Reti e Internet

Internet - o più semplicemente 'the Net', 'la rete' - è una sorta di meta-rete costituita da molte reti telematiche connesse tra loro. Non ha importanza quale sia la tecnologia che le unisce: cavi, fibre ottiche, ponti radio, satelliti, o altro. Non è neanche rilevante di che tipo siano i computer connessi: dal piccolo personal computer al grosso elaboratore, o *mainframe*. Punto di forza di Internet, e motivo del suo velocissimo espandersi, è la sua capacità di 'parlare' un linguaggio universale, adatto alla quasi totalità degli elaboratori esistenti.

Secondo le stime più recenti, si calcola che Internet colleghi più di 50 milioni di computer host (da non confondere con i computer degli utenti finali, che si stima siano ormai più di 200 milioni). Alcune delle linee di comunicazione più importanti fra quelle che compongono la rete, essendo le principali arterie attraverso le quali transita il flusso di dati, prendono il nome di '*backbone*' (dorsali). Backbone sono, per esempio, le linee portanti delle imponenti reti accademiche americane NSFnet (*National Science Foundation Network*) e CSnet (*Computer Science Network*), o i cavi transoceanici che collegano le reti europee con quelle statunitensi.

Internet nacque nel 1969 come rete sperimentale costruita per il Dipartimento della Difesa degli Stati Uniti dall'ARPA (*Advanced Research Project Agency*).

La rete fu chiamata ARPANET e il progetto aveva due scopi principali:

1) sviluppare la tecnologia che consentisse di condividere risorse tra computers di tipo diverso e con differenti sistemi operativi;
2) sviluppare metodi per assicurare comunicazioni affidabili tra computers persino quando parti della rete erano danneggiate o non funzionanti efficientemente, come sarebbe potuto accadere nel caso di una guerra nucleare. Il risultato di questi sforzi fu lo sviluppo di protocolli che costituiscono l'Internet Protocol Suite detta impropriamente TCP/IP dai nomi dei due principali protocolli che la compongono (*Transfer Control Protocol / Internet Protocol*), che rappresenta la base per tutte le comunicazioni su Internet.

Internet è oggi la rete più capillarmente diffusa a livello mondiale, e può essere definita come l'insieme di reti interconnesse tramite varie tecnologie (linee telefoniche, fibre ottiche, satelliti, ...) che utilizzano protocolli standard di comunicazione, appunto l'Internet Protocol Suite.

Questi protocolli permettono comunicazioni tra macchine aventi diversi hardware di rete e differenti sistemi operativi, fissando un insieme di regole sulla modalità dello scambio informativo a vari livelli, pensati indipendenti nelle loro funzionalità.

Normalmente Internet non connette singoli computers ma reti locali (**LAN**, Local Area Network). L'unità organizzativa di base su Internet è infatti la rete. Ogni computer su Internet deve appartenere ad una rete di computer che a sua volta può essere o parte di una rete più grande, come ad esempio una rete regionale, o la rete di un fornitore commerciale di accesso ad Internet (ISP, *Internet Service Provider*). Un ISP è una compagnia commerciale che vende la connessione ad Internet; i tipi di accesso forniti possono essere o tramite linea telefonica (a commutazione di circuito), utilizzando i protocolli SLIP (*Serial Line Internet Protocol*, poco efficiente e ormai in disuso) o PPP (*Point-to-Point Protocol*), o tramite linea dedicata.

I computer su Internet sono identificati da numeri detti indirizzi **IP** (*Internet Protocol address*) e di solito anche da nomi. Un particolare nome o numero può riferire unicamente un singolo computer e l'indirizzo identifica una connessione di rete. Le comunicazioni tra computers basate su regole standard o protocolli avvengono proprio grazie al fatto che ogni nodo connesso alla rete Internet viene identificato in modo univoco da un indirizzo.

Le Reti

Una rete è definita come:

Un insieme di nodi di elaborazione totalmente autonomi connessi mediante un opportuno sistema di comunicazione in grado di interagire mediante scambio di messaggi – indipendentemente dalla piattaforma – al fine di condividere le risorse messe a disposizione della rete.

I nodi di una rete vengono collegati attraverso canali trasmissivi di vario tipo, potendo classificare le reti per ***tecnologia trasmissiva***:

- **Punto-punto** Due soli nodi collegati agli estremi del canale lo utilizzano pariteticamente. Si realizza con due doppini o con due fibre ottiche. È il canale tipico delle topologie a stella e ad anello.
- **Punto-Multipunto** Un nodo, il master, comunica con tutti gli altri, gli slaves. Tipico dei sistemi con un mainframe. Molto usato in passato, ora in disuso
- **Broadcast** Canale di comunicazione condiviso da tutti i nodi. Un pacchetto inviato ad un nodo è *diffuso* e ricevuto da tutti gli altri. È il canale tipico delle topologie a bus.

Un criterio alternativo di classificazione rispetto alle tecnologia trasmissiva è la **scala dimensionale** delle reti. In questo contesto si distingue fra ***reti locali***, ***reti metropolitane*** e ***reti geografiche***.

Distanza fra processori	Ambito	Tipo di rete
10 m.	Stanza	Rete locale
100 m.	Edificio	Rete locale
1 km.	Campus	Rete locale
10 km.	Città	Rete metropolitana
100 km.	Nazione	Rete geografica
1000 km.	Continente	Rete geografica
10.000 km.	Pianeta	Internet (rete di LAN)

La distanza tra nodi è un fattore molto importante, poiché a differenti scale dimensionali si usano differenti tecniche con velocità (*capacità*) molto alte (10-1000 Mbps e oltre nelle LAN, 2-140 Mbps nelle MAN) su brevi distanze e via via minori per lunghe tratte a parità di mezzo trasmissivo (velocità comprese tra 9.6Kbps e 2Mbps nelle WAN proprietarie obsolete).

Topologie di rete

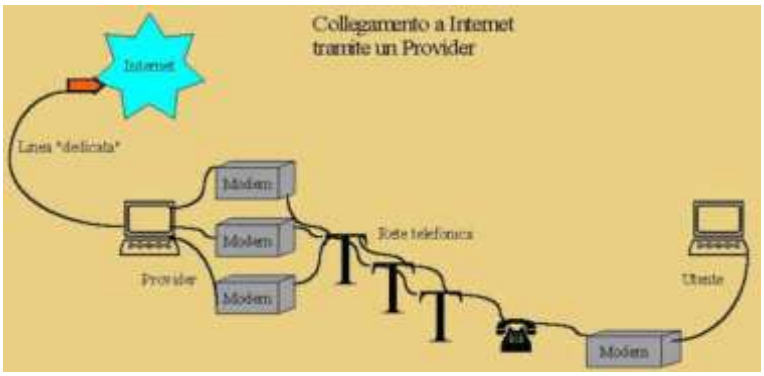
- **Stella**
  con centro stella attivo, le informazioni provenienti da un nodo vengono commutate solo sul nodo di destinazione. Con centro stella passivo, le informazioni provenienti da un nodo vengono smistate a tutti gli altri nodi.
  Vantaggio:basso numero di canali. Svantaggio: vulnerabilità ai guasti del nodo centrale.
  Esempi: l'estrema periferia della rete telefonica, rete via satellite (il centro stella è il satellite, le stazioni di terra i nodi).
- **Anello**
  Può essere bidirezionale o unidirezionale. Usata nelle MAN e in alcune LAN.
  Vantaggio: basso numero di canali. Svantaggio: bassa tolleranza ai guasti
- **Bus**
  Un solo canale condiviso da tutti i nodi. Molto usata nelle LAN.
  Vantaggio: economicità, semplicità di connessione. Svantaggio: bassa tolleranza ai guasti.
- **Maglia parzialmente connessa**
  È la topologia tipica delle reti geografiche. Svantaggio: topologia non regolare.
  Vantaggio: tolleranza ai guasti e flessibilità nella scelta del numero di canali.
  Esempio: Internet

La tipologia delle connessioni di rete[1]

Il collegamento di un computer può essere basato su diverse **infrastrutture hardware**. In generale possiamo suddividere tutti questi diversi sistemi e apparati in due categorie principali:

- collegamenti **permanenti**
- collegamenti **temporanei**

La connessione permanente a Internet implicava fino a un paio di anni fa **linee dedicate** e costi di investimento iniziali e di gestione piuttosto alti, in genere non alla portata del singolo utente; interessava dunque soprattutto enti e aziende, che entravano in rete come fornitori di informazioni e servizi.



La diffusione dei collegamenti **ADSL** e quella ancor più recente dei collegamenti in fibra ottica per privati (*FastWeb*) hanno tuttavia modificato la situazione: anche se i collegamenti temporanei restano al momento lo strumento più usato per collegarsi a Internet da casa, il numero di utenti privati con collegamenti permanenti alla rete è in continua crescita.

Le connessioni temporanee (sfruttando linee di trasmissione **commutate**) restano le meno costose per chi faccia un uso occasionale di Internet, sfruttando di norma provider gratuiti e numeri di accesso a tariffe agevolate.

Collegamenti permanenti attraverso linee dedicate

Internet, abbiamo già ricordato, è una rete costituita da un insieme di reti interconnesse. Per collegamento permanente attraverso linea dedicata, o collegamento **diretto** si intende appunto l'inserimento di un computer all'interno di una di queste sottoreti locali, o la creazione di una nuova sottorete collegata ad Internet.

Nel primo caso il procedimento, abbastanza semplice poiché esiste già una rete connessa ad Internet, richiede solo di aggiungere un computer a tale rete, e assegnare al nuovo host un indirizzo libero. Per indirizzo libero si intende uno degli indirizzi disponibili per la rete in questione non utilizzato da nessun altro host. Naturalmente questa operazione è possibile solo se il numero di computer collegati non ha esaurito il numero massimo di host consentiti. Vedremo che tale numero è determinato dalla *classe* della rete.

Nel secondo caso il procedimento è un pò più complesso. In primo luogo occorre richiedere ad un fornitore di connettività abilitato (*provider*) la possibilità di allacciare una nuova sottorete.

L'accesso normalmente viene affittato, ed ha costi variabili a seconda della larghezza di banda - ovvero della capacità dei cavi - e della classe di rete che si intende avere.

---

[1] Da “Internet 200x “ libro in rete http://www.liberliber.it/mediateca/libri/c/calvo/internet_2004/html/01_indice.htm

In realtà attualmente sono disponibili per utenti privati gli indirizzi **IP** detti "**privati**" (definiti nella RFC-1918), che non possono partecipare al *routing* pubblico globale. Questi IP addresses sono stati riservati per l'uso interno nelle organizzazioni (un azienda oppure un appartamento domestico).

Gli **indirizzi privati sono riservati** in ogni classe IP, come illustrato nella seguente tabella.

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

Un **indirizzo IP privato molto usato nei *router* ADSL** domestici è il 192.168.1.1 che di solito identifica il router stesso, mentre ai PC collegati alla rete di casa vengono assegnati indirizzi all'interno della subnet 192.168.1.0/24. Una rete domestica e' considerata una "**organizzazione**" a livello di rete, e quindi puo' utilizzare gli indirizzi privati al suo interno. Quando c'e' necessita' di collegarsi a internet, normalmente si utilizza un IP pubblico "prestato" dal service provider che fornisce il servizio ADSL. L'interfaccia tra i due dominii di routing, privato (casa) e pubblico (internet), viene gestita tramite la Network Address Translation**.**

In secondo luogo occorre affittare o acquistare un cavo fisico che colleghi la nuova rete a quella del fornitore di accesso scelto. Si noti che non necessariamente la funzione di fornitore di accesso e quella di fornitore di cavo coincidono.

Per collegare la nuova sottorete ad Internet è necessario avere un computer speciale che viene chiamato *Internet router* o *Internet gateway*. Questo dispositivo è il terminale del cavo di collegamento dedicato, ed è a sua volta collegato al *router* della rete del fornitore, già connesso ad Internet.

