Sommario

[Introduzione 3](#_Toc442173204)

[Classificazione 3](#_Toc442173205)

[Architetture di rete 5](#_Toc442173206)

[Client/Server 5](#_Toc442173207)

[Client 6](#_Toc442173208)

[Server 6](#_Toc442173209)

[Come funziona una rete client/server 6](#_Toc442173210)

[Come comunicano client e server 7](#_Toc442173211)

[Esempi di sistemi client/server: 7](#_Toc442173212)

[Peer to Peer 8](#_Toc442173213)

[Come funziona un’architettura p2p 8](#_Toc442173214)

[Internet 8](#_Toc442173215)

[La storia di Internet 8](#_Toc442173216)

[I servizi Internet 9](#_Toc442173217)

[Extranet 9](#_Toc442173218)

[IP 9](#_Toc442173219)

[IPv4 9](#_Toc442173220)

[IPv6 10](#_Toc442173221)

[URL 10](#_Toc442173222)

[I nomi di dominio 10](#_Toc442173223)

[Il www 11](#_Toc442173224)

[Utilizzare la rete 11](#_Toc442173225)

[Il Modem 11](#_Toc442173226)

[I browser 12](#_Toc442173227)

[I motori di ricerca 13](#_Toc442173228)

[Il dns 14](#_Toc442173229)

[Com’è fatto 15](#_Toc442173230)

[Come lavora 15](#_Toc442173231)

[Il protocollo http 16](#_Toc442173232)

[L’ipertesto 16](#_Toc442173233)

[La sicurezza in Internet 17](#_Toc442173234)

[Informazioni sensibili, quali sono, perché proteggersi 17](#_Toc442173235)

[Vari tipi di attacchi 17](#_Toc442173236)

[Gli antivirus 18](#_Toc442173237)

[La crittografia 18](#_Toc442173238)

[Il protocollo https 18](#_Toc442173239)

[I certificati 18](#_Toc442173240)

[Differenza tra http e https 19](#_Toc442173241)

[Casi d’uso 20](#_Toc442173242)

[Richiesta di un video al server YouTube 20](#_Toc442173243)

[DNS: 22](#_Toc442173244)

# Introduzione

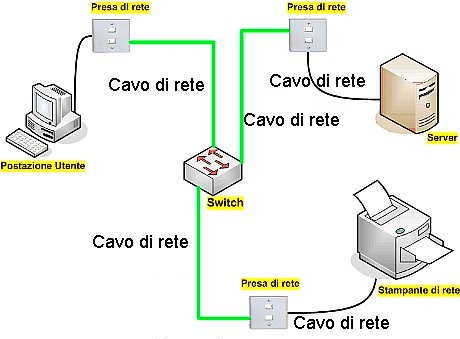
Una rete informatica è un insieme di PC (appartenenti allo stesso ambiente oppure messi a distanza) e di altri dispositivi che sono collegati tra loro. Se i computer sono collegati in rete è possibile condividere risorse software (files, programmi) e risorse hardware (modem, stampanti, scanner, ecc). La più grande rete di computer attualmente esistente è INTERNET che è anche definita la “RETE DELLE RETI” oppure “RETE GLOBALE”: collega tra le reti di tutto il pianeta.

# Classificazione

Le reti possono essere classificate in base a : estensione geografica, canale di trasmissione, topologia, connessione.

1. In baseall’ **ESTENSIONE GEOGRAFICA** si classificano in:

* **PAN (Rete personale)**:la rete si estende intorno a chi la utilizza e solo per alcuni metri
* **LAN (Rete locale)**: la rete si estende all’ interno di un edificio o di un comprensorio



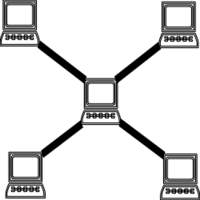
* **WLAN (rete senza fili)**: la rete utilizza la RADIO FREQUENZA (RF), permettendo di muoversi all’ interno dell’area di copertura (in genere è all’incirca un centinaio di metri all’aperto)
* **CAN (Campus area network)**: la rete è interna ad un campus universitario o ad un insieme di edifici vicini che possono essere collegati con cavi propri senza dover utilizzare servizi di operatori di telecomunicazione
* **MAN (rete metropolitana):** la rete si estende all’interno di una città
* **WAN (rete geografica):** la rete si estende oltre i limiti precedenti

