei cavi tradizionali: è un sistema molto flessibile che può essere integrato con le tipiche reti via cavo. Le WLAN operano a frequenze di 2.4GHz.

Ma se entriamo nello specifico quali benefici possiamo riscontrare nell'utilizzo di una rete WLAN? Innanzitutto più produttività e una totale libertà di spostarsi all'interno delle varie zone dei propri uffici potendo accedere sempre al server o a Internet. Un'installazione semplice e veloce, non ci sono più cavi da collegare. I costi di impianto sono molto ridotti.

Per quanto riguarda la sicurezza invece questo tipo di LAN è estremamente sicura perché deriva da applicazioni militari e questo la rende tecnicamente più sicura di una rete via cavo, in più utilizzano il sistema di trasmissione DSSS (Direct Sequence Spread Spectrum) che rende il segnale radio molto stabile, privo di interferenze e praticamente impossibile da intercettare.
Se invece vogliamo parlare della portata fisica gli apparecchi wireless lavorano su radio frequenze e per questo il loro propagarsi dipende in larga misura dall'ambiente in cui si trovano. Come si apprende spesso leggendo le caratteristiche degli apparecchi radiotrasmittenti, la loro portata

aumenta o diminuisce a seconda che ci si trovi in spazi aperti (un campus universitario) o in spazi chiusi (un ufficio). Gli apparecchi wireless di molti costruttori arrivano a distanze dell'ordine di 150 metri, al massimo delle prestazioni (~10 Mbps), ma installando più Access Point, questa distanza può essere incrementata.
Abbiamo appena nominato un dispositivo chiamato Access Point ma che cos'è?

L'Access point è il ponte di comunicazione tra le periferiche wireless ed eventualmente anche tra una rete wireless e una via cavo. Ogni Access Point aggiuntivo vi permette di estendere il raggio di copertura della vostra WLAN. Gli utenti potranno spostarsi all'interno dell'azienda senza perdere la connessione.
L'Access Point è chiaramente parte integrante della WLAN e per ciò è sempre richiesto, salvo nel caso di un collegamento "peer-to-peer" (così come nelle LAN tradizionali si possono collegare massimo due periferiche con un cavo diretto senza un HUB), ma in tutti gli altri casi il cuore della WLAN rimane l'Access point, sempre consigliato, anche nelle soluzioni peer-to-peer per regolare e ottimizzare il traffico, nonché per creare una porta di accesso a Internet. Il numero degli utenti per una WLAN è teoricamente illimitato poiché può essere ampliato semplicemente aggiungendo ulteriori Access Point e anche diversificando i canali di trasmissione se aumentano gli utenti, ma gli spazi rimangono invariati; fino a 3 canali contemporanei viene garantita la totale assenza di interferenze. Il numero di utenti che un singolo Access point può supportare contemporaneamente dipende dal traffico che si genera.
Poiché la banda disponibile viene condivisa tra gli utenti, così come avviene per le tradizionali.
Per quanto riguarda invece le interferenze tuttavia trattandosi di apparecchi radio vi è sempre la possibilità che vi siano delle interferenze esterne (telefoni portatili, forni a microonde, telecomandi, etc.).
Molti produttori prevedono queste possibilità in fase di progettazione prendendo adeguate misure perché queste interferenze non si verifichino cercando di salvaguardare l'affidabilità di questa rete.

Tecniche di accesso alla LAN

Qunado parliamo di tecnica di accesso ad una rete intendiamo l'algoritmo con il quale la stazione ottiene il diritto a trasmettere.

Esistono due tipi di algoritmi, quelli a contesa e quelli senza contesa:

A contesa (casuale)
- CSMA/CD
- CSMA/CA
- ALOHA
- ALOHA "SLOTTED"

Senza contesa (deterministico)
- TOKEN PASSING
- SLOTTED RINK
- REGISTER INSERTION

In particolare ci soffermeremo sul Token Passing, sul CSMA/CD e sull'Aloha.

