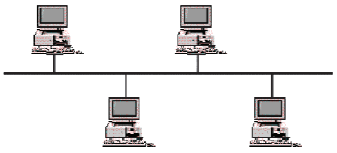
RETI di COMPUTER

Una rete di calcolatori è un insieme di computer (in genere eterogenei, cioè diversi per *hardware* e sistema operativo) che sono collegati allo scopo di condividere risorse e scambiarsi informazioni. Le risorse condivise possono essere di diverso tipo. Gli esempi più comuni sono rappresentati dalla connessione ad Internet, stampanti e spazio su disco. I vantaggi delle risorse condivise vanno quindi dal risparmio economico (non serve avere una stampante per ogni computer) ad un incremento di produttività.
Ogni nodo di una rete corrisponde generalmente a un elaboratore, che spesso viene definito host (elaboratore host), o anche stazione; i collegamenti tra questi nodi consentono il passaggio di dati in forma di pacchetti.

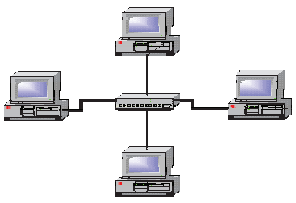
Le Reti possono essere classificate per

Estensione:
LAN (*local area network*), **rete locale:** quando la rete è contenuta nell'ambito di un edificio, o di un piccolo gruppo di edifici adiacenti; **WLAN** (wireless LAN) se il collegamento è senza fili;
MAN (*metropolitan area network*), **rete metropolitana:** quando la rete è composta dall'unione di più LAN nell'ambito della stessa area metropolitana, in altri termini si tratta di una rete estesa sul territorio di una città;
WAN (*wide area network*), **rete geografica:** quando la rete è composta dall'unione di più LAN e di più MAN, estendendosi geograficamente oltre l'ambito di una città singola.

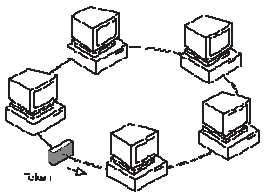
Topologia:
A **BUS**: ogni computer è connesso solamente e direttamente ad un mezzo trasmissivo lineare, lungo il quale si propagano in entrambe le direzioni le trasmissioni di ogni singolo computer.



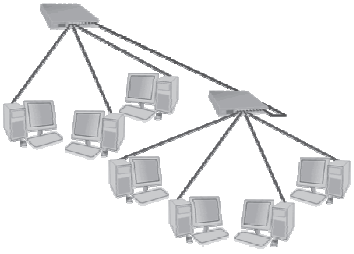
A **STELLA**: tutti i computer sono connessi direttamente ad un nodo centrale detto centro stella.



Ad **ANELLO**: i computer formano una struttura ad anello chiuso, in cui ognuno riceve dati dal precedente e li ripete al successivo. I dati fluiscono solamente in senso orario o antiorario.



Ad **ALBERO**: è una estensione della rete a bus, solitamente utilizzata in reti con un numero piuttosto ampio di computer. In una struttura ad albero, al posto dei singoli nodi possono esservi diramazioni prive di strutture ad anello.



Architettura:
tecnologie utilizzate (sia hardware che software) per la trasmissione dei dati: mezzi trasmissivi (doppino in rame, cavo coassiale, fibra ottica, canali radio e satellitari), schede di rete, pacchettizzazione dei dati, dispositivi di interconnessione (hub, switch, router), protocolli di comunicazione. Le architetture principali sono:
Ethernet per reti locali (LAN) con topologia a bus e a stella
Token Ring per reti locali (LAN) ad Anello
FDDI (Fiber Distribuited Data Interface) per reti di grandi dimensioni (MAN e WAN) e utilizzano la fibra ottica.

Nell'ambito delle LAN, l'architettura più utilizzata è **Ethernet**.

Sempre nell'ambito delle LAN i computer collegati possono assumere 3 ruoli diversi:
- client (usano ma non forniscono risorse di rete)
- server (forniscono risorse di rete)
- entità paritetiche (usano e forniscono risorse di rete – peer to peer)

Il ruolo svolto da ogni computer è stabilito dal Sistema Operativo utilizzato (windows server e Linux per server, windows XP, Mac OsX e Linux per client o peer to peer)
In base al Sistema Operativo utilizzato le reti si possono ulteriormente suddividere in:
- **reti client/server** dove sono presenti computer che funzionano da client e uno o più computer che funzionano da server
- **reti peer to peer** dove non ci sono computer server e tutti i computer possono condividere e usare risorse attraverso la rete
- **reti ibride** reti client/server che possono anche condividere risorse come nelle reti peer to peer.

La comunicazione tra due computer di una rete avviene inviando dati (sottoforma di bit) attraverso un opportuno canale trasmissivo; i dati sono raggruppati in pacchetti, ogni pacchetto è formato da 2 parti: l'intestazione (header) contenente tra l'altro l'indirizzo del mittente e del destinatario e i dati veri e propri (payload); tale tecnica di trasmissione è detta **commutazione di pacchetto**. I pacchetti possono essere instradati su percorsi differenti per giungere a destinazione. Quando un computer riceve un pacchetto esamina l'indirizzo di destinazione e se questo coincide con il proprio indirizzo trattiene il pacchetto per poi ricompattarlo con gli altri.

Il protocollo di comunicazione definisce un insieme di regole di comunicazione che i vari apparati di rete devono rispettare.
A qualunque livello della nostra esistenza è necessario un protocollo per comunicare: in un colloquio tra due persone, chi parla invia un messaggio all'altra che, per riceverlo, deve ascoltare.
Volendo proseguire con questo esempio, si può anche considerare il problema dell'inizio e della conclusione della comunicazione: la persona con cui si vuole comunicare oralmente deve essere raggiunta e si deve ottenere la sua attenzione, per esempio con un saluto, alla fine della comunicazione occorre un modo per definire che il contatto è terminato, con una qualche forma di commiato. Quanto appena visto è solo una delle tante situazioni possibili. Si può immaginare cosa accada in un'assemblea o in una classe durante una lezione.

La distinzione più importante tra i protocolli è quella che li divide in connessi e non connessi.
Il protocollo non connesso, funziona in modo simile all'invio di una cartolina, o di una lettera, che contiene l'indicazione del destinatario ma non il mittente. In tal caso, il protocollo non fornisce il mezzo per determinare se il messaggio è giunto o meno a destinazione.
Il protocollo connesso prevede la conferma dell'invio di un messaggio, la ritrasmissione in caso di errore e la ricomposizione dell'ordine dei pacchetti.

Affinché i computer di una rete possano comunicare correttamente è necessario che tutti utilizzino lo stesso protocollo.

La gestione della comunicazione in una rete è un problema complesso; in passato, questo è stato alla base delle maggiori incompatibilità tra i vari sistemi, a cominciare dalle differenze legate all'hardware.
Il riferimento comune al protocollo di comunicazione per le reti è rappresentato dal modello OSI (Open system interconnection), diventato parte degli standard ISO.
Il modello cosiddetto OSI/ISO propone una suddivisione "astratta", per la gestione della rete, in strati (layer) o livelli. I livelli previsti sono 7, per tradizione, vanno visti nel modo indicato nell'elenco seguente, dove il primo livello è quello più basso ed è a contatto del supporto fisico di trasmissione, mentre l'ultimo è quello più alto ed è a contatto delle applicazioni utilizzate dall'utente.

- **Livello 7 Applicazione**

Interfaccia di comunicazione con i programmi (*Application program interface*).

- **Livello 6 Presentazione**

Formattazione e trasformazione dei dati a vario titolo, compresa la cifratura e decifratura.

- **Livello 5 Sessione**

Instaurazione, mantenimento e conclusione delle sessioni di comunicazione.

- **Livello 4 Trasporto**

Invio e ricezione di dati in modo da controllare e, possibilmente, correggere gli errori.

- **Livello 3 Rete**

Definizione dei pacchetti, dell'indirizzamento e dell'instradamento in modo astratto rispetto al tipo fisico di comunicazione.

- **Livello 2 Collegamento dati** (*data link*)

Definizione e controllo della correttezza delle sequenze dei **bit** (trame o *frame*) trasmesse.

- **Livello 1 Fisico**

Trasmissione dei dati lungo il supporto fisico di comunicazione.

I dati da trasmettere attraverso la rete, vengono prodotti al livello più alto del modello, quindi, con una serie di trasformazioni e aggiungendo le informazioni necessarie, vengono passati di livello in livello fino a raggiungere il primo, quello del collegamento fisico. Nello stesso modo, quando i dati vengono ricevuti dal livello fisico, vengono passati e trasformati da un livello al successivo, fino a raggiungere l'ultimo.
In questo modo, si può dire che ad ogni passaggio verso il basso i pacchetti vengano imbustati in pacchetti (più grandi) del livello inferiore, mentre, a ogni passaggio verso l'alto, i pacchetti vengono estratti dalla busta di livello inferiore. In questa circostanza, si parla preferibilmente di PDU di livello *n* (*Protocol data unit*) per identificare il pacchetto realizzato a un certo livello del modello OSI/ISO.
Nel passaggio da un livello a quello inferiore, l'imbustamento implica un aumento delle dimensioni del pacchetto, ovvero del PDU. A certi livelli, può essere introdotta la frammentazione e la ricomposizione dei pacchetti, a seconda delle esigenze di questi.

Due concetti sono legati a un modello a strati:

- verticale, gerarchico: il software a livello superiore esegue richieste al livello sottostante e da questo riceve risposte;
- orizzontale, alla pari: strati corrispondenti di macchine diverse conversano tramite lo stesso protocollo

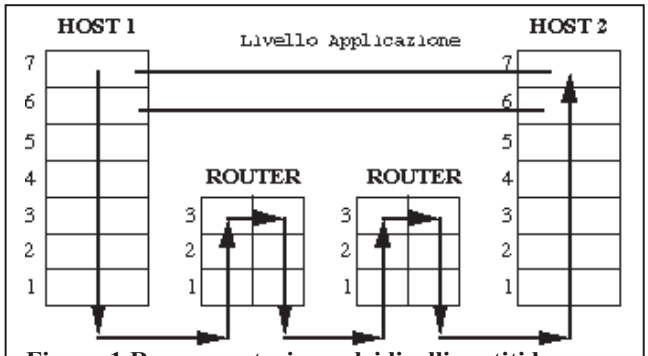


Figura 1 Rappresentazione dei livelli gestiti lungo un cammino

Nella pratica nessun protocollo reale rispetta rigorosamente la pila del modello OSI/ISO.
Oggi il protocollo standard di comunicazione più diffuso e usato da tutti i computer interconnessi ad Internet è TCP/IP.
TCP/IP (suite di protocolli) è stato sviluppato dalla Defense Advanced Research Projects Agency (DARPA) negli anni 60 ed è costituito da solo 4 livelli.

- **Livello 4 Applicazione**

Interfaccia di comunicazione con i programmi (prot. *FTP, HTTP, POP3, SMTP …*).

- **Livello 3 Trasporto**

Invio e ricezione di dati in modo da controllare e, possibilmente, correggere gli errori (prot. *TCP, UDP)*

- **Livello 2 Internet**

Definizione dei pacchetti, dell'indirizzamento e dell'instradamento in modo astratto rispetto al tipo fisico di comunicazione (*prot. ARP,RARP,ICMP,IP)*

- **Livello 1 Collegamento alla rete** (*data link*)

Definizione e controllo della correttezza delle sequenze dei **bit** (trame o *frame*) trasmesse.
Trasmissione dei dati lungo il supporto fisico di comunicazione

Confronto tra lo standard di "***diritto***" e lo standard "***de facto***"

Modello OSI/ISO	Modello TCP/IP
Applicazione	**Applicazione**
Presentazione	
Sessione	
Trasporto	**Trasporto**
Rete	**Internet**
Collegamento dati	**Collegamento alla rete**
Fisico	

L'architettura **TCP/IP** è oggi lo standard dell'interconnessione di reti.
Si parla di **Internetwork** quando reti diverse (sia LAN che MAN o WAN) sono collegate fra loro. La rete **Internet** si chiama cosi perché è un'infrastruttura di *internetworking*, cioè di interconnessione tra reti diverse.

