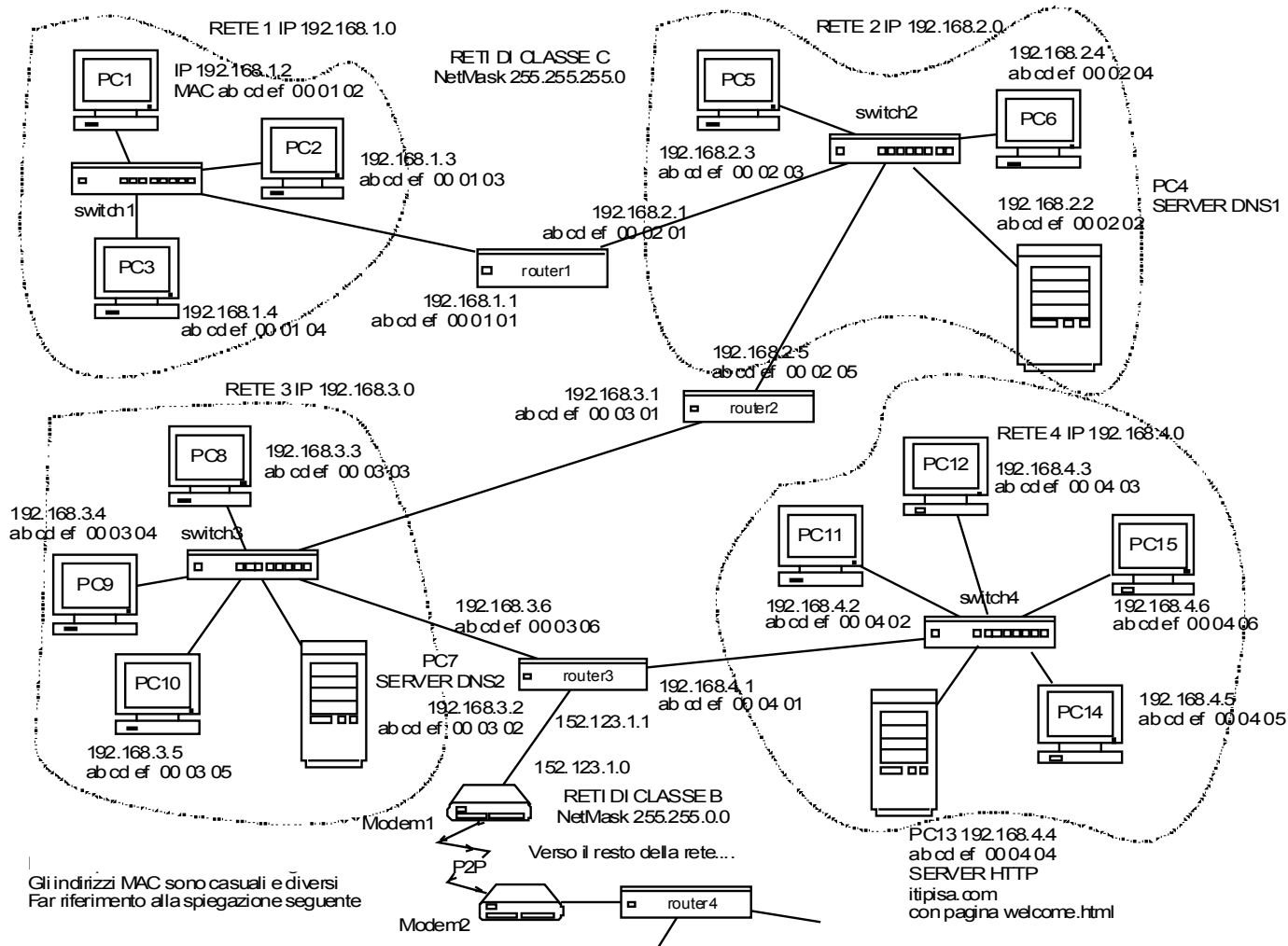


Come funziona Internet:

Scenario: comunicazione fra 4 reti di computer interconnesse fra loro



I messaggi che i vari nodi della rete si scambiano (pensiamo a una lettera, ma potrebbe essere un messaggio di gestione della rete, ad esempio una interrogazione DNS) sono divisi in pacchetti (pensiamo a una lettera suddivisa in più pagine) per ragioni di:

- 1) **migliore utilizzo della rete**: in genere non è necessario inviare immediatamente tutto il documento, in quanto esso è utilizzato (ad esempio letto) un frammento alla volta; i tempi morti fra l'invio di un pacchetto e l'altro possono essere utilizzati per l'invio dei messaggi di altri utenti della rete.
- 2) **miglior controllo di integrità**. Tutti i pacchetti sono riscontrati (ovvero il mittente riceve una conferma della ricezione) e controllati per capire se sono arrivati corretti o meno; in caso contrario vengono rispediti. I pacchetti sono ovviamente numerati per poterli poi riassemblare e ottenere il documento originale corretto. Se il messaggio viene trasmesso intero, un errore causa la ritrasmissione dell'intero messaggio; suddividendolo in pacchetti un errore causa la ritrasmissione del solo pacchetto che contiene l'errore. E' più facile inoltre controllare tanti piccoli pacchetti che un singolo grosso messaggio.

Pensiamo a una persona che entra in un negozio di mobili e acquista una cucina; il negozio invierà la cucina non tutta intera ma smontata e suddivisa in pacchetti (numerati), ognuno dei quali sarà singolarmente controllato in trasmissione e anche in ricezione in modo da poterlo ripeditare se difettoso e potrà essere affidato a spedizionieri diversi seguendo percorsi e tempi di consegna diversi. E' chiaramente più semplice che spedire l'intera cucina montata, cosa che anche se teoricamente fattibile con un enorme camion, costringerebbe quantomeno a monopolizzare la strada per il suo passaggio. Non è detto che i pacchetti debbano fare la stessa strada, e quindi non è neanche detto che arrivino nell'ordine con il quale sono stati spediti. Anche per questo sono numerati.

Per gestire lo scambio dei messaggi nel modo più efficiente e affidabile possibile, praticamente ogni dispositivo di rete è contraddistinto da due numeri identificativi (che dovrebbero essere unici, anche se vedremo che tale restrizione non è sempre necessaria) detti INDIRIZZI: l'indirizzo fisico o MAC address e l'indirizzo di rete o IP address.

Ruolo degli indirizzi IP e degli indirizzi MAC Ethernet (MAC address. MAC = medium access control = controllo di accesso al mezzo trasmissivo: il canale, il cavo o la frequenza radio):

L'**IP, indirizzo di rete**, o **indirizzo logico**, è analogo al numero civico dei palazzi; **il router usa l'IP come un postino usa il numero civico**.

Il **MAC, detto anche indirizzo fisico**, è analogo al numero degli interni nelle scale dei palazzi: il postino (il router) individua i palazzi con il numero civico (l'IP) e consegna i documenti al portiere del palazzo (lo switch) che li smista in base all'interno (il MAC). **Lo switch usa il MAC come il portiere usa il numero interno**.

Quindi in definitiva: l'IP permette ai router (postino) di trovare le reti di appartenenza dei computer (i palazzi dove abitano le persone),

mentre il MAC permette agli switch (portiere) di trovare il computer nella rete (la persona nel palazzo).

Nota: non ci dovrebbero essere due indirizzi IP uguali. In realtà questo non è strettamente necessario perchè i router "nascondono" gli IP delle reti dietro di esso. La restrizione può essere limitata all'interno della stessa rete.

Con riferimento alla situazione della figura a pagina 1:

rete 1: indirizzo di rete IP: 192.168.1.0 con 3 pc:

PC1: indirizzo IP: 192.168.1.2 indirizzo MAC (ethernet) ab cd ef 00 01 02

PC2: indirizzo IP: 192.168.1.3 indirizzo MAC (ethernet) ab cd ef 00 01 03

PC3: indirizzo IP: 192.168.1.4 indirizzo MAC (ethernet) ab cd ef 00 01 04

rete 2: indirizzo di rete IP: 192.168.2.0 con 3 pc:

PC4: indirizzo IP: 192.168.2.2 indirizzo MAC (ethernet) ab cd ef 00 02 02

PC5: indirizzo IP: 192.168.2.3 indirizzo MAC (ethernet) ab cd ef 00 02 03

PC6: indirizzo IP: 192.168.2.4 indirizzo MAC (ethernet) ab cd ef 00 02 04

Le reti 1,2 sono interconnesse fra loro con un router1 avente 2 interfacce con indirizzi IP

192.168.1.1 indirizzo MAC (ethernet) ab cd ef 00 01 01

192.168.2.1 indirizzo MAC (ethernet) ab cd ef 00 02 01

rete 3: indirizzo di rete IP: 192.168.3.0 con 4 pc:

PC7: indirizzo IP: 192.168.3.2 indirizzo MAC (ethernet) ab cd ef 00 03 02

PC8: indirizzo IP: 192.168.3.3 indirizzo MAC (ethernet) ab cd ef 00 03 03

PC9: indirizzo IP: 192.168.3.4 indirizzo MAC (ethernet) ab cd ef 00 03 04

PC10: indirizzo IP: 192.168.3.5 indirizzo MAC (ethernet) ab cd ef 00 03 05

La rete 3 è collegata alle reti 1 e 2 con un router2 avente 2 interfacce con indirizzi IP

192.168.3.1 indirizzo MAC (ethernet) ab cd ef 00 03 01

192.168.2.5 indirizzo MAC (ethernet) ab cd ef 00 02 05

rete 4: indirizzo di rete IP: 192.168.4.0 con 5 pc:

PC11: indirizzo IP: 192.168.4.2 indirizzo MAC (ethernet) ab cd ef 00 04 02

PC12: indirizzo IP: 192.168.4.3 indirizzo MAC (ethernet) ab cd ef 00 04 03

PC13: **itipisa.com** indirizzo IP: 192.168.4.4 indirizzo MAC (ethernet) ab cd ef 00 04 04

PC14: indirizzo IP: 192.168.4.5 indirizzo MAC (ethernet) ab cd ef 00 04 05

PC15: indirizzo IP: 192.168.4.6 indirizzo MAC (ethernet) ab cd ef 00 04 06

la rete 4 è collegata alle reti 1,2,3 con un router3 avente 2 interfacce con indirizzi IP:

192.168.4.1 indirizzo MAC (ethernet) ab cd ef 00 04 01

192.168.3.6 indirizzo MAC (ethernet) ab cd ef 00 03 06

Il router3 possiede anche una terza interfaccia di indirizzo 153.123.1.1 con MAC aa bb ef 00 00 01 per collegarsi alla rete 153.123.1.0.

Ogni router è dotato di tante interfacce quante sono le reti che interconnette; ogni interfaccia deve avere un indirizzo IP che fa parte della rete alla quale la interfaccia stessa è collegata.

PC4 e PC7 sono **server DNS** (domain name system) che fornisce le corrispondenze fra indirizzi e nomi simbolici (nomi di dominio). Il sistema DNS rende pubblico il fatto ad esempio che a itipisa.com corrisponde a PC13 di IP 192.168.4.4

PC13 è un **server HTTP** che ospita siti web composti da pagine html; il server è reso noto in rete dal server DNS su PC7 con il nome simbolico itipisa.com. Il server ospita ad esempio la pagina web welcome.html. Quindi questa pagina sarà identificata dall'URL (uniform resource locator) <http://itipisa.com/welcome.html>

Esempio 1:

PC1 di rete 1 vuol spedire un messaggio a PC14 di rete 4.

1) Il software di rete su PC1 (**TCP/IP protocol stack**) spezza il messaggio in (supponiamo) 3 pacchetti: P1, P2 e P3 (il numero dei pacchetti dipende dalla lunghezza del messaggio e dalla lunghezza stabilita per i pacchetti, che è un parametro da ottimizzare). Vediamo la spedizione di P1.

2) P1 è completato aggiungendo una intestazione (detto header **TCPIP**) che contiene l'IP del destinatario e quello del mittente. Nel nostro caso quindi a P1 vengono aggiunti 192.168.1.2 e 192.168.4.5 (più altre informazioni). Indichiamo il nuovo pacchetto con P1 + 192.168.1.2 + 192.168.4.5.

3) a P1 viene aggiunta una altra intestazione (detta **header ethernet**) che contiene il MAC address del router1. Il pacchetto così completato viene inviato allo switch1 che lo invia a sua volta al router1 al quale è eventualmente collegato, utilizzando appunto il MAC address. Se PC1 volesse inviare un messaggio a un PC della sua stessa rete, ad esempio PC2, dovrebbe semplicemente completare il pacchetto con il MAC di PC2 invece che con quello del router1. Nel nostro caso quindi P1 diventa alla fine P1 + 192.168.1.2 + 192.168.4.5 + ab cd ef 00 01 01 (MAC router1 porta lato rete1). E' il primo **HOP** (salto) che il pacchetto effettua.

4) Il router1 controlla l'IP del destinatario (192.168.4.5) e se scopre che questo IP appartiene a una delle reti alle quali è collegato lo consegna allo switch dopo aver sostituito il MAC della porta di ricezione con quello della rete di inoltro. Se invece non appartiene a nessuna delle reti a cui è collegato lo inoltra agli eventuali router ai quali è collegato, quindi verso le altre reti, sempre dopo aver sostituito il MAC della porta di provenienza con quello del(i) nuovo(i) router di inoltro. Se alla fine non si riesce a instradare il pacchetto in nessuna rete entro un tempo ragionevole, l'ultimo router interrogato propagherà all'indietro un messaggio di "Host Unreachable" o "No route to Host" (nodo irraggiungibile). Nel nostro caso

192.168.4.5 non appartiene alla rete2 (l'unica altra rete a cui è collegato) 192.168.2.0 (scopre ciò con l'and fra l'IP e la netmask) alla quale il router1 è collegato, pertanto router1 completa con il MAC del router2 della porta che si affaccia a rete2 (che o ha già scoperto in precedenza o scopre ora con il protocollo ARP) e lo invia ad esso, cercando di inoltrarlo quindi nella rete2, al router2 che ripeterà il processo. Il pacchetto diventa quindi: P1 + 192.168.1.2 + 192.168.4.5 + ab cd ef 00 02 05 (MAC router2 porta lato rete2).

5) Il router2 ripete lo stesso procedimento e scopre ancora che 192.168.4.5 non appartiene a nessuna delle reti alle quali è collegato; pertanto sostituisce nuovamente il MAC con quello del router3 e lo affida ad esso, cercando di inoltrarlo nella rete 3. Il pacchetto diventa quindi: P1 + 192.168.1.2 + 192.168.4.5 + ab cd ef 00 03 06 (MAC router3 porta lato rete3).

6) Il router3 ripete lo stesso procedimento e scopre ancora che 192.168.4.5 APPARTIENE A UNA delle reti alle quali è collegato: rete4; pertanto si procura con il protocollo ARP il MAC corrispondente a PC14 avente IP 192.168.4.5 e sostituisce finalmente il MAC con quello di PC4 e consegna il pacchetto allo switch4 (cioè lo inoltra dentro rete4) che finalmente lo consegna a PC14. Il pacchetto diventa quindi: P1 + 192.168.1.2 + 192.168.4.5 + ab cd ef 00 04 05 (MAC PC14).

7) Lo stesso procedimento si ripete ora per i rimanenti pacchetti P2 e P3 nei quali è stato suddiviso il messaggio, anche se come detto, a seconda delle condizioni di traffico, tempi e instradamenti possono cambiare.

Esempio 2:

PC1 è un **computer client** che ospita un **browser http** (google chrome, per esempio) con cui l'utente di PC1 cerca di accedere a <http://itipisa.com/welcome.html>.

Il software di rete su PC1 si rende conto, consultando un suo database di server già noti (risolti), che non conosce itipisa.com, ovvero l'indirizzo IP di PC13 che lo ospita. Per scoprire l'indirizzo e poter poi inviare correttamente la richiesta del documento immette in rete una richiesta, detta **interrogazione DNS**, che in pratica dice: chi conosce l'indirizzo IP di itipisa.com? Pertanto affida questa richiesta al router più vicino che la instrada verso la rete a lui più vicina, rete2. La rete 2 contiene un server DNS (PC4). Se esso conosce la risposta la invia indietro a PC1, altrimenti affida la richiesta al router che collega la rete2 con la rete3. Il router 3 instrada la richiesta dns all'interno della rete che contiene PC7, che è un server DNS. Di nuovo, se PC7 conosce l'IP di PC13 lo invia indietro a PC1, altrimenti prosegue la ricerca instradando la richiesta verso la prossima rete e verso il prossimo server DNS. Quando finalmente PC1 è venuto in possesso dell'IP di PC13 può finalmente inviargli la richiesta della pagina welcome.html. Il processo descritto prende il nome di **name resolution**. A questo punto PC13 comincia a inviare a PC1 il contenuto della pagina. Per motivi di efficienza un grosso quantitativo di dati (che chiameremo messaggio) è suddiviso in parti più piccole (che chiameremo pacchetti). Ogni pacchetto è corredato, come una lettera, dell'indirizzo mittente (sorgenete) e destinatario. Questo suddivisione è utile perchè così mentre l'utente di PC1 sta utilizzando una parte del messaggio (ad esempio la prima pagina di un testo) la rete può essere impiegata per trasmettere dati di altri utenti, ritardando la trasmissione delle altre pagine dell'utente PC1 fino a quando esse si renderanno effettivamente necessarie. Per tale utilizzo discontinuo e per il fatto che le tante reti che costituiscono internet formano una rete con tante maglie e quindi percorsi interconnesse da router, non è detto che i pacchetti che costituiscono il messaggio debbano seguire tutti la stessa strada; i router quindi hanno proprio la funzione di instradare i pacchetti del messaggio lungo il percorso più breve o meno congestionato, con minor traffico. Fanno questo con degli algoritmi particolari sui quali sorvoliamo per semplicità. Sono in realtà anche loro dei computer con un loro sistema operativo. A che serve l'indirizzo MAC? Esso serve a compiere il passo finale per la consegna dei pacchetti: è un pò come l'interno nelle scale dei palazzi che ci permette di trovare gli appartamenti, mentre l'indirizzo IP ci permette di trovare le reti così come l'indirizzo della rete stradale ci permette di trovare i palazzi. E' utilizzato dagli switch che collegano i pc della rete fra loro e al router per individuare il computer destinazione. Quando uno switch riceve un pacchetto destinato ad un pc, ad esempio PC6, non lo inoltra utilizzando direttamente l'indirizzo IP, ma piuttosto invia a tutti i pc della sua rete la domanda: chi possiede l'indirizzo IP 192.168.2.4? PC6 che lo possiede risponderà inviando il suo indirizzo MAC (ethernet) ab cd ef 00 02 04. Questo processo viene chiamato **ARP (address resolution protocol = protocollo di risoluzione degli indirizzi)**. A questo punto il pacchetto può essere consegnato. Il processo si ripete per gli altri pacchetti, magari in modo un pò più veloce perchè gli switch e i router, che sono nell'ordine più "intelligenti", avranno imparato i percorsi e quali sono quelli migliori da seguire a seconda delle condizioni di traffico. Questo spiega perchè in certi momenti la rete appare più lenta o veloce che in altri.

Nota: non ci dovrebbero essere due MAC address uguali. Anche questo non è strettamente necessario anche se più pericoloso perchè senza questa restrizione, essendo le apparecchiature di rete vendute in modo casuale, potrebbe accadere che uno acquisti due apparecchiature di rete con gli stessi MAC montandole all'interno della stessa rete; in tal caso si avrebbe un conflitto con conseguente malfunzionamento. Esistono dei database mondiali gestiti dai costruttori per evitare che ciò accada. **Chi assegna i MAC? I costruttori dei dispositivi hardware, in base a regole stabilite dallo IEEE (International Electronic and Electrotechnical Engineering institute = Istituto internazionale degli ingegneri elettronici ed elettrotecnici).**

Chi assegna gli IP?

All'interno di una rete locale abbiamo due possibilità:

1) **manuale (o fissa)**, ad esempio scegliendoli fra quelli della classe C (difficilmente avremo una rete locale con più di 254 nodi); dovranno essere tutti diversi e saranno numerati ad esempio da 192.168.x.2 a 192.168.x.254 (x sarà l'identificativo di rete, ad esempio 1 o 2 e via di seguito, quindi 254 reti, da 0 a 255). 192.168.x.1 identificherà il router (chiamato in genere impropriamente dal software windows "default gateway"), 192.168.x.0 identificherà la rete x. L'indirizzo 192.168.x.255 indica il cosiddetto indirizzo broadcast: un messaggio indirizzato a questo IP è inviato a tutti i nodi della rete. Questi messaggi non sono riscontrati dai destinatari, nel senso che non inviano una conferma di ricezione al mittente. Dobbiamo poi impostare la maschera di rete (255.255.255.0 per gli indirizzi di classe C) e uno o più indirizzi di server DNS, senza tale impostazione non riusciremo ad accedere ad alcun sito web, anche se la connessione di rete funziona. L'indirizzo 127.0.0.1 è il cosiddetto indirizzo locale (local host), e identifica il nodo sul quale ci troviamo a lavorare sulla rete. Quando compriamo un router in genere esso è accessibile all'indirizzo 192.168.1.1 o 192.168.0.1 o 192.168.1.254 o 192.168.0.254. A tale indirizzo risponde un server web integrato nel router stesso con il quale possiamo configurarlo.

2) **automatica (o dinamica)**, sfruttando una funzionalità presente all'interno dei router, chiamata server DHCP (Dynamic Host Configuration Protocol = protocollo per la configurazione dinamica dei nodi di rete). Tale server fornisce a ciascun nodo della rete locale che fa capo al router dove il server DHCP risiede un indirizzo IP univoco nella rete, insieme alla maschera di rete. Questo ci evita di dover assegnare manualmente gli indirizzi IP e di doverceli ricordare per evitare conflitti quando aggiungiamo nuovi nodi, ma è meno sicuro e rende l'avvio della rete più lento, in quanto tutte le volte che accendiamo i PC e il router la configurazione viene reinizializzata e gli indirizzi vengono rinnovati. Il fatto che gli indirizzi siano dinamici, cioè possano cambiare di volta in volta introduce delle problematiche con il funzionamento dei server, che è invece meglio che siano allocati staticamente.

Su internet la scelta avviene più o meno con le stesse modalità, ma con la differenza che mentre per i nodi client (i "nostri" PC) avere un indirizzo IP che ci viene elargito dal nostro fornitore di servizi (di connettività, come si dice, Wind, Telecom, Fastweb per dirne alcuni, in gergo si chiamano ISP=internet service provider) e ci viene comunicato nuovo ogni volta che accendiamo il router non è un gran male, dal momento che non siamo pubblici, e non ci deve corrispondere un nome di dominio in un DNS, per un server invece (ad esempio il server del motore di ricerca di google in

Italia, google.it che ha IP=173.194.40.56) è necessario che tale IP sia FISSO, come si suol dire statico, altrimenti bisognerebbe cambiarlo tutte le volte che il server e il router a cui è connesso vengono accesi, e informare di ciò tutti i DNS!! Si può fare (si chiama appunto IP dinamico e si parla quindi di dynamic DNS) ma è più complicato, lento e incline a malfunzionamenti (potrebbe succedere che a più server venga dato lo stesso IP). L'IP statico deve essere rilasciato (A PAGAMENTO) da una apposita autorità di controllo della rete internet: lo **IANA (Internet Assigned Number Authority)** che ha diramazioni e uffici in tutti gli stati del mondo. Quindi se vogliamo installare un server http (Apache per esempio) sul nostro PC per ospitare un sito web e renderlo pubblico non basta installare Apache e mettere il sito che costituisce l'ipertesto dentro la apposita cartella **htdocs** che ospita i siti; dobbiamo comprare un IP statico e un nome di dominio dallo IANA che lo registra nel suo DNS (la registrazione poi piano piano, man mano che si accede al sito, si propagherà negli altri DNS in giro per il mondo). Se non facciamo così il nostro bel sito sarà visibile solo se di volta in volta comunichiamo a chi ci vuole navigare l'indirizzo IP che è stato momentaneamente assegnato al nostro PC server, servendo a ben poco!!

Principali server possibili:

- 1) server http: ospita pagine WEB (html). uno famoso è APACHE.
- 2) server FTP: ospita file di tutti i tipi: i file non sono però visualizzabili direttamente come in un browser web ma scaricabili e caricabili in modo massivo.
- 3) server POP: posta elettronica in ingresso
- 4) server SMTP: posta elettronica in uscita
- 5) server IMAP: posta elettronica via web, senza client sul proprio PC (tipo katamail.com)
- 5) server NTP: distribuisce l'ora su Internet
- 6) server musicali per internet radio: rendono disponibili brani musicali su internet, funzionano come una vera e propria radio
- 7) server video: rendono disponibili video su internet.
- 8) server DNS. Come detto implementano il sistema di traduzione nomi simbolici (URL) <--> indirizzo IP. Senza di essi internet sarebbe difficilissimo da usare: occorrerebbe conoscere gli indirizzi IP di qualsiasi cosa!!!
- 9) proxy server (di vario tipo) sono delle specie di memorie tampone che mantengono le informazioni più recentemente accedute (ad esempio pagine web) evitando di doverle reperire di nuovo dalla sorgente ad ogni richiesta. Possono comunque svolgere anche delle funzioni di protezione, controllo di accesso e redirectione.

Ne esistono comunque molti altri tipi.