Token passing

E' una tecnica non a contesa conveniente soprattutto per le reti ad anello. Ogni stazione riceve a turno dalla stazione che la precede secondo il senso di trasmissione un messaggio particolare, detto TOKEN. Esso comporta l'autorizzazione a trasmettere. Esaurito il diritto a trasmettere il token deve essere ceduto alla stazione successiva, determinando quindi uno schema di assegnazione del diritto alla trasmissione di tipo non preferenziale ed egualmente distribuito.
Quando una stazione deve trasmettere aspetta che il gettone passi da lei, se questo è libero ci scive sopra i suoi dati e lo mette in stato BUSY, quando il gettone arriva alla stazione destinataria questa preleva i dati e mette nel gettone il "COPIED BIT", quando il gettone ritorna dal trasmittente questo lo rimette nello stato "FREE", così che possa trasmettere un'altra stazione.

CSMA/CD (Collision Detect)

Questa tecnica è un miglioramento della ALOHA, in quanto prima di trasmettere ascolta se vi è già una trasmissione in corso, e trasmette solo in caso negativo; durante la trasmissione continua a controllare quanto avviene sul cavo e si interrompe appena rileva una collisione. Il messaggio inviato raggiunge tutte le staioni ma viene memorizzato solo dal destinatario. Inoltre bisogna tenere conto della durata della finestra di collisione, siccome prima di raggiungere un'altra stazione il segnale impiega un certo tempo se una di queste controlla il canale prima che questo messaggio sia passato, lei pensa che il canale sia libero e perciò trasmette effettuando così una collissione. Quindi la finestra di collisione non è nient'altro che il periodo minimo che un messaggio impiega ad arrivare.

Schema a contesa Aloha

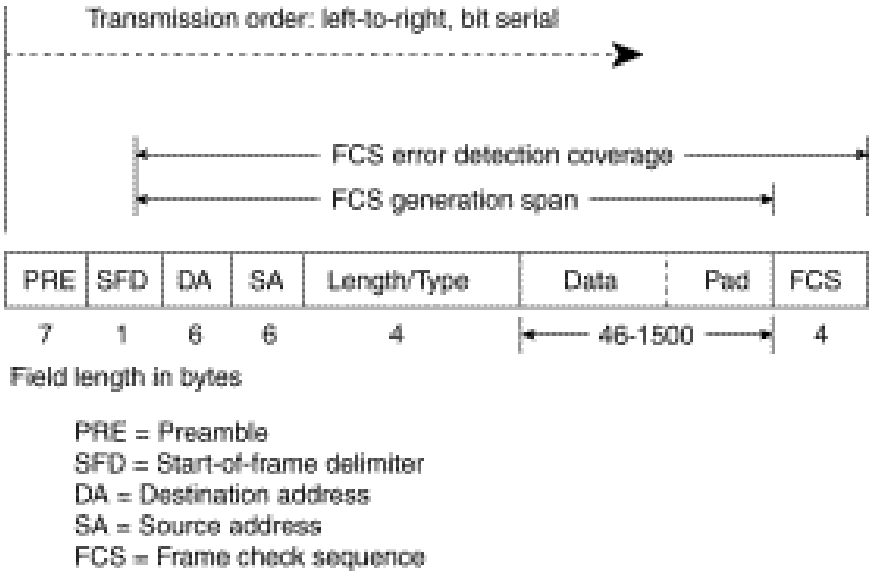
I dati vengono inviati sulle frequenze UHF utilizzando lo schema a pacchetti, secondo il quale la loro lunghezza è predefinita.
Appena una stazione deve trasmettere un messaggio questa lo invia sulla linea, se un'altra stazione ha inviato anche le i un messaggio si avrà una contesa. Non ricevendo entro il tempo prefissato la risposta di avvenuta ricezione da parte dei rispettivi destinatari le stazioni si accorgono di quanto è accaduto, in tal caso ognuna delle due stazioni attende un periodo casuale prima di riinviare il

messaggio. Problema diquesto metodo è che la contesa genera a sua volta altra contesa, facendo collassare la rete.

