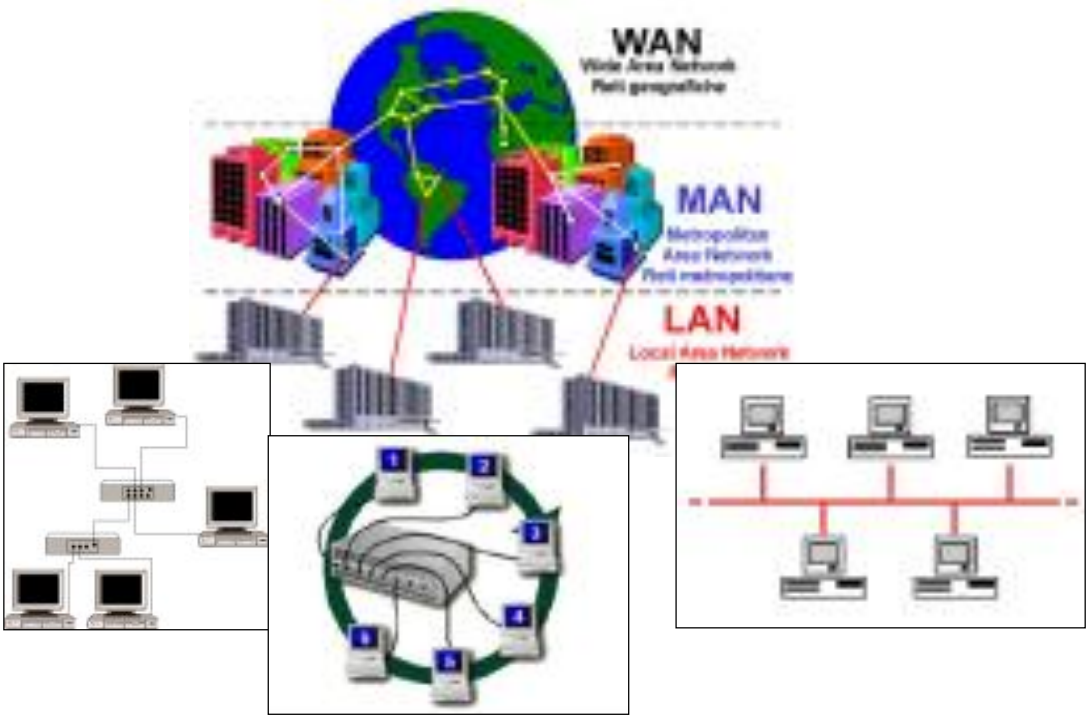
LE RETI



LA TELEMATICA

Definizione (*da Wikipedia.org)*

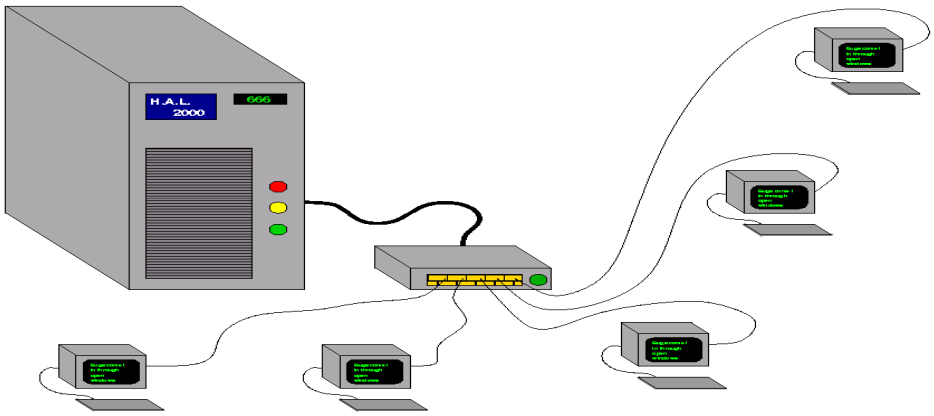
"Il termine **telematica** è spesso usato come sinonimo di *teleinformatica* ad indicare metodologie e tecniche delle telecomunicazioni e dell'informatica associate per realizzare l'elaborazione a distanza delle informazioni." (*da wikipedia.org*)

Si tratta quindi di un settore dell'informatica che si occupa dell'integrazione tra tecnologie dell'informazione e tecnologie delle telecomunicazioni.

Un po' di storia….

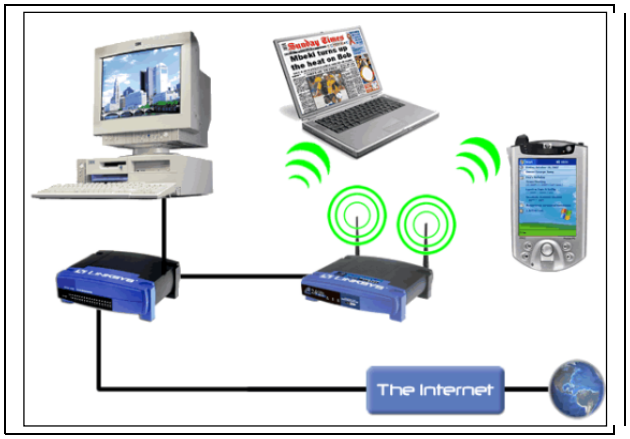
Parlando di telematica occorre fare una distinzione tra
- *sistemi di elaborazione centralizzati*
- *sistemi di elaborazione distribuiti*

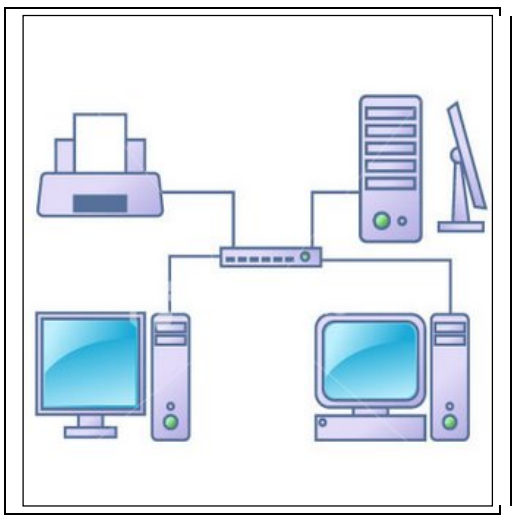
SISTEMI CENTRALIZZATI
Quando si utilizzano *sistemi centralizzati*, parecchi utenti (locali o remoti) sono collegati ad un unico calcolatore centralizzato in cui risiede tutta la potenza elaborativa.



Problemi: un guasto al sistema blocca il lavoro di tutti gli utenti; non c'è autonomia di elaborazione.

SISTEMI DISTRIBUTI
Con i *sistemi distribuiti* siamo in presenza di un insieme di elaboratori, collegati tra loro attraverso una rete, che condividono risorse (hardware e/o software); si parla di *rete di computer*.





VANTAGGI DI UN AMBIENTE DI RETE

Una rete di telecomunicazioni fra calcolatori permette:

1. lo **scambio di informazioni** fra gli utenti dei calcolatori stessi, come e-mail , dati, documenti immagini, eccetera…

2. **condividere le risorse** di un calcolatore con tutti gli altri nella rete.

Tramite una rete di calcolatori è possibile avere accesso a risorse, siano esse di elaborazione, di memorizzazione, di stampa che altrimenti potrebbero non essere disponibili per tutti, per ragioni di costo o di complessità.
La rete di calcolatori può quindi essere vista come una sorta di calcolatore esteso che, tramite le funzioni di comunicazione, fa, di un insieme di calcolatori isolati, un sistema integrato che rende disponibili una serie di risorse ad una più vasta popolazione di utenti.
Oltre alla condivisione delle risorse, tra gli altri vantaggi che una rete di computer offre rispetto a un sistema centralizzato, possiamo elencare:

- **migliore rapporto costo/prestazioni**: rispetto ai sistemi centralizzati, i piccoli sistemi collegati in rete offrono un basso costo dell'hardware, con lo stesso numero di utenti, una velocità di utilizzo superiore, in quanto ogni utente non condivide in modo significativo l'hardware, ma principalmente i dati (e talvolta i programmi);
- **facilità di espansione del sistema**: ogni sistema può essere configurato ed espanso a seconda delle esigenze specifiche dell'azienda e quindi con hardware differenti ed in tempi differenti, dando la possibilità di investire risorse economiche in modo mirato; è possibile inoltre aumentare le prestazioni del sistema, aumentando il numero di elaboratori (**scalabilità**);
- **maggiore affidabilità del sistema**: con l'uso di componenti hardware e software tolleranti ai guasti (**fault tolerance**) il guasto di un personal computer non blocca il lavoro degli altri;
- **maggiori vantaggi organizzativi**; un operatore che viaggia dotato di terminale portatile può svolgere le sue mansioni ovunque ci sia un collegamento in rete alla propria azienda.

SICUREZZA IN UN AMBIENTE DI RETE

Una rete di calcolatori, oltre ad offrire i vantaggi descritti precedentemente, pone un importante problema legato alla sicurezza del sistema informatico.

Le problematiche di sicurezza tipiche sono:

1. Riservatezza della comunicazione

2. Mantenimento dell'integrità dei servizi.

Per quanto riguarda la riservatezza della comunicazione, è necessario evitare:

- che i dati relativi ad una particolare comunicazione fra calcolatori possano essere intercettati e letti, in quanto questi dati possono essere di tipo sensibile (password, dati personali, numero di carta di credito, eccetera);
- che un calcolatore possa comportarsi in modo malevole prendendo il posto di un altro calcolatore, sostituendosi ad esso nella comunicazione con altri al fine di appropriarsi di dati sensibili o per l'uso di servizi a lui non permessi.

Per quanto riguarda l'integrità dei servizi:

- è necessario garantirsi dall'eventualità che utenti malevoli, utilizzando la rete di calcolatori possano interferire con il normale funzionamento di sistemi server.

Un esempio di questo tipo, che ha avuto particolare rilevanza anche sulla stampa, è relativo agli attacchi ai server Internet di grandi enti, non avente lo scopo di attentare alla sicurezza dei dati, ma semplicemente di interferire con il normale funzionamento dei server (rendere impossibile l'uso della posta elettronica o dei server Web, eccetera).