Per i livelli 1 e 2 "Collegamento dati" e "Fisico" si farà riferimento al modello OSI/ISO per gli altri livelli si farà riferimento al modello TCP/IP
Per i livelli 1 e 2 il progetto OSI prende il nome di progetto IEEE 802.x (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers – ente privato USA che rilascia standardizzazioni in vari campi tecnici tra cui le reti)

Livello 1 Fisico (*physical layer*)
Si occupa di trasmettere sequenze di bit (0 e 1) su mezzi trasmissivi.
I mezzi trasmissivi son di 3 tipi:
elettrici (cavi, es. UTP categoria 5)
wireless (onde radio)
ottici (propagazione della luce - LED, laser, fibre ottiche)
La tecnologia più diffusa, per il livello 1 e 2 con mezzi trasmissivi elettrici, si chiama Ethernet.
Il termine Ethernet si riferisce a un insieme di tecnologie indicate dal progetto IEEE 802.3 e caratterizza gli elementi tipici del livello 1, che oltre al mezzo trasmissivo, sono:

- **scheda di rete** o **NIC** (Network Interface Card), ogni scheda di rete ha un indirizzo univoco a livello mondiale detto **MAC Address** composto da 6 byte (i primi 3 byte identificano l'azienda produttrice e i successivi 3 byte indicano il numero progressivo relativo alle schede prodotte dall'azienda)

- **Hub** o **ripetitori**, semplici apparecchiature di interconnessione per reti a stella costituiti da un minimo di 4 porte che collegano fra loro gruppi di computer; è possibile collegare più Hub in serie per aumentare il numero di connessioni; ogni pacchetto di dati trasmesso da un qualsiasi computer (host) viene ricevuto dall'hub su una porta e trasmesso a tutti gli altri computer collegati.

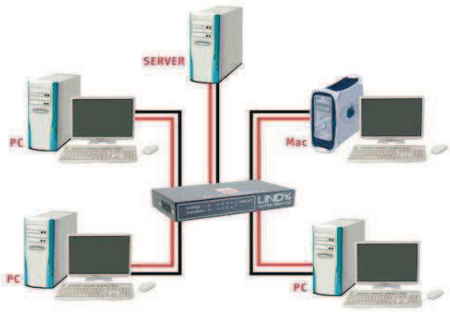
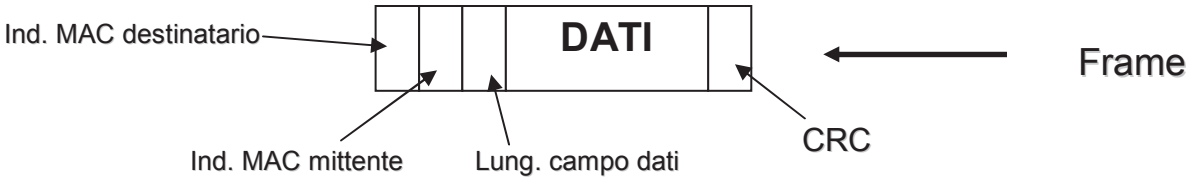


Figura 2 I dati vengo inviati a tutti i PC

Livello 2 Collegamento dati (***data link layer***)
Il tipo di hardware utilizzato nel primo livello determina il modo in cui avviene effettivamente la comunicazione. In Ethernet (IEEE 802.3) la struttura del pacchetto di dati è:



Il mezzo trasmissivo (canale che collega tutti i nodi) è condiviso mediante un algoritmo di "tecnica a contesa" detto **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection).
L' algoritmo CSMA/CD prevede che la stazione che vuole trasmettere, ascolti la linea per verificare che non ci siano altre trasmissioni in corso e se la linea è libera trasmette il proprio messaggio rimanendo però in ascolto che non avvengano "collisioni" (cioè un'altra stazione ha iniziato a trasmettere il proprio messaggio); al verificarsi della collisione le stazioni coinvolte bloccano la trasmissione per riprovare dopo un'attesa di un tempo pseudo-casuale.

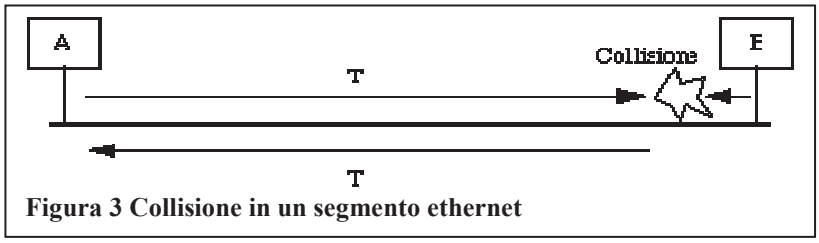


Figura 3 Collisione in un segmento ethernet

Le velocità di trasmissione variano da 10, 100 Mbps (mega bit per secondo), 1 Gbps.
La distanza massima tra due stazioni con doppino UTP cat. 5 è di circa 100 m.
Al livello 2 l'interconnessione può essere fatta tramite:

Switch, dispositivi più intelligenti degli HUB; essi si avvalgono degli indirizzi contenuti in ciascun pacchetto per gestire il flusso del traffico di rete. Monitorando i pacchetti che riceve, uno switch "impara" a riconoscere i dispositivi che sono collegati alle proprie porte per poi inviare i pacchetti solamente alle porte pertinenti. Lo switch riduce la quantità di traffico non necessario, dato che le informazioni ricevute nella porta vengono trasmesse solo al dispositivo con il giusto indirizzo di destinazione, e non come negli hub, a tutte le porte.

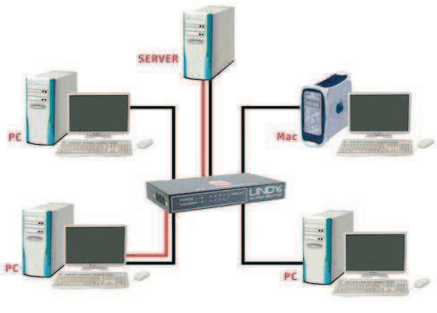


Figura 4 I dati vengo inviati solo al PC coinvolto

Livello Internet Protocol

Il protocollo **IP** si occupa di fornire allo strato superiore un "*servizio per la consegna dei dati*" che nasconde l'infrastruttura sottostante. Esso recapita il pacchetto dei dati, **datagramma** (segmento di DATI contenuto del Frame ethernet) dalla *sorgente* alla *destinazione* attraverso un sistema di reti eterogenee interconnesse da più linee dove sono possibili più tragitti; non sono previsti meccanismi di affidabilità e controllo dell'errore; il datagramma può essere frammentato in più parti, ciascuna trasportata individualmente e riassemblata a destinazione. Se la *sorgente* e la *destinazione* appartengono alla stessa rete il recapito avviene direttamente, altrimenti si deve passare attraverso un "sistema intermedio" detto **Router** che consente, a questo livello l'interconnessione fra reti.
Si dice che il protocollo IP fornisce un servizio **connection less** inaffidabile.

ROUTER: dispositivi in grado di reinstradare un pacchetto in una rete di tipo geografico.
E' dotato di una tabella di instradamento, aggiornata di frequente, che gli consente di conoscere i router che lo circondano e di stabilire quale sia la via migliore per far giungere a destinazione il pacchetto.

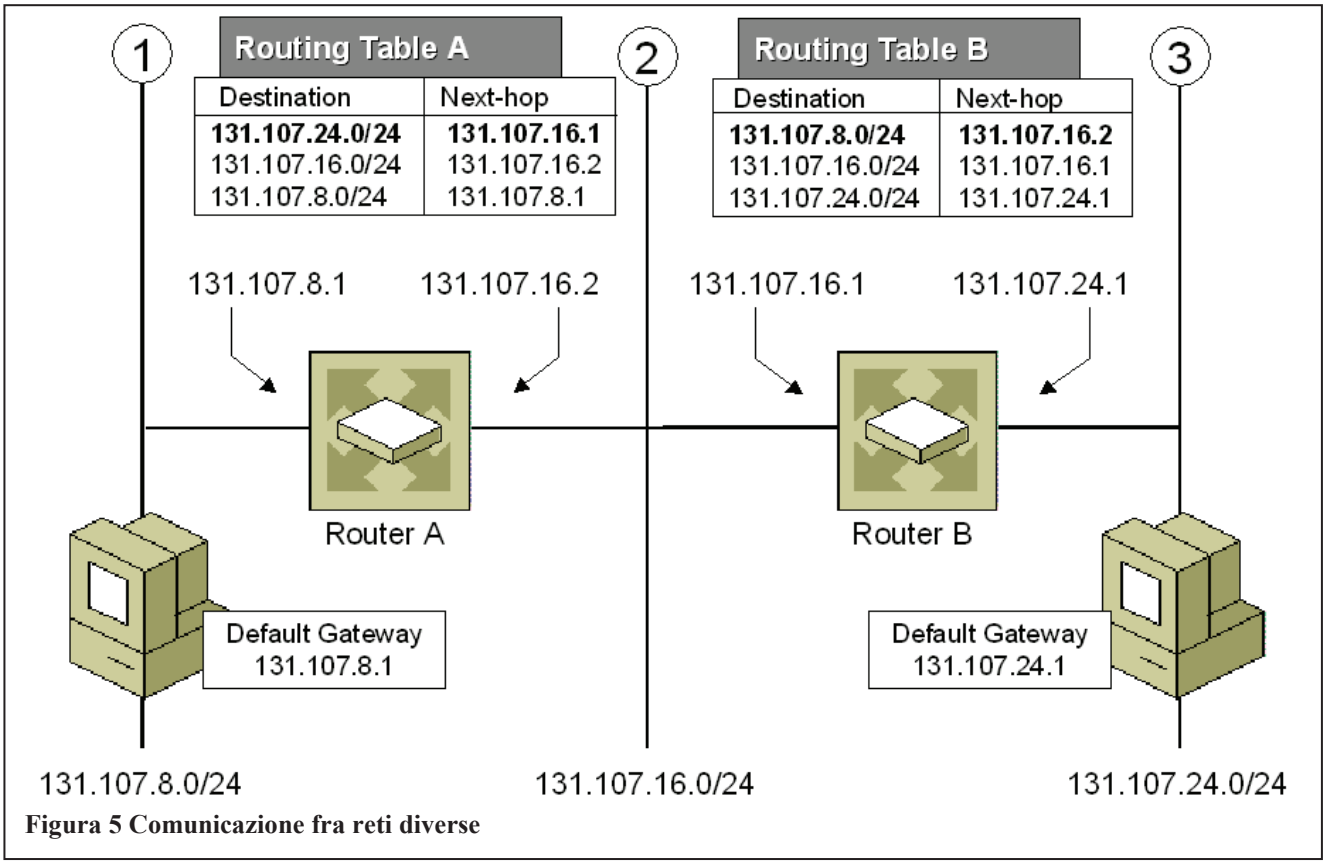


Figura 5 Comunicazione fra reti diverse

Per poter identificare *host sorgente* e *host destinazione* ogni host e ogni router della rete devono avere un indirizzo (IP) univoco che distingue le reti fra loro e che distingue gli host all'interno della stessa rete. L'indirizzo IP è formato da due parti: indirizzo di rete e indirizzo di host, ogni scheda di rete deve avere un indirizzo IP (i router e i server hanno più schede di rete e ciascuna deve avere un proprio indirizzo IP). Tutti gli Host hanno un ulteriore indirizzo, detto loopback, indirizzo fittizio che rappresenta "se stesso" ed è utilizzato per diagnostica e per simulare connessioni di rete di un host con se stesso.

L'indirizzo IP è formato da 32 bit (4 byte) ed è rappresentato da 4 numeri decimali di valore compreso tra 0 e 255, separati dal punto, es. 10.0.2.100, una parte dell'indirizzo specifica la rete (**net-ID**) ed una parte identifica l'host (**host-ID**) all'interno della rete.