Formato trame

All'inizio avevamo parlato dei livelli OSI e avevamo detto che nel nostro caso il livello 2 era importante in una rete LAN; ora abbiamo parlato delle tecniche di accesso al mezzo; ma realmente i dati che si vogliono inviare in che formato sono?

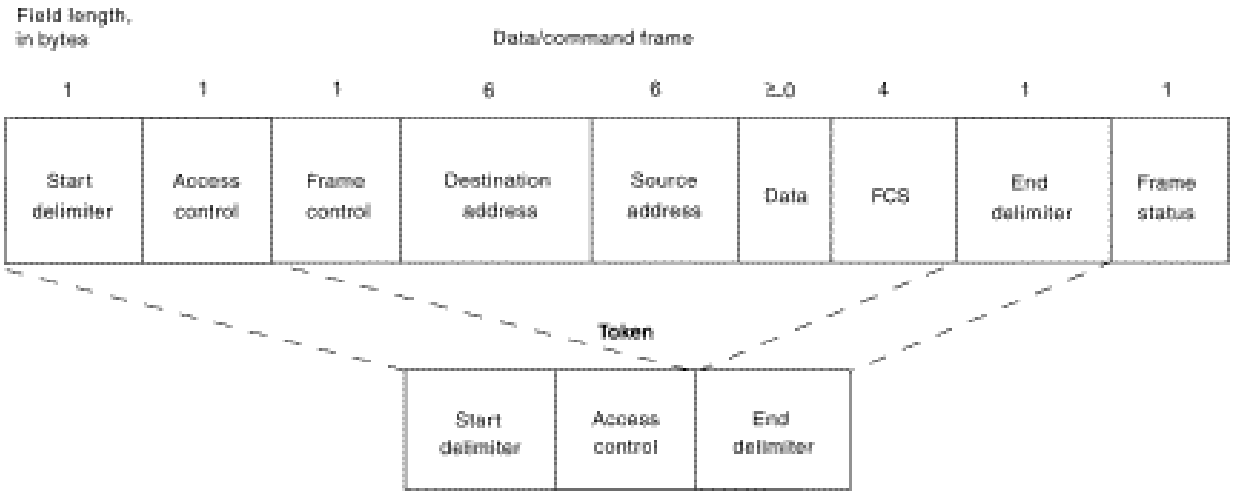
Trama MAC del CSMA/CD



- **Preamble (PRE)**—(7 bytes). Il PRE è un modello che contiene una sequenza di uni e di zeri che dicono alle stazioni riceventi che una trama sta arrivando, questo serve per sincronizzare la trama-ricevente.
- **Start-of-frame delimiter (SOF)**—(1 byte). Il SOF è un modello che avvicenda di uni e zeri e finisce con due bit a 1 consecutivi indicando che il prossimo pezzo è il bit più sinistro nel byte più sinistro dell'indirizzo della destinazione.
- **Destination address (DA)**—(6 bytes). Il campo di DA identifica quale stazione riceverebbe la cornice. Il bit più sinistro nel campo di DA indica se l'indirizzo è un indirizzo individuale (indicandolo con uno 0) o un indirizzo di gruppo (indicandolo con un 1). Il secondo bit dalla sinistra indica se il DA è amministrato globalmente (indicandolo con uno 0) o localmente amministrato (indicandolo con un 1). I rimanenti 46 bit sono un valore unicamente assegnato che identifica una singola stazione, un gruppo definito di stazioni o tutte le stazioni della rete.
- **Source addresses (SA)**—(6 bytes). Il campo di SA identifica la stazione che invia. Il SA sempre è un indirizzo individuale e il bit più sinistro nel campo di SA sempre è 0.
- **Length/Type**—(4 bytes). Questo campo o indica il numero di byte di dati del MAC-client che sono contenuti nel campo dei dati della frame, o la type-ID della finestra se la cornice che usa una configurazione opzionale è assemblata. Se i campi Length/Type sono meno o uguali a 1500, il numero dei byte di LLC nel campo dei Dati è uguale al valore del campo Length/Type. Se i Length/Type sono di valore più grande a 1536, la cornice è una cornice del tipo opzionale, e i Length/Type identificando il particolare tipo di cornice che è spedita o ricevuta.
- **Data**—(*n* bytes). N è meno o uguale a 1500. Se la lunghezza del campo dei Dati è meno che 46, il campo dei Dati deve essere esteso aggiungendo un riempimento (un blocco) sufficiente per portare la lunghezza del campo dati a 46 byte.

- **Frame check sequence (FCS)**—(4 bytes). Questa sequenza contiene 32-bit di controllo ciclio della ridondanza (CRC) valore che è creato dal MAC che spedisce ed è ricalcolato dal MAC ricevente per controllare se la finestra è corrotta. Il FCS è generato sul DA, SA, Length/Type, e i campi dei Dati.

Trama MAC del TOKEN-RING



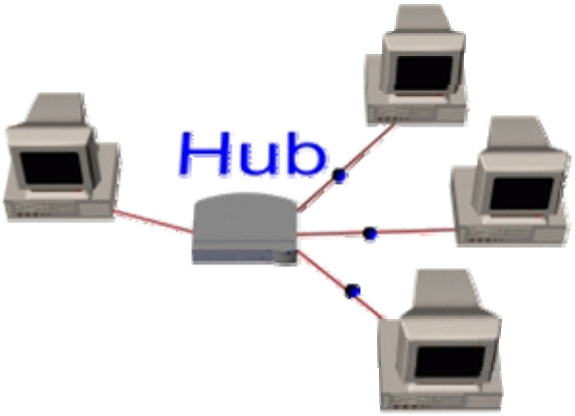
- **Start delimiter**— Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte**— Contiene il campo Prioritario (i 3 bit più significativi) e il campo della Prenotazione (i 3 bit più significativi), così come un bit del gettone (rendeva differente un gettone da una cornice del data/command) e un bit di monitor (usato dal monitor attivo per determinare se una cornice sta circondando l'anello).
- **End delimiter**— Segnala la fine del gettone o cornice del data/command. Questo campo contiene anche bit per indicare se una cornice è danneggiata e per identificare la cornice che è l'ultima in una sequenza logica.

- **Frame-control bytes**— Indica se la cornice contiene dati o informazioni del controllo. In cornici del controllo, questo byte specifica il tipo di informazioni del controllo.
- **Destination and source addresses**— Consiste in due campi dell'indirizzo a 6-byte identificando la destinazione e gli indirizzi della stazione di origine.
- **Data**— Indica che la lunghezza del campo è limitata dal gettone dell'anello che definisce il tempo massimo in cui una stazione può tenere il gettone.
- **Frame-check sequence (FCS)**— È archiviato dalla stazione d'origine con un valore calcolato dipendente dai contenuti della cornice. La nstazione di destinazione ricalcolerà il valore per determinare se la cornice era danneggiata. In tal caso, la cornice è scartata.
- **Frame Status**— È un campo di 1 byte che termina una cornice del command/data. Il Frame Status include l'indicatore dell'indirizzo riconosciuto e l'indicatore della trama copiata.

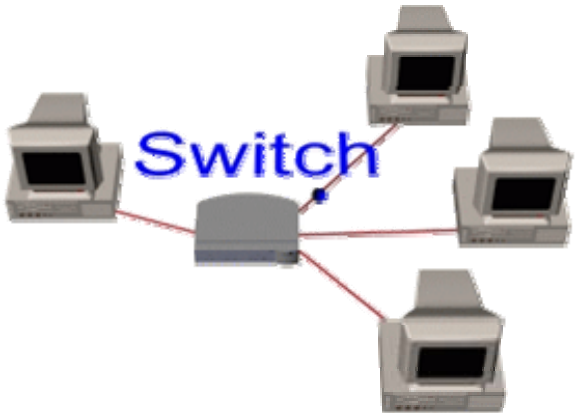
HUB e SWITCH

Abbiamo parlato delle varie topologie delle LAN e del cablaggio di rete; ma per realizzare il collegamento tra i vari pc avremo bisogno di dispositivi appositi che permettano di collegare insieme più calcolatori realizzando la nostra rete LAN; questi dispositivi sono detti HUB e SWITCH.

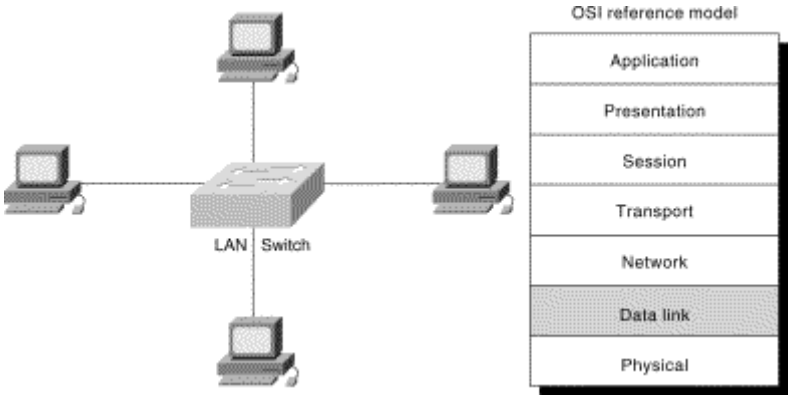
Gli HUB si differiscono dagli SWITCH per il modo in cui avviene la trasmissione del traffico di rete infatti con un HUB quando due stazioni “parlano” tra loro l’intera banda viene occupata mentre con uno SWITCH la banda viene divisa in sottobande.
Con il termine "HUB" ci si riferisce a volte ad un componente dell'apparecchiatura di rete che collega assieme i PC, ma che in effetti funge da ripetitore, questo perché trasmette o ripete tutte le informazioni che riceve, a tutte le porte.
Gli HUB possono essere usati per estendere una rete. Tuttavia ciò può produrre una grande quantità di traffico superfluo, poiché le stesse informazioni vengono inviate a tutti i dispositivi di una rete.



Gli SWITCH si avvalgono degli indirizzi di ciascun pacchetto per gestire il flusso del traffico di rete. Monitorando i pacchetti che riceve, uno SWITCH "impara" a riconoscere i dispositivi che sono collegati alle proprie porte per poi inviare i pacchetti solamente alle porte pertinenti (divisione della banda in sottobande).
Lo SWITCH riduce la quantità di traffico non necessario, dato che le informazioni ricevute nella porta vengono trasmesse solo al dispositivo con il giusto indirizzo di destinazione, e non come negli hub, a tutte le porte.



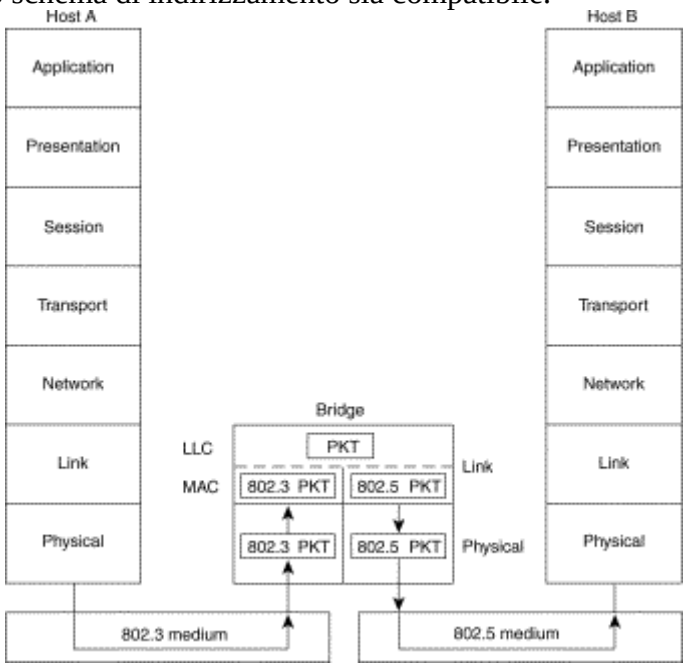
Gli SWITCH e gli HUB vengono spesso utilizzati nella stessa rete. Gli HUB ampliano la rete fornendo un numero maggiore di porte, mentre gli SWITCH dividono la rete in sezioni più piccole e meno congestionate.



In una piccola rete, gli HUB sono all'altezza del traffico di rete generato. Generalmente quando la rete raggiunge i 25 utenti, occorre eliminare il traffico non necessario. A tal fine, uno SWITCH adatto suddivide la rete.

BRIDGE

Il BRIDGE è un dispositivo con il compito di interconnettere più LAN tra loro anche di topologie diverse patto che il loro schema di indirizzamento sia compatibile.



Il BRIDGE mette in connessione due (o più) reti limitandosi a intervenire nei primi due livelli del modello OSI/ISO. Di conseguenza, il BRIDGE è in grado di connettere tra loro solo reti fisiche dello stesso tipo.
In altri termini, si può dire che il BRIDGE sia in grado di connettere reti separate che hanno uno schema di indirizzamento compatibile.
Il BRIDGE più semplice duplica ogni pacchetto, del secondo livello OSI/ISO, nelle altre reti a cui è connesso; il BRIDGE più sofisticato è in grado di determinare gli indirizzi dei nodi connessi nelle varie reti, in modo da trasferire solo i pacchetti che necessitano questo attraversamento.
Dal momento che il BRIDGE opera al secondo livello OSI/ISO, non è in grado di distinguere i pacchetti in base ai protocolli di rete del terzo livello (TCP/IP, IPX/SPX, ...), e quindi trasferisce indifferentemente tali pacchetti.
Teoricamente, possono esistere BRIDGE in grado di gestire connessioni con collegamenti ridondanti, in modo da determinare automaticamente l'itinerario migliore per i pacchetti e da bilanciare il carico di utilizzo tra diverse connessioni alternative. Tuttavia, questo compito viene svolto preferibilmente dai router.

ROUTER

Il ROUTER mette in connessione due (o più) reti intervenendo al terzo livello del modello OSI/ISO. Di conseguenza, il ROUTER è in grado di trasferire solo i pacchetti di un determinato tipo di protocollo di rete (TCP/IP, IPX/SPX...), indipendentemente dal tipo di reti fisiche effettivamente connesse. In altri termini, si può dire che il ROUTER sia in grado di connettere reti separate che hanno schemi di indirizzamento differenti, ma che utilizzano lo stesso tipo di protocollo di rete al terzo livello OSI/ISO.
L'instradamento dei pacchetti attraverso le reti connesse al router avviene in base a una tabella di instradamento che può anche essere determinata in modo dinamico, in presenza di connessioni ridondanti, come già accennato per il caso dei bridge.

Un ROUTER permette di convertire i protocolli (solo i primi tre livelli)e permette così di passare da una LAN ad una WAN.
Se vogliamo convertire tutti e sette i livelli dovremo utilizzare un GATEWAY.

Bibliografia

Le informazioni raccolte in questa dispensa sono state prelevate da varie fonti:

- Reti Locali- Matthew G. Naugle
- www.tuttoreti.it
- www.cisco.com
- Spiegazione in classe prof. Paolo Macchi
- www.bcentral.it