1. In base al **CANALE DI TRASMISSIONE** si classificano in:

* **RETI LOCALI:** Vengono realizzate usando un sistema di cablaggio strutturato con cavi UTP a cui può essere affiancata o sostituita una rete senza fili
* **RETI PUBBLICHE - DISTRIBUZIONE:** Sono gestite da operatori di telecomunicazioni che offrono servizi di telecomunicazioni a privati o aziende
* **RETI DI TRASPORTO:** Reti che servono per trasportare le informazioni tra le centrali di un operatore di telecomunicazioni

1. In base alla **TOPOLOGIA** si classificano in:

* **RETI A STELLA**



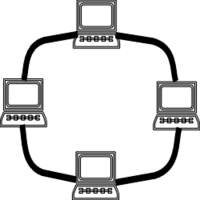
Ogni nodo è connesso ad un sistema centrale con un cavo individuale.

Il sistema centrale può essere un nodo con particolari funzioni (server), un hub o uno switch.

Il cablaggio è molto complesso e c’è bisogno di un gran numero di cavi.

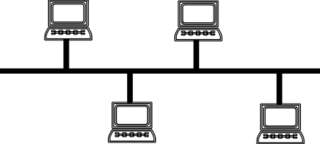
E’ molto utilizzata perché ogni nodo ha un suo collegamento privato per cui se s’interrompe si danneggia solo quello inoltre il nodo centrale può eseguire la diagnostica e permette di monitorare tutti i segnali che vengono smistati in rete.

* **RETI AD ANELLO**

****

Ogni nodo riceve il messaggio dal nodo che lo precede e se non è destinato a lui lo invia al nodo successivo.

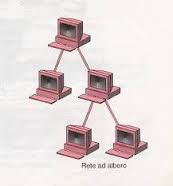
* **RETI A BUS**



Tutti i nodi della rete sono connessi direttamente allo stesso cavo.

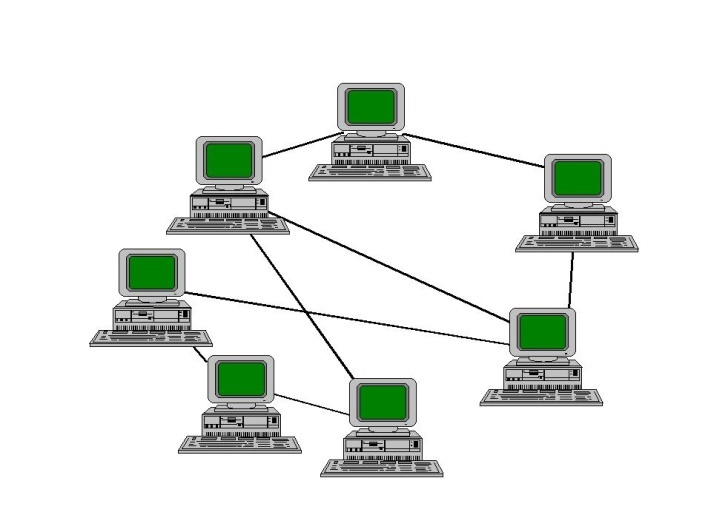
Ogni nodo della rete ha un suo indirizzo unico diverso da tutti gli altri e questo permette al nodo di identificare il messaggio che è indirizzato ad esso. L’interruzione del cavo fa candere l’intera rete.

* **RETI AD ALBERO:**



E’ una generalizzazione della topologia a bus infatti viene realizzata collegando insieme più reti a bus

* **RETE A MAGLIA**



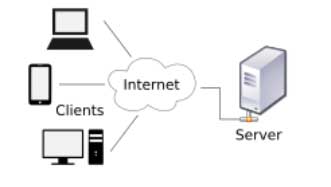
E’ una rete ad anello alla quale vengono aggiunti i collegamenti di ciascun nodo con tutti gli altri nodi quindi non c’è una sequenza ma ciascun nodo è collegato con tutti gli altri. Questa è la rete **A MAGLIA TOTALE**. La rete può essere anche **A MAGLIA PARZIALE**: è sempre una rete ad anello ma dove alcuni nodi sono collegati ad altri

# Architetture di rete

## Client/Server

Il sistema client/server (letteralmente cliente/serviente) è un'architettura di rete in cui un computer “client” o “host” si connette ad un server per l’utilizzo di un certo servizio, ad esempio la condivisione di una risorsa hardware o software con altri client, grazie a questo tipo di architettura.