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

- **Classe A**: il primo bit è 0; sette bit sono riservati al net-ID e 24 all'host-ID. Abbiamo cioè (2 alla 7) 128 reti di classe A, ciascuna delle quali ha un numero di host pari a circa 17 milioni (2 alla 24). Es. 20.9.0.200 individua l'host di indirizzo 9.0.200 nella rete 20
- **Classe B**: i primi due bit sono 10; quattordici bit sono riservati al net-ID e i rimanenti 16 all'host-ID. Questo significa 16383 reti di classe B, ognuna con 65533 host. Es. 131.154.10.21 individua l'host di indirizzo 10.21 nella rete 131.154
- **Classe C**: i primi tre bit sono 110; 21 bit sono riservati al net-ID e 8 all'host-ID. Abbiamo due milioni circa di reti di classe C, con 254 nodi per rete.
  Es. 192.168.1.104 individua l'host di indirizzo 104 nella rete 192.168.1
- **Classe D**: i primi bit sono 1110; 28 bit di indirizzo multicast per oltre 250 milioni di canali.
- **Classe E**: i primi bit sono 1111; 28 bit per usi futuri e ricerca

Indirizzi speciali:

- l'indirizzo **0.0.0.0** indica "questo host di questa rete" e viene utilizzato in fase di boot (avvio del sistema operativo) quando ancora l'host non conosce il proprio indirizzo IP
- l'indirizzo **10.0.0.0** indica la rete 10 (classe A)
- l'indirizzo **192.168.1.0** indica la rete 192.168.1 (classe C)
- l'indirizzo **255.255.255.255** (tutti i bit 1) indica l'indirizzo broadcast della rete e viene utilizzato per un inviare un pacchetto IP broadcast a tutti gli host della rete
- l'indirizzo con tutti 1 nel host-ID indica l'indirizzo broadcast della rete indicata nel net-ID, es. **130.90.255.255** indica l'indirizzo broadcast della rete 130.90.0.0 e permette di inviare un pacchetto a tutti gli host di quella rete; di conseguenza, un indirizzo broadcast non può essere utilizzato per identificare un computer host.
- l'indirizzo **127.0.0.0** indica la rete di loopback e la scheda di rete assume sempre l'IP **127.0.0.1**

Tre serie di indirizzamento sono riservate ad "indirizzi privati"; possono essere utilizzati all'interno di una rete privata e non devono mai essere esposti verso la rete esterna (Internet)

- **10.0.0.0** (una rete di classe A)
- da **172.16.0.0** a **172.31.0.0** (16 reti di classe B)
- da **192.168.0.0** a **192.168.255.0** (256 reti di classe C)

Per identificare quali bit definiscono la rete (net-ID) e quali bit definiscono gli host (host-ID) si utilizza una "maschera" (**Subnet Mask**), anch'essa di 32 bit con il seguente significato:

- se un bit della maschera vale 1, il corrispondente bit dell'indirizzo IP fa parte dell'indirizzo di rete (net-ID)
- se un bit della maschera vale 0, il corrispondente bit dell'indirizzo IP fa parte dell'indirizzo di host (host-ID)

Con questa convenzione
gli indirizzi di classe A hanno maschera **255.0.0.0**
gli indirizzi di classe B hanno maschera **255.255.0.0**
gli indirizzi di classe C hanno maschera **255. 255. 255.0**

La coppia indirizzo IP-Subnet Mask può essere rappresentata anche indicando quanti sono i bit 1 della subnet mask: es. **192.168.100.2 – 255.255.255.0** oppure **192.168.100.2/24**.

Ogni Host oltre ad avere un indirizzo IP univoco, con relativa subnet mask, deve avere anche un indirizzo IP di Default Gateway, tale indirizzo indica il dispositivo (router) preposto al collegamento con un'altra rete, spesso la rete Internet. Ogni volta che l'indirizzo dell'host destinazione non appartiene alla stessa rete dell' host sorgente, quest'ultimo chiede al default gateway di stabilire la connessione a nome suo.
Tutti i computer locali devono stare nella stessa rete (avere la stessa subnet mask).

Gli indirizzi IP pubblici vengono assegnati dalla ICANN (Internet Corporation for Assigned Names and Numbers) che a sua volta delega organizzazioni regionali (Europa, Asia,….) che a loro volta delegano altre organizzazioni nazionali: per l'Europa: RIPE; per l'ITALIA: GARR

Essendo quasi esaurito lo spazio di indirizzamento è già stato predisposto un nuovo protocollo IPv6 che andrà a sostituire l'attuale IPv4. IPv6 prevede 128 bit (16 byte) contro i 32 bit di IPv4, pertanto lo spazio di indirizzamento sarà illimitato.

Possiamo riassumere il modo in cui IP recapita il datagramma: se *host sorgente* e *host destinazione* fanno parte della stessa rete, il datagramma viene consegnato direttamente utilizzando il protocollo di *data link layer* sottostante; in caso contrario della rete del sorgente deve far parte un *router* (default gateway) capace di trasmettere il datagramma attraverso le reti che interconnettono sorgente (mittente) e destinazione (destinatario), il datagramma trasmesso dal *router* verrà instradato ad altri router direttamente connessi e cosi via fino al raggiungimento della destinazione. (fig. 5)

Livello di Trasporto

Il Livello di Trasporto si occupa di fornire allo strato superiore un "*servizio di trasferimento dei dati*" tra due host, che nasconde l'infrastruttura sottostante. Il servizio offerto può essere:

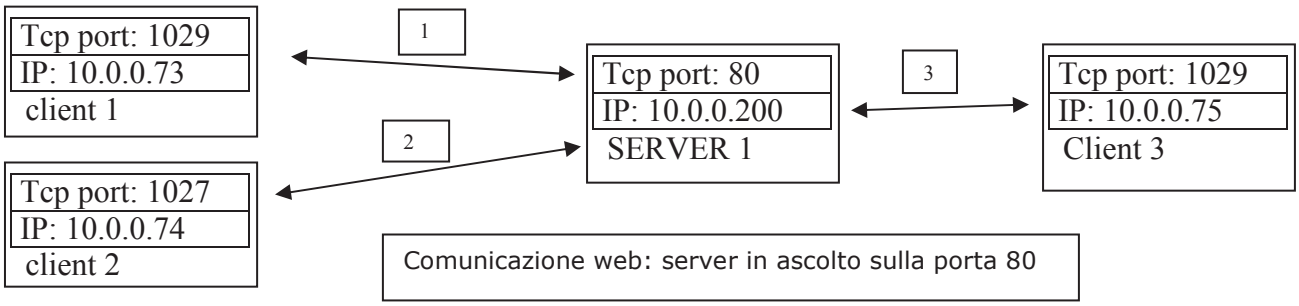
- *affidabile* e *orientato alla connessione* per gestire il controllo del flusso dei dati (integrità, completezza, ordinamento, controllo errori, ritrasmissione); i dati vengono trasmessi con un procedimento in 3 fasi (handshaking):
  - si stabilisce la connessione tra i due host
  - si inviano i dati attraverso la connessione
  - si chiude la connessione
- *inaffidabile* e non *orientato alla connessione*, ogni blocco di dati viene inviato e non ci si preoccupa se è arrivato o meno a destinazione

I protocolli utilizzati sono:

TCP (Transmission Control Protocol) *affidabile* e *orientato alla connessione*

UDP (User Datagram Protocol) *inaffidabile* e non *orientato alla connessione*

Entrambi i protocolli utilizzano delle **porte di comunicazione**, ogni pacchetto TCP o UDP contiene una *porta mittente* e *porta destinazione.* Perché ogni pacchetto possa essere ricevuto dal destinatario, occorre che questo sia in "ascolto" su una porta prestabilita, altrimenti si nega l'apertura della connessione. In generale, una applicazione che deve "svolgere un servizio" (server) attraverso la rete, starà in ascolto sempre sulla stessa porta, in modo che chi deve usufruire del servizio sappia come farlo indicando il nome del servizio e la porta di ascolto (es. http e 80). L'applicazione che vuole accedere al servizio, per contro, aprirà una propria porta locale qualsiasi, purché non utilizzata, per ricevere i pacchetti del servizio richiesto.



In TCP/IP una connessione è identificata da una quadrupla di valori: indirizzo IP sorgente, TCP/UDP port sorgente, indirizzo IP destinatario, TCP/UDP port destinatario detta socket.

Es. (10.0.0.73:1029; 10.0.0.200:80) per la connessione 1

Le porte da 0 a 1023 sono definite porte privilegiate o **well known ports**, e servono per indirizzare un certo servizio
Le porte da 1024 a 65535 sono lasciate libere per le porte utenti, cioè quelle scelte dall'applicativo client come porta sorgente (per la connessione 1 porta 1029 scelta dal client web o browser).
Nella tabella seguente vengono riportati i numeri di porta di alcuni tra i servizi più noti.

Numero di porta	Servizio
20	FTP-DATA *File Tranfer Protocol* (dati)
21	FTP *File Tranfer Protocol* (controllo)
23	TELNET Connessione di terminale
25	SMTP *Simple Mail Transport Protocol*
53	*DOMAIN Server* di nomi del dominio DNS
67	DHCP *Dynamic Host Configuration Protocol*
80	HTTP *HyperText Tranfer Protocol*
110	POP3 *Post Office Protocol*
119	NNTP Protocollo di trasferimento news USENET
143	IMAP *Internet Message Access Protocol*
194	IRC (internet relay chat)

Applicazioni che usano TCP
Tutte quelle che richiedono affidabilità dei dati, e che non hanno bisogno della comunicazione multicast/broadcast

- **ftp** (file transfer, port 21)
- **ssh** (login remoto criptato, port 22)
- **telnet** (login remoto, port 23)
- **smtp** (posta elettronica, port 25)
- **pop3** (posta elettronica, port 110)
- **IMAP (**posta elettronica, port 143)
- **http** (il protocollo del World Wide Web, port 80)
- **https** (il protocollo sicuro del World Wide Web, port 443)

Applicazioni che usano UDP
Tutte quelle che necessitano di risparmiare il "tempo" richiesto dalla connessione, ed implementano a livello di applicazione il controllo della correttezza dei dati, ad esempio applicativi che scambiano dati con molti host rapidamente, per i quali dover stabilire ogni volta una connessione e' peggio che ritentare se qualcosa va storto

- **dns** (domain name service , port 53)
- **dhcp (**dynamic host configuration protocol, port 67)

Livello Applicazione

I protocolli di questo livello svolgono un lavoro utile alle applicazioni utente (posta elettronica, web, ecc..). Verranno esaminate alcune delle applicazioni più utilizzate.

FTP (File Transfer Protocol)
è un protocollo affidabile, connection-oriented, di trasferimento file da un computer all'altro che supportano questo protocollo.

PoP3 (Post Office Protocol)
è un protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente su di un host per scaricare le e-mail del relativo account. I messaggi di posta elettronica, per essere letti, devono essere scaricati sul computer (questa è una notevole differenza rispetto all'IMAP), anche se è possibile lasciarne una copia sull'host. Il protocollo POP3 non prevede alcun tipo di cifratura, quindi le password utilizzate per l'autenticazione fra server e client passano in chiaro.

SMTP (Simple Mail Transport Protocol)
è il protocollo standard per la trasmissione di e-mail.

IMAP (Internet Message Access Protocol oppure Interactive Mail Access Protocol)
è un protocollo per la ricezione di e-mail, alternativa più moderna al POP3. Entrambi permettono ad un client di accedere, leggere e cancellare le e-mail da un server, ma con alcune differenze. Con IMAP la posta resta sul server e quindi può essere letta da postazioni diverse e più utenti possono utilizzare la stessa casella di posta.

DNS (Domain Name System)
Il DNS è un servizio utilizzato per la risoluzione di nomi di Host e dei nomi di Dominio (es. www.tron.vi.it) in indirizzi IP. Tale servizio è realizzato tramite un database distribuito, costituito dai server DNS.
Questa funzione è essenziale per l'usabilità di Internet, visto che gli esseri umani preferiscono ricordare nomi testuali, mentre gli Host ed i router sono raggiungibili utilizzando gli indirizzi IP.

HTTP (Hyper Text Transfer Protocol)
è un protocollo usato come principale sistema per la trasmissione di informazioni sul web. HTTP funziona con un meccanismo richiesta/risposta: il client (es. IE, Firefox) esegue una richiesta ed il server web (es. Apache, IIS) restituisce la risposta. Nel protocollo http la connessione viene generalmente chiusa una volta che una particolare richiesta (o una serie di richieste correlate) è stata soddisfatta. Questo comportamento rende il protocollo HTTP ideale per il World Wide Web, in cui le pagine molto spesso contengono dei collegamenti (link) a pagine ospitate da altri server. Talvolta però pone problemi agli "sviluppatori di contenuti web", perché la natura senza stato (**stateless**) costringe ad utilizzare dei metodi alternativi per conservare lo stato dell'utente. Spesso questi metodi si basano sull'uso dei cookie e delle sessioni. Dal momento che tutto il traffico HTTP è anonimo e in chiaro, sono state sviluppate diverse alternative per garantire differenti livelli di sicurezza, in termini di cifratura del traffico ed autenticazione del server e dell'utente. Il protocollo **HTTPS**, protocollo HTTP utilizzato in combinazione con lo strato SSL (Secure Socket Layer), porta standard TCP 443 è attualmente quello che garantisce un buon livello di sicurezza. In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso lo scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione. Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione.

Il protocollo **http** è uno degli elementi base del servizio più conosciuto e più utilizzato di Internet cioè il **W**orld **W**ide **W**eb (Web), esso indica un sistema di distribuzione delle informazioni, basato sull'infrastruttura di Internet. Oltre al protocollo http, il Web si basa su altri due meccanismi per rendere le informazioni prontamente disponibili al più vasto insieme possibile di utenti:

- Uno schema di denominazione uniforme per localizzare le risorse sul Web, gli URI.
- Ipertesto, per una facile navigazione tra le risorse, linguaggio HTML.

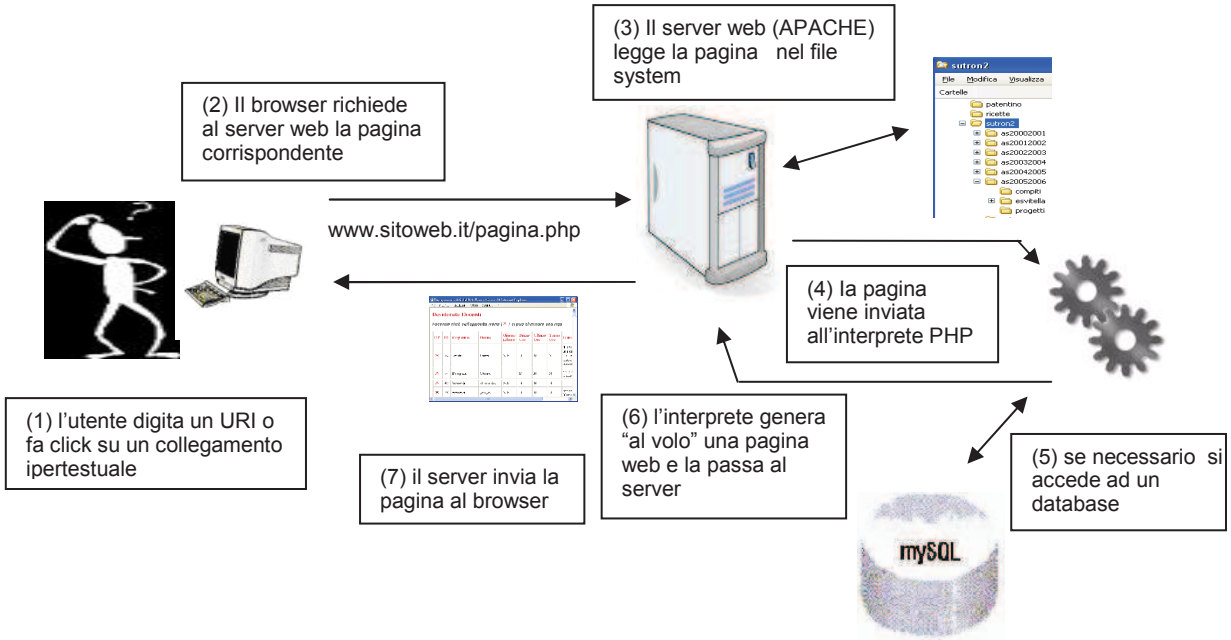
Un **U**niform **R**esource **I**dentifier (**URI**, acronimo più specifico rispetto ad "URL") è una stringa che identifica una risorsa nel Web in maniera univoca: un documento, un'immagine, un file, un servizio, un indirizzo di posta elettronica, ecc. L'URI è comunemente chiamato "indirizzo web":
es. "http://www.tron.vi.it"
HTML (**H**yper **T**ext **M**ark-up **L**anguage) è un linguaggio usato per descrivere i documenti ipertestuali disponibili nel Web. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web.
Le pagine scritte nel linguaggio HTML devono essere interpretate da un programma detto **browser** (es. Internet Explorer, Firefox, ecc.) o **client web**.

Un insieme organizzato di pagine web tra loro collegate che si riferiscono ad uno stesso argomento o ad una stessa Azienda forma un **sito Internet** o **sito Web**.

Essendo il linguaggio HTML un semplice linguaggio di "marcatura" non è possibile gestire contenuti dinamici (es. animazioni, visualizzazione di dati estratti da un Database). Per superare queste limitazioni sono stati definiti strumenti capaci di generare pagine HTML dinamiche. Per dare al web una maggiore interattività e dinamicità sono state perseguite due strade. Da un lato sono state aumentate le funzionalità dei browser attraverso un'evoluzione del linguaggio HTML (fogli di stile o css) e la possibilità d'interpretazione di linguaggi di scripting (**JavaScript**). Dall'altro si è migliorata l'elaborazione lato server attraverso una nuova generazione di linguaggi integrati con il Web Server (JSP, **PHP**, ASP, ASP.NET,…) trasformando i Web Server in quelli che sono oggi più propriamente noti come Application Server.
La diffusione di queste soluzioni ha consentito di avviare l'utilizzo del web come piattaforma applicativa che oggi trova la sua massima espressione nei Web Service. Scopo dei Web Service è di limitare il più possibile le attività di implementazione, consentendo di accedere a servizi software resi disponibili in rete, assemblarli secondo le proprie necessità e pagarli soltanto per il loro utilizzo effettivo, metodologia individuata nella terminologia anglosassone come pay per use, on demand software.

Nonostante tutte queste evoluzioni, il web rimane, ancora e soprattutto, una gigantesca biblioteca di pagine HTML statiche on-line. Però, lo standard HTML se da un lato con la sua semplicità ha contribuito all'affermazione del web, dall'altro ha la grossa limitazione di occuparsi solo ed esclusivamente della formattazione dei documenti, tralasciando del tutto la struttura ed il significato del contenuto. Questo pone notevoli difficoltà nel reperimento e riutilizzo delle informazioni. Per rendersi conto di questo è sufficiente eseguire una ricerca utilizzando uno dei molti motori disponibili in rete e ci si accorgerà che, delle migliaia di documenti risultanti dalla query, spesso solo una piccola percentuale è d'interesse per la ricerca che s'intendeva fare. Ad esempio, per un qualsiasi motore di ricerca, non esiste alcuna differenza fra il termine Rossi nel contesto Il Sig. Rossi ed il termine Rossi nel contesto Capelli Rossi, rendendo la ricerca molto difficile.
La risposta a questo problema è venuta dal consorzio W3C, che ha assunto il ruolo di governo nello sviluppo di standard e protocolli legati al web, mediante la definizione dello standard **XML** (e**X**tensible **M**arkup **L**anguage), un metalinguaggio che consente la creazione di nuovi linguaggi di marcatura (ad es. lo stesso HTML è stato ridefinito in XML come **XHTML**). Sua caratteristica innovativa è la possibilità di aggiungere informazioni semantiche sui contenuti attraverso la definizione di opportuni tag.

Architettura di un sito dinamico



Nel caso di un sito statico bastano i punti (1), (2), (3) e (7)

Ulteriori Definizioni

Intranet ed Extranet

Reti che forniscono agli utenti servizi analoghi a quelli offerti da Internet: web, posta elettronica, news, ecc.; sono di natura privata e possono estendersi anche su grandi distanze collegando filiali o sedi staccate della stessa Azienda o Istituzione. Sono considerate delle WAN private e possono utilizzare connessioni proprie o sfruttare quelle della rete Internet. La differenza consiste nel fatto che nella Intranet l'accesso è consentito solo dal suo interno, mentre nella Extranet è consentito l'accesso dall'esterno della rete stessa ma solo a soggetti selezionati come Agenti, Fornitori, Collaboratori ecc. che devono identificarsi con un qualche sistema di autenticazione (es. username e password)

Elenco di alcuni comandi per effettuare una semplice diagnostica di rete

ipconfig (ifconfig in Linux/Unix)

elenca tutte le schede di rete attive; questo è il primo passo da fare sempre prima di qualunque configurazione (ed anche dopo per controllare che sia tutto a posto) per vedere lo stato del sistema. Un risultato possibile è il seguente:

```
C:\>ipconfig

Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
        Stato supporto . . . . . . . . . . . : Supporto disconnesso

Scheda Ethernet Connessione rete senza fili:
        Suffisso DNS specifico per connessione: tron.intra
        Indirizzo IP. . . . . . . . . . . . . : 192.168.1.2
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.1.1
```

ping

serve ad inviare un pacchetto speciale (protocollo ICMP con funzione di Echo Request) che chiede un risposta alla macchina di destinazione (protocollo ICMP con funzione di Echo Reply). Il comando si invoca specificando l'IP della macchina da controllare, o specificando il nome, ma i questo caso deve anche funzionare il DNS.

Un esempio di uso, in ambiente windows è il seguente:

```
C:\>ping 192.168.1.1

Esecuzione di Ping 192.168.1.1 con 32 byte di dati:

Risposta da 192.168.1.1: byte=32 durata=6ms TTL=255
Risposta da 192.168.1.1: byte=32 durata=7ms TTL=255
Risposta da 192.168.1.1: byte=32 durata=6ms TTL=255
Risposta da 192.168.1.1: byte=32 durata=7ms TTL=255

Statistiche Ping per 192.168.1.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 6ms, Massimo =  7ms, Medio =  6ms
```

Il comando invia un pacchetto al secondo, e nel caso riceve sempre risposta riportando il tempo che ci è voluto. Al termine stampa anche una statistica. Questo ci dice che la macchina con IP 192.168.1.1 è attiva ed è raggiungibile.

tracert (traceroute in Linux/Unix)

permette di controllare il collegamento, che come dice il nome serve a tracciare la strada che fanno i pacchetti per arrivare alla destinazione indicata.

Un esempio di uso, in ambiente windows è il seguente:

```
C:\>tracert www.google.it

Rilevazione instradamento verso www.l.google.com [64.233.183.104]
su un massimo di 30 punti di passaggio:
  1     3 ms     2 ms     2 ms  192.168.1.1
  2    60 ms    55 ms    56 ms  milz-lns-1-24.swip.net [212.151.128.133]
  3    60 ms    55 ms    54 ms  milz-lns-1.vlan10.swip.net [212.151.133.65]
  4    60 ms    56 ms    56 ms  milz-ds-2.gigabiteth2-23.swip.net [212.151.158.21]
  5   170 ms   165 ms   166 ms  mil2-core.gigabiteth1-0.swip.net [130.244.193.209]
  . . . . . .
 13   168 ms   165 ms   168 ms  72.14.232.141
 14   168 ms   164 ms   164 ms  216.239.43.89
 15   171 ms   167 ms   166 ms  64.233.183.104
Rilevazione completata.
```

netstat

comando diagnostico molto utile ed estremamente complesso, che permette di visualizzare una grande quantità di informazioni relative alla rete. Nell'esempio si utilizza per visualizzare tutte le connessioni attive sul computer

```
C:\>netstat -an

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno       Stato
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:10110        0.0.0.0:0              LISTENING
  TCP    192.168.1.2:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    192.168.1.2:138        *:*
  UDP    192.168.1.2:1900       *:*
```