Il traffico in entrata e uscita dalla nostra rete passerà attraverso questo 'cancello'

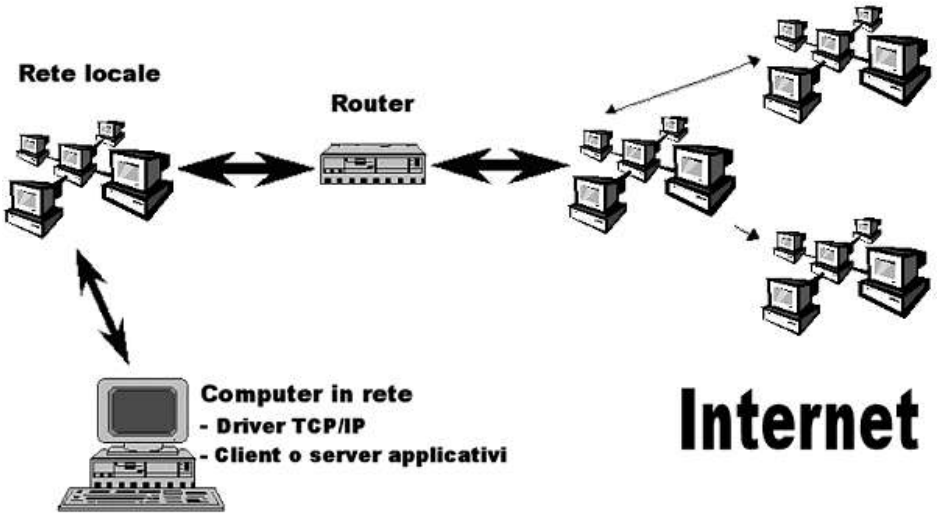


figura: Schema di un **collegamento diretto**

Le infrastrutture di rete usate nelle interconnessioni vanno dal cavo Ethernet o Token-ring, usati all'interno delle piccole sottoreti locali, fino alle dorsali continentali in fibra ottica. Come si diceva, i protocolli “TCP/IP” sono sostanzialmente indipendenti dalla tipologia dell'hardware usato nella connessione.

Naturalmente dopo avere predisposto il collegamento fisico, bisognerà installare e configurare su tutti i computer che si vorrà collegare i *driver* TCP/IP (assegnando l'indirizzo IP) e i vari software client o server che si desidera utilizzare.

In alternativa, è possibile anche assegnare un nome di **dominio** ai computer, richiedendolo all'autorità competente per l'assegnazione e registrandolo presso un DNS. Di norma tutti i fornitori di connettività a terzi si occupano delle pratiche necessarie a tale fine. Si noti che è possibile anche avere più di un nome di dominio per un singolo host. Infatti il DNS consente di associare più indirizzi simbolici ad uno stesso indirizzo IP. In questo modo lo stesso computer può rispondere, eventualmente fornendo diversi servizi, a più di un nome. A seconda del tipo di connettività che si possiede è anche possibile installare e gestire un sistema di DNS locale, che effettui la risoluzione dei nomi assegnati agli host della rete. Le operazioni di configurazione e di manutenzione di una rete non sono propriamente semplici. È necessario dunque disporre di figure professionali specifiche, gli amministratori di rete, che garantiscano la funzionalità della rete e che sappiano intervenire nel caso di problemi.

L'accesso temporaneo mediante linea commutata

Fino a pochi anni fa l'utente finale che non aveva accesso ai centri di calcolo di enti e università dotate di collegamento diretto, poteva utilizzare i servizi di rete solo in via indiretta, collegandosi (via modem) ad un host mediante un software di emulazione terminale, e usando i programmi di rete installati su tale macchina (esattamente come su Internet avviene con il collegamento telnet).

A partire dall'inizio degli anni 90 questo tipo di 'collegamenti mediati' è stato completamente rimpiazzato da una modalità di connessione assai più avanzata, che permette di collegare pienamente alla rete un computer anche senza disporre di linee dedicate. A tale fine sono stati sviluppati due protocolli: il *Serial Line Internet Protocol* (*SLIP*), poco efficiente e ormai in disuso, e il *Point-to-Point Protocol* (***PPP***), attualmente utilizzato dalla maggioranza degli utenti Internet.

Il **PPP** permette di stabilire in modo dinamico una connessione "TCP/IP" piena utilizzando un collegamento di tipo 'punto/punto', che connette direttamente una macchina chiamante a un host gia connesso in rete. Rientrano in questo tipo di collegamenti le linee parallele, le linee seriali e il loro successore *Universal Serial Bus* (USB). Poiché attraverso queste linee è possibile connettere un computer ad una linea telefonica commutata (analogica o digitale), il protocollo PPP consente di collegare un computer alla rete anche senza disporre di una infrastruttura di rete dedicata e permanente. In effetti di norma esso viene utilizzato proprio per effettuare collegamenti Internet mediante modem e linea telefonica analogica, o adattatore ISDN e linea telefonica digitale.

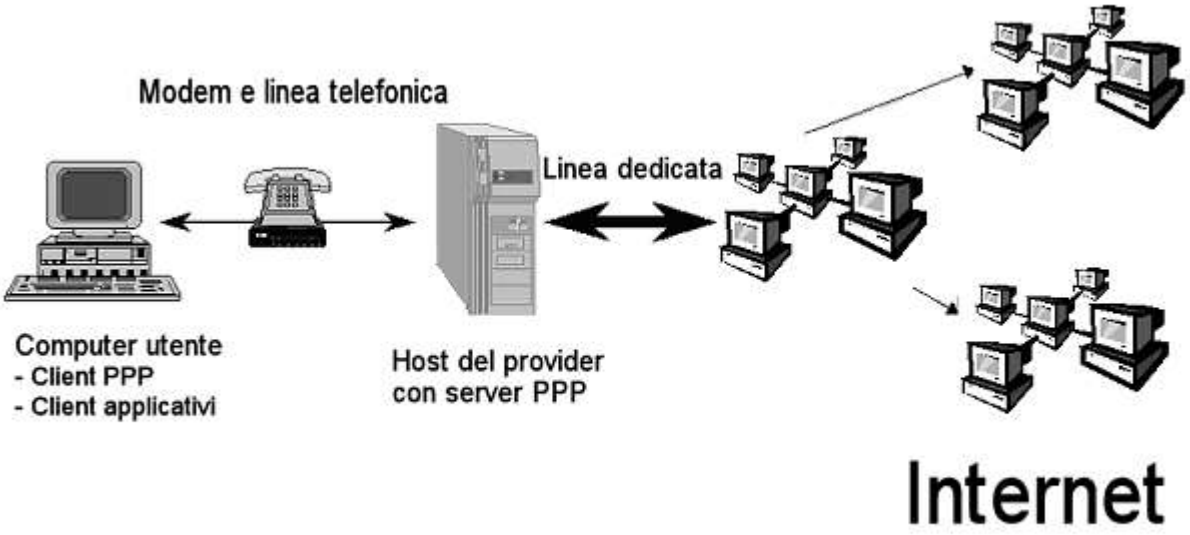


figura: Schema di un collegamento **PPP su linea commutata**

Il **PPP** è un protocollo che si basa su una interazione *client-server*. Il **server PPP** viene installato su un computer dotato di una connessione diretta ad Internet e di una serie di modem connessi ad altrettante linee telefoniche. Esso inoltre deve avere a disposizione un certo 'pacchetto' di indirizzi IP disponibili. Il PPP infatti consente l'assegnazione dinamica degli indirizzi IP: quando un utente effettua la connessione, riceve un indirizzo che rimane assegnato al suo computer solo per il tempo della connessione, e che rimane poi libero per altri utenti. Il **client PPP** invece risiede sul computer che 'chiede' il collegamento. Tutti i sistemi operativi moderni ne sono dotati, e dispongono di interfacce notevolmente semplificate per configurare i parametri necessari alla connessione, alla portata anche di utenti inesperti. Esso si occupa di effettuare la telefonata al server e di gestire le transazioni di autenticazione: ogni client infatti è associato ad una coppia nome utente/password che gli permette di utilizzare i servizi del fornitore di accesso. Fintanto che la connessione rimane attiva, il computer chiamante diviene un nodo della rete a tutti gli effetti, con un suo indirizzo e dunque visibile dagli altri nodi. In teoria è possibile anche fornire dei servizi di rete, anche se a tale fine un computer dovrebbe essere sempre in linea. Poiché il collegamento con linea commutata si paga in ragione del tempo (almeno in tutte le nazioni europee) anche se la chiamata è urbana, mantenere aperta una connessione per periodi prolungati fa immediatamente alzare i costi delle bollette ben oltre le (pur care) tariffe dei collegamenti permanenti. Inoltre la linea commutata viene usata anche per le normali chiamate vocali, e dunque non può essere occupata troppo a lungo.

Ma soprattutto la connessione su **linea telefonica commutata** presenta dei forti **limiti in termini di velocità**. Le linee analogiche permettevano di arrivare con i modem più efficienti (quelli dotati del protocollo V90) alla velocità teorica di circa 50 mila bps in entrata e 33 mila bps in uscita. Questi limiti, a dire il vero, si facevano sentire anche se il computer veniva utilizzato per accedere ai servizi di rete. Infatti, la trasmissione di informazioni multimediali richiede lo spostamento di centinaia o migliaia di kilobyte, che, anche alle velocità massime supportate dalle connessioni via modem, obbligavano ad attese molto lunghe.

Un'alternativa più efficiente alla comunicazione su linee telefoniche analogiche è rappresentata dalla già citata tecnologia ISDN (*Integrated Services Digital Network*). Si tratta di un sistema di trasmissione digitale che si basa sul normale doppino telefonico e su speciali adattatori denominati *ISDN Terminal Adaptor*, e impropriamente chiamati 'modem ISDN'. L'accesso base ISDN è costituito da una coppia di linee a 64 mila bps, che consentono anche da una utenza domestica di arrivare a una velocità massima di 128 mila bps. I costi telefonici di questo accesso sono ormai allineati a quelli delle linee analogiche in tutti i paesi europei, mentre gli abbonamenti presso i provider di servizi Internet sono talvolta leggermente più cari. La commercializzazione di ISDN ha subito molti ritardi, e solo oggi sta iniziando a diffondersi, specialmente presso l'utenza professionale. Paradossalmente, il ritardo con cui è stata introdotta ha reso ISDN una tecnologia 'anziana' prima ancora che il suo impiego uscisse dalla fase sperimentale. I servizi di rete multimediali, infatti, richiedono già ora risorse assai più elevate.

Una possibile soluzione, con l'opportunità di cablare in fibra ottica anche le abitazioni private, è venuta dalla tecnologia **ADSL**[2] (*Asymmetric Digital Subscriber Line*, Linea Utente Digitale Asimmetrica). Sfruttando intensamente le tecniche di compressione dei dati, ADSL permette di ricevere dati a 8 milioni di bps e di inviare a 1 milione di bps (per questo viene definita 'asimmetrica') attraverso i normali cavi telefonici a doppino di rame. Inoltre ADSL, a differenza di ISDN, non è una linea commutata, ma permette di realizzare a basso costo un collegamento permanente, restando comunque in grado di veicolare comunicazioni vocali.

Specifica importante nel confronto tra infrastrutture è il *bit rate* tra due host normalmente connessi da più tratte: coincide con quella della tratta più lenta espressa come massimo numero di bit per secondo che può attraversare la tratta.

---

[2] Per approfondimento consulta la guida http://www.adslforum.it/introduzione.htm

IL MODELLO ISO/OSI

Per ridurre la complessità della progettazione, il *software di rete* si presenta organizzato per livelli (layers). Ogni livello svolge dei compiti ben definiti. Esso interagisce con i due livelli adiacenti fornendo certi servizi al livello immediatamente superiore e utilizzando i servizi fornitigli dal livello immediatamente inferiore.

Un modello di riferimento è cosa diversa da un'architettura di rete:

Modello di riferimento	definisce il numero, le relazioni e le caratteristiche funzionali dei livelli, ma non definisce i protocolli effettivi
Architettura di rete	definisce, livello per livello, i protocolli effettivi

Il modello **ISO/OSI** (International Standard Organization – Open Systems Interconnection) ha lo scopo di:

- fornire uno standard per la connessione di *sistemi aperti*, cioé in grado di colloquiare gli uni con gli altri;
- fornire una base comune per lo sviluppo di *standard* per l'interconnessione di sistemi;
- fornire un modello rispetto a cui *confrontare* le varie architetture di rete.

Esso non include di per sé la definizione di protocolli specifici (che sono stati definiti successivamente, in documenti separati e rimangono uno standard "de iure" soppiantati dagli standard tecnologici "de facto" come l'architettura "TCP/IP").

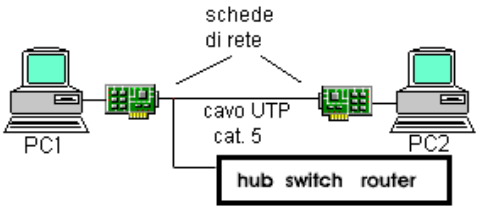
È quindi importante solo come riferimento comune ai concetti che riguardano le reti per la definizione del numero, delle relazioni e delle caratteristiche funzionali dei livelli allo scopo di definire le specifiche generali del software e dell'hardware di una rete. Esso prevede *7 diversi livelli indipendenti*:

Application
Presentation
Session
Transport
Network
Data Link
Physical

Physical

Effettua la trasmissione delle *sequenze binarie* sul canale di comunicazione[3].