Questi sistemi sono l'evoluzione dei sistemi basati sulla condivisione semplice delle risorse: la presenza di un server permette ad un certo numero di client di condividerne le risorse, lasciando che sia il server a gestire gli accessi alle risorse per evitare conflitti di utilizzazione tipici dei primi sistemi informatici.



### Client

Il client è di limitata complessità perché si limita ad operare come interfaccia verso il server. In generale nel campo informatico il termine client indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server.

Un computer collegato ad un server tramite una rete, al quale richiede uno o più servizi utilizzando protocolli di rete, è un esempio di client.

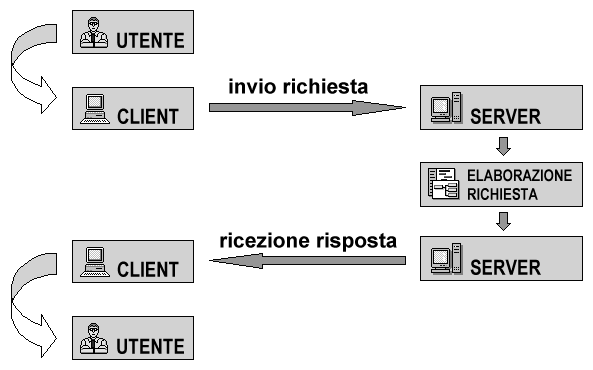
### Server

Il software server, oltre alla gestione logica del sistema, deve implementare tutte le tecniche di gestione degli accessi, allocazione e rilascio delle risorse, condivisione e sicurezza dei dati o delle risorse.

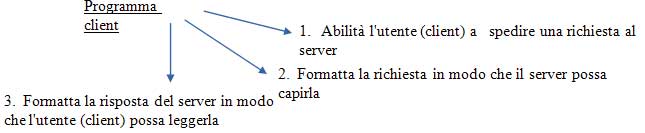
Ad esempio un server di posta elettronica è paragonabile ad un qualunque ufficio postale perché gli utilizzatori per accedere via client alla loro cassetta di posta elettronica devono essere stati autorizzati. In modo analogo un utente deve possedere la chiave della cassetta sita presso un ufficio postale dalla quale vuole prelevare la corrispondenza.

### Come funziona una rete client/server

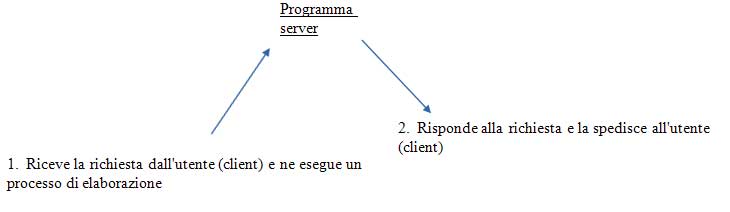
Il funzionamento dell'interazione tra client e server viene illustrato nel seguente schema, dove si a un utente, al quale corrisponde un client, e un server, che come abbiamo detto del paragrafo precedente gestisce ed elabora le richieste del client:



Quando l'utente (client) spedisce una sua richiesta ad un server deve possedere un **software applicativo** (programma client)



**Contemporaneamente** sul server viene eseguito un opportuno programma per gestire le richieste che vengono ricevute dai vari client



### Come comunicano client e server

Al fine che avvenga la comunicazione tra il client e il server, è necessario che entrambe utilizzino un **linguaggio comun**e, che prende il nome di protocollo applicativo. Nelle reti web esistono vari protocolli, in funzione dei tipi di dati che vengono trasferiti sulla rete.

HTTP, *hyper-text-transfert-protocol*, per il trasferimento di ipertesti (o pagine web)

FTP, *file-transfert-protocol*, per iltrasferimento di file (ad esempio utorrent)

SMTP, *simple-mail-transfert-protocol*, per il trasferimento di messaggi di posta elettronica

### Esempi di sistemi client/server:

Web server: per la gestione dell'interazione via web tra server e client

File server: per la condivisione dei file

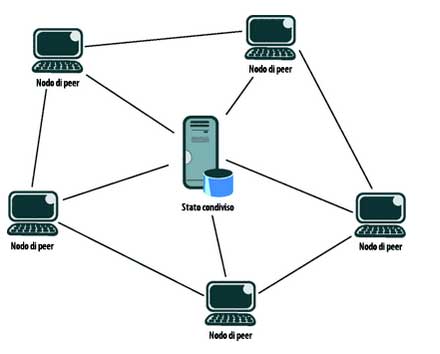
FTP server: per la gestione dell'upload/download dei file

Database server: per la gestione di grandi moli di dati

Groupware: per la gestione d'informazioni riguardanti gruppi di lavoro

Print server: per la condivisione delle stampanti

## Peer to Peer

Il Peer to Peer o semplicemente P2P è un archittettura di rete in cui i nodi, in questo caso peer, hanno ruoli e capacità equivalenti nello scambio di informazioni. In un sistema “peer to peer” i partecipanti condividono le proprie risorse contribuendo attivamente alla fornitura di un servizio.

Questa architettura può essere applicata a qualsiasi tipo di tecnologia di rete e di applicazione.

Il P2P è utilizzato soprattutto nelle aziende perché è il sistema adatto, visto che i computer hanno tutti lo stesso ruolo e c’è un server centrale che contiene i dati.

### Come funziona un’architettura p2p

1. Ogni utente (peer) partecipa alla fornitura di un servizio;
2. In contemporanea si ha un **“servant”** che sarebbe un peer che agisce da client e da server nello stesso momento.
3. Nel sistema p2p la qualita dei servizi che vengono messi a disposizione dipendono dalle risorse che ogni peer mette a disposizione **autonomamente.**

A differenza dei sistemi client/server nei peer to peer gli utenti (peer) accedono alle risorse a seguito di una fase di ricerca. Inoltre **non utilizzano il DNS** e la loro connettività non è **permanente.**

# Internet

Internet è una rete globale, composta da decine di migliaia di reti di computer, che mette a disposizione innumerevoli servizi dedicati principalmente alla comunicazione. Collegati attraverso mezzi di trasmissione ed in grado di dialogare fra di loro tramite convenzioni e regole comuni, chiamate protocolli di rete, ed è accessibile da milioni di persone del mondo intero, si tratta solo di evitare che due dispositivi, connessi come nodo alla rete, abbiano lo stesso indirizzo IP.

## La storia di Internet

Internet nasce 1969 negli Stati Uniti, sotto nome di ARPANET.

ARPANET nasce come risultato di un progetto di un ente governativo per applicazioni militari e scientifiche, capace di creare una rete affinché i ricercatori dei centri di ricerca universitari potessero connettersi a altri computer di altre università e con il vantaggio di poter mandare dei messaggi e poterli indirizzare e reindirizzare su percorsi diversi per raggiungere la destinazione, e la rete avrebbe potuto continuare a funzionare anche se i computer fossero stati distrutto da un attacco militare.

Verso 1980 Internet diventa una infrastruttura di comunicazione consolidata, ma solo negli anni ’90 riesce avere un grosso sviluppo che la fa diventare in pochi anni la rete mondiale, grazie all'apertura alle imprese e alle applicazioni commerciali.

## I servizi Internet

Ci sono molti servizi che Internet ci mette a disposizione come ad esempio molte pagine ad accesso libero, con costante aggiornamento.

Tra i servizi più importanti offerti da Internet ci sono il World Wide Web, la posta elettronica, le comunicazioni vocali basate sul protocollo VoIP e la messaggeria istantanea “IM”.

## Extranet

**Extranet** Rete informatica interna a un'organizzazione ad esempio un azienda, che viene messa a disposizione anche di alcuni soggetti esterni (clienti, fornitori, partner commerciali ecc.) con un accesso regolato da password.

Extranet viene usato maggiormente dall’aziende per: lo scambio di grandi documenti elettronici, distribuzione dei cataloghi, programmi di addestramento per il personale, accesso fornito da altre aziende e per la distribuzione di informazioni di interesse comune con aziende partner.

## IP

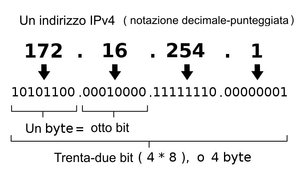
Un **indirizzo IP** (dall'inglese **Internet Protocol address**) - in [informatica](https://it.wikipedia.org/wiki/Informatica) e nelle [telecomunicazioni](https://it.wikipedia.org/wiki/Telecomunicazioni) - è un'etichetta numerica che identifica univocamente un dispositivo, detto *[host](https://it.wikipedia.org/wiki/Host" \o "Host),* collegato a una [rete informatica](https://it.wikipedia.org/wiki/Rete_informatica) che utilizza l'[Internet Protocol](https://it.wikipedia.org/wiki/Internet_Protocol) come [protocollo di rete](https://it.wikipedia.org/wiki/Protocollo_di_rete).

Serve essenzialmente a due funzioni: identificare un dispositivo sulla rete e di conseguenza fornire il percorso per essere raggiunto da un altro [terminale](https://it.wikipedia.org/wiki/Terminale_(informatica)) o [dispositivo di rete](https://it.wikipedia.org/wiki/Dispositivi_di_rete) in una comunicazione dati a [pacchetto](https://it.wikipedia.org/wiki/Pacchetto_(reti)).

### IPv4

L'indirizzo IPv4 è costituito da 32 [bit](https://it.wikipedia.org/wiki/Bit) (4 [byte](https://it.wikipedia.org/wiki/Byte)) suddiviso in 4 gruppi da 8 bit (1 byte), separati ciascuno da un punto (notazione *dotted*) (es. 11001001.00100100.10101111.00001111).   
Ciascuno di questi 4 byte è poi convertito in formato [decimale](https://it.wikipedia.org/wiki/Sistema_numerico_decimale) di più facile identificazione (quindi ogni numero varia tra 0 e 255 essendo 2^8=256).

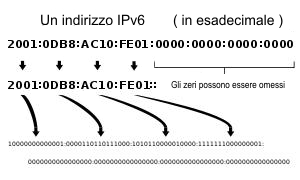
Un **esempio** di indirizzo IPv4 è 195.24.65.215.



### IPv6

L'indirizzo IPv6 è costituito da 128 bit (16 [byte](https://it.wikipedia.org/wiki/Byte)), viene descritto da 8 gruppi di 4 cifre [esadecimali](https://it.wikipedia.org/wiki/Sistema_numerico_esadecimale" \o "Sistema numerico esadecimale) che rappresentano 2 [byte](https://it.wikipedia.org/wiki/Byte" \o "Byte)ciascuno (quindi ogni numero varia tra 0 e 65535) separati dal simbolo "due punti".

Un **esempio** di indirizzo IPv6 è 2001:0DB8:0000:0000:0000:0000:0000:0001, che può essere abbreviato in 2001:DB8::1 (i due punti doppi rappresentano la parte dell'indirizzo che è composta di soli zeri consecutivi. Si può usare una sola volta, per cui se un indirizzo ha due parti composte di zeri la più breve andrà scritta per esteso).



## URL

***URL*** è l’acronimo di Uniform Resource Locator che significa localizzatore universale di risorse, ed è una sequenza di caratteri che identifica l’ indirizzo di una risorsa in Internet. E’ l’elemento che ci permette di trovare un sito web, cioè l’indirizzo che noi digitiamo nel browser quando cerchiamo una pagina o un file.

Analizziamo le parti che compongono una URL, come ad esempio [**http://www.giardini.it/index.htm**](http://www.giardini.it/index.htm)**:**

La prima parte indica con una parola chiave il tipo di server a cui si punta: può trattarsi di un server http,di un server ftp, di un server telnet, eccetera… In questo caso la parola chiave “**http**” indica che ci si riferisce ad un server web.

La seconda parte indica il nome simbolico dell’ host su cui si trova il file. L’host è [**www.giardini.it**](http://www.giardini.it)

La terza parte indica nome e posizione del singolo documento o file a cui ci si riferisce. (**index.htm**) Tra la prima e la seconda parte vanno inseriti i caratteri “ **: / /** “

La barra **/** (**slash**) è un separatore che consente di costruire il percorso per arrivