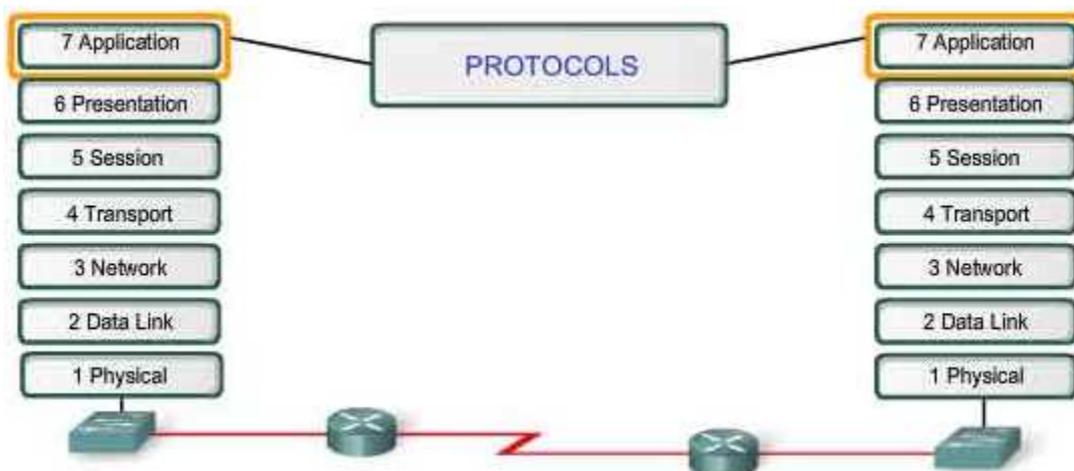
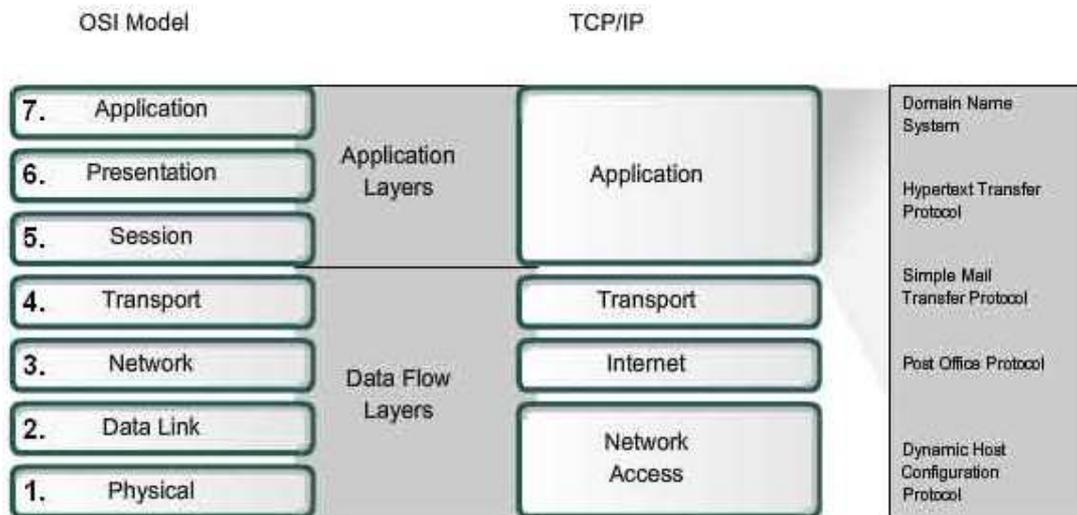


Il livello Application



Nel nostro modello di architettura (e anche nell'architettura TCP/IP) sopra il livello transport c'è il livello **application**, nel quale viene effettivamente svolto il lavoro utile per l'utente.

In questo livello si trovano diverse tipologie di oggetti:

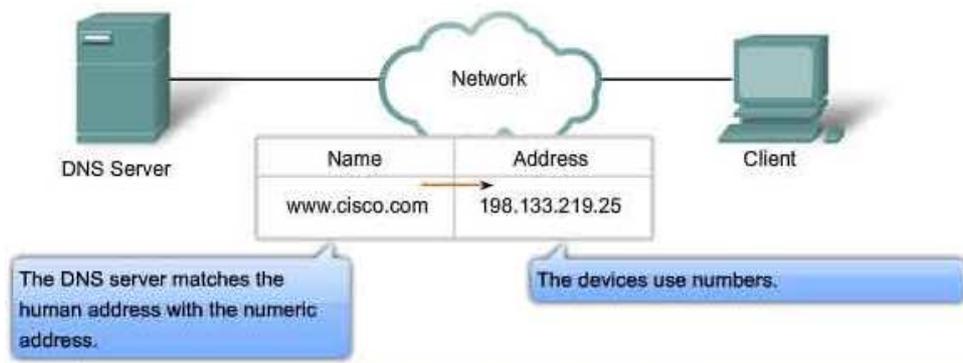
- **protocolli di supporto a tutte** le applicazioni, come per esempio il **DNS (Domain Name System)**;
- **protocolli di supporto ad applicazioni** di tipo standardizzato, come ad esempio:
 - **SNMP** (Simple Network Management Protocol) per la gestione della rete;
 - **FTP** (File Transfer Protocol) per il trasferimento di file;
 - **SMTP e POP3** (Simple Mail Transfer Protocol e Post Office Protocol) per la posta elettronica;
 - **HTTP** (HyperText Transfer Protocol) alla base del **World Wide Web (WWW)**;
 - **DHCP** (Dynamic Host Configuration Protocol) consente di ottenere gli indirizzi IP
- **applicazioni** scritte in conformità ai protocolli di cui sopra;
- **applicazioni proprietarie**, basate su regole di dialogo private (ad esempio, un'applicazione di tipo client/server per la gestione remota di un magazzino).

DNS



Poiché riferirsi a una risorsa (sia essa un host oppure l'indirizzo di posta elettronica di un utente) utilizzando un indirizzo **IP numerico** (della forma x.y.z.w) è estremamente scomodo, si è creato un meccanismo tramite il quale tali risorse possono essere identificate tramite un **nome logico**, cioè una stringa di caratteri (molto più comprensibile per un essere umano).

La corrispondenza fra gli indirizzi IP numerici ed i nomi logici si effettua mediante l'uso del DNS.

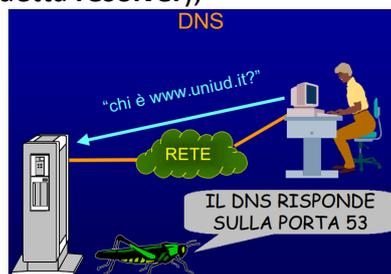


Esso consiste di:

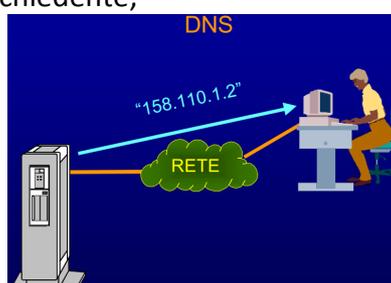
1. uno **schema gerarchico** di nominazione, basato sul concetto di dominio (**domain**);
2. un **database distribuito** che implementa lo schema di nominazione;
3. un **protocollo** per mantenere e distribuire le informazioni corrispondenti.

Il funzionamento, in breve, è il seguente:

- quando un'applicazione deve collegarsi ad una risorsa di cui conosce il nome logico (ad es. fisica.unipd.it), **invia una richiesta al DNS server locale** (l'applicazione chiama per questo una apposita procedura di libreria detta **resolver**);



- il DNS server locale, se conosce la risposta, la invia direttamente al richiedente. Altrimenti interroga a sua volta un DNS server di livello superiore, e così via. Quando finalmente **arriva la risposta**, il DNS server locale la passa al richiedente;



- quando l'applicazione riceve la risposta (costituita del numero IP della risorsa in questione) **crea una connessione TCP** con la (o spedisce segmenti UDP alla) destinazione, usando l'indirizzo IP testé ricevuto.

Lo spazio dei nomi **DNS è uno spazio gerarchico**, organizzato in domini, ciascuno dei quali può avere dei sottodomini.

Esiste un insieme di domini di massimo livello (top-level domain), i più alti nella gerarchia.

Nel caso di un host, la forma del nome logico è costituita da un certo numero di sottostringhe separate da punti, come nell'esempio seguente:

host.subdomain3.subdomain2.subdomain1.topleveldomain

dove:

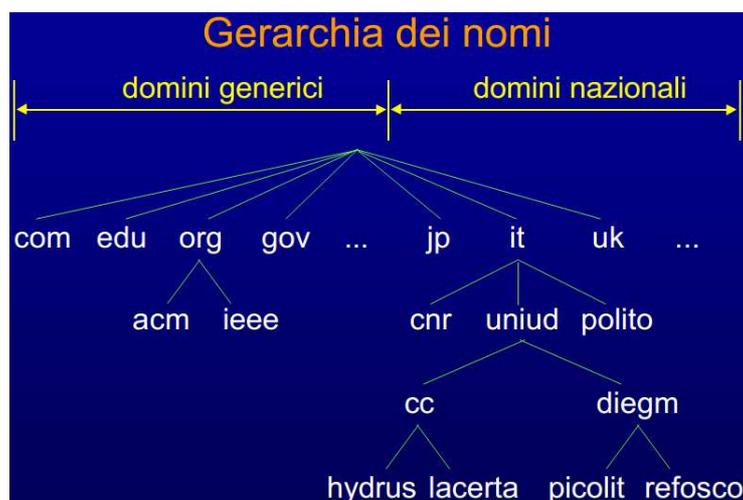
- la prima sottostringa (quella più a sinistra) identifica il **nome dell'host;**
- le altre sottostringhe (tranne quella più a destra) identificano ciascuna un **sottodominio** del dominio di cui alla sottostringa seguente;
- l'ultima sottostringa (quella più a destra) identifica il **top-level domain** di appartenenza.

Sono definiti, fra gli altri, i seguenti top-level domain:

- com aziende
- edu università
- gov istituzioni governative
- mil istituzioni militari
- net fornitori d'accesso
- org organizzazioni non-profit

Ogni nazione ha un suo top-level domain. Ad esempio:

- au Australia
- ch Svizzera
- fr Francia
- it Italia
- jp Giappone
- uk Inghilterra



Ogni dominio è responsabile della creazione dei suoi sottodomini, che devono essere registrati presso una apposita autorità.

L'estensione di un dominio è del tutto indipendente da quella delle reti e sottoreti IP. Ogni dominio ha la responsabilità di fornire il servizio DNS per quanto di propria competenza. Ossia, deve poter rispondere a interrogazioni riguardanti tutti gli host contenuti nel dominio stesso.

Ciò si ottiene predisponendo un **name server** (o più di uno), che è un processo in grado di gestire le seguenti informazioni:

- informazioni di corrispondenza fra nomi simbolici e indirizzi IP. Per ogni host del dominio esiste un **descrittore di risorse (resource record)** che contiene tali informazioni; tale record è detto **authoritative record**, in quanto è gestito dal DNS server responsabile del dominio (che è supposto fornire sempre informazioni corrette e aggiornate);
- **l'identità dei name server responsabili dei sottodomini** inclusi nel dominio, così da poter inviare loro le richieste che gli pervengono dall'alto della gerarchia;
- **l'identità del name server responsabile del dominio** di livello immediatamente superiore, così da potergli inviare le richieste che gli pervengono dal basso della gerarchia.

Una **richiesta che arriva** a un name server può dunque viaggiare verso l'alto nella gerarchia oppure (dal momento in cui perviene a un top-level domain server) verso il basso, a seconda dei casi.

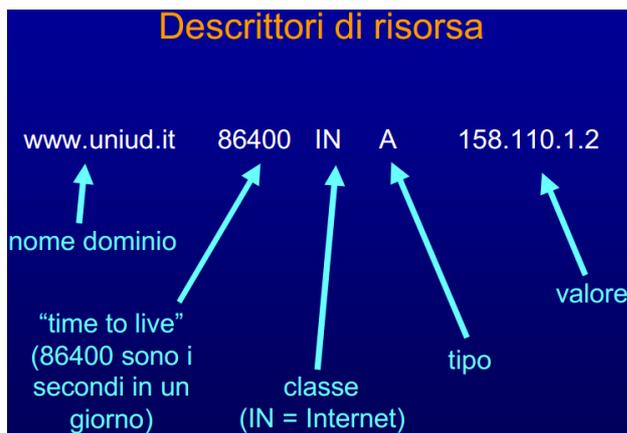
Quando **una risposta ritorna** indietro, essa viene tenuta dal server in una sua cache per un certo periodo; qui costituisce un nuovo record, detto **cached record** perché contiene della informazione che potrebbe anche divenire, col passare del tempo, obsoleta e non più corretta.

Un esempio di **resource record** (relativo a un host) è:

```
fisica.unipd.it 86400 IN A 151.100.17.110
```

dove:

fisica.unipd.it	domain_name:	nome simbolico.
86400	time_to_live:	la quantità di tempo (in secondi) trascorsa la quale il record viene tolto dalla cache.
IN	class:	classe del record (Internet in questo caso).
A	type:	tipo del record (Address in questo caso).
151.100.17.110	value:	indirizzo IP numerico.

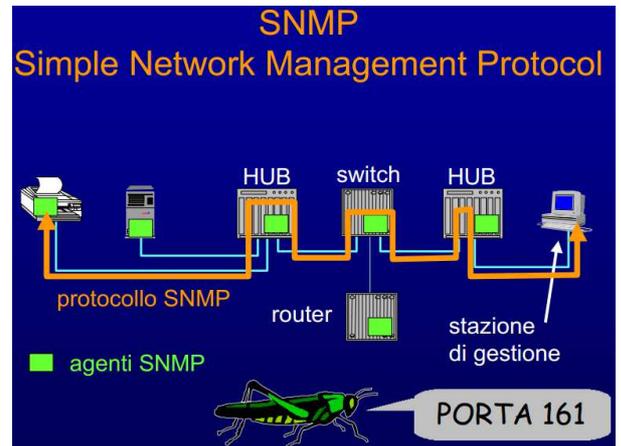


Tipi di descrittori		
SOA	start of authority	parametri per questa zona
A	address	indirizzo IP
MX	mail exchange	dominio che accetta la posta (+ priorità per gestire più alternative)
CNAME	canonic name	utilizzato per creare alias di nomi di dominio (es. di posta elettronica)
PTR	pointer	alias per un indirizzo IP
HINFO	host information	descrizione della CPU e del S.O. in ASCII
TXT	text	testo ASCII non interpretato

Il **nslookup** ha molte opzioni disponibili per attività di sperimentazione e verifica del DNS processo. Il **ipconfig /displaydns** da ulteriori informazioni.

SNMP Simple Network Management Protocol

- Consente la gestione di nodi della rete attraverso la rete stessa
- Consente attività diverse
 - configurazione di apparecchiature
 - statistiche sul traffico
 - segnalazione di guasti



Posta elettronica

La posta elettronica è uno dei servizi più consolidati ed usati nelle reti. In Internet è in uso da circa 20 anni, e prima del WWW era senza dubbio il servizio più utilizzato.

Un servizio di posta elettronica, nel suo complesso, consente di effettuare le seguenti operazioni:

- **comporre** un messaggio;
- **spedire** il messaggio (a uno o più destinatari);
- **ricevere** messaggi da altri utenti;
- **leggere** i messaggi ricevuti;
- **stampare, memorizzare, eliminare** i messaggi spediti o ricevuti.

Di norma, un messaggio ha un formato ben preciso. In Internet un messaggio ha un formato costituito da un header e da un body, separati da una linea vuota.

Lo header è a sua volta costituito da una serie di linee, ciascuna relativa a una specifica informazione (identificata da una parola chiave che è la prima sulla linea); alcune informazioni sono:

To	indirizzo di uno o più destinatari.
From	indirizzo del mittente.
Cc	indirizzo di uno o più destinatari a cui si invia per conoscenza.
Bcc	blind Cc: gli altri destinatari non sanno che anche lui riceve il messaggio.
Subject	argomento del messaggio.
Sender	chi materialmente effettua l'invio (ad es. nome della segretaria).

RFC 822: campi assimilabili a quelli della busta

To:	destinatario/i primario/i
Cc:	destinatario/i secondario/i (copia per conoscenza)
Bcc:	copia per conoscenza non notificata ai destinatari primari e secondari
From:	mittente
Sender:	indirizzo di posta elettronica del mittente
Received:	linea aggiunta da ogni agente di trasferimento lungo il percorso
Return-Path:	può specificare il percorso da seguire per la risposta

RFC 822: campi assimilabili a quelli dell'intestazione

Date:	data e ora di invio del messaggio
Reply-To:	indirizzo di posta elettronica a cui inviare le risposte
Message-Id:	identificatore (unico) del messaggio per futuri riferimenti
In-Reply-To:	Message-Id a cui si sta rispondendo
References:	altri Message-Id di riferimento
Keywords:	parole chiave scelte dall'utente
Subject:	argomento del messaggio (una riga)

Il body contiene il testo del messaggio, in caratteri ASCII. L'ultima riga contiene solo un punto, che identifica la fine del messaggio.

Gli indirizzi di posta elettronica in Internet hanno la forma:

username@hostname

dove

username è una stringa di caratteri che identifica il destinatario,

hostname è un nome DNS oppure un indirizzo IP.

Ad esempio, giovanni@gmail.com è l'indirizzo di posta elettronica di Giovanni.

La posta elettronica viene implementata in Internet attraverso la cooperazione di due tipi di sottosistemi:

- Mail User Agent (**MUA**);
- Mail Transport Agent (**MTA**).

Il primo permette all'utente finale di:

- **comporre** messaggi;
- **consegnarli** a un MTA per la trasmissione;
- **ricevere e leggere** messaggi;
- **salvarli o eliminarli**.

Il secondo si occupa di:

- **trasportare** i messaggi sulla rete, fino alla consegna a un MTA di destinazione;
- **rispondere** ai MUA dei vari utenti per consegnare loro la posta arrivata; in questa fase l'MTA richiede ad ogni utente una password per consentire l'accesso ai messaggi.

Corrispondentemente, sono definiti due protocolli principali per la posta elettronica:

- **SMTP** (Simple Mail Transfer Protocol) per il trasporto dei messaggi:
 - dal MUA di origine ad un MTA;
 - fra vari MTA, da quello di partenza fino a quello di destinazione;
- **POP3** (Post Office Protocol versione 3) per la consegna di un messaggio da parte di un MTA al MUA di destinazione.

Recentemente sono stati introdotti altri protocolli più sofisticati, quali

- **IMAP** (Interactive Mail Access Protocol) e
- **DMSP** (Distributed Mail System Protocol), il cui supporto però non è ancora molto diffuso nel software disponibile agli utenti.

Come avviene la trasmissione di un messaggio? Supponiamo che l'utente

pippo@libero.it

spedisca un messaggio a

maria@gmail.com

e immaginiamo che:

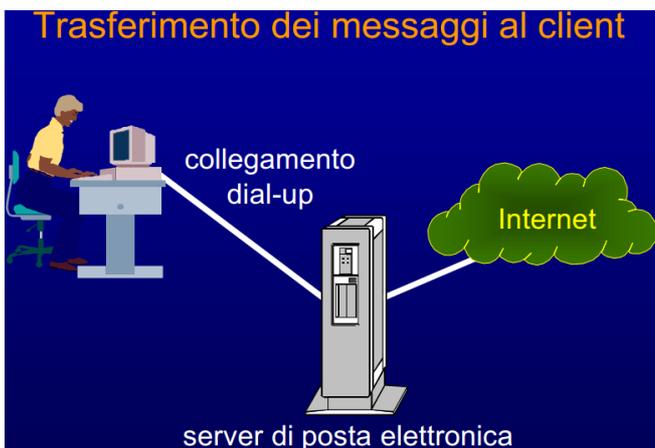
- Pippo usi un **MUA** configurato per consegnare la posta ad un **SMTP** server in esecuzione sull'host **mailer.libero.it**;
- Maria abbia un **MUA** configurato per farsi consegnare la posta da un **POP3** server in esecuzione sull'host **mailer.gmail.com**.

La sequenza di azioni che hanno luogo è la seguente:

1. Pippo compone il messaggio col suo MUA, che tipicamente è un programma in esecuzione su un PC in rete;
2. appena Pippo preme il pulsante SEND, il suo MUA:
 - interroga il DNS per sapere l'indirizzo IP dell'host mailer.libero.it;
 - apre una connessione TCP ed effettua una conversazione SMTP con il server SMTP in esecuzione sull'host mailer.libero.it, per mezzo della quale gli consegna il messaggio;
 - chiude la connessione TCP;
3. Pippo se ne va per i fatti suoi;

4. il server SMTP di mailer.libero.it:
 - chiede al DNS l'indirizzo IP di gmail.com;
 - scopre che è quello dell'host mailer.gmail.com;
 - apre una connessione TCP e poi una conversazione SMTP con il server SMTP in esecuzione su quell'host e gli consegna il messaggio scritto da Pippo;
5. Maria lancia il suo MUA;
6. appena Maria preme il pulsante "check mail", il suo MUA:
 - interroga il DNS per avere l'indirizzo IP dell'host mailer.gmail.com;
 - apre una connessione TCP e poi una conversazione POP3 col server POP in esecuzione su mailer.gmail.com e preleva il messaggio di Pippo, che viene mostrato a Maria.

Si noti che libero.it e gmail.com in genere corrispondono a un dominio nel suo complesso e non ad un singolo host, al fine di rendere gli indirizzi di posta elettronica indipendenti da variazioni del numero, dei nomi logici e degli indirizzi IP degli host presenti nel dominio.



Nel DNS ci sono opportuni record detti di tipo **MX (Mail Exchange)**, che si occupano di indicare quale host effettivamente fa da server SMTP per un dominio.

Nel nostro esempio avremo, nel DNS server di Gmail, i record:

- mailer.gmail.com A 100.10.10.5
- gmail.com MX mailer.gmail.com

Il secondo record è un record di tipo MX, e indica che tutta la posta in arrivo per chiunque@gmail.com deve essere consegnata all'host mailer.gmail.com, e cioè quello che ha l'indirizzo IP 100.10.10.5

Infine, vanno citate due significative estensioni di funzionalità della posta elettronica:

- possibilità di inviare messaggi di posta contenenti informazioni di qualunque tipo (per esempio programmi eseguibili, immagini, filmati, suoni, ecc.) attraverso lo standard **MIME** (Multipurpose Internet Mail Extension);
- possibilità di inviare messaggi con firma digitale o crittografati, con lo standard **S/MIME** (Secure/MIME).

DHCP

Dynamic Host Configuration Protocol (DHCP) servizio consente ai dispositivi su una rete di ottenere gli indirizzi IP e altre informazioni da un server DHCP. Questo servizio permette quindi di automatizzare l'assegnazione di indirizzi IP, subnet mask, gateway IP e altri parametri di rete.

Il server DHCP sceglie un indirizzo da un intervallo di indirizzi preconfigurati e lo assegna all'host per un determinato periodo.

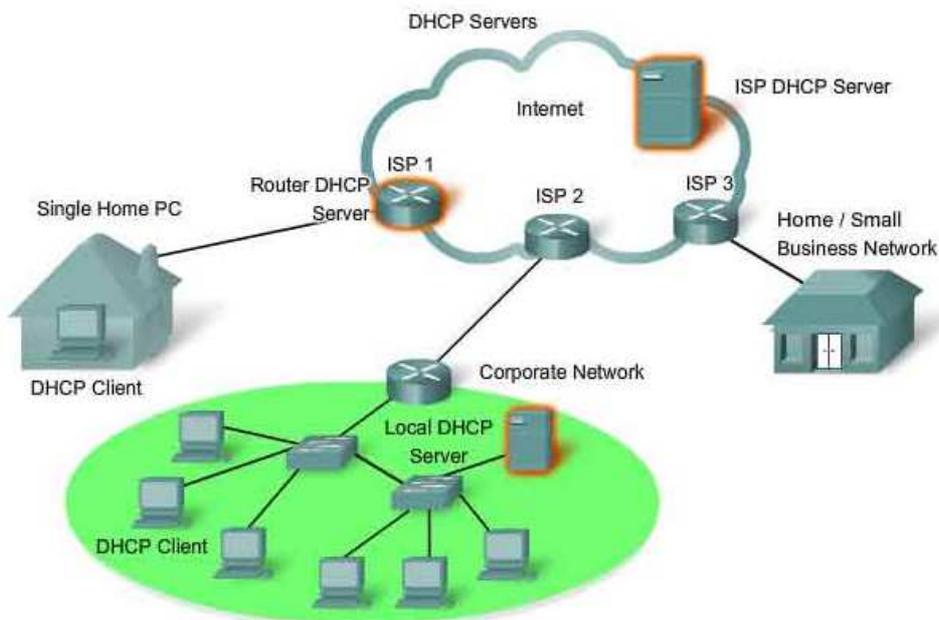
Su grandi reti locali, o in cui l'utente popolazione cambia frequentemente, DHCP è preferito. I nuovi utenti possono arrivare con un portatile e avere bisogno di una connessione. Altri sono nuovi posti di lavoro che devono essere collegati. Piuttosto di avere l'amministratore di rete che assegna gli indirizzi IP per ogni postazione di lavoro, è più efficiente di avere indirizzi IP assegnati automaticamente mediante il protocollo DHCP.

Gli indirizzi distribuiti da DHCP non vengono assegnati a host, ma sono solo affittati per un periodo di tempo.

Se l'host è spento o al di fuori della rete, l'indirizzo è restituito al DHCP per il riutilizzo. Questo è particolarmente utile con gli utenti mobili che vanno e vengono su una rete. Gli utenti possono liberamente muoversi da un luogo ad un altro e stabilire una connessione. L'host può ottenere un indirizzo IP, una volta l'hardware di connessione è attivo, sia attraverso una cablata o wireless LAN. DHCP rende possibile di accedere a Internet tramite hotspot wireless negli aeroporti o caffè. Non appena entrerete in una determinata area, il vostro computer portatile client DHCP contatta il server DHCP locale tramite una connessione wireless. Il server DHCP assegna un indirizzo IP a un computer portatile.

Come è mostrato in figura vari tipi di apparecchiature possono fungere da DHCP server quando in esse è attivo un software per il servizio DHCP. Il server DHCP nella maggior parte delle medie e grandi reti è di solito un PC-based server locale dedicato. Reti domestiche con il server DHCP di solito riceve la sua configurazione IP direttamente dal provider di servizi Internet.

DHCP può costituire un rischio per la sicurezza, perché qualsiasi dispositivo collegato alla rete possono ricevere un indirizzo. Molti usano entrambe le due reti DHCP e indirizzamento statico. Il DHCP viene utilizzato per finalità generali di host come ad esempio dispositivi di utente finale, e fissa gli indirizzi che possono essere utilizzati per i dispositivi di rete, come gateway, switch, server e stampanti.



Senza DHCP, gli utenti devono configurare manualmente l'indirizzo IP, la subnet mask e altre impostazioni di rete, al fine di aderire alla rete. Il server DHCP mantiene un pool di indirizzi IP per qualsiasi DHCP client abilitato quando il client è acceso.

Quando un dispositivo DHCP configurato si connette alla rete, il client trasmette un pacchetto **DHCP DISCOVER** per identificare qualsiasi server DHCP disponibile sulla rete.

Un server DHCP risponde con **DHCP OFFERTA**, che è una offerta di locazione con un indirizzo IP assegnato, con maschera di sottorete, server DNS, gateway predefinito e informazioni, nonché la durata del contratto di uso.

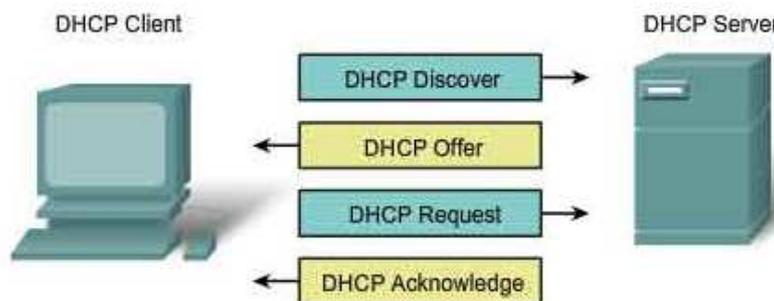
Il client può ricevere più i pacchetti DHCP OFFER se vi è più di un server DHCP sulla rete locale, quindi deve scegliere tra loro, e trasmettere un pacchetto di richiesta DHCP che identifica l'esplicito server e offerta di locazione che il cliente accetta.

Un client può scegliere di richiedere un indirizzo che aveva già assegnato dal server. Supponendo che l'indirizzo IP richiesto dal cliente, o offerti dal server, è ancora valido, il server potrebbe restituire un messaggio **DHCP ACK** che riconosce al cliente il contratto di uso.

Se l'offerta non è più valida - forse a causa di un time-out o un altro client che ripartisce il contratto di uso - il server risponderà con un messaggio **DHCP NAK**.

Se un messaggio DHCP NAK è tornato, il processo di selezione deve iniziare di nuovo con una nuova DHCP DISCOVER messaggio che viene trasmesso. Una volta che il cliente ha il contratto di uso, deve essere rinnovato prima della scadenza attraverso un altro messaggio di richiesta DHCP.

Il server DHCP assicura che tutti gli indirizzi IP sono unici (un indirizzo IP non può essere assegnato a due differenti dispositivi di rete contemporaneamente). Utilizzo di DHCP consente amministratori di rete di riconfigurare facilmente client di indirizzi IP senza dover apportare modifiche manualmente ai clienti. La maggior parte degli Internet provider utilizzano il protocollo DHCP per assegnare gli indirizzi ai loro clienti che non richiedono un indirizzo statico.



Il servizio DHCP utilizza un processo diviso in quattro fasi:

1. DHCPDISCOVER
2. DHCPOFFER
3. DHCPREQUEST
4. DHCPACK

Il **DHCPDISCOVER** (richiesta di IP) è il primo passaggio nel quale il client fa una richiesta a un indirizzo broadcast. Questo perchè l'indirizzo del server DHCP, servente per fare la richiesta di IP, è sconosciuto, il client allora esegue la

- richiesta da un IP uguale a **0.0.0.0** e
- come destinazione a **255.255.255.255**.

Nel messaggio del dhcpdiscover sono contenuti

- **gli indirizzi hardware e**
- **il nome del client,**

in modo che il server riesca a risalire al mittente e quindi al giusto client.

Nel **DHCPOFFER** (offerta di IP), tutti i server DHCP che ricevono una richiesta effettuano il broadcasting di un **mesaggio DHCPOFFER**, comprendente

- l'indirizzo hardware del client,
- un IP, una subnet mask,
- la durata effettiva del lease e infine
- l'indirizzo IP del server offrente.

Il server invia un messaggio. Il client seleziona l'IP della prima offerta ricevuta. Il server inoltre "registra" l'IP rilasciato, in modo da non rilasciarlo a un altro client.

Il **DHCPREQUEST** (selezione di IP), terzo passaggio del processo DHCP, avviene dopo che il client ha ricevuto un messaggio **DHCPOFFER**, cioè l'offerta dell'IP da parte del server. Il client accetta l'indirizzo IP, offerto da un server DHCP, e rifiuta tutte le altre offerte.

Il **DHCPACK** (ACKnowledgment) avviene quando il client accetta un IP in modo corretto. In poche parole, il messaggio **DHCPACK** non è altro che una conferma che il client dà al server.

Al contrario, se l'esito è quindi negativo, viene effettuato il broadcasting di un messaggio **DHCPNACK** (messaggio negativo).

DHCP Nack

Il DHCP Nack (Negative ACKnowledgment), è un pacchetto che viene trasmesso dal server DHCP quando il client ha richiesto un indirizzo IP che non è possibile utilizzare nella attuale subnet.

DHCP Relay Agent

Dopo quanto scritto, ci possiamo porre delle domande: sulla mia rete quanti server DHCP mi servono? Mi servono tanti server DHCP quanti sono i segmenti della rete? Assolutamente no. Possiamo usare un DHCP Relay Agent.

WWW e HTTP

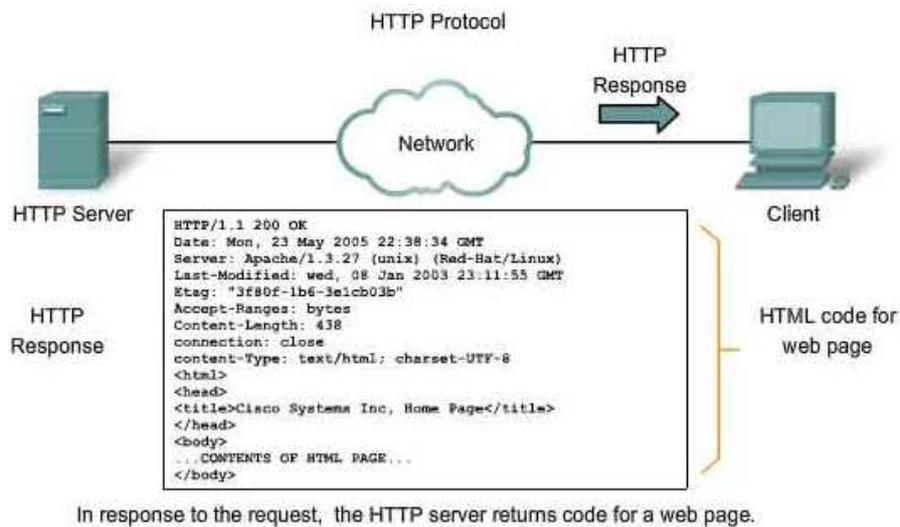
Quando un indirizzo web (o un URL) viene digitato in un browser Web, il browser Web stabilisce una connessione al servizio web in esecuzione sul server utilizzando il protocollo **HTTP**. **URL** (Uniform Resource Locator) e **URI** (Uniform Resource Identifier) sono i nomi associare la maggior parte delle persone con indirizzi web. L'URL `http://www.mysite.com/index.html` è un esempio di un URL che fa riferimento a una risorsa specifica - una pagina web di nome **index.html** su un server identificato come **mysite**. I browser web sono le applicazioni client che i computer utilizzano per connettersi al World Wide Web e di accedere alle risorse memorizzati su un server web.

Il server risponde con le risorse e, al momento del ricevimento, il browser interpreta i dati e le presenta all'utente. I browser sono in grado di interpretare e presentare molti tipi di dati, come ad esempio testo in formato semplice o **HTML (Hypertext Markup Language)**. Altri tipi di dati, tuttavia, si possono richiedere con altro servizio o programma, di solito denominato plug-in o add-on. Prendiamo per esempio l'URL: `http://www.mysite.com/web-server.htm`. In primo luogo, il browser interpreta le tre parti del URL:

- **http** (il protocollo o di regime)
- **www.mysite.com** (il nome del server)
- **Web-server.htm** (il nome di file specifici richiesti).

Il browser poi converte il nome del server in un indirizzo numerico, che utilizza per connettersi al server. Utilizzando il protocollo HTTP, il browser invia una richiesta GET al server e richiede il file **web-server.htm**.

Il server a sua volta, invia il codice HTML di questa pagina web al browser. Infine, il browser decifra il codice HTML e formata pagina per la finestra del browser.



L'Hypertext Transfer Protocol (HTTP), uno dei protocolli TCP/IP suite, è stato originariamente sviluppato per pubblicare e recuperare le pagine HTML ed ora è usato in diversi sistemi di informazione. HTTP è utilizzato in tutto il World Wide Web per il trasferimento dei dati ed è uno dei più diffusi protocolli di applicazione.

HTTP specifica una richiesta / risposta di protocollo. Quando un client, tipicamente un browser web, invia un messaggio di richiesta ad un server, il protocollo HTTP definisce i tipi di messaggi utilizza il client per richiedere la pagina web e anche i tipi di messaggi il server utilizza per rispondere. I tre tipi di messaggi comuni sono GET, POST, PUT.

GET è una richiesta di dati da client. Un browser invia il messaggio GET per una richiesta di pagine da un server web. Come Una volta che il server riceve la richiesta GET, essa risponde con indicazioni sulla riga di stato.

POST e **PUT** sono usati per richiedere il caricamento dei dati al server Web. Per esempio, quando l'utente immette i dati in una form incorporato in una pagina web, POST include i dati del messaggio inviato al server.

Differenze tra...

GET POST

Indicato per pochi parametri

Indicato per grandi quantità di dati

Solo parametri testuali

Dati in qualsiasi formato (testi, immagini, video)

Possibilità di inserire un URL con parametri opportuni all'interno di una pagina HTML

Solo in risposta ad una form

es.

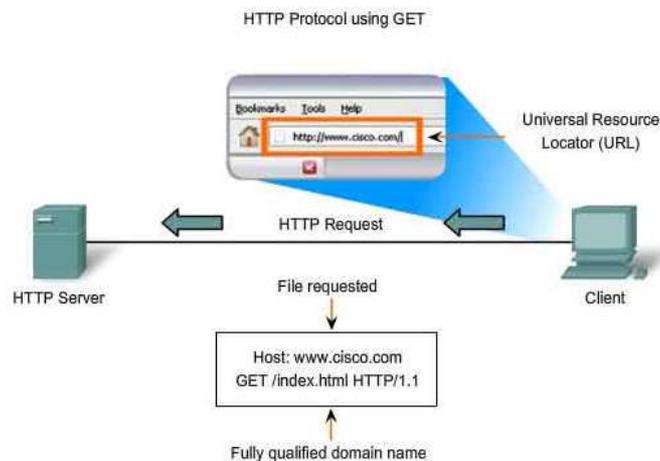
```

... <A HREF="http://www.altavista.com/cgi-bin/search?query=complexity">Ricerca Altavista sulla complessità</A>...

```

Anche se è notevolmente flessibili, **HTTP non è un protocollo di sicurezza**. I messaggi **POST** inviano informazioni al server in formato testo che può essere intercettata e letta. Allo stesso modo, le risposte del server, di solito le pagine HTML, sono anche in chiaro.

Per la comunicazione sicura su Internet, **HTTPS è il protocollo utilizzato** per l'accesso o la pubblicazione delle informazioni sul server web. Con HTTPS è possibile utilizzare l'autenticazione e la crittografia per la protezione dei dati che viaggiano tra il client e il server. HTTPS prevede norme aggiuntive per trasferire i dati tra l'applicazione e il livello Transport Layer.



FTP

File Transfer Protocol (FTP) è un altro protocollo comunemente utilizzato del **livello application**.

FTP è stato sviluppato per consentire il trasferimento di file tra un client e un server.

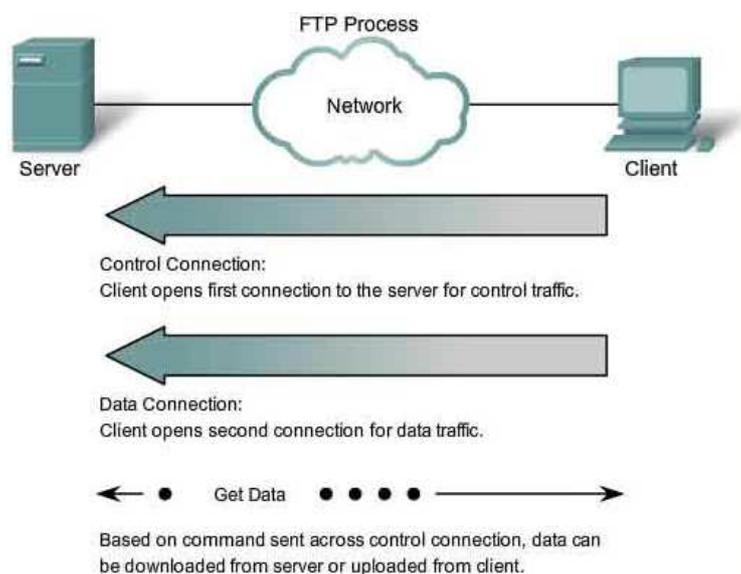
Un client FTP è un'applicazione che gira su un computer che viene utilizzato per l'upload e il download dei file da un server che esegue il demone FTP.

Per trasferire i file con successo, **FTP richiede due connessioni tra il client e il server:**

1. una per i **comandi** e le risposte,
2. l'altra per l'effettivo **trasferimento** di file.

Il client stabilisce la prima connessione al server alla **porta 21**. Questa connessione viene utilizzata per il controllo del traffico, composto di comandi client e server risposte.

Il client stabilisce la seconda connessione al server sulla porta **TCP 20**. Questa connessione è per l'effettivo trasferimento di file e viene creato ogni volta che c'è un file trasferiti. Il trasferimento dei file può avvenire in entrambe le direzioni. Il client può scaricare, un file dal server e può caricare un file sul server.



```
Microsoft Windows [Versione 6.3.9600]
(c) 2013 Microsoft Corporation. Tutti i diritti riservati.

C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>nslookup
Server predefinito:  google-public-dns-a.google.com
Address:  8.8.8.8

> www.google.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Risposta da un server non autorevole:
Nome:      www.google.com
Addresses: 2a00:1450:4002:80a::2004
           216.58.205.164

> www.facebook.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Risposta da un server non autorevole:
Nome:      star-mini.c10r.facebook.com
Addresses: 2a03:2880:f11c:8083:face:b00c:0:25de
           31.13.93.36
Aliases:   www.facebook.com

>
```

```
sb.l.google.com
-----
Nome record . . . . . : sb.l.google.com
Tipo record . . . . . : 1
Durata (TTL). . . . . : 225
Lunghezza dati. . . . . : 4
Sezione . . . . . : Risposta
Record A (Host) . . . . : 216.58.205.174

ocsp05.actalis.it
-----
Nome record . . . . . : ocsp05.actalis.it
Tipo record . . . . . : 5
Durata (TTL). . . . . : 388
Lunghezza dati. . . . . : 8
Sezione . . . . . : Risposta
Record CNAME . . . . . : ocsp.actalis.it

Nome record . . . . . : ocsp.actalis.it
Tipo record . . . . . : 1
Durata (TTL). . . . . : 388
Lunghezza dati. . . . . : 4
Sezione . . . . . : Risposta
Record A (Host) . . . . : 109.70.240.130

cs9.wac.phicdn.net
-----
Nome record . . . . . : cs9.wac.phicdn.net
Tipo record . . . . . : 1
Durata (TTL). . . . . : 329
Lunghezza dati. . . . . : 4
Sezione . . . . . : Risposta
Record A (Host) . . . . : 93.184.220.29

C:\>
```