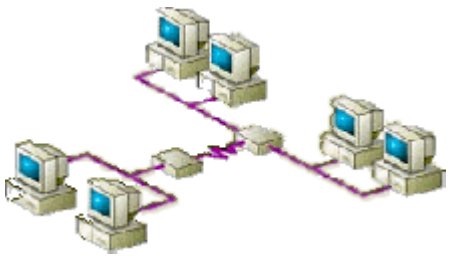
STRUTTURA DI UNA RETE DI CALCOLATORI

Una rete di telecomunicazioni di calcolatori è un sistema che si compone di:

a) apparati **terminali** con cui si interfaccia direttamente l'utente finale ;

b) **linee di collegamento** che permettono fisicamente la trasmissione a distanza delle informazioni sotto forma di segnali elettromagnetici;

c) **nodi di rete** che svolgono le funzioni necessarie a garantire il corretto trasferimento delle informazioni all'interno della rete .



Oltre alla parte Hardware una rete è dotata anche di una componente Software, si parla di Sistema Operativo di rete (NOS Network Operating System).

Tale software di base è in grado di mettere a disposizione, e gestire, la condivisione delle risorse di rete, intendendo come risorse quanto messo a disposizione dal sistema informativo nel suo complesso (stampanti, file server, db server, …).

Ne esistono diversi e sono sempre costruiti in relazione stretta con il S.O. della macchina ospitante (es. WinNT Server).

AMBIENTI CLIENT/SERVER

Nelle reti di calcolatori fino ad oggi si è sempre utilizzata una comunicazione di tipo client/server.
Con questi termini si intende che alcuni calcolatori ben identificabili, detti **server**, mettono a disposizione informazioni e servizi a cui altri calcolatori della rete, detti **client**, accedono con modalità opportune.

Un tipico esempio è il **WWW** in cui i server mettono a disposizione dei client pagine di testo, immagini, eccetera, che siano reperibili e visualizzabili tramite i normali **browser** (Internet Explorer, Netscape, Opera, eccetera).
Questo modello di dialogo è di tipo asimmetrico nel senso che i due soggetti partecipanti alla comunicazione svolgono funzioni diverse: il server mette a disposizione le informazioni, il client le reperisce e le rende consultabili localmente dall'utente.

In una rete Client/Server:

- è possibile **controllare gli accessi,** nel senso che è possibile regolamentare l'accesso di computer stand-alone attraverso la creazione di appositi profili utente in ciascuna postazione; sul server viene memorizzata la lista degli utenti e le relative autorizzazioni;
- è possibile **pianificare le attività,** è quindi possibile stabilite gli orridi accesso di ogni singolo utente o gruppi di utenti, concedere ad essi particolari permessi (es. se e quando connettersi a Internet) e in genere l'uso delle risorse;
- è possibile **ottimizzare la gestione dei sistemi e del software;** sui computer stand-alone, eventuali crash possono rendere necessarie reinstallazioni sia del sistema operativo che di tutto il software; con una rete Client/Server è possibile creare immagini degli hard-disk dei client, in modo che il ripristino completo possa avvenire in pochi minuti; allo stesso modo è possibile effettuare l'installazione remota di nuovo software (**deploying**).

AMBIENTI PEER-TO-PEER (RETI PARITETICHE)

Il server smette di esistere e tutti i calcolatori connessi alla rete possono contemporaneamente agire come server e/o come client.
Nel dialogo peer-to-peer si perde quindi la nozione di server e tutti i calcolatori possono allo stesso tempo rendere disponibili informazioni e reperirne dagli altri.
In questo caso esistono ancora alcuni calcolatori che svolgono funzione di server solamente per le funzioni di centralizzazione degli indici di informazioni disponibili.
Tramite questi indici i singoli computer possono scoprire chi mette a disposizione certe informazioni sulla rete e collegarsi direttamente a questi per il loro reperimento.

Il dialogo relativo alle informazioni vere e proprie è quindi sempre diretto fra il fornitore ed il fruitore di informazioni senza l'intermediazione di un server.
I server per l'indicizzazione sono necessari in quanto i singoli calcolatori possono collegarsi e scollegarsi alla rete di dialogo.
I singoli calcolatori una volta collegati in rete si connettono a questi server per comunicare quali informazioni loro rendano disponibili e per conoscere quali informazioni siano già disponibili e presso chi.

In una rete Peer-to-Peer:

- non ci sono **server dedicati**;
- tutti i computer possono essere indistintamente client e / o server delle risorse;
- non esistono **amministratori della rete**, ma ogni utente ha il compito di gestire il proprio computer;
- la **sicurezza e l'amministrazione della rete** non sono centralizzate; l'unica sicurezza garantita è la protezione all'accesso fisico del singolo computer;
- la **stabilità della rete** diminuisce velocemente quando il numero dei computer/utenti cresce;
- ci deve essere un **numero limitato di computer.**

TIPOLOGIE DI COLLEGAMENTO

Esistono varie tipologie di collegamenti fra terminali o nodi di una rete:

a) **Punto-punto**: Collega due e solo due nodi senza passare per un nodo intermedio. All'aumentare del numero di nodi una tale rete può diventare complessa per il numero di linee. Si può ovviare a ciò sostituendo i collegamenti fisici con collegamenti logici dotando i nodi della capacità di inoltrare i messaggi.

b) **Punto-multipunto** : Singola linea condivisa da più di due nodi. Vantaggioso per ridurre il numero di linee richieste per il collegamento tra i nodi e quindi ridurre i costi. I nodi collegati ad una linea multipunto devono avere gli strumenti per il controllo dell'accesso alla linea, così da evitare conflitti con gli altri nodi dal momento che la linea è condivisa. La manipolazione dei messaggi avviene tramite gli indirizzi.

TECNOLOGIA TRASMISSIVA

Riguarda la modalità di invio dei dati da parte dei nodi emittenti della rete verso i nodi riceventi.

a) **Unicast** : la trasmissione è unicast quando è inviata da un mittente ed è destinata ad un solo computer ricevente. Vi è una associazione 1 a 1 tra i computer che vogliono comunicare; un nodo trasmette allo stesso tempo ad un sottoinsieme dei nodi della rete.

b) **Broadcast** : Il mittente invia un messaggio che sarà ricevuto da tutti gli altri computer della rete. La comunicazione è uno a molti. Un computer trasmette e tutti ricevono il messaggio.

c) **Multicast** : Il mittente invia un messaggio che sarà ricevuto da un preciso gruppo di computer destinatari, non a tutti quelli della rete. La comunicazione è uno a molti. Un computer trasmette e tutti quelli del gruppo ricevono il messaggio.

DIREZIONE DELLA COMUNICAZIONE

Inoltre su di una linea di collegamento fra i terminali A e B il flusso di informazioni può essere di tipo:

a) **monodirezionale o simplex** : A invia dati a B;

b) **monodirezionale alternato o half duplex** : A invia informazioni a B, quando A "*tace*" B può inviare informazioni ad A e viceversa;

c) **bidirezionale o full duplex** : A e B possono contemporaneamente inviare informazioni all'altro.

TIPO DI SEGNALE: SEGNALE ANALOGICO E DIGITALE

Pensando a oggetti 'analogici' vengono subito in mente la televisione, la radio, le musicassette, i dischi in vinile e in generale tutte le vecchie apparecchiature e i supporti di memorizzazione per contenuti audiovisivi. Molti di questi oggetti sono stati sostituiti recentemente da oggetti 'digitali'. Basti pensare ai CD che hanno sostituito le musicassette e i vinili, i DVD le VHS, la tv digitale (satellitare e terrestre) la televisione tradizionale, le fotocamere digitali le tradizionali macchine fotografiche ecc.
Per rendere immediata la comprensione delle differenze tra i due 'mondi', prendiamo come riferimento per il segnale analogico un orologio a pendolo e per il digitale un orologio digitale appunto che segna ore e minuti.
Possiamo pensare a analogico come *analogo*: analogo al mondo reale. In uno strumento analogico la grandezza misurata è rappresentata per analogia con una certa disposizione dei componenti dello strumento. Così in un orologio analogico, l'ora è rappresentata dall'angolo descritto dalla lancetta corta rispetto a una posizione di riferimento, corrispondente alle ore 12. Si può notare inoltre che la lancetta compie un movimento costante e continuo nel passare da un riferimento ad un altro.

Il termine digitale ha origine dalla parola inglese *digit* cioè cifra. In uno strumento digitale la grandezza misurata è rappresentata da un valore numerico. Le cifre che compongono il numero definiscono la precisione dello strumento, così il nostro orologio è preciso 'al minuto'. Può segnare 14 minuti oppure 15, ma tra 14 e 15 c'è un salto, per questo il segnale digitale viene anche detto discreto: esso può assumere un solo valore possibile tra una gamma limitata.
Solitamente il segnale fatto di numeri viene codificato in formato binario anziché nel solito decimale e questo semplifica molto la trasmissione e l'elaborazione dei dati in quanto esistono solo due stati (1 e lo 0) invece che dieci. In questo caso quello che viene registrato è un'astrazione del segnale reale.

La codifica digitale fu inventata per ovviare ai disturbi che spesso corrompevano i segnali elettromagnetici. Questo rappresenta il grande vantaggio del segnale digitale, essendoci una netta distinzione tra 1 e 0, aperto e chiuso, acceso e spento, non c'è il rischio che una lieve modifica del segnale deteriori i contenuti.
Tra i dispositivi digitali possiamo naturalmente citare il computer in tutte le sue varianti, dalla calcolatrice tascabile al mainframe, mentre la linea telefonica tradizionale è analogica. Per questo sono necessari dispositivi per la trasformazione del segnale da digitale ad analogico (***modulazione***), e viceversa (***demodulazione***).
Tali dispositivi sono detti **MODEM** *(**MO**dulator/**DEM**odulator*).
Un modem può essere una scheda istallata in uno slot interno al computer oppure al di fuori di esso ed è collegato ad un dispositivo di comunicazione seriale o porta COM. Sul mercato ce ne sono di diversi tipi, marche e modelli.
Modem si differenziano gli uni dagli altri in base alla velocità, misurata in baud, con cui trasmettono i dati.

MEZZI DI TRASMISSIONE

Tutti i nodi di una rete devono avere una particolare scheda, la **scheda di rete**, che serve per il collegamento del nodo al canale, o mezzo, fisico.

I mezzi fisici utilizzati per la trasmissione dei dati sono di tre tipi:

a) **mezzi elettrici (cavi)**; si usa l'energia elettrica per trasferire i segnali sul mezzo;

b) **mezzi wireless (onde radio)**; in questo caso si sfruttano onde elettromagnetiche;

c) **mezzi ottici (fibre ottiche)**; con le fibre ottiche si usa la luce.

I parametri prestazionali di questi mezzi sono:

a) **larghezza di banda,** serve per determinare quanti bit al secondo è possibile trasferire;

b) **affidabilità,** ogni mezzo presenta una certa probabilità di errore nella trasmissione;

c) **prestazioni,** determinano la distanza massima in un collegamento;

d) **caratteristiche fisiche,** a seconda del mezzo si usano fenomeni diversi per la trasmissione, occorre perciò sfruttare tecnologie differenti.