Specifica i **livelli elettrici**[4] cioè i segnali fisici corrispondenti a 0 e 1, la durata del segnale che identifica il bit in protocolli asincroni (start - stop), i **livelli funzionali** (trasmissione simultanea in due direzioni o no distinguendo[5] DTE e DCE), i **livelli meccanici** come il tipo e la forma dei connettori, il tipo, le dimensioni e le impedenze dei cavi, ..etc



Specifica le *caratteristiche hardware* del controller e della scheda di rete

[3] I dispositivi che interconnettono a questo livello con la funzione di amplificare ed adattare sono i REPEATER.

[4] RS232 vs USB

[5] Nella terminologia CCITT un data terminal equipment è un dispositivo di elaborazione, tipicamente un host e un data communication equipment è un dispositivo che funge da punto di accesso: l'interfaccia di linea (con o senza modem).

Data Link[6] **(collegamento dati** nel confronto tra *protocolli di linea***)**

Si occupa della trasmissione/ricezione dei dati (*sequenze di byte*) fra due nodi collegati direttamente tramite un canale fisico[7]. Il mezzo appare una linea esente da errori (colloquio logico tra due nodi). Organizza i dati in pacchetti (frames) di lunghezza variabile da qualche byte al migliaio di bytes aggiungendo delimitatori (*FRAMING*): i protocolli di linea[8] assicurano la trasparenza e provvedono ad evitare che nel campo dati compaiano caratteri o sequenze di bit scelti come delimitatori (tecnica "character stuffing" o "bit stuffing").Verifica la presenza di errori aggiungendo in coda al pacchetto da trasmettere una FCS, (*Frame Control Sequence*) ed aspetta riscontro (ACK) per ogni frame inviato, realizzando il ***controllo di flusso***[9]. Serve, quindi, per gestire procedure di correzione di errore facendo una richiesta di ritrasmissione.

In *tecnologia broadcast* controlla l'accesso al canale condiviso con gestione collisioni.

Network

Gestisce l'instradamento dei pacchetti attraverso la rete (*ROUTING*[10]) determinando quali nodi intermedi essi devono attraversare per giungere a destinazione. La scelta del percorso logico (box-to-box) ottimale tra sub-net in una WAN è di solito in funzione del numero di *hop* (salti) tra dispositivi Router (instradatori). Gestisce la congestione (molti ingressi nel router ed unica uscita) e si occupa dell'*ACCOUNTING* (pagamento dell'uso a seconda del traffico generato).

Transport

È il primo livello orientato all'utente della rete: governa la comunicazione con il livello paritario della stazione remota e fornisce un servizio *end-to-end* indipendente dalla rete sottostante e trasparente per l'utente; può frammentare le **P**rotocol **D**ata **U**nit (*segmenti* con dimensione massima MSS consigliata) in modo che abbiano dimensioni idonee al livello 3; può rivelare/correggere gli errori (assicurando AFFIDABILITÀ se ***connesso*** come il ***TCP***), effettua il ***controllo di flusso*** con controllo sul *time-out* MULTIPLESSANDO o gestendo la diffusione (*broadcasting* a molti destinatari).

---

[6] Per approfondire

[7] I dispositivi che interconnettono a questo livello sono detti BRIDGE (con approfondimento del sottolivello MAC)

[8] Su linee pubbliche (con master che gestisce in modo polling/selecting in reti multipunto o con metodo a contesa in reti punto a punto) si inviano due possibili formati di frame: *orientati al byte* (come il BSC dell'IBM con caratteri ASCII Data Link Escape come delimitatori) o *orientati al bit* (HDLC dell'ISO-OSI con Flag cioè sequenze di bit 01111110 come delimitatori e campi di lunghezza fissa: FLAG - ADDRESS ricevente - CONTROLLO – dati – CRC – FLAG Ad eccezione del campo Codice a Ridondanza Ciclica (16 bit) e del campo dati (lunghezza tipica 1500 bit) i campi sono lunghi 1 byte; il campo controllo (dati/comandi) contiene il numero progressivo e l'ACK di riscontro).

[9] La tecnica *STOP AND WAIT* prevede anche un timer in mancanza di riscontro e la numerazione dei frame; migliore è la tecnica *SLIDING WINDOWS* dove si inviano più frame (finestra) prima di attendere riscontro. Per migliorare l'uso della banda si realizza il *PIGGYBACKING* cioè il riscontro è inviato nel frame dei dati.

[10] Il routing può essere STATICO o ADATTIVO con metodo DATAGRAM o VIRTUAL CHANNEL (canale logico commutato e connesso)

Session

È responsabile dell'organizzazione del dialogo, della sincronizzazione tra due applicazioni (tipica necessità di memorizzare account del cliente passando da una pagina web all'altra, in siti di *e-commerce*) e del conseguente scambio dati. Autorizza a turno le parti a trasmettere (*token management*) gestendo il dialogo mono o bidirezionale.

Presentation

Gestisce la sintassi e la semantica dell'informazione da trasferire nel caso in cui questa è rappresentata in modi diversi dai calcolatori che devono comunicare. Assicura uno scambio informativo con caratteri di sicurezza e privatezza (*CRITTOGRAFIA dagli inizi ad oggi*).

Application

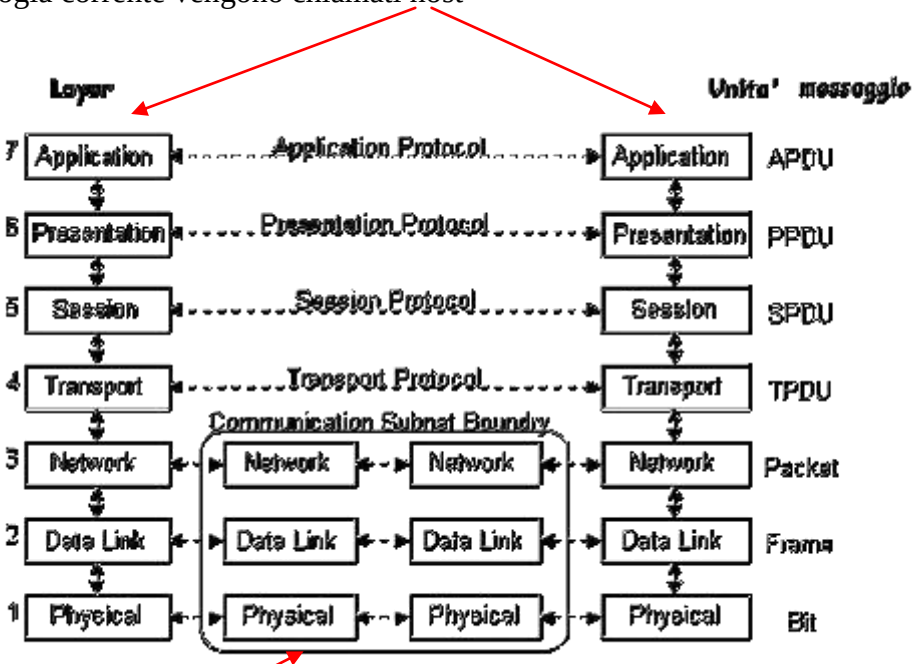
a questo livello appartengono le applicazioni utente e di sistema (comunicazione tra processi applicativi *cooperanti* che condividono risorse in *sistemi distribuiti*)

Nel modello OSI l'architettura di rete prevede due tipi di sistemi:

End System (ES)

hanno il compito di eseguire le applicazioni
realizzano tutti i livelli dell'architettura

Nella terminologia corrente vengono chiamati host



Intermediate System (IS)

svolgono funzioni connesse con l'internet working , instradano i messaggi sulla rete;
realizzano solo i primi 3 livelli della pila OSI

Nella terminologia corrente tali elementi di commutazione (*switching element*) vengono chiamati **router** (in USA Gateway[11])

Ogni livello comprende :

un insieme di **servizi** da fornire al livello superiore
uno o più **protocolli**

Servizi e protocolli sono spesso confusi, ma sono concetti ben distinti.

Servizio	insieme di operazioni primitive che un livello offre al livello superiore. Come tali operazioni siano implementate non riguarda il livello superiore.
Protocollo	insieme di regole che governano il formato ed il significato delle informazioni (messaggi, frame, pacchetti) che le peer entity si scambiano fra loro su host diversi. Le entità usano i protocolli per implementare i propri servizi.

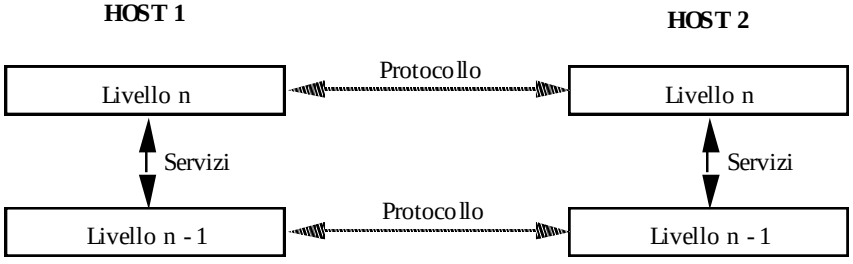


Figura: Relazione fra protocolli e servizi

[11] Gateway, a livello 7, connette servizi di ambienti altrimenti incompatibili

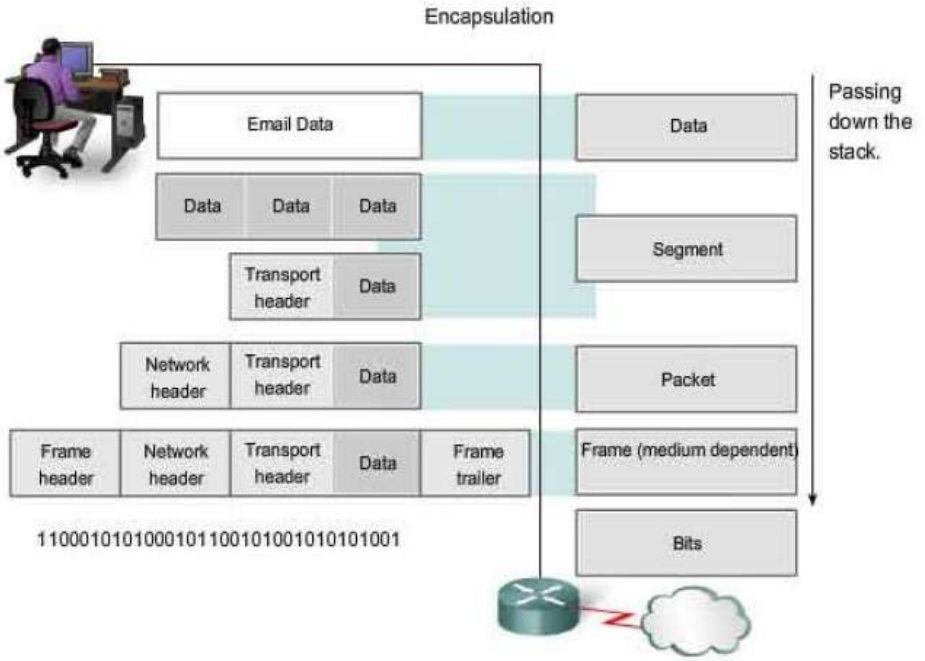
L’insieme dei *livelli* e dei *protocolli* definisce un' *architettura di rete*. Tutti i servizi di un livello vengono resi disponibili a quello superiore mediante insiemi di procedure, chiamate primitive di servizio o semplicemente **primitive**.

L’insieme delle primitive e dei servizi forniti al livello superiore è chiamato *interfaccia*.

Quando due nodi comunicano fra di loro, ogni livello su ciascun nodo scambia informazioni sia con i livelli adiacenti che con il livello paritetico dell’altro nodo.

Il trasferimento di un pacchetto da un nodo A al livello paritetico di un nodo B viene effettuato attraverso i seguenti passi:
A inoltra il pacchetto attraverso i livelli sottostanti fino a quello fisico
Il livello fisico effettua la trasmissione del pacchetto verso B il quale acquisisce il pacchetto tramite il livello fisico e lo inoltra verso i livelli superiori fino al livello paritetico con quello di A

Due livelli paritetici comunicano fra di loro scambiandosi pacchetti chiamati **PDU** (**P**rotocol **D**ata **U**nit).



Ogni livello N aggiunge al pacchetto proveniente dal livello superiore N+1 le informazioni di controllo del suo protocollo (PCI, Protocol Control Information).
Queste informazioni vengono preposte (*header*) alla PDU del livello N e costituiscono la N-PDU. La N-PDU a sua volta viene imbustata nella busta di livello N-1 e così via.

Per ogni livello, eccetto il primo, OSI definisce un set di **4 primitive**:

Request	Un' entità chiede che il livello sottostante faccia qualcosa
Indication	Un' entità viene informata di un evento dal livello sottostante
Response	Un' entità intende rispondere ad un certo evento
Confirm	È arrivata la risposta ad una richiesta precedente

Per "**entità**", OSI intende un *processo* (software) o un *componente hardware programmabile*

Per i servizi, OSI standardizza due modalità:

- servizi con conferma (***confirmed***), in cui il livello che riceve qualcosa, conferma l'avvenuta ricezione
- servizi senza conferma (***unconfirmed***), in cui il livello che riceve qualcosa non invia alcuna conferma l'avvenuta ricezione

I servizi unconfirmed usano solo le prime due primitive. I servizi confirmed usano anche le altre due.

Il modello di riferimento OSI specifica le funzioni di ciascun livello ma non il modo in cui queste devono essere implementate. Quest'ultimo compito è lasciato agli sviluppatori di software di rete.

Per quanto riguarda i protocolli possono essere di due tipi: ***connesso*** (CONS) e ***non connesso*** (CLNS).

In un protocollo ***connesso*** lo scambio dati avviene attraverso tre fasi:

- creazione di una connessione con l'host remoto
- trasferimento dei dati
- chiusura della connessione

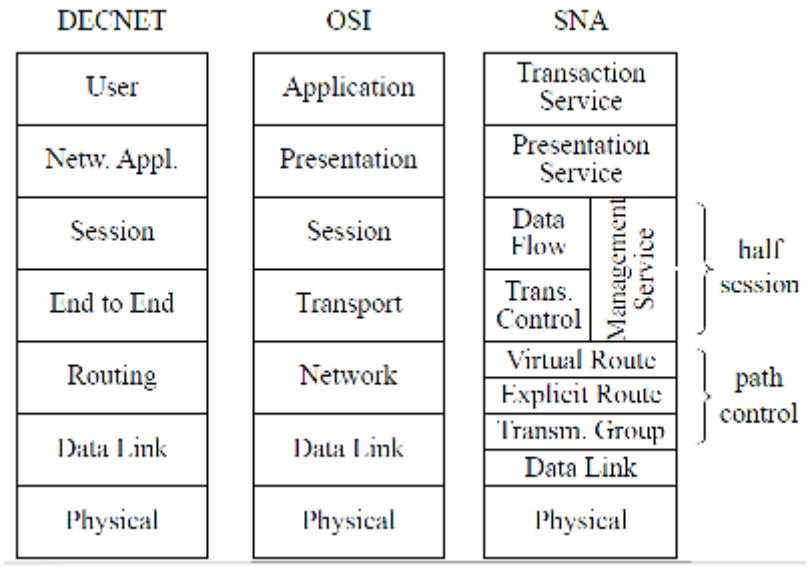
L'indirizzo completo del mittente e del destinatario viene specificato solo nella fase di creazione della connessione. Nelle trasmissioni successive si fa riferimento all'identificativo della connessione. Il protocollo garantisce la consegna dei pacchetti a destinazione, il che significa: le PDU sono inviate e ricevute secondo lo stesso ordine. A tale scopo ogni pacchetto viene numerato in modo che il ricevente possa riassemblare i dati secondo l'ordine prestabilito.
In caso di errori nella ricezione il ricevente richiede la ritrasmissione di tutti i pacchetti o di una parte di essi . Viene effettuato il *controllo di flusso*, cioè la sincronizzazione fra il processo che trasmette e quello che riceve.

In un protocollo ***non connesso*** invece non si stabilisce nessuna connessione. Ogni pacchetto trasmesso quindi deve contenere gli indirizzi completi di mittente e destinatario. Il protocollo può rilevare la presenza di errori scartando le PDU errate ma non può correggerli in quanto non può richiedere la ritrasmissione dei pacchetti errati. Per i protocolli non connessi i pacchetti vengono chiamati **datagram**.

Nel corso degli ultimi trent'anni sono state prodotte numerose architetture (alcune preesistevano a OSI stessa) proprietarie, de iure e de facto.

Un'architettura **proprietaria** è basata su scelte indipendenti ed arbitrarie del costruttore, ed è generalmente incompatibile con architetture diverse. Nel senso più stretto del termine è un'architettura per la quale il costruttore non rende pubbliche le specifiche, per cui nessun altro può produrre apparati compatibili. Esempi:

- IBM SNA (System Network Architecture)
- Digital Decnet Phase IV



Un'architettura **standard de facto** è un'architettura basata su specifiche di pubblico dominio (per cui diversi costruttori possono proporre la propria implementazione) che ha conosciuto una larghissima diffusione. Esempi:

- Internet Protocol Suite[12] (detta anche architettura TCP/IP).

Un'architettura **standard de iure** è un'architettura basata su specifiche (ovviamente di pubblico dominio) approvate da enti internazionali che si occupano di standardizzazione. Anche in questo caso ogni costruttore può proporne una propria implementazione. Esempi:

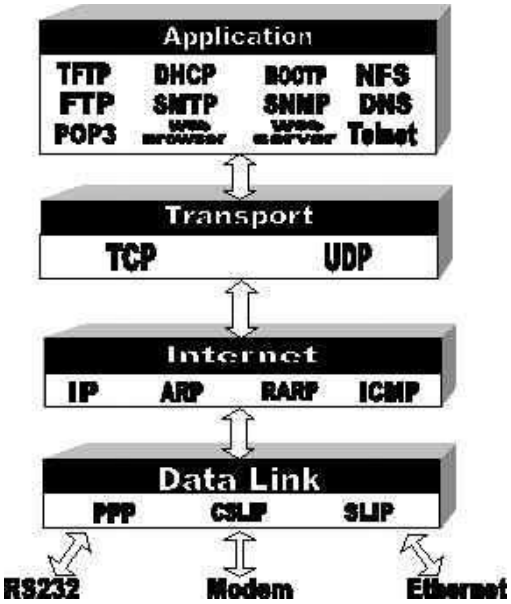
- standard IEEE 802 per le reti locali[13];
- architettura OSI (Open Systems Interconnection);
- Decnet Phase V (conforme allo standard OSI).

---

[12] Un *open standard*, ovvero le specifiche della suite sono liberamente utilizzabili da chiunque. Questo ha permesso il rapido diffondersi di implementazioni per ogni sistema operativo e piattaforma esistente, implementazioni spesso distribuite gratuitamente o integrate in modo nativo nel sistema stesso. Inoltre la suite è indipendente dal modo in cui la rete è fisicamente realizzata: può appoggiarsi indifferentemente su una rete locale Ethernet, su una linea telefonica (a commutazione di circuito o dial up), su un cavo in fibra ottica ATM, su una rete di trasmissione satellitare... e così via. Anzi consente di integrare facilmente diverse tecnologie hardware in una unica struttura logica di comunicazione, come appunto è avvenuto per Internet.

[13] 802.3 o ISO 8802.3 detta ETHERNET CSMA/CD a 10 Mbps (con codifica Manchester che per rappresentare lo "0" presenta una transizione da –0,85V a 0,85V e transizione opposta per l'"1"), a 100Mbps o FAST ETHERNET, a 1 e 10 Gbit (dette rispettivamente 802.3z e 802.3ae), ISO 8802.7 o FDDI (Fiber Distributed Data Interface) su fibra ottica; 802.5 detta TOKEN RING dell'IBM (con codifica Manchester differenziale che presenta transizioni da –3 /-4,5V a +3/+4,5V) ed 802.4 detta TOKEN BUS.

L'insieme dei protocolli utilizzati su un host e relativi ad una specifica architettura di rete va sotto il nome di ***pila di protocolli (protocol stack)***. Si noti che un host può avere contemporaneamente attive più pile di protocolli.



Oggi l'architettura di rete di gran lunga più diffusa, la più importante, rimane l'architettura Internet Protocol Suite, su cui è basata Internet: standard tecnologico che definisce i protocolli effettivi specificati in documenti RFC per **rete packet-switched** ed a livello internetwork **connectionless** con riferimento ad un modello gerarchico a ***4 strati***:

Applicazione (i servizi offerti da Internet),

Trasporto,

Internetwork

e una non meglio specificata interfaccia alla scheda di rete (**NIC** o Network Interface Controller).

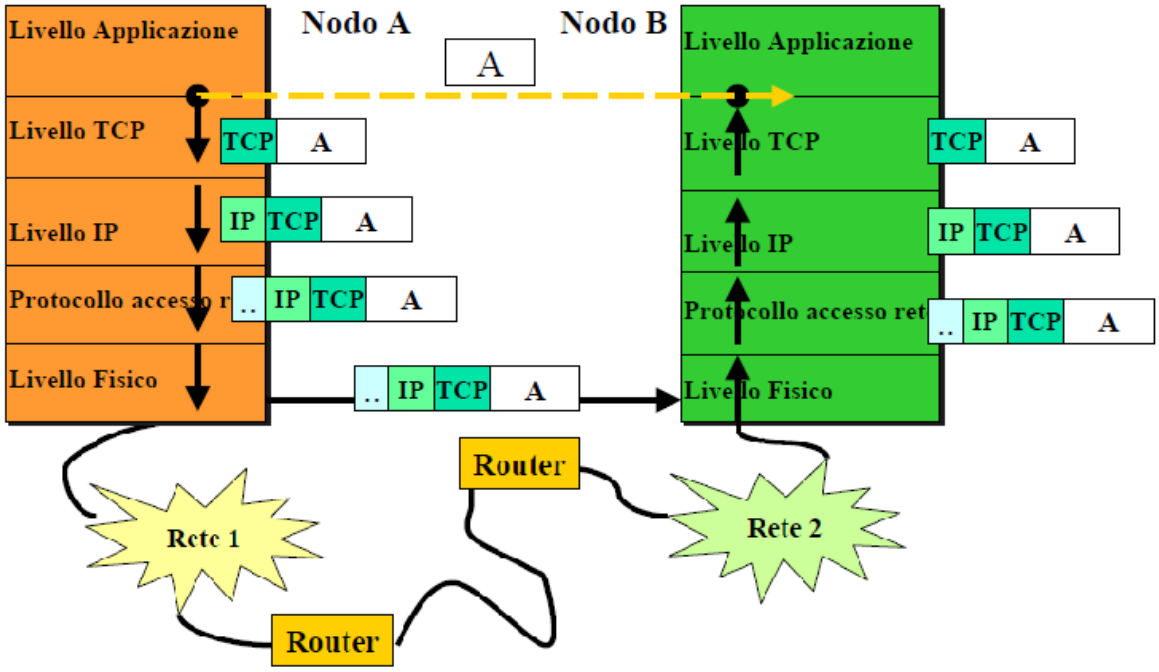
I protocolli Internet Protocol Suite

Uno degli scopi di ARPANET era lo sviluppo di uno strumento che permettesse a computers aventi diverso hardware e diversi sistemi operativi di comunicare. Questo fu realizzato attraverso la creazione di un insieme di protocolli, cioè un insieme di regole e convenzioni che tutti i computer su Internet dovevano seguire per poter comunicare. Furono infatti creati degli standards che descrivono le più importanti regole di comunicazione su Internet; l'insieme di questi standards viene riferito come Internet Protocol Suite, prendendo il nome dai due più importanti protocolli che lo compongono: il Transmission Control Protocol (TCP) e l'Internet Protocol (IP).

Il **TCP** (a livello di trasporto) converte i messaggi che devono essere inviati da un computer ad un altro in una sequenza di segmenti aggiungendo ad ognuno di essi un "header" che contiene varie informazioni tra cui il numero di sequenza del segmento. È orientato alla connessione e prevede comunicazioni affidabili full-duplex con tecnica a "finestre scorrevoli" e controllo di time-out.

I segmenti vengono poi passati al protocollo **IP** (livello di rete sottostante) che aggiunge ad ogni pacchetto un altro "header" che contiene gli indirizzi IP del computer di partenza e del computer di destinazione e istruzioni per instradare il pacchetto attraverso le varie reti su Internet.

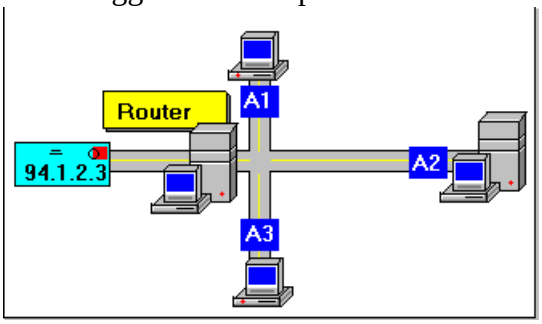
I pacchetti saranno ulteriormente frammentati in *frames* e verranno infine inviati come sequenze di livelli elettrici sul mezzo fisico di connessione della rete locale ed inoltrati ad un router della rete locale.



Un **router** è un dispositivo di comunicazione che interconnette due o più reti e che direziona i pacchetti ai computer di destinazione (a volte anche *multiprotocollo*).

Il termine router (instradatore) implica che questa entità non solo trasferisce pacchetti da una rete ad un'altra, ma prende anche delle decisioni sul percorso che tali pacchetti dovrebbero seguire. Infatti tale dispositivo è in grado di agire a livello di indirizzi di rete e, in funzione di opportuni algoritmi di instradamento, è in grado di inoltrare un pacchetto non soltanto verso una rete che garantisca la sua corretta consegna, ma cercando di ottimizzare il percorso in funzione di parametri che possono rappresentare il costo della tratta, la velocità trasmissiva associata ad un certo link, ecc.. In genere si considerasno il numero di *HOP* o salti tra un router e l'altro.

Quando un pacchetto arriva al router questo provvede a leggere l'indirizzo IP di destinazione contenuto nell' header e ad inoltrarlo ad un altro router che è connesso ad un'altra rete; questo processo continua finchè non viene raggiunto il computer di destinazione.



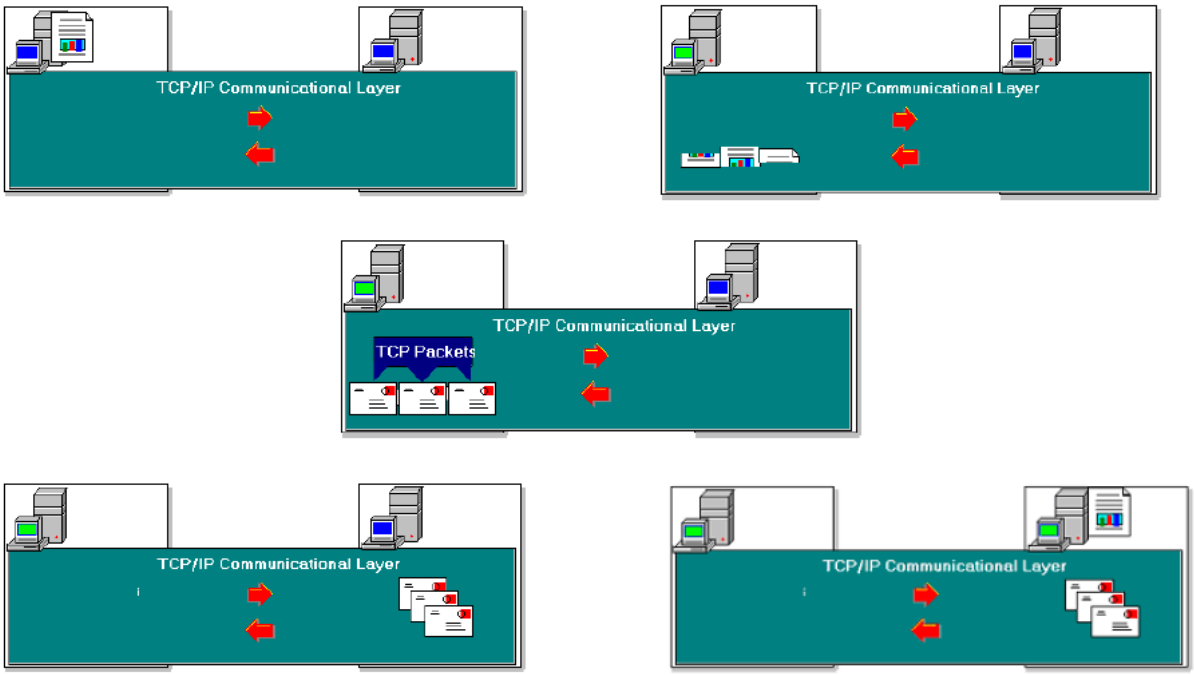
I pacchetti che formano un messaggio viaggiano pertanto attraverso una serie di routers e di reti finchè non raggiungono il computer remoto. Su tale computer il software di rete provvederà a togliere gli headers e a riassemblare i vari pacchetti così da formare il messaggio originale.

Quanto descritto mostra un aspetto chiave di Internet: la **commutazione di pacchetto**.

Commutazione di pacchetto

In una rete a commutazione di pacchetto l'informazione da trasmettere è suddivisa in pacchetti di dimensione abbastanza piccola; ad ognuno di essi viene aggiunta un'intestazione che contiene tutta l'informazione necessaria affinché il pacchetto sia inoltrato alla sua destinazione finale.

I pacchetti sono inviati individualmente attraverso la rete e vengono poi riassemblati nella loro forma originale quando arrivano sul computer destinazione.



Poiché ogni pacchetto porta con sè la sua identificazione, una data rete può trasportare nello stesso tempo pacchetti provenienti da computers differenti.

La commutazione di pacchetto permette quindi a più utenti di inviare informazioni attraverso la rete in modo efficiente e simultaneo, risparmiando tempo e costi sulle linee telefoniche, sulle connessioni radio e via satellite. E poiché i pacchetti possono prendere strade alternative sulla rete, la trasmissione dei dati è facilmente mantenuta anche se parti della rete sono danneggiate o non funzionano efficacemente.

All'interno del **modello gerarchico** a 4 strati su cui si basa l'**Internet Protocol Suite** – a confronto con i 7 del modello OSI – si sono sviluppati i protocolli sotto-elencati:

livello ***Applicazione*** (corrisponde ai livelli Applicazione, Presentazione e Sessione del modello OSI).

Esempi di ***protocolli applicativi***[14]:
HTTP (HyperText Transport Protocol) per il World Wide Web,
NNTP (Network News Transport Protocol) per UseNet sistema che permette la condivisione di messaggi distribuiti elettronicamente in tutto il mondo in formato standard suddivisi per argomento in categorie chiamati newsgroup (bacheche elettroniche per conferenze in rete);
DNS per mapping tra nomi simbolici e indirizzi numerici che identificano in modo univoco un host connesso ad Internet,
SMTP (Simple Mail Transport Protocol[15]), IMAP (Interactive Mail Access Protocol) o POP3 (Post Office Protocol[16]) per la posta elettronica,
Telnet per connessione interattiva con host remoto (login remoto) o il più attuale SSH (Secure Shell in modalità cifrata su porta 22),
streaming multimedia (protocollo proprietario TCP o UDP),
internet telephony (protocollo proprietario tipicamente UDP),
file server remoto (NSF con protocollo TCP o UDP).

- livello ***Trasporto***: protocolli TCP connesso e UDP non connesso (nel caso di comunicazioni brevi e veloci senza accordo tra parti né garanzia di consegna)
- livello ***Internetwork*** o Rete (protocollo **IP** ad esempio)
- ed un non meglio definito livello di ***interfaccia alla scheda di rete*** o Network Interface Controller (corrisponde ai livelli Data link e Fisico del modello OSI)

La suite usa a livello **collegamento dati** i protocolli IEEE 802.3 per reti locali e X.25 per reti geografiche (suite X.25 del CCITT ora ITU-T per reti a pacchetto e circuito virtuale, nata nel '70 per trasmettere dati su linee analogiche e precedente a OSI, distingue tre livelli gerarchici: fisico, trama e pacchetto; il protocollo a livello di pacchetto dà nome alla suite che denomina DTE il lato utente e DCE il lato rete).

---

[14] Altre applicazioni sono PING e FINGER entrambe col pregio di velocizzare: la prima seve per verificare se un host è attivo e connesso in rete senza una vera connessione; la seconda per verificare se esiste una "casella postale" per un certo utente su una macchina senza invio di e-mail. Altra risorsa Internet è l'IRC (Internet Relay Chat) che usa una rete a parte per comunicare, via tastiera, in tempo reale.

[15] Per trasmettere a server di posta SMTP (porta 25 per gestione dei messaggi in uscita) e leggere con protocollo IMAP (su porta 143) senza copia sul PC dell'utente cioè "in remoto".

[16] Per leggere e comunicare con autentificazione con server di posta POP3 (porta 110 per gestione messaggi in entrata) prevedendo download in locale

In topologie **punto a punto** usa un protocollo orientato al byte (**PPP**) molto simile alla trama dell'HDLC

PPP

Il protocollo HDLC ha la grave carenza di non avere una modalità standard per **trasmettere sullo stesso canale pacchetti generati da diversi protocolli di livello superiore**. Per questo motivo è stato creato un nuovo protocollo come **estensione di HDLC** detta **PPP** (*Point to Point Protocol*).

FLAG	*ADDRESS*	*CONTROL*	*PROTOCOL*	*INFO*	*FCS*	*FLAG*
1 byte	*1 byte*	*1 byte*	*2 byte*	*Da 512 a 1500 byte*	*2 byte*	*1 byte*

Il campo informativo, insieme ai dati costituenti il messaggio da trasmettere, contiene le intestazioni (*header*) dei protocolli di livello superiore per un totale di *32 byte*.

La differenza principale rispetto ad HDLC risiede nella presenza di un campo ***protocol*** lungo 2 ottetti. Si noti inoltre che PPP pone **limitazioni** ai valori leciti per alcuni altri campi ed in particolare:

- Il campo *address* deve sempre contenere la sequenza binaria 11111111 che corrisponde alla codifica *broadcast*. PPP non assegna indirizzi alle stazioni essendo un protocollo punto-punto.
- Il campo *control* deve sempre contenere la sequenza 11000000, cioè la trama deve essere un U-frame di tipo UI (Unnumbered Information). La trasmissione è sempre di tipo non connesso e la lunghezza del campo control è sempre un ottetto.
- Il campo *information* ha una lunghezza compresa tra 0 e 1500 ottetti. La lunghezza massima può essere cambiata di comune accordo alle stazioni.
- Il campo FCS ha una lunghezza di 2 ottetti, ma può essere portato a 4 di comune accordo dalle stazioni.

I protocolli di comunicazione della suite risolvono in modo molto efficiente i tipici problemi di ogni sistema telematico:

* **sfruttare** al meglio le risorse di comunicazione disponibili
* permettere un **indirizzamento efficiente** e sicuro dei computer collegati, anche se questi sono diversi milioni
* garantire con la massima **sicurezza** il buon fine della comunicazione
* permettere lo **sviluppo** di risorse e servizi di rete evoluti e facilmente utilizzabili dall'utente.

Dimensioni consigliate dei segmenti (TPDU – Transport Protocol Data Unit)

E' necessario definire la lunghezza del segmento oltre che **in funzione delle capacità di trasmissione del mittente e di ricezione del destinatario**, anche e soprattutto **in funzione delle caratteristiche della rete**, come per esempio la grandezza massima del frame fisico, o Maximum Transfer Unit (MTU).

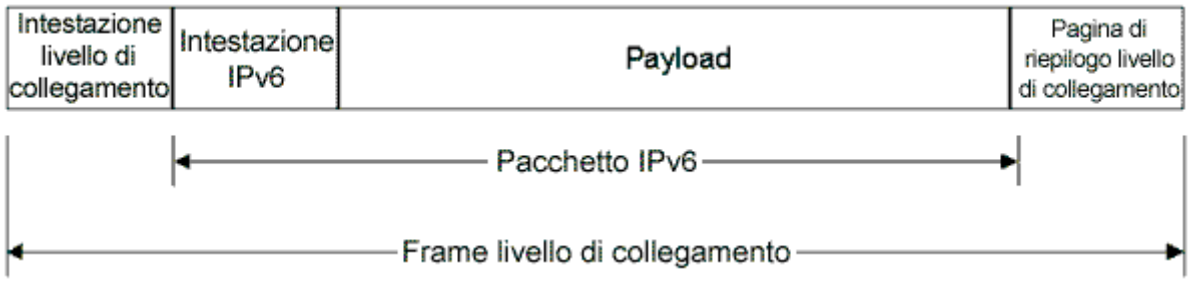
Valori della MTU (maximum transfer unit) per una serie di reti diverse.

Rete	MTU
Hyperlink	65535
Token Ring IBM (16 Mbit/sec)	17914
Token Ring IEEE 802.5 (4 Mbit/sec)	4464
FDDI	4532
Ethernet	1500
X.25	576

La MTU più piccola fra due stazioni viene in genere chiamata *path MTU*, che dice quale é la lunghezza massima oltre la quale un pacchetto inviato da una stazione ad un'altra verrebbe senz'altro frammentato. Si tenga conto che non è affatto detto che la path MTU sia la stessa in entrambe le direzioni, perché l'instradamento può essere diverso nei due sensi, con diverse tipologie di rete coinvolte.

Il protocollo TCP definisce una lunghezza massima di un segmento o *maximum segment size* MSS (**Maximum Segment Size**) che annuncia all'altro capo della connessione la dimensione massima del segmento di dati che può essere ricevuto, così da evitare la frammentazione. E' indipendente dalla semantica (un indirizzo può essere spezzato in più segmenti) e di norma viene impostato alla dimensione della MTU dell'interfaccia meno la lunghezza delle intestazioni di IP e TCP se entrambi gli estremi della connessione si trovano nella stessa rete fisica, altrimenti lo standard raccomanda di utilizzare un valore di **536 byte**, equivalente alla dimensione normale di un datagramma IPv4 meno le dimensioni standard delle intestazioni IP e TCP sommate insieme, 40 byte appunto.

Nel caso della più attuale versione 6 (IPv6) si richiede un livello di Data Link che supporti una dimensione minima del pacchetto IPv6 di 1280 byte (con 40 byte di intestazione IP) e si consiglia una dimensione MTU a 1500 byte (tipica d'incapsulamento ETHERNET II) preferendo collegamenti con MTU configurabile[17].



[17] Un esempio di collegamento con MTU configurabile è il PPP con Maximum Receive Unit

Il 3-Way Handshaking

La sessione TCP si apre attraverso il metodo di Handshake a tre vie. Ogni segmento del protocollo TCP è numerato, e precisamente ogni segmento contiene:

- Il numero del pacchetto (SEQN)
- Il numero dell'ultimo pacchetto ricevuto dall'host mittente aumentato di uno (ACKN)

Ogni host tiene quindi in memoria due contatori che contengono il numero del successivo pacchetto da inviare e quello da ricevere.

Il 3-Way Handshaking serve a sincronizzare i due contatori fra gli host.

Esso funziona in questo modo:

- L'host mittente invia un pacchetto con il flag SYN impostato su 'on'.
- Il ricevente riceve la richiesta e risponde a sua volta con un pacchetto con il flag di sincronizzazione SYN 'on', il numero di sequenza per i segmenti da inviare, il numero di sequenza per quelli da ricevere.
- L'host mittente, ricevuti questi pacchetti, risponde con un segmento contenente i due numeri sequenziali dei segmenti.

In modo analogo il TCP utilizza questo sistema per **terminare la connessione** **(four-way handshake)** assicurandosi che la trasmissione dei dati sia realmente terminata.

In sintesi: se in risposta al *Syn* arriverà un *Syn/Ack*, sapremo che la porta è aperta e che qualcuno dall'altra parte è in ascolto. In caso contrario, riceveremo un *Rst* e quindi nessuna possibile porta cui collegarsi.

Questo metodo ha il vantaggio di essere estremamente semplice e rapido e nello stesso tempo è facilmente rilevabile. Infatti, alla ricezione del Syn/Ack di risposta, la funzione connect() manderà l'Ack che completerà la connessione, la cui traccia finirà nel log di qualsiasi daemon ci sia dall'altra parte, per cui, un eventuale hacker, a meno di mascherarsi attraverso un proxy socks, sarà già alla fine del viaggio nel tentativo di scan.

Indirizzi IP (Livello Rete: connectionless[18], non affidabile, best-effort-delivery**)**

Un indirizzo IPv4[19] è un numero a 32 bit che viene scritto come quattro segmenti di otto bit ciascuno (bytes) che sono espressi in forma decimale e separati da punti XXX.YYY.ZZZ.TTT.

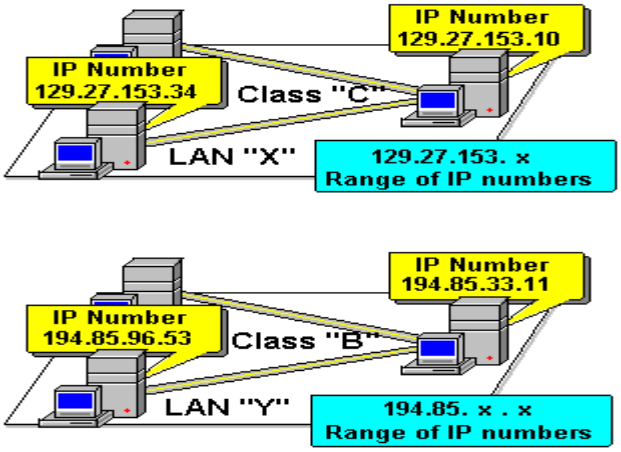
L'indirizzo è suddiviso in due campi, chiamati ***campo rete*** e ***campo host***. Il campo rete identifica, all'interno di Internet, la rete a cui l'host è connesso (così che tutti gli host di una stessa rete hanno lo stesso campo rete), mentre il campo host identifica un particolare host attaccato ad una data rete.

Il campo rete dell'indirizzo IP è assegnato da un'autorità centrale, il NIC (**N**etwork **I**nformation **C**enter), mentre amministratori locali hanno la responsabilità dell'assegnazione dei singoli indirizzi di host per una data rete.

Gli indirizzi IP vengono distinti in ***5 classi*** o forme standard per **IPv4** (classe per reti estese con oltre 16 milioni di host, classe per reti con max 65536 host, classe per piccole reti cioè minore di 256 host, una per distribuzione dei dati "multicasting" ed una riservata per usi futuri).

A	0 Rete	Host	Host	Host
B	10 Rete	Rete	Host	Host
C	110 Rete	Rete	Rete	Host
D	1110	Indirizzo multicast		
E	11110	Riservato per usi futuri		

Tali cinque classi (A, B, C, D, E) si differenziano in funzione di quanti dei quattro bytes sono utilizzati per identificare la rete e quanti per identificare gli host. Più precisamente gli indirizzi IP di classe A sono caratterizzati dall'avere 1 byte per il campo rete e 3 bytes per il campo host (reti estese), disposizione opposta per quelli di classe C (piccole reti), gli indirizzi IP di classe B hanno 2 bytes per il campo rete e 2 bytes per il campo host (con max 65536 host appunto), gli indirizzi di classe D sono riservati alla distribuzione dei dati in modo *diffuso* e la classe E è quella riservata per usi futuri. Le due classi più comunemente usate sono la B e la C. Le grosse organizzazioni preferiscono avere una rete di classe A o B che poi suddividono, tramite una mascheratura (Subnet Mask), in sottoreti.



[18] Essendo "senza connessione" è necessario l'indirizzo del destinatario del pacchetto, il pacchetto può non arrivare ma in caso di guasto (di un router) si farà il possibile per recapitare il pacchetto per vie alternative

[19] Definito nel 1981 su RFC 791 http://www.faqs.org/rfcs/rfc791.html

IPv6: più ampio spazio di indirizzamento

Un indirizzo **IPv6** è a 128 bits (8 campi da 16 bits) con rappresentazione esadecimale e due punti come simbolo di separazione: ogni blocco a 16 bits viene infatti convertito in numero esadecimale a 4 cifre e separato da ":"

`2001:0db8:85a3:0000:1319:8a2e:0370:7344` rappresenta un indirizzo IPv6 valido

Spesso, in forma semplificata, si eliminano gli zeri iniziali (pur se ogni blocco deve contenere almeno una cifra es. ff02:0:0:0:0:0:0:2) e può essere compresso sostituendo ai blocchi che contengono solo zeri il simbolo "::" (l'esempio precedente diventa ff02::2).

È stato proposto all'interno della suite sviluppata da **I**nternet **E**ngineering **T**ask **F**orce inizialmente detta *IP - The next generation*):

- non identifica un nodo ma le interfacce[20] relative (*collegamenti*),
- semplifica l'intestazione (7 campi in 40 byte invece di 13 in 20 byte dell'IPv4)
- e la modifica (senza checksum, c'è un campo etichetta del flusso per indicare ai router una speciale gestione dei pacchetti),
- semplifica il compito dei router che non frammentano i pacchetti che ritrasmettono (anche se possono frammentare i pacchetti che generano loro stessi) con MTU minimo a 1280 byte (invece che 576 byte dell'IPv4 con frammentazione eventuale nei router),
- introduce sicurezza e migliore qualità del servizio.
- Non sono previsti *nè subnet mask, nè indirizzi broadcast.*

Esistono infatti tre tipi di indirizzo IPv6:

- unicast (unica interfaccia),
- multicast (più interfacce con indirizzi solo di destinazione non intermedi),
- anycast (attualmente assegnati solo ai router come indirizzi destinazione)

" Se l'intero pianeta, terraferma e acqua, fosse coperto di computer, IPv6 permetterebbe di utilizzare 7×10^{23} indirizzi IP per metro quadro … "

Si distinguono IPv6 per **host** e per **router**:

- IPv6 **per host**: di solito un host IPv6 dispone di più indirizzi IPv6, anche con una sola interfaccia. Ad un host IPv6 vengono assegnati i seguenti indirizzi unicast:
  - Un indirizzo locale del collegamento per ciascuna interfaccia
  - Indirizzi unicast per ciascuna interfaccia (che possono essere un indirizzo locale del sito e uno o più indirizzi unicast globali aggregabili equivalenti a quelli pubblici dell'IPv4)
  - Un indirizzo di loopback (::1) per l'interfaccia di loopback (elaboro come se fosse in arrivo)

  Un host IPv6 tipico è ***multihomed*** (dispone di più interfacce o indirizzi) in quanto dispone di almeno due indirizzi attraverso i quali è in grado di ricevere pacchetti: un indirizzo locale del collegamento per il traffico del collegamento locale e un indirizzo locale del sito instradabile o aggregabile.

  Inoltre, ciascun host è in grado di eseguire l'ascolto del traffico sui seguenti indirizzi multicast:
  - Indirizzo multicast di tipo "tutti i nodi" dell'ambito locale del nodo (ff01::1)
  - Indirizzo multicast di tipo "tutti i nodi" dell'ambito locale del collegamento (ff02::1)
  - Indirizzo del nodo richiesto per ciascun indirizzo unicast
  - Indirizzi multicast dei gruppi aggiunti

[20] In Linux ogni interfaccia è distinta da un nome (es. 'eth0' interfaccia ETHERNET; 'fddi0' interfaccia con fibra)

- IPv6 **per router**: a un router IPv6 vengono assegnati gli indirizzi unicast seguenti:
  - Un indirizzo locale del collegamento per ciascuna interfaccia
  - Indirizzi unicast per ciascuna interfaccia (che possono essere un indirizzo locale del sito e uno o più indirizzi unicast globali aggregabili)
  - Un indirizzo anycast subnet-router
  - Indirizzi anycast aggiuntivi (opzionali)
  - Un indirizzo di loopback (::1) per l'interfaccia di loopback

  Inoltre, ciascun router è in grado di eseguire l'ascolto del traffico sui seguenti indirizzi multicast:
  - Indirizzo multicast di tipo "tutti i nodi" dell'ambito locale del nodo (ff01::1)
  - Indirizzo multicast di tipo "tutti i router" dell'ambito locale del nodo (ff01::2)
  - Indirizzo multicast di tipo "tutti i nodi" dell'ambito locale del collegamento (ff02::1)
  - Indirizzo multicast di tipo "tutti i router" dell'ambito locale del collegamento (ff02::1)
  - Indirizzo multicast di tipo "tutti i router" dell'ambito locale del sito (ff05::2)
  - Indirizzo del nodo richiesto per ciascun indirizzo unicast
  - Indirizzi multicast dei gruppi collegati

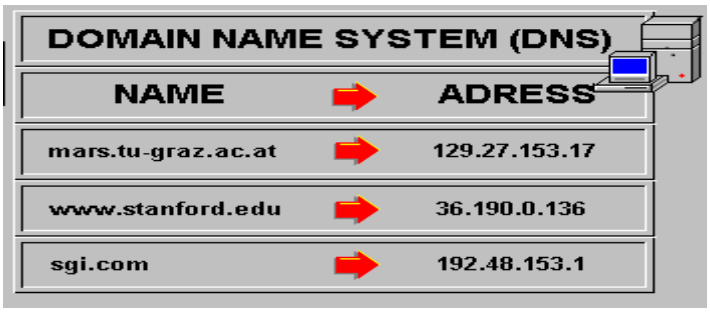
Servizi offerti da INTERNET (Livello Applicazione)

DNS[21] (Domain Name System)

Sebbene i computers usino gli indirizzi IP per comunicare, questi stessi numeri possono essere difficili da ricordare. Da ciò deriva che ai computers e alle reti vengono di solito assegnati anche dei nomi: la combinazione tra il nome di un computer e quello della rete a cui esso appartiene forma l'indirizzo simbolico (*domain name*) per quel particolare computer connesso ad Internet.

Questo sistema di nomenclatura viene definito Domain Name System (DNS). I vantaggi di questo servizio sono la possibilità dell'uso di indirizzamento indipendente da quello numerico.

Ogni computer connesso ad Internet è pertanto conosciuto, oltre che con un indirizzo IP, anche con un indirizzo simbolico. Quest'ultimo indirizzo è formato da gruppi di caratteri separati dal punto e viene definito da regole precise. Esiste infatti una relazione tra gli indirizzi simbolici assegnati ai computer e la loro collocazione geografica; relazione che invece non esiste per l'indirizzo IP.



Per fare un esempio che chiarifichi quanto detto mostriamo come è strutturato l' indirizzo simbolico di un computer della LAN (Local Area Network):

domain name: *"nomecomputer".nomereparto.nomeditta.it*

tale indirizzo si legge da destra a sinistra:

dominio principale: *it* (Italia; altri es. *fr*, *uk*, *edu*, ...)
sottodominio: *nomeditta* (La ditta che richiede un indirizzio IP)
istituto cittadino: *nomereparto* (Reparto della ditta)

Per contattare un computer su Internet occorre indicare il suo indirizzo IP o il suo domain name; ogni qual volta viene dato l'indirizzo simbolico questo deve essere convertito nel corrispondente indirizzo IP.

Poiché per qualsiasi computer sarebbe impossibile tenere localmente una lista aggiornata dei domain names e degli indirizzi IP di tutti i computer connessi ad Internet, ad ogni rete su Internet è richiesto di avere accesso ad *almeno due computer* che vengono chiamati *Name Servers*.

Un **Name Server** è un data-base che contiene appunto un elenco di corrispondenze domain name - indirizzo IP per un sottoinsieme degli host connessi ad Internet; sono queste macchine che rendono possibile l'utilizzo di indirizzi simbolici al posto di lunghe stringhe di numeri per indirizzare un computer connesso ad Internet. I Name Servers vengono contattati dagli host appartenenti ad una rete ogni volta che un programma che gira su un computer della rete medesima specifica un domain name. Se il Name Server primario non ha l'indirizzo IP per quell'indirizzo simbolico, esso contatterà altri Name Servers finchè non ne verrà trovato uno che possiede l'indirizzo IP corrispondente a quell'indirizzo simbolico. Questo indirizzo IP sarà poi ritornato al computer locale e sostituito all'indirizzo simbolico nel programma che ne faceva uso.

---

[21] Applicazione con uso del protocollo **UDP** (su porta 53) http://www.faqs.org/rfcs/rfc768.html

Altri servizi offerti da INTERNET (Livello Applicazione)

I servizi offerti da Internet spaziano in qualsiasi settore del sapere, e pertanto e` facile intuire come il loro uso possa aprire utili prospettive in tutti i settori. Tali servizi offrono infatti nuovi strumenti di lavoro che permettono di allargare in tempi brevissimi le informazioni. I servizi di base disponibili su Internet sono rappresentati da due importanti applicazioni che fanno parte integrante dell'Internet Protocol Suite: FTP e Telnet.

FTP[22] (File Transfer Protocol) è un programma applicativo di trasferimento file che permette agli utenti di trasmettere o ricevere file arbitrariamente grandi tra macchine eterogenee.

Telnet[23] è un protocollo di terminale remoto. Esso permette all'utente di un computer di collegarsi ad una macchina remota e di aprire su di essa una sessione di login interattiva, nel corso della quale e` possibile lanciare dal computer programmi residenti sull'elaboratore remoto. Telnet permette pertanto ad apparecchiature di basso costo collegate in rete, quali PC, di fornire servizi di buona qualità se messe in grado di sfruttare le risorse di sistemi remoti più evoluti.

Ma oltre alle funzionalità FTP e Telnet esistono altri servizi resi disponibili su Internet; tali servizi possono a grandi linee essere divisi in quattro gruppi:

- **posta elettronica e Mailing List**, che permettono agli utenti di contattarsi e inviarsi messaggi, e, nel caso delle Mailing List, di distribuire messaggi ad un grande uditorio;
- **UseNet**, é un sistema che permette la condivisione di messaggi distribuiti elettronicamente in tutto il mondo in formato standard. I messaggi scambiati su Usenet sono suddivisi per argomento in categorie chiamati newsgroups;
- **File Servers**, che sono depositi di informazione e dati a cui si può accedere attraverso Internet per inviare o prendere particolari files;
- **World Wide Web** (WWW), che permette agli utenti di consultare, in base alle proprie esigenze, i contenuti di data-base multimediali distribuiti su Internet.

Posta elettronica e Mailing List

La posta elettronica rappresenta la connessione personale che un utente ha su Internet. Tale servizio fornisce la possibilità di scambiare in modo rapido comunicazioni private tra individui e si basa sugli stessi concetti del servizio postale: un utente invia la posta ad altri utenti, specificando il loro indirizzo, e riceve da questi messaggi grazie al fatto che ogni utente possiede un indirizzo di e-mail che lo identifica univocamente all'interno di Internet.

Il vantaggio principale del servizio di posta elettronica consiste proprio nella rapidità delle comunicazioni: il messaggio inviato giunge infatti sempre a destinazione in un tempo dell'ordine dei secondi o al massimo di ore. Un altro vantaggio è rappresentato dal fatto che è possibile allegare ad un messaggio di posta elettronica immagini, suono, video e persino software.

Le Multi-purpose Internet Mail Extensions (**MIME**) rendono possibile questa potenzialità. Lo standard MIME consente infatti di spedire tramite posta elettronica documenti complessi. Raramente, in presenza di interruzioni su collegamenti della rete, può succedere che un messaggio spedito dall'utente non giunga a destinazione. In tal caso il messaggio, arricchito da alcune righe da

[22] Su porta 20 per dati e 21 per controllo
[23] su porta 23

cui si può comprendere quale problema sia intervenuto, viene rispedito al mittente. L'efficienza del servizio di posta elettronica dipende molto anche dall'uso che ne viene fatto: l'utente dovrebbe infatti aprire la propria casella postale ad intervalli di tempo regolari per evitare grossi accumuli di messaggi e che un messaggio arrivato regolarmente a destinazione rimanga non letto. Ricordiamo alcuni gestori di posta come Eudora, Outlook, Netscape.

Mailing lists

Quando un certo numero di persone condividono un interesse comune e` naturale che la posta mandata tra gli individui di quel gruppo possa essere di interesse anche per altri. Questi interessi comuni hanno portato alla creazione di mailing lists a cui un utente può iscriversi. Tale iscrizione permette di inviare messaggi ad un indirizzo centrale, da cui poi sono inoltrati a tutti gli utenti appartenenti alla mailing list. Le mailing lists possono essere gestite da un moderatore che ha il compito di accettare o meno le iscrizioni e di eliminare eventuali messaggi non inerenti al gruppo di interesse.Gli ovvi vantaggi delle mailing lists sono quelli di fornire informazioni condivise tra grandi gruppi di utenti e facilitare la discussione "online" di argomenti di interesse.

UseNet[24]

Netnews, o Usenet, é un sistema che permette la condivisione di messaggi distribuiti elettronicamente in tutto il mondo in formato standard. I messaggi scambiati su Usenet sono suddivisi per argomento in categorie chiamati newsgroups. Questi messaggi possono contenere sia testo che informazioni codificate in modo binario. Un utente può registrarsi a qualsiasi newsgroups di interesse e guardando il soggetto dei messaggi (il soggetto descrive l'argomento contenuto in un messaggio) può selezionare quali leggere; questo meccanismo differisce da quello delle mailing lists dove invece ogni utente iscritto ad una lista riceve obbligatoriamente tutti i messaggi inviati all'indirizzo centrale. Un’altra differenza rispetto alle mailing list é che un utente può registrarsi ad un qualsiasi newsgroups di interesse senza bisogno di avere una casella di posta elettronica, condizione che e` invece indispensabile per potersi iscrivere ad una mailing list. Inviando un messaggio[25] ad un certo newsgroup un utente, alle prese con un qualsivoglia tipo di problema, può intraprendere una discussione che coinvolge centinaia di persone in tutto il mondo.

File Servers

I File Servers (remoti o NFS) sono dei grandi contenitori di dati messi a disposizione di tutti gli utenti di Internet. Tali DataBase sono pubblicamente accessibili, e i documenti in essi contenuti possono essere recuperati o mediante FTP o tramite posta elettronica.

[24] NNTP su porta 119. Gli antenati delle newsgroup sono le BBS (Bulletin Board System) amatoriali

[25] Per liste e UseNet esistono elenchi e cataloghi ma le *conferenze via Web* o FORUM non fanno capo ad una risorsa centralizzata ed è impossibile catalogarli: sono siti o gruppo di pagine in sito per visualizzare un elenco di messaggi, leggerli e scriverne di nuovi in risposta o su altro argomento (ad esempio il forum di La Repubblica).

World Wide Web[26]

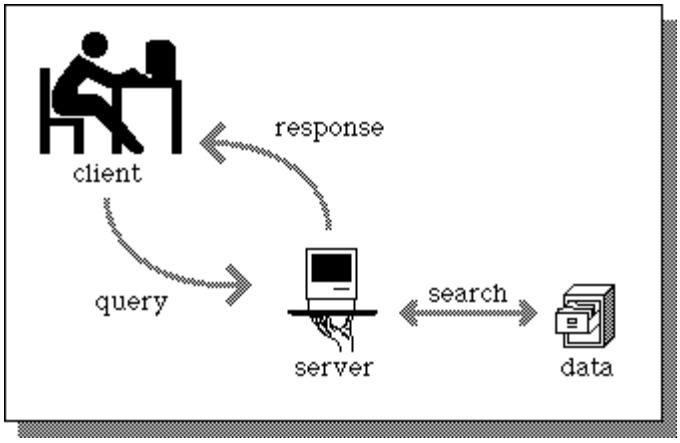
Il più interessante servizio Internet di questi ultimi anni è sicuramente il WWW (World Wide Web). Il **WWW**, istituito dal CERN (European Laboratory for Particle Physics), nacque come un consorzio di utenti che ha realizzato una sintassi standard, non proprietaria, denominata HTML (HyperText Markup Language) per la composizione di documenti. L'HTML permette il corretto display di files provenienti da computer differenti, superando cosi` l'incompatibilità tra il formato di documenti provenienti da differenti piattaforme hardware e software. L'aspetto più importante del WWW è l'uso dell'ipertesto.

L'**ipertesto** è una metodologia che consente collegamenti associativi, ed è stato originariamente utilizzato per connettere parole, file e paragrafi (strutture di un testo), in modo dinamico, per mezzo di collegamenti determinati in modo interattivo dalle associazioni inerenti il materiale testuale sotto studio.

Ad esempio, in un ipertesto generalmente le parole chiave che determinano un link sono evidenziate in maniera tale che il lettore venga messo a conoscenza dell'esistenza del collegamento e possa decidere se e quando sfruttarlo, magari effettuando un semplice clic con il mouse sopra ad una parola chiave.

Il **WWW** (protocollo HTTP) permette agli utenti di consultare, in base alle proprie esigenze, i contenuti di ***data-base*** *multimediali distribuiti* su Internet.

Una caratteristica fondamentale di tutti i servizi offerti da Internet è l'utilizzazione del modello **Client/Server**.



Un Server è un *processo* (un software speciale che risiede su un certo computer presente da una qualche parte sulla rete), sempre attivo e in attesa, accetta richieste da più client ed invia automaticamente risposte.

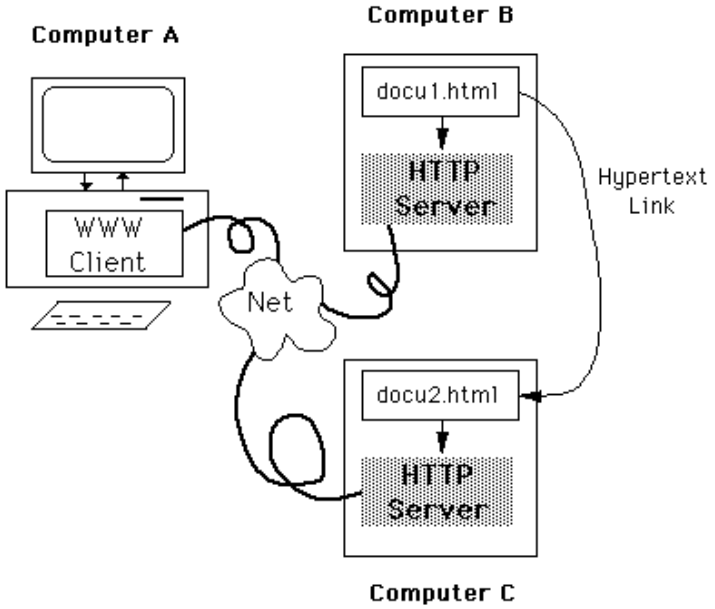
Gli utenti per usufruire dei servizi offerti da un Server devono utilizzare un software speciale chiamato Client che permette di comunicare con un Server sulla rete, facendo richieste.

Pertanto il Client rappresenta un'interfaccia che fornisce l'accesso ad un Server che eroga un particolare servizio. Esistono Web Server, Server FTP, Server Mail, ecc. e parallelamente Web Client (i *browser*), Client FTP, Client per la gestione della posta elettronica, ecc.

[26] HTTP su porta 80 (protocollo TCP)

In particolare un **Web Server** deve essere in grado di usare il tipico protocollo del WWW chiamato *http* che serve per *trasferire informazioni in modo da rendere efficiente il caricamento di ipertesti* e si basa su REGOLE standard o PROTOCOLLI "TCP/IP" (Protocol Internet Suite) nell'interagire col *Browser* (esempio di programma client).

In particolare i Servers WWW sono interconnessi tra di loro così da formare l'intera rete WWW; in tal modo una volta che un utente ha stabilito un contatto con un Server può anche comunicare con tutti gli altri.



Per poter accedere ad un Server WWW occorre che sul computer dell'utente sia in esecuzione un Client WWW.

I Client WWW (browsers[27]), i più diffusi dei quali sono Mozilla-Firefox, Google e Internet Explorer, permettono all'utente di navigare all'interno della grande quantità di informazione resa disponibile all'interno di Internet.

Descriviamo ora più dettagliatamente il WWW, data la sempre maggiore importanza assunta da questo servizio Internet.

Le componenti tecnologiche primarie del WWW sono:

Hypertext Markup Language (HTML),

Hypertext Transport Protocol (HTTP)

e Uniform Resource Locator (URL).

[27] Processo per creare connessione (possibilità di scambi informativi in rete), leggere da server e visualizzare in locale un documento web. I browser più attuali rendono disponibili altri servizi di rete infatti contengono moduli software in grado di accedere alle risorse di rete eseguendo diversi protocolli (oltre ad HTTP, anche FTP, news, smtp, pop3 e/o imap etc.). In IE con i *CANALI* informativi si offre "informazione a domicilio" (*information push*) tecnologia che crea un utente-spettatore invece di un utente-navigatore e propone servizi organizzati secondo la metafora dei canali radio o televisdivi con alcuni programmi client detti "tuner" (sintonizzatori).

L'HTML (linguaggio di marcatura) permette ad un autore di strutturare un documento con diversi tipi di intestazione, grafica e caratteri tipografici e di indicare dove mettere le associazioni per l'ipertesto. L'autore deve inoltre specificare come risolvere le associazioni, dove trovare le immagini, il suono, il film o il testo quando l'utente sceglie una data associazione.

Il protocollo HTTP (HyperText Transfer Protocol), come abbiamo visto, è l'insieme di regole che i Client ed i Server WWW utilizzano per comunicare. HTTP è infatti la prima parola che digitiamo nel browser quando vogliamo accedere ad una pagina Web. Questa parola indica al browser quali regole utilizzare quando inizia la comunicazione con un server Web.

Il terzo componente del WWW è l'**URL** (Uniform Resource Locator) che permette di specificare in modo standard oggetti o risorse sulla rete. L'URL rappresenta infatti uno schema di indirizzamento standardizzato che identifica in modo univoco una risorsa Internet (per es. una pagina Web, un'immagine, un server FTP, ecc.). Un URL ha una struttura gerarchica che si legge da sinistra a destra:

- la prima parte dell' URL e` la specifica del protocollo (ad esempio "http" o anche “file”).
- la seconda parte dell' URL e` il nome del server dove la risorsa risiede.
- la terza parte riguarda il nome del file, con o senza path.

Gli schemi di indirizzamento per messaggi di posta e su server NNTP sono leggermente diversi.

Nel caso di **messaggi di posta** la forma dell' URL è

mailto: id_utente@id_host

Nel caso di messaggi su server **NNTP** la forma dell' URL è

news : nome_newsgroup[: numero_messaggio]

senza una locazione assoluta della risorsa ma indipendente dalla collocazione: ogni client reperirà dal server locale il messaggio ad es: news: comp.text.xml : 1223334

Le funzioni di indirizzamento (ottimamente risolte dall'URL) e di identificazione (risolte in modo non ottimale dall'URL) si possono però distinguere: nasce così la tecnologia sperimentale **URN** (Uniform Resource Name) per identificare una risorsa in modo più catalogabile (nel '95 le specifiche, nel '96 IETF crea un gruppo per definirne gli standard).

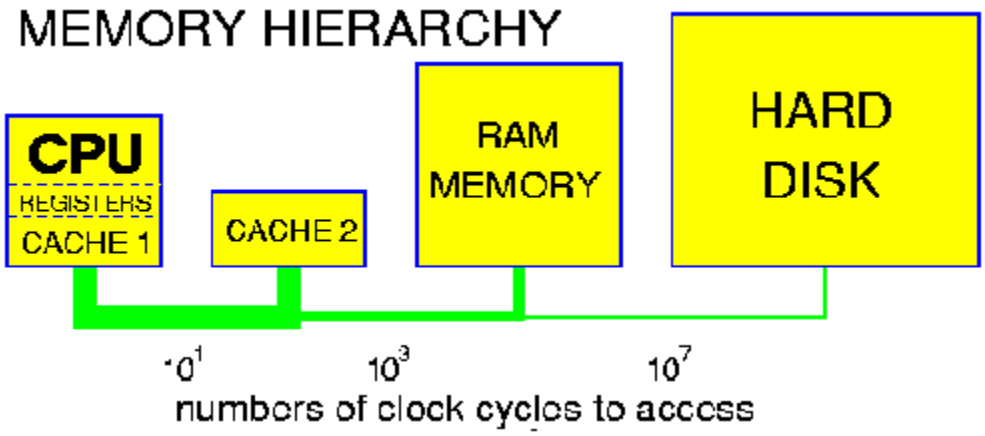
Proxy Server

L'aumento costante e continuo del numero degli utenti di Internet rende sempre più insufficiente la velocità di trasferimento dati tramite rete geografica. Il principale responsabile del traffico sulla rete è il servizio WWW.

I Client WWW possono migliorare l'accesso on-line alle pagine Web mediante due meccanismi:

1. uso di una memoria cache;
2. utilizzo di proxy server.

In modo trasparente all'utente il browser utilizza una memoria **cache** in cui conserva una copia locale dei documenti già visualizzati: questa caratteristica permette di riconsultare le pagine esplorate in precedenza senza doverle scaricare nuovamente dai server WWW remoti.



Quando l'informazione è preventivamente memorizzata sul computer locale e l'utente desidera vedere una pagina Web una seconda volta, il Client recupera così l'informazione localmente. La cache è infatti una zona di memoria nella quale vengono conservate le pagine Web precedentemente visitate allo scopo di velocizzarne un eventuale futuro caricamento.

Per quanto riguarda l'utilizzazione dei **proxy servers** occorre ricordare che molto spesso più Client WWW appartenenti ad uno stesso dominio o situati in una ristretta area geografica richiedono contemporaneamente le stesse pagine HTML ad un importante WWW Server situato in un'altra zona della terra. Ciò implica che quel WWW Server debba trasferire la stessa pagina tante volte quante sono le richieste dei Client, provocando così un'enorme spreco di larghezza di banda e rallentando notevolmente il trasferimento dati.

Per ovviare a questo problema sono stati creati i Proxy Server che sono dei software che mantengono copie locali delle pagine Web più richieste. Il proxy si può identificare come l'insieme di un calcolatore e di un software particolare detto "proxy server", a cui ci si appoggia per velocizzare i collegamenti ai siti su Internet. Se si configura un browser perché utilizzi un proxy, tutte le richieste di pagine Web fatte da quel client non arriveranno direttamente ai servers remoti ma saranno rivolte al proxy server, il quale a sua volta può rispondere direttamente al client oppure contattare i server remoti per farsi spedire i documenti richiesti che poi inoltrerà al computer dell'utente.

Appendici:

- **Gli RFC e gli Standard**
- **Corrispondenza tra Porte e Servizi**

Gli RFC e gli Standard

Fin dal 1969 i documenti e gli articoli che trattano di argomenti relativi ai protocolli TCP/IP e alla rete Internet, e che sono stati sanzionati ufficialmente dalla Internet Activities Board (IAB)[28] o da un precedente comitato equivalente, vengono raccolti e numerati.

Questi documenti sono i *Request For Comments* (RFC). Sono identificati da una sigla consistente delle lettere ``RFC'' seguite da un numero progressivo.

Al momento gli RFC sono circa 2000. A intervalli regolari viene pubblicato un RFC che funge da indice e da descrittore dello stato degli RFC.

Gli RFC non vengono mai ritirati ma possono diventare obsoleti e venire rimpiazzati, come autorevolezza, da RFC più recenti.

Alcuni RFC sono considerati di base per la documentazione della evoluzione della rete Internet. Questi vengono listati regolarmente in altri RFC.

Tutti gli RFC sono disponibili su server **ftp** della rete Internet, che vengono tenuti aggiornati. A volte vengono anche pubblicati su CDROM o altri supporti magnetici.

[28] Un comitato dell' Internet Engineering Task Force (IETF) che insieme all'Internet Engineering Steering Group (IESG) definisce le specifiche dell' **Internet Protocol suite**, pubblicate in documenti ufficiali come *standards track* RFCs. Come risultato, tale pubblicazione gioca un ruolo importante per il processo di standardizzazione di Internet. Le RFCs devono innanzi tutto essere pubblicate come Internet Drafts.

Corrispondenza tra Porte e Servizi

Affinché su una determinata macchina possano essere attivati più servizi, deve essere indicato il numero di porta corrispondente ad un determinato servizio. Le porte sono rappresentate da un numero di 2 byte (16 bit), pertanto è possibile utilizzare un numero compreso tra 0 e 65536.

I numeri delle porte sono divisi in tre gruppi:

- **Well-Known-Ports** (0 – 1023): Queste porte sono assegnate univocamente dall'**Internet Assigned Numbers Authority (**IANA**).**
- **Registered Ports** (1024 – 49151): L'uso di queste porte viene registrato a beneficio degli utenti della rete, ma non esistono vincoli restrittivi
- **Dynamic and/or Private Ports** (49152 – 65535): Non viene applicato nessun controllo all'uso di queste porte

Per esempio:

Descrizione Servizio	Porta
FTP (File Transfer Protocol)	20 - 21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
HTTP (Hypertext Transfer Protocol)	80
POP3 (Post Office Protocol)	110
NNTP	119

FTP Su porta 20 per dati e 21 per controllo (protocolloTCP o UDP)

NNTP su porta 119 (protocollo TCP o UDP). Gli antenati delle newsgroup sono le BBS (Bulletin Board System) amatoriali.

Per liste e UseNet esistono elenchi e cataloghi ma le *conferenze via Web* o FORUM non fanno capo ad una risorsa centralizzata ed è impossibile catalogarli: sono siti o gruppo di pagine in sito per visualizzare un elenco di messaggi,
leggerli e scriverne di nuovi in risposta o su altro argomento (ad esempio il forum di La Repubblica).

Porte TCP

7 **ECHO** - Servizio Echo;
20 **FTP DATA** - File Transfer Protocol Dati;
21 **FTP** - File Transfer Protocol Controllo;
22 **SSH** - Secure Shell Remote Login Protocol
23 **TELNET** - Telnet Protocol;
25 **SMTP** - Simple Mail Transfer Protocol;
53 **DNS** - Server dei nomi di dominio;
67 **BOOTPS** - (Dhcp) Bootstrap Protocol Server;
68 **BOOTPC** - (Dhcp) Bootstrap Protocol Client;
80 **HTTP** - Hypertext Transmission Protocol;
110 **POP3** - Post Office Protocol 3;
111 **SUNRPC** - Sun RPC Portmap;
113 **AUTH** - Servizio autenticazione;
119 **NNTP** - Network News Transfer Protocol;
137 **NETBIOS-NS** - NETBIOS Name Service
138 **NETBIOS-DGM** - NETBIOS Datagram Service
139 **NETBIOS-SSN** - NETBIOS Session Service
143 **IMAP** - Internet Mail Access Protocol;
389 **LDAP** - Lightweight Directory Access Protocol;
443 **HTTPS** - http protocol over TLS/SSL;
515 **PRINTER** - Spooler;

Porte UDP

7 **ECHO** - Servizio Echo;
20 **FTP DATA** - File Transfer Protocol Dati;
21 **FTP** - File Transfer Protocol Controllo;
53 **DNS** - Server dei nomi di dominio;
67 **BOOTPS** - (Dhcp) Bootstrap Protocol Server;
68 **BOOTPC** - (Dhcp) Bootstrap Protocol Client;
69 **TFTP** - Trivial File Transfer Protocol;
111 **SUNRPC** - Sun RPC Portmap;
119 **NNTP** - Network News Transfer Protocol
123 **NTP**- Network Time Protocol;
137 **NETBIOS-NS** - NETBIOS Name Service;
138 **NETBIOS-DGM** - NETBIOS Datagram Service;
139 **NETBIOS-SSN** - NETBIOS Session Service;
161 **SNMP** - Simple Network Management Protocol (SNMP);
162 **SNMP** - TRAP Simple Network Management Protocol Trap;
515 **PRINTER** - Spooler;

RFC 793 - Transmission Control Protocol http://www.faqs.org/rfcs/rfc793.html

RFC 768 - User Datagram Protocol http://www.faqs.org/rfcs/rfc768.html

RFC 791 - Internet Protocol http://www.faqs.org/rfcs/rfc791.html

Internet RFC/STD/FYI/BCP Archives **Indice** http://www.faqs.org/rfcs/
Motore di ricerca http://www.faqs.org/cgi-bin/rfcsearch