I mezzi elettrici più usati sono fondamentalmente il **cavo coassiale** e il **doppino telefonico**.
Il doppino telefonico è il mezzo più vecchio e comune dei due. Consiste di due fili intrecciati ad elica tra loro, e può essere sia schermato (**STP** – Shielded Twisted Pair) che non schermato (**UTP** - Unshielded Twisted Pair).

Il doppino viene utilizzato all'inizio per le connessioni terminali nella telefonia, cioé per quel tratto che va dall'apparecchio alla centrale. Una versione del STP con più avvolgimenti e un migliore isolamento viene usato per il traffico dati su lunghe distanze.

Il cavo coassiale è composto da un conduttore centrale ricoperto di isolante, all'esterno del quale vi è una calza metallica. Il cavo coassiale era usato per lunghe tratte telefoniche ma è stato sostituito dalla fibra ottica, ora rimane in uso per la televisione via cavo e per l'uso in reti locali.

Le fibre ottiche sono costituite da un sottilissimo cilindro centrale in vetro (core), circondato da uno strato di vetro esterno (cladding), con un diverso indice di rifrazione e da una guaina protettiva. Le fibre ottiche sfruttano il principio della deviazione che un raggio di luce subisce quando attraversa il confine fra due materiali diversi (core e cladding nel caso delle fibre).
La deviazione dipende dagli indici di rifrazione dei due materiali. Oltre un certo angolo, il raggio rimane intrappolato all'interno del materiale.
Le fibre ottiche hanno delle prestazioni eccellenti: totale immunità da disturbi elettromagnetici e possono raggiungere velocità di trasmissioni pari a 50.000 Gb/s, ossia 50 terabit al secondo con un bassissimo tasso d'errore.
Le distanze massime per un collegamento di questo tipo sono di circa 30 kilometri, per collegamenti di lunghezza maggiore si introducono ripetitori e amplificatori lungo la tratta.
Le fibre ottiche sono unicamente adatte a collegamenti Punto-Punto, non essendo possibile prelevare o inserire il segnale in un punto intermedio.
La trasmissione senza fili si effettua su diverse lunghezze d'onda, e sono le onde radio, microonde, raggi infrarossi, luce visibile e ultravioletti. Il comportamento di questo mezzo dipende dalla lunghezza d'onda e dalla banda utilizzata, le prestazioni possono variare ampiamente. La trasmissione del segnale che trasporta l'informazione avviene tramite una antenna collegata al calcolatore.

STRATEGIE DI COLLEGAMENTO

Le strategie di collegamento indicano il modo in cui viene stabilito il collegamento tra due nodi che vogliono comunicare.
Una linea è **dedicata** quando può essere utilizzata in esclusiva tra due nodi che vogliono comunicare.
Una linea è **commutata** quando è utilizzata per la comunicazione tra più coppie diverse di elaboratori in esclusiva tra due nodi che vogliono comunicare.

Per un **nodo** della rete, la **commutazione** è il modo secondo cui una qualsiasi linea di ingresso al nodo viene associata logicamente o fisicamente con una qualsiasi linea di uscita.
Lo scopo è di operare uno scambio sul flusso di informazioni dall'ingresso verso l'uscita.
E' possibile operare due diversi tipi di commutazione: **a circuito** e **a pacchetto** .

La commutazione di circuito

La rete crea un **canale** di comunicazione dedicato fra due terminali che vogliono colloquiare detto **circuito**.
Il circuito è riservato ad uso esclusivo dei terminali chiamante e chiamato.
Esiste quindi un ritardo iniziale dovuto al tempo necessario per instaurare il circuito, dopodiché la rete è trasparente per gli utenti ed equivale ad un collegamento fisico diretto.
Si possono quindi evidenziare le seguenti fasi della comunicazione:

a) Instaurazione del circuito: prima che le informazioni di utente possano essere trasmesse la rete deve instaurare un circuito fra terminale chiamante e terminale chiamato tramite un'opportuna fase di segnalazione.
b) Dialogo: i due terminali si scambiano informazioni utilizzando il circuito.
c) Disconnessione del circuito: al termine del dialogo il circuito deve essere rilasciato, al fine di poter essere utilizzato per altre chiamate.

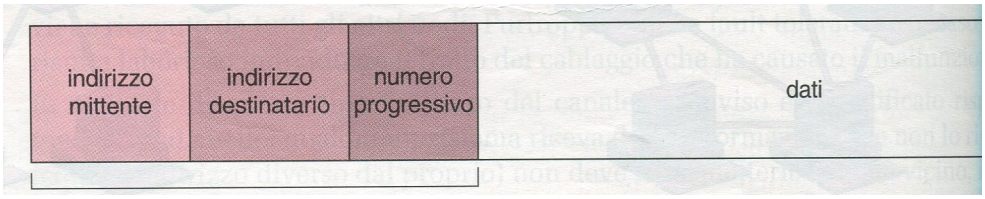
L'esempio tipico di rete a **commutazione di circuito** è la rete telefonica.

La commutazione di pacchetto

Trasporta informazioni in forma numerica. Le informazioni dell'utente sono strutturate in messaggi unitamente ad opportune informazioni di segnalazione quali indirizzamento, verifica della correttezza delle informazioni, eccetera.

Per ragione di opportunità tecnologica Il messaggio è suddiviso in piccoli pacchetti , **datagram**, che vengono messi sul canale e viaggiano nella rete fino a destinazione. Ogni pacchetto informativo è come una entità a se stante ed è formato da un'intestazione (header) e da un campo dati.

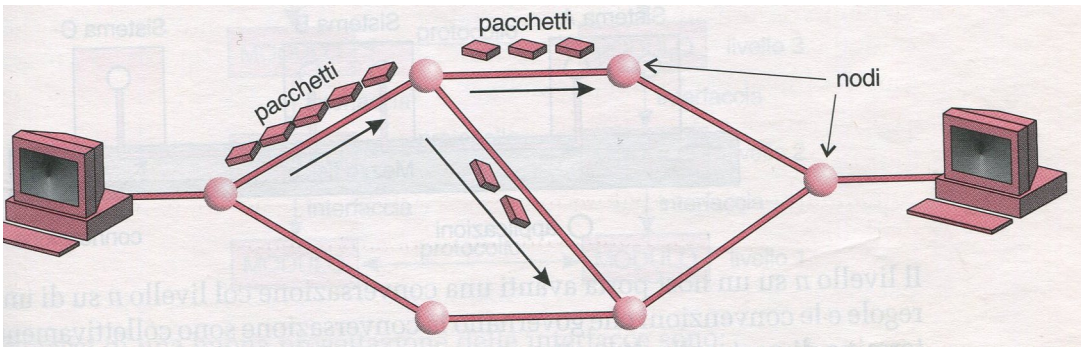
L'intestazione contiene le informazioni di controllo come sorgente, destinazione, numero progressivo del pacchetto nel messaggio.



Ogni nodo decide il percorso migliore per il pacchetto nel momento in cui lo riceve, pertanto è possibile che pacchetti facenti parte dello stesso flusso informativo seguano strade diverse, per poi essere ricostruiti a destinazione. La consegna del messaggio non è garantita perché il percorso dei pacchetti è calcolato dinamicamente quindi i pacchetti possono arrivare a destinazione non nello stesso ordine in cui sono stati inviati. La ricostruzione dell'informazione viene fatta dal nodo destinatario utilizzando il numero di progressivo di pacchetto presente nell'header.

Il mezzo trasmissivo è condiviso da più nodi e la sua capacità è sfruttata al massimo. Questa tecnica è adatta per lo scambio dati fra elaboratori dove c'è la necessità di spedire pacchetti a raffica.

Esempi di reti a commutazione di pacchetto sono tutte le moderne reti di calcolatori, compresa **Internet.**



Vantaggi e svantaggi

La **commutazione di circuito** offre i seguenti vantaggi:

a) il circuito è dedicato e garantisce sicurezza ed affidabilità;
b) il tempo di trasferimento delle informazioni è costante e dipende solamente dalla distanza fra i terminali e dal numero di nodi da attraversare, in quanto la rete è trasparente al dialogo;
c) le procedure di controllo sono limitate ad inizio e fine chiamata.

Al contrario, per le stesse ragioni la commutazione di circuito offre minore flessibilità:

a) la velocità di trasferimento delle informazioni è fissata dalla capacità del circuito e non si può variare se non attivando più circuiti in parallelo;
b) se le sorgenti di informazione hanno un basso tasso di attività il circuito è sottoutilizzato.

A proposito di quest'ultima considerazione prendiamo ad esempio il circuito che collega il nostro telefono a quello del chiamato quando eseguiamo una telefonata: l'utilizzo del circuito è del solo 30-40%. Infatti in termini medi durante una telefonata per metà del tempo parliamo e per l'altra metà ascoltiamo, quindi il non utilizzo del circuito in ciascuna direzione è all'incirca per il 50% del tempo, a cui si aggiungono le normali pause del parlato portando questo valore a oltre il 60%.

La **commutazione di pacchetto** ha i seguenti vantaggi:

a) le linee di collegamento sono condivise in modo dinamico da più chiamate l'efficienza nella loro utilizzazione risulta maggiore;
b) i pacchetti vengono accodati e trasmessi non appena possibile
c) la linea è inutilizzata solo se non ci sono pacchetti da trasmettere
d) non rifiuta mai una connessione
e) è possibile assegnare priorità ai pacchetti

Mentre gli Svantaggi della Commutazione di Pacchetto sono:

a) Difficile garantire qualità del servizio (i pacchetti potrebbero essere ritardati o persi)
b) Vengono introdotti dei carichi aggiuntivi (overhead) in quanto i pacchetti devono viaggiare insieme ad informazioni di controllo per poter essere correttamente istradati
c) La rete può congestionarsi poiché si accettano sempre pacchetti si potrebbe arrivare ad una situazione di saturazione

CLASSIFICAZIONE DELLE RETI IN BASE ALLA DISTANZA

La storia delle reti di telecomunicazioni ha visto nascere diverse soluzioni a problemi di tipo eterogeneo, che vanno dalla necessità di comunicare a grande distanza tramite il telegrafo o il telefono, fino alla possibilità di interconnettere tra loro computer residenti nella stessa stanza o edificio.
Questa diversità di problematiche ha comportato tradizionalmente una classificazione delle reti sulla base della distanza coperta dalle reti stesse:

a) **LAN** - Local Area Network o **reti locali**: tipicamente sono reti private per l'interconnessione di computer ed altri apparati appartenenti ad un unico ente o azienda;

b) **MAN** - Metropolitan Area Network o **reti metropolitane**: possono essere reti private o pubbliche e fornire servizi di vario tipo in ambito urbano, dall'interconnessione di computer, alla telefonia, alla TV via cavo;

c) **WAN** - Wide Area Network o **reti geografiche**: in passato erano le reti dei grandi gestori tipicamente pubblici che fornivano servizi e connettività a livello nazionale; oggi, dopo la deregulation, possono anche appartenere a privati ed offrire connettività a livello mondiale.

La differenza tra questi tre tipi di reti in termini di distanza coperta è rappresentata nella tabella seguente:

Area coperta	**Distanza**	**Tipo di rete**
Stanza	10 metri	LAN
Edificio	100 metri	LAN
Campus	1 KM	LAN
Città	10 KM	MAN
Stato o Nazione	1000 KM	WAN
Continente	5000 KM	WAN
Pianeta	10000 KM	WAN

LE RETI LOCALI

Una **rete locale** (**LAN**) può essere definita come un'infrastruttura di telecomunicazioni che consente ad apparati indipendenti di comunicare in un' area limitata attraverso un canale fisico condiviso ad elevata velocità di trasmissione (bit-rate) e con bassi tassi di errore.

Quindi, se si parla di reti locali, si intendono reti caratterizzate da estensione geografica limitate (l'area occupata dalla rete locale non può superare distanze tra le 5 e le 7 miglia (circa 8 - 11 km.). Spesso è limitata in un solo edificio o in un gruppo di edifici chiusi in un'area delimitata ,velocità di trasmissione (bit-rate) medio-alta, compresa tra 10-1000 Mbps (associata ad una bassa probabilità di errore per bit) e costi relativamente bassi.
Sono utilizzate per condividere risorse software (file, db, programmi) e risorse hardware (dischi, stampanti…) nell'ambito dell'attività aziendale.
In genere il sistema di cablaggio di una rete locale include oltre ai cavi anche altri componenti necessari all'inserimento della stazione in rete (Hub, Switch,Bridge….).

LA RETE LOCALE WIRELESS (WLAN)

Il termine WLAN (Wireless LAN = LAN senza fili) indica una rete locale che non utilizza cavi per la trasmissione dei dati tra i computer della rete.

I mezzi trasmissivi utilizzati nella tecnologia wireless possono essere:

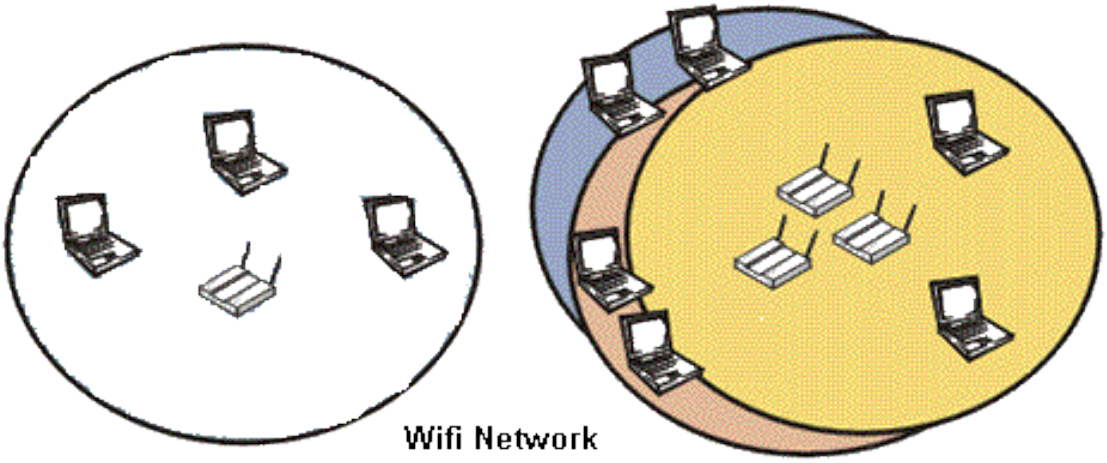
- le onde radio a bassa potenza
- la luce infrarossa (ormai quasi in disuso e sostituita da dispositivi Bluetooth)
- i sistemi laser

Le *onde radio* sono utilizzate dalle reti tipo **Wi-Fi,** cioè reti che devono coprire ambienti in cui le diverse postazioni da collegare possono essere separate da muri o da intercapedini.
Le reti basate su *infrarossi* sono utilizzate per collegare dispositivi "visibili" direttamente, sono lente e spesso utilizzano dispositivi dedicati, infatti sono in disuso e sostituite quasi totalmente dai dispositivi **Bluetooth** (Bluetooth = metodo per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio sicura a corto raggio; vengono cercati i dispositivi entro un raggio di qualche decina di metri, tali dispositivi sono coperti dal segnale e Bluetooth li mette in comunicazione tra di loro)

Le reti basate su *Laser* sono utilizzate normalmente per collegare sottoreti costruite utilizzando altre tecnologie. Un tipico esempio è il collegamento delle reti di due edifici vicini.

I due componenti fondamentali di una rete wireless sono:

- l'**Access Point,** cioè il dispositivo attraverso il quale l'utente ha accesso alla rete
- i **Wireless Terminal**, cioè qualsiasi computer dotato di scheda di rete che soddisfi i requisiti di uno standard wireless



Un aspetto interessante delle WLAN è il fatto di poter essere integrata in una rete Ethernet tradizionale cablata con doppino telefonico. Un esempio potrebbe essere una rete Ethernet di due PC alla quale, attraverso un Access Point possono poi collegarsi altri utenti dotati di computer portatili.
Quindi, un utente dotato di un computer portatile può usufruire dei servizi della rete spostandosi fisicamente all'interno dell'area di copertura del segnale.

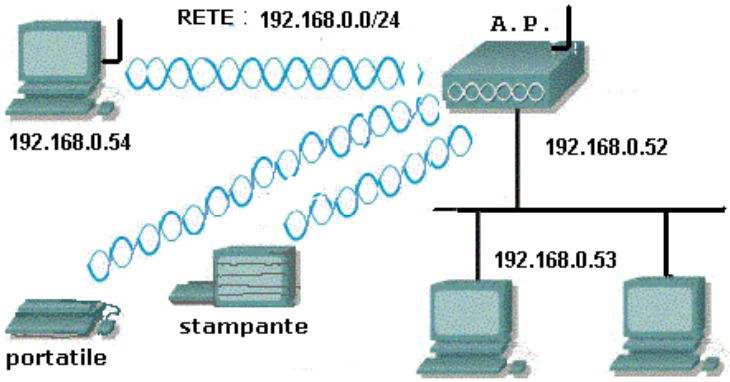


Fig.1 Configurazione in Access Point

Il problema della sicurezza nelle reti wireless

Il problema principale delle reti senza filo è la sicurezza. I segnali radio, essendo diffusi nell'etere, possono essere intercettati senza difficoltà. Di conseguenza è necessario prendere contromisure per garantirne la riservatezza.

Lo standard si crittografia inizialmente proposto per questo compito era il **WEP**, ma la debolezza di questo protocollo, che lo rendevano poco sicuro, imposero ben presto una sua sostituzione con il **WPA**, che utilizza una variante dell'algoritmo WEP a cui sono state rimosse le principali debolezze.

Il protocollo WPA2, ratificato nel 2004, garantisce un'elevata sicurezza ma non è compatibile con le apparecchiature della generazione precedente.

Si consiglia di considerare le reti senza filo come reti a bassa sicurezza, vietando agli utenti collegati di accedere a dati riservati senza un ulteriore livello di sicurezza, ed utilizzare una VPN (Virtual Private Network) se necessario.
*Una **Virtual Private Network** o **VPN** è una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come per esempio Internet. Lo scopo delle reti VPN è di dare alle aziende le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche.*

Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere; per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia. (Osservazioni: per collegarti da casa alle cartelle presenti sul server della scuola utilizzi una VPN !)

TOPOLOGIA DELLE LAN

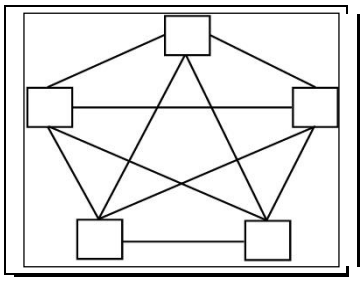
Una rete di telecomunicazioni può essere rappresentata con un grafo, ossia una struttura logica, composta da nodi e da archi.
Possiamo suddividere quindi i nodi in nodi di accesso quando si tratta di terminali e ad essi sono connessi degli utilizzatori o dei fornitori di servizi, e nodi di transito quando ad essi non sono connessi gli utenti ma solo altri nodi di transito o nodi di accesso.

I rami sono gli elementi che permettono il trasferimento dei dati da un'estremità all'altra.

La struttura del grafo è anche **topologia** della rete.
Le topologie più diffuse per le reti locali sono le seguenti.

Topologie a maglia regolare

La più semplice topologia possibile è quella a maglia completa, rappresentata nella figura successiva, in cui tutti i nodi sono collegati fra loro a due a due.
Questa topologia ha l'indiscutibile vantaggio di prevedere un collegamento punto-punto diretto fra qualunque coppia di nodi. Ha però il grande svantaggio di richiedere un numero di linee di collegamento che cresce con il quadrato del numero dei nodi.
Per una rete di N nodi sono necessarie N(N-1)/2 linee. È quindi una topologia che poco si addice a reti con molti nodi.



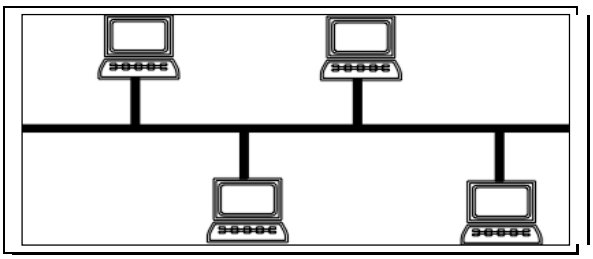
Topologia a maglia irregolare

Topologia a bus

Tutti i nodi della rete sono connessi direttamente allo stesso cavo. Richiede un mezzo trasmissivo bidirezionale, che ammetta cioè la propagazione del segnale in entrambe le direzioni.
Ogni nodo della rete ha un proprio indirizzo unico che lo distingue da tutti gli altri, ciò permette al nodo di identificare il messaggio indirizzato ad esso. Un segmento che usa una topologia a bus è un lungo filo, generalmente un cavo coassiale, chiuso alle estremità con un "terminatore" (resistenza da 50 W). La trasmissione è di tipo **broadcast** , quindi quando una macchina trasmette, tutte le altre ricevono il segnale.

Quando una stazione invia un messaggio, il segnale elettrico viaggia in entrambe le direzioni fino a raggiungere la fine del cavo dove è assorbito dal tappo impedendo che rimbalzi indietro. Mentre il segnale si propaga nel canale i nodi hanno il tempo di esaminare l'indirizzo di destinazione e prelevare i dati solo se è riconosciuto il proprio indirizzo. Nelle topologie a bus il numero di nodi collegati è limitato perché ogni nodo aggiunto assorbe una parte del segnale e al di sotto di una certa soglia il valore del segnale non è più riconoscibile e si deve ricorrere ad un ripetitore. L'uso, in questa topologia, di un cablaggio semplice (pochi fili!) e di hardware di rete economico sono sicuramente dei **vantaggi**.

La contropartita è che, essendo il mezzo trasmissivo fisicamente condiviso da tutte le stazioni, esso risulta soggetto a collisioni quando più macchine vogliono trasmettere contemporaneamente, inoltre l'interruzione del cavo porta alla caduta dell'intera rete.



Topologia a bus

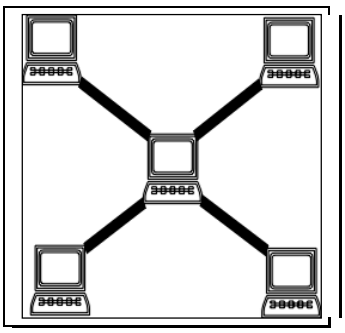
Topologia a stella

Sebbene si sia sviluppata tardi, la topologia a stella è divenuta la topologia più popolare.
Nella topologia a stella tutti i computers sono connessi, tramite un tratto dedicato, ad un nodo centrale . Il collegamento di ogni macchina al centro stella è un collegamento punto-punto, si realizza utilizzando tipicamente **doppino** ritorto o fibra ottica, a seconda della distanza da coprire.
Il nodo centrale può essere un semplice rigeneratore di segnali (**HUB**) o anche un apparecchio intelligente.

La soluzione a *stella passiva* (Hub) è una trasmissione di tipo broadcast, infatti i pacchetti inviati da una stazione ad un'altra sono ripetuti su tutte le porte dell'hub. Questo permette a tutte le stazioni di vedere qualsiasi pacchetto inviato sulla rete, ma solo la stazione a cui il pacchetto è indirizzato lo copierà.
La topologia a stella è una topologia più robusta rispetto quella a bus.

Uno dei vantaggi è rappresentato dal fatto che se vi è un'interruzione su una delle connessioni della rete solo il computer attaccato a quel segmento ne risente mentre tutti gli altri computers continuano ad operare normalmente (in una rete a bus un'interruzione sul mezzo trasmissivo compromette invece il funzionamento dell'intera rete). Ovviamente se non funziona correttamente il nodo di centrale tutta la rete smette di funzionare.

Rispetto ad altre topologie, il cablaggio è molto più complesso e richiede un alto numero di cavi, quindi il costo è più elevato. Nonostante questo essa è utilizzata perché ogni nodo ha un proprio collegamento privato che se si interrompe danneggia solo questo. Inoltre il nodo centrale può realizzare funzioni di diagnostica e permettere di monitorare tutti i segnali che sono smistati nella rete.



Topologia a stella

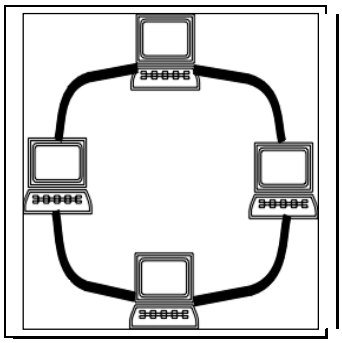
Topologia ad anello

Prevede il collegamento fisico di ogni macchina alla macchina successiva, e l'ultima macchina viene collegata alla prima. Ne risulta un anello unidirezionale in cui ogni macchina ha anche la funzionalità di ripetizione dei messaggi delle altre.

Quando una macchina deve trasmettere, inserisce il messaggio sull'anello, trasmettendolo alla macchina a valle.
Ogni macchina riceve il messaggio e lo ritrasmette in avanti, fino a tornare alla macchina sorgente, che toglie il messaggio dall'anello.
La macchina destinataria, oltre a ricevere e ritrasmettere il messaggio, lo trattiene e in genere ne modifica una parte per confermare al mittente l'avvenuta corretta ricezione.
Questa conferma è caratteristica solo della topologia ad anello.
La ripetizione del segnale ne permette l' amplificazione , quindi non ci sono i problemi di indebolimento con l'aggiunta di nuovi nodi. L'anello può essere dunque abbastanza ampio, i limiti di estensione riguarda la distanza tra nodo e nodo.

Gli svantaggi sono i seguenti :

1. Il malfunzionamento di una stazione o di una linea provocano l'interruzione della intera rete
2. L'inserimento di una nuova stazione provoca l'interruzione del funzionamento dell'intera rete.



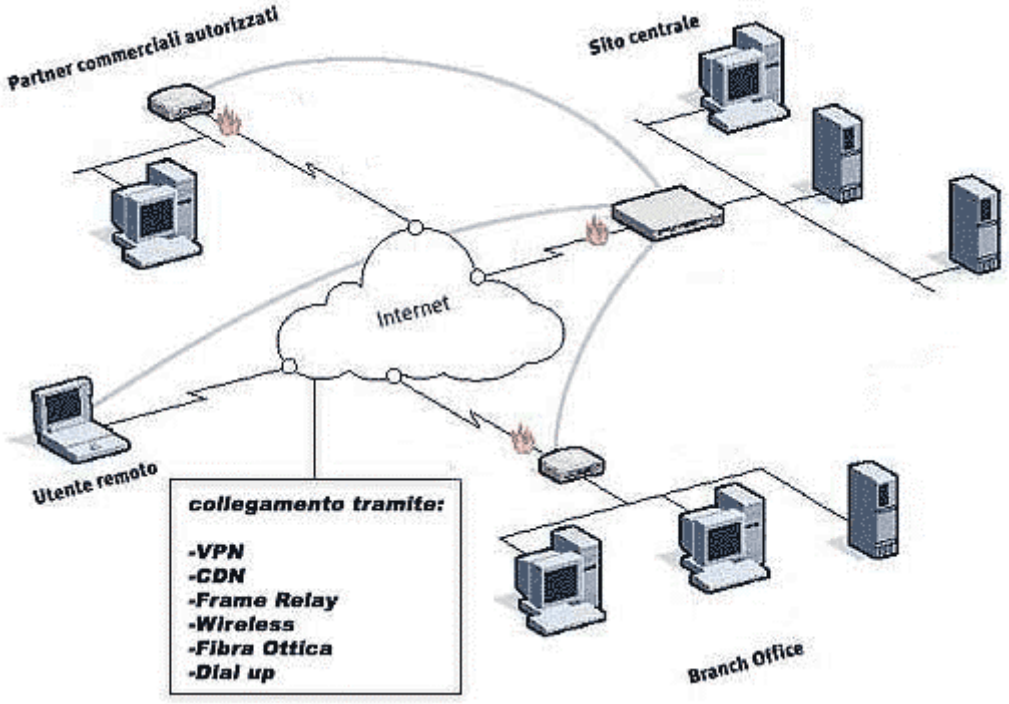
Topologia ad anello

RETI GEOGRAFICHE O WAN

Una Rete Geografica (WAN, Wide Area Network), contrariamente alla LAN, è una rete che si estende su spazi ampi e, normalmente, non adiacenti.
Naturalmente una WAN non è detto sia esclusivamente costituita da singoli calcolatori remoti l'uno rispetto all'altro: di solito una WAN è costituita da LAN interconnesse tra loro tramite altre reti, pubbliche e/o private, delle quali condividono il traffico.
Le reti geografiche possono essere pubbliche o private.

Un esempio semplice di rete geografica è dato da una rete aziendale fisicamente costituita da due LAN, che si sviluppano in edifici posti città diverse, collegate tra loro stabilmente via Internet per mezzo di software specifico in grado di trasferire esclusivamente il traffico aziendale .

Oppure una situazione illustrata dalla figura seguente:



La tecnologia di trasmissione delle WAN è mista e utilizza le linee telefoniche esistenti caratterizzate da notevoli estensioni. Poiché le linee tradizionali trasferiscono dati a bassa velocità e con tasso d'errore non trascurabile, le WAN risultano molto più lente delle LAN. Per questo recentemente oltre ai classici canali trasmessivi queste reti utilizzano satelliti e ponti radio.
L'interconnessione di reti di computer o stazioni singole attraverso una rete geografica (**internetworking)** si realizza tipicamente mediante dispositivi dedicati, i router, il cui compito fondamentale è quello instradare i pacchetti da un nodo sorgente cercando di farli arrivare al nodo di destinazione.
Poiché le WAN utilizzano le infrastrutture esistenti, la topologia più comune è a maglia irregolare.
A livello mondiale, oggi la rete principale è "Internet", ma ci sono numerosi altri esempi di WAN.
In realtà, negli ultimi decenni sono state sviluppate decine di reti geografiche tra le quali ricordiamo quelle militari e di polizia, le reti per la gestione dei grandi archivi pubblici, le reti per la raccolta delle giocate (Enalotto etc.), le reti che connettono i centri di grandi industrie e le loro filiali, i sistemi di prenotazione (treni, aerei, agenzie di viaggio) ed altre ancora.

I PROTOCOLLI DI COMUNICAZIONE

Per lo sviluppo delle telecomunicazioni risultano fondamentali gli standard, che definiscono delle serie di regole secondo cui i sistemi e le reti di telecomunicazioni devono operare.

Un protocollo è infatti un insieme di regole e di convenzioni che governano la comunicazione tra sistemi di elaborazione comunicanti. I computer in una rete impiegano protocolli ben definiti per comunicare.

Grazie ad essi è possibile che reti di paesi diversi possano interconnettersi (si pensi alla rete telefonica con la teleselezione internazionale), che i terminali di utente continuino a funzionare anche in reti diverse (si pensi alla radio, alla televisione, al telefono cellulare) e così via.
La problematica della definizione e negoziazione degli standard ha quindi accompagnato da sempre il mondo delle reti telecomunicazioni.

Diversi enti pubblici e privati si sono occupati di queste problematiche e sono stati, a vario titolo promotori di standard:

1. **ISO (International Standard Organization)** - **http://www.iso.org**;

2. **IEEE (Institute of Electrical and Electronics Engineers)** - http://www.ieee.org;

3. **CCITT (Comite Consultatif International Telegraphique ed Telephonique)**

MODELLO DI COMUNICAZIONE A STRATI

Per realizzare reti di calcolatori che siano sistemi aperti è necessario:

a) delineare un modello di riferimento per la comunicazione fra calcolatori che sia base comune di questi sistemi;
b) giungere alla definizione di standard universalmente accettati che specifichino in modo preciso le funzioni che sono necessarie per realizzare la comunicazione.

La maggior parte delle reti moderne è organizzata in livelli. I livelli sono caratterizzati da una struttura gerarchica tale per cui ognuno di essi è in grado di comunicare soltanto con i livelli adiacenti attraverso "meccanismi" predefiniti detti interfacce. Ogni livello di rete delle singole macchine comunica con i livelli corrispondenti delle altre mediante "regole" predefinite chiamate protocolli. La comunicazione non è diretta, ma avviene passando attraverso i livelli inferiori del proprio computer i quali aggiungono informazioni di vario tipo al messaggio che viene inviato all'altro computer. Il messaggio , attraverso i vari livelli, raggiunge il mezzo fisico di trasmissione e viene inviato alla seconda macchina, in corrispondenza della quale risale la gerarchia dei livelli risale ad arrivare a destinazione.

Per comprendere i meccanismi basilari di funzionamenti del software di rete si può pensare alla seguente analogia umana, nella quale due personaggi (X e Y) vogliono dialogare tra loro nonostante siano geograficamente distanti e parlino lingue differenti. Il livello più astratto è rappresentato dai sue personaggi che si inviano i messaggi. Supponiamo che il primo messaggio venga inviato da X a Y. Il messaggio verrà tradotto in Inglese dal livello dei traduttori. Il messaggio tradotto sarà poi passato alle segretarie, che si faranno carico di spedire il fax con il messaggio tradotto. Il livello più basso è rappresentato dal mezzo fisico su cui viaggia il contenuto del fax. Quando il segnale del fax giunge a destinazione, deve compiere il tragitto inverso: deve essere correttamente interpretato dal si positivo del fax in ricezione, quindi deve

essere stampato correttamente dalle segretarie, successivamente passato ai traduttori, che lo consegneranno a Y , il quale ne interpreterà il risultati

MODELLO ISO-OSI

Nei primi anni '80 l' **ISO** promuove un'azione volta alla definizione di un modello di riferimento a strati e di una serie di standard per protocolli e interfacce atti a realizzare dei sistemi aperti. Questo lavoro prende il nome di **Open System Interconnection** o **OSI** .

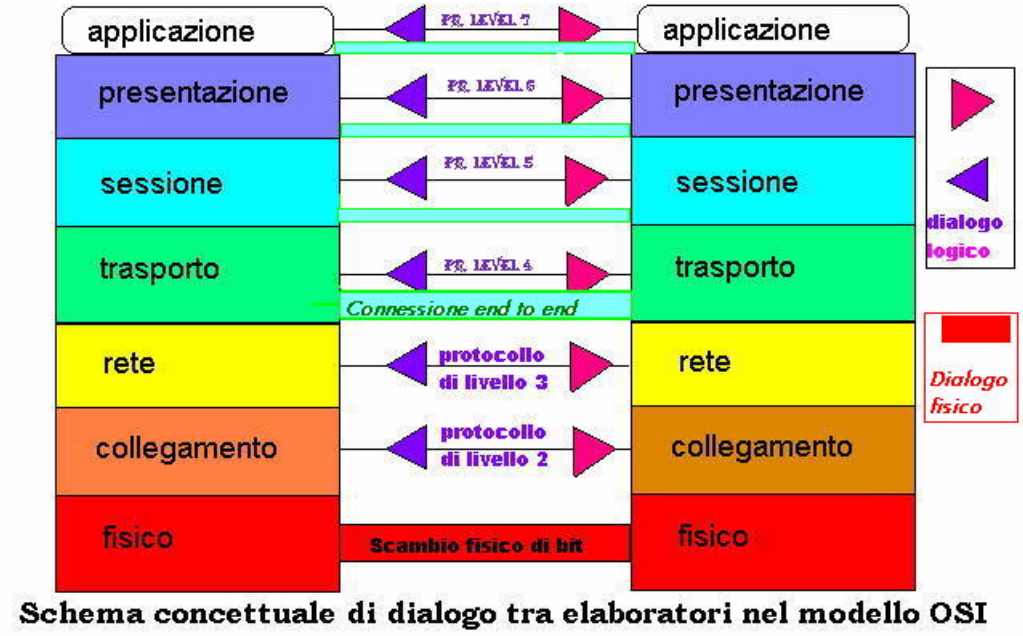
L' **ISO-OSI (Open System Interconnection) Reference Model** ha lo scopo di:

a) fornire uno standard per la connessione di sistemi aperti;
b) fornire una base comune per lo sviluppo di nuovi standard per l'interconnessione di sistemi;
c) fornire un modello rispetto a cui confrontare le architetture di rete.

All'interno del modello OSI esiste una simmetria strutturale tra due sistemi che intendono cooperare come spiegato precedentemente. Ogni informazione che deve essere inviata da un sistema all'altro passa da un livello a quello immediatamente inferiore, il quale eseguirà le funzioni che gli sono proprie ed aggiungerà alle informazioni pervenutigli dal livello superiore delle proprie informazioni di controllo prima di passare i dati al livello sottostante. Questo processo si ripete sino a quando non si giunge al livello più basso che provvederà a trasmettere sul mezzo fisico tutte le informazioni giunte dall'alto.

Il processo di aggiungere informazione ai dati originali mentre questi passano attraverso i vari livelli è chiamato "incapsulamento".

OSI è costituito da 7 livelli:



Schema concettuale di dialogo tra elaboratori nel modello OSI

1. **strato fisico**; ha come compito principale quello di effettuare il trasferimento fisico delle cifre binarie tra i due sistemi in comunicazione;

2. **strato di collegamento (data link)**; la sua funzione fondamentale è quella di rivelare e recuperare gli errori trasmissivi che potrebbero essersi verificati durante il trasferimento fisico. Viene inserito il **MAC-Address**(*indirizzo della scheda di rete*)

3. **strato di rete (network)**; rende invisibile allo strato superiore il modo in cui sono utilizzate le risorse di rete per la fase di instradamento (routine). Il messaggio viene diviso in pacchetti. Viene inserito *l'header del pacchetto*. Viene definito il percorso ottimale per l'instradamento dei pacchetti.

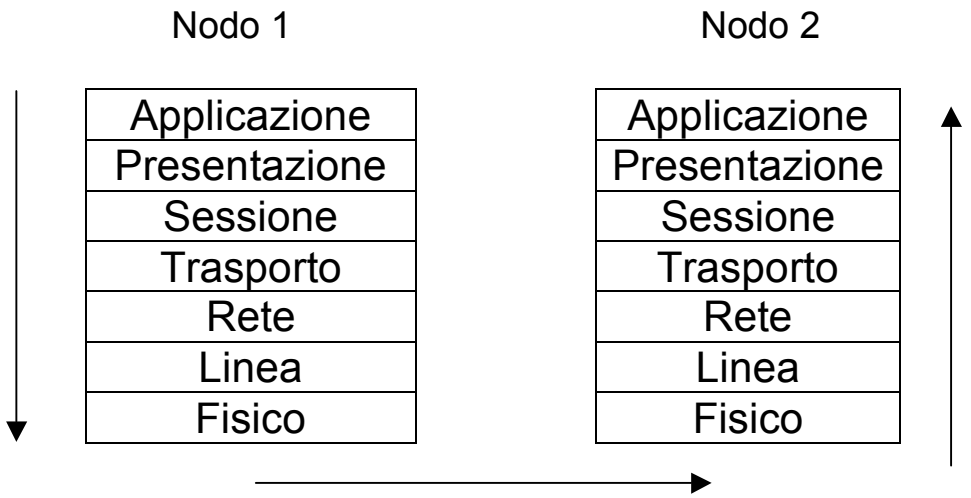
4. **strato di trasporto (transport)**; fornisce le risorse per il trasferimento trasparente di informazioni. Sfrutta il percorso deciso dal livello sottostante in modo da mantenere la correttezza della loro struttura indipendentemente dai sistemi posti nei nodi.

5. **strato di sessione (session)**; assicura la possibilità di instaurare un colloquio tra due sistemi. Realizza l'interfaccia tra l'utente e la rete controllando il login. Svolge quindi funzioni di sicurezza permettendo la connessione solo tra i nodo autorizzati.

6. .**strato di presentazione (presentation)**; è interessato alla sintassi e alla semantica delle informazioni da trasferire. Le informazioni vengono decodificate per renderle visibili ai normali dispositivi di Input/Output degli utenti.

7. **strato di applicazione (application)**; ha lo scopo di fornire ai processi residenti nei due sistemi in comunicazione i mezzi per accedere all'ambiente OSI. Consente ai software applicativi di accedere ai servizi della rete. Esempi di servizi offerti: il trasferimento dei file, la posta elettronica, la condivisione dei dati multimediali.

Esempio di trasmissione secondo il modello ISO/OSI



MODELLO INTERNET

La rete **Internet** si è sviluppata al di fuori dal modello ISO-OSI e presenta una struttura solo parzialmente aderente al modello **OSI.**

Il nome più accurato per l'architettura di rete utilizzata è Internet Protocol Suite, anche se comunemente si fa riferimento alla sigla TCP/IP

I protocolli appartenenti a questa architettura sono specificati tramite standard che si chiamano RFC (Request For Comments) facilmente reperibili sulla rete Internet.

L'architettura TCP/IP rappresenta una standard "de facto" attualmente impiegato per la rete Internet di estensione mondiale.

Il protocollo TCP/IP è più semplice rispetto all'architettura ISO/OSI.

Esso è suddiviso in 4 livelli:

1. *Livello interfaccia di rete (Network)*
2. *Livello Internet (Internetwork)*
3. *Livello Trasporto*
4. *Livello Applicazione*

Applicazione
Presentazione
Sessione
Trasporto
Rete
Linea
Fisico

Processo/ Applicazione
TCP
IP
Rete

1. **strato di accesso alla rete** (network access layer), comprende le funzioni che nel modello OSI sono comprese negli strati fisico, di collegamento e parte di quello di rete; questo strato non specifica i livelli 1 e 2 della rete ma utilizza quelli normalmente disponibili e conformi agli standard (es. per reti locali Ethernet, Token-Ring, ecc.). A questo livello viene identificato il Mc Address;

2. **Strato Internet Protocol** (IP) si occupa di instradare i messaggi sulla rete, ma ha anche funzione di frammentazione e riassemblaggio dei messaggi e di rilevazione (ma non correzione) degli errori; quando i pacchetti arrivano dal Livello Trasporto, l'Internet Protocol (IP) vi aggiunge un header (intestazione) che include:
   - Indirizzo IP del mittente
   - Indirizzo IP del destinatario.

   Questo livello stabilisce anche che strada deve fare un pacchetto per arrivare al destinatario.

3. **strato di trasporto** (TCP); al livello di trasporto troviamo il protocollo TCP che mette in coda i messaggi delle applicazioni (browser e server), li indirizza e li trasmette sottoforma di pacchetti; il buon fine della spedizione è attestato da una ricevuta di ritorno. Anche questo è un collegamento virtuale tra le due applicazioni, i cui dettagli sono demandati al livello di rete. Il TCP è utilizzato dalle applicazioni di rete che richiedono una trasmissione affidabile dell'informazione, mentre un altro protocollo di trasporto è il UDP (User Datagram Protocol) molto più semplice di TCP ed utilizzato quando non è richiesta l'affidabilità di TCP (ad es. per la videoconferenza).TCP è un protocollo con conferma, UDP è un protocollo senza conferma.

4. **strato di applicazione** (application protocol); nell'architettura Internet non sono previsti gli strati di sessione e di presentazione, ma solo quello di applicazione; questo strato contiene i protocolli utilizzati poi dai programmi residenti sulle macchine. Alcuni protocolli utilizzati in questo strato sono **FTP** (File Transfer Protocol - per il trasferimento dei file), **POP** (Post Office Protocol) e **SMTP** (Simple Mail Transfer Protocol) per la posta elettronica, **Telnet** che consente ad un utente locale di collegarsi ed utilizzare le risorse di un elaboratore remoto connesso alla rete, **HTTP** (HyperText Transfer Protocol - per le pagine Web), **DNS** (Domain Name Server – è una base di dati distribuita e replicata per gestire la corrispondenza tra nomi mnemonici ed indirizzi IP). Quando vogliamo collegare il nostro browser a un server web per effettuare una consultazione di pagine Web, stabiliamo un collegamento (virtuale) a livello applicazione.

GLI APPARATI

All'interno di una LAN i nodi possono costituire le stazioni di lavoro oppure servire per altre funzioni fondamentali per migliorare l'efficienza della rete, il traffico e l'interconnessione tra segmenti diversi di una stessa rete o fra LAN diverse. Descriviamo brevemente i seguenti dispositivi:

Descriviamo brevemente i seguenti dispositivi:

Repeater, Hub	**Switch, Bridge**	**Router**	**Gateway**	**Firewall**

Facendo riferimento al modello ISO/OSI, ognuno di questi oggetti è utilizzato esclusivamente per consentire la comunicazione su un livello ben preciso:

<table>
<tr><td>Livello Fisico</td><td colspan="2">Repeater, Hub</td></tr>
<tr><td>Livello Data link</td><td colspan="2">Switch e Bridge</td></tr>
<tr><td>Livello Network</td><td>Router</td><td rowspan="2">Gateway</td></tr>
<tr><td>Livello Trasporto</td><td></td></tr>
<tr><td>Livello Sessione</td><td colspan="2" rowspan="3">Firewall</td></tr>
<tr><td>Livello Presentazione</td></tr>
<tr><td>Livello Applicativo</td></tr>
</table>

L' **HUB** è un concentratore di rete in grado di amplificare il segnale ed inviarlo al segmento successivo. Opera al livello 1 dell'OSI, livello fisico, tratta la trama solo dal punto di vista del segnale elettrico e non del suo contenuto. Viene utilizzato per suddividere la rete in segmenti permettendo un cablaggio più semplice.

Lo **SWITCH** è un dispositivo in grado di commutare il segnale che gli arriva soltanto sul segmento a cui è indirizzato e non agli altri. Crea una connessione tra uno dei canali di ingresso e uno di uscita in base al contenuto del pacchetto, è infatti in grado di leggere i campi contenenti gli indirizzi di destinazione e provenienza.

Lavora al livello 2 dello standard OSI è, quindi, più evoluto degli Hub.

Uno switch risulta più efficiente di un hub perché isola il traffico locale a ciascuna porta: le stazioni connesse direttamente allo switch vedranno solo il traffico **broadcast** e quello diretto a loro stesse, migliorando così l'utilizzazione del mezzo trasmissivo.

Alle porte dello **switch** possono essere connessi degli hub, realizzando in questo modo un'architettura a stella gerarchica.

Il **BRIDGE** è un dispositivo che collega due LAN che possono essere simili o diverse (es.: Ethernet e Token Ring). Esso opera a livello di collegamento dati (livello 2 dello standard OSI). E' un dispositivo in grado di memorizzare un intero pacchetto, eventualmente modificarlo lievemente aggiungendo o togliendo campi dall'intestazione prima di inoltrarlo sulla rete. Nel caso di reti simili il compito del bridge è quello di separare il traffico tra le reti ed inoltrare sull'altra rete soltanto i pacchetti che le sono effettivamente destinati. Nel caso di reti diverse opera un collegamento tra le due che altrimenti non sarebbe possibile. Unica eccezione è fatta per i frame *broadcasting* che il bridge ha la capacità di riconoscere ed inoltrare a tutti i componenti delle reti collegate.

I ROUTERS sono apparecchiature più complesse e tipicamente più costose dei bridges.

Un router opera al Livello Rete (livello3 del modello OSI). Tale dispositivo è un sistema che interconnette due o più reti, ed è necessario quando due reti usano lo stesso Livello Trasporto ma hanno differenti Livelli di Rete.

Il termine router (instradatore) implica che questa entità non solo inoltra i pacchetti da una rete ad un'altra, ma prende anche delle decisioni sul percorso che tali pacchetti dovrebbero seguire. Infatti tale dispositivo, in funzione di opportuni algoritmi di instradamento, inoltra un pacchetto da una LAN ad un'altra cercando di ottimizzarne il percorso in funzione di parametri quali il costo della tratta, la velocità trasmissiva associata ad un certo link, ecc.. I routers ovviamente comunicano tra di loro e condividono informazioni che permettono loro di determinare qual è il miglior tragitto.
Un router oltre alle funzioni di instradamento esegue anche operazioni di filtraggio sui pacchetti che riceve. Tale dispositivo può filtrare i pacchetti tra le LAN con operazioni più complesse rispetto a quelle eseguite da un bridge; infatti con i router e' anche possibile selezionare quali computers sono abilitati ad accedere a certe reti locali e quali devono essere scartati.

Il **GATEWAY** è una macchina dedicata che interconnette due o più reti diverse. E' concettualmente simile al bridge, ma affronta il problema della conversione tra i protocolli che può presentarsi nell'interconnessione tra reti diverse. Tale compito è tanto più complesso quanto più alto è il livello di protocollo nel quale si opera, generalmente non si va oltre il livello di rete o di trasporto (livelli 3 e 4 dello standard OSI). La conversione avviene di solito dal protocollo della rete di provenienza ad un protocollo comune di interconnessione e da questo al protocollo della rete di destinazione. I gateway sono molto più lenti dei bridge, quindi vengono comunemente impiegati nelle WAN.

Il mercato offre sempre più raramente il bridge o il router puro: tutte le case offrono apparecchiature complesse, in grado di combinare le singole funzionalità.

FIREWALL

Può essere un programma o un vero e proprio computer dedicato, che si inserisce fra la rete aziendale e quella esterna in modo da costringere il passaggio di tutto ciò che transita attraverso un unico punto di ingresso e uscita dove si provvede ad effettuare opportuni controlli. I firewall proteggono da violazioni della sicurezza riguardanti la *riservatezza, l'integrità, e l'autenticità*.

Sui computer che fungono da firewall vengono eseguiti particolari programmi che esaminano tutti i messaggi in transito e decidono se lasciarli passare o fermarli. Tipicamente, vengono lasciati entrare nella zona protetta soltanto i messaggi provenienti da persone o computer autorizzati o riconosciuti, ad esempio, tramite una password. In questo modo, è possibile proteggere i computer situati nella zona protetta, creando attorno ad essi una "barriera telematica" che fermi i tentativi di intrusione non autorizzati. Al giorno d'oggi sono disponibili sistemi di firewall molto efficienti e sicuri.

IMPLEMENTAZIONE DI UNA LAN

Ogni computer, per potersi connettere ad altri computer in rete locale od in rete globale (Web), deve avere installato una scheda di rete ed inoltre deve avere un UNICO indirizzo per essere identificabile univocamente e per poter così ricevere i pacchetti ad esso destinati; una specie di targa identificativa.

Questa identificazione viene implementata mediante:

- un indirizzo univoco detto Mac Address, che ogni scheda di rete possiede, determinato dal costruttore in fase di produzione ed è costituito da sei codici esadecimali (48 bit) ;
- un indirizzo IP collegato al Mac Address; è un numero composto da quattro ottetti di bit (32 bit) (da 1.1.1.1 a 255.255.255.255),

Non esistono due schede di rete con lo stesso MAC Address e pertanto, non essendo modificabile dall'utente, il computer viene identificato nella rete in maniera univoca.

GLI INDIRIZZI IP

Il sistema di numerazione di rete del protocollo TCP/IP è stato fissato nel 1981. Ad ogni singola macchina della rete viene assegnato un diverso indirizzo IP composto di 32 bit, cioè 4 byte, che la identifica. In notazione decimale, ciò significa quattro numeri ognuno dei quali va da 0 a 255.
È usuale separare i quattro byte (sia in notazione binaria che decimale) con dei punti.

Ecco un indirizzo IP nelle notazioni binaria e decimale

11001000.10000101.10101111.01100001
200.133.175.97

L'indirizzo IP ha una prima parte (che può essere composta dal primo, dai primi due, o dai primi tre byte) che indica il numero di rete , **Net ID** (Network Address o Indirizzo di Rete) e una seconda parte (gli altri byte) che indica il numero della macchina all'interno della rete **Host ID** (Host Address o Indirizzo del singolo host)

Indirizzi di classe A - Struttura

Si è convenuto definire indirizzi di classe A quegli indirizzi IP in cui il primo bit è 0 (quindi quelli in cui l'equivalente primo numero decimale è compreso tra 0 e 127) e il primo byte rappresenta il numero di rete mentre gli altri tre byte rappresenta il numero della macchina all'interno della rete.

Quindi un byte è dedicato alla rete e tre byte sono dedicati al computer; gli indirizzi di questa classe sono adatti a quelle poche e grandi organizzazioni, che hanno reti con numerosi computer.

Con questo tipo di indirizzi si possono indirizzare solo poche reti (128 in totale ma in realtà solo 126 perché i numeri di rete 0 e 127 non si possono usare) ma ognuna con un numero molto elevato di possibili nodi $2^{24} – 2 = 16.777.214$, il primo e l'ultimo indirizzo non si possono usare).
Alle reti molto ampie, per esempio quella dell'esercito americano, vengono assegnati blocchi di indirizzi di classe A.

Ecco alcune organizzazioni alle quali è stato assegnato un blocco di indirizzi di classe A (quindi più di 16 milioni di nodi all'interno della rete):

Hewlett Packard (15.0.0.0)
Apple Computer (17.0.0.0)
Stanford University (36.0.0.0)
Posta Americana (56.0.0.0)

Indirizzi di classe B - Struttura

Negli indirizzi IP i cui primi due bit sono 10 (e quindi il cui primo numero decimale è tra 128 a 191) i primi due byte rappresentano il numero di rete, e gli altri due byte rappresentano il numero della macchina all'interno della rete.
Gli indirizzi di questa classe sono adatti alle medie organizzazioni, che hanno reti con un numero medio di computer.

Ci sono 2^{14} blocchi di questi indirizzi (circa 16.000), di questi attualmente ne sono stati assegnati circa 12000 (65%). Ogni blocco consiste di un numero massimo teorico
di $2^{16} – 2 = 65.534$ indirizzi.

Esempi di organizzazioni alle quali è stato assegnato un blocco di indirizzi di classe B:
University of Utah (128.110.0.0)
Princeton University (128.112.0.0)
Technische Universität Hamburg (132.28.0.0)
Red Lion Hotels (170.10.0.0)

Indirizzi di classe C - Struttura

Infine gli indirizzi IP i cui primi tre bit sono 110 (primo numero decimale da 192 a 223) si dicono di classe C o /24: qui, i primi tre byte indicano la rete e l'ultimo byte può indicare, per ogni rete, fino a 254 macchine all'interno della rete.
Gli indirizzi di questa classe sono adatti alle numerose piccole organizzazioni, che hanno reti con pochi computer.

Poiché i primi tre bit sono fissi, ci sono 2^{21} (circa 2.000.000) possibili reti di classe C; attualmente ne sono definite circa 800,000 (40%).
Una piccola organizzazione (una società, una scuola) può per esempio ricevere un blocco di 254 indirizzi che vanno da 192.66.12.1 fino a 192.66.12.254.
Il blocco 195.31 è uno di quelli assegnati all'Italia; ecco alcuni blocchi di indirizzi italiani:

Magistrato delle Acque di Venezia (195.31.130.0)
Cassa di Risparmio di Ferrara (195.31.137.0)
Gruppo Coin (195.31.151.224)
Comune di Bologna (195.31.141.128)

Altre classi

Sono previste anche la classe D (bit iniziali 1110, indirizzi tra 224 e 239) i cui indirizzi sono riservati per applicazioni di multicast, e la classe E (bit iniziali 1111, indirizzi tra 240 e 254) i cui indirizzi sono riservati per usi futuri.

IPv6

L'utilizzo degli indirizzi IP nel formato descritto (IPv4) permette di indirizzare 126 reti di classe A, oltre 16000 reti di classe B, e oltre 2000000 di reti di classe C, che possono però disporre di un numero massimo di host pari a 254. Alcune stime hanno stabilito che all'incirca ogni anno il numero delle reti connesse a Internet raddoppia. Questo enorme sviluppo mette in luce il problema dell'**esaurimento** degli indirizzi IP disponibili. Il protocollo IPv6 rappresenta la soluzione definitiva ai problemi di indirizzamento.

.

La sua caratteristica più importante è il più ampio spazio di indirizzamento: poiché questi riserva 128 bit per gli indirizzi IP. Così IPv6 gestisce 2^{128} (circa $3{,}4 \times 10^{38}$) indirizzi, mentre IPv4, che consente un numero di bit per l'indirizzamento pari ad un quarto di quelli per IPv6, ossia 32, gestisce soltanto 2^{32} (circa 4×10^{9}) indirizzi. Quantificando con un esempio, per ogni metro quadrato di superficie terrestre, ci sono 655.570.793.348.866.943.898.599 indirizzi IPv6 unici (cioè 655 571 miliardi di miliardi), ma solo 0,000007 IPv4 (cioè solo 7 IPv4 ogni milione di metri quadrati). L'adozione su vasta scala di IPv6 risolverebbe senz'altro il problema dell'esaurimento degli IP disponibili.

Convenzioni

Un indirizzo che ha tutti i bit del numero di macchina uguali a 0 non indica una determinata macchina ma la rete stessa a cui apparterrebbe tale macchina.

Per esempio:

- l'indirizzo di classe A 00010001.00000000.00000000.00000000 cioè 17.0.0.0 indica la rete della Apple,

- quello di classe B 10000000.01110000.00000000.00000000 cioè 128.112.0.0 indica la rete della Princeton University

- e quello di classe C 11000011.00011111.10001001.00000000 cioè 195.31.137.0 la rete della Cassa di Risparmio di Ferrara.

Un indirizzo che ha tutti i bit del numero di macchina uguali a 1 non indica una particolare macchina ma viene utilizzato per identificare tutti gli host della rete : si tratta del cosiddetto indirizzo di broadcasting sulla rete indicata. Gli indirizzi di broadcasting delle tre reti indicate qui sopra sono

00010001.11111111.11111111.11111111 cioè 17.255.255.255

10000000.01110000.1111111.11111111 cioè 128.112.255.255

11000011.00011111.10001001.11111111 cioè 195.31.137.255

Gli indirizzi (di classe A) che iniziano con 127 hanno un uso riservato; tra questi

127.0.0.1 = indica la macchina stessa (localhost)

MASCHERE DI SOTTORETE (SUBNET MASK)

Quando si configura un indirizzo IP, è sempre necessario definire anche una **maschere di sottorete (subnet mask)**, la cui funzione è quella di mascherare una parte dell'indirizzo IP, in modo che il protocollo TCP/IP riesca a distinguere il Net ID dall'Host ID. Ciò renderà più veloci le comunicazioni tra i computer .
Come gli indirizzi IP, la subnet mask è composta da un quartetto di byte e ha la funzione di indicare al computer qual è la parte dell'indirizzo IP da considerare per identificare i computer che si trovano sulla stessa rete. In altri termini, attraverso la subnet mask un computer riesce a capire se un altro computer si trova sulla sua stessa rete o su un'altra (i computer che appartengono alla stessa rete hanno la parte identificata dalla subnet mask uguale a 255).

Esempio di indirizzo pubblico di classe C:
66.249.85.0-255
Subnet mask= 255.255.255.0

Esempio di classe B (indirizzi privati cioè di rete locale, non visibile in Internet):
192.168.0.125
subnet mask: 255.255.0.0
192.168.1.12 questo appartiene alla stessa sottorete

Altro esempio di classe B:
66.249.0-255.0-255
subnet mask: 255.255.0.0

Classe A:
66. 0-255.0-255.0-255
subnet mask: 255.0.0.0

INDIRIZZI DELLE RETI PRIVATE

Nelle reti locali interne private, non collegate con Internet, non è consigliato usare indirizzi pubblici (visibili), ma solo indirizzi speciali, a loro riservati.

La Internet Assigned Numbers Authority (IANA) ha riservato i seguenti tre blocchi di indirizzi IP per reti private

da 10.0.0.0 a 10.255.255.255 (una singola rete di classe A)
da 172.16.0.0 a 172.31.255.255 (16 reti contigue di classe B)
da 192.168.0.0 a 192.168.255.255 (256 reti contigue di classe C)

ASSEGNAZIONE DEGLI INDIRIZZI IP

Gli indirizzi IP sono assegnati da un'unica autorità e quindi sono garantiti univoci a livello mondiale.
Il RIPE (Réseau IP Européens) è l'ente preposto all'assegnamento degli indirizzi IP per il continente Europeo; per il continente americano l'ente preposto è l'ARIN; per l'Asia e il Pacifico è l'APNIC.
In Italia è stato istituito un apposito organismo, denominato **Registration Authority Italiana,** al quale ci si deve rivolgere per registrare un dominio di tipo *.it* , questo è l'organismo responsabile dell'assegnazione dei nomi di dominio, della gestione dei registri e del Name Server primario per il *top-level domain .it*
Tutti questi organismi sono coordinati dall'ICANN (Internet Corporation for Assigned Names and Numbers).

In realtà l'indirizzo non identifica necessariamente una macchina, ma una connessione alla rete. Per esempio, un router ha almeno due indirizzi, avendo connessioni ad almeno due reti. Questo in quanto un router appartiene a entrambe le reti, e quindi sono necessari due indirizzi dato che un IP address ha posto per un solo indirizzo di rete.

Indirizzo mnemonico:

www.google.it

viene tradotto attraverso il Servizio DNS (Domain Name Server) nel corrispondente indirizzo fisico

NAME SERVER

Dato che l'indirizzo può essere a volte abbastanza ostico da ricordare, è possibili associare a ogni host anche un nome, che può essere utilizzato come mnemonico per un IP address, e la cui risoluzione è responsabilità di particolari macchine chiamate *name server*. In realtà il name server è un programma software che può girare in qualunque macchina connessa alla rete, e che mantiene l'associazione tra nomi e indirizzi IP, fornendo tali corrispondenze quando richiesto da un altro programma chiamato *name resolver*. Di fatto, si preferisce far girare il name server su una macchina dedicata, che prende anch'essa, a questo punto, il nome di name server. Potete pensare al name server come a una agenda telefonica elettronica, che contiene una lista parziale di nomi e numeri telefonici. In internet non esiste un singolo elenco telefonico, ma tanti name server che cooperano per fornire quello che è un vero e proprio elenco distribuito. In realtà il sistema funziona in modo gerarchico, un po' come se una certa agenda contenesse solo i prefissi internazionali e il puntatore alle agende di ogni singolo stato, le quali a loro volta contengono i prefissi regionali e i puntatori agli elenchi regionali, e così via, fino ad arrivare all'agenda che contiene solo le estensioni telefoniche di un singolo edificio.

In Internet, i nomi sono basati su una serie di regole dette Domain Name Server (DNS), che si basa appunto su uno schema gerarchico in cui il nome è suddiviso in varie parti separate fra loro da punti, come vedremo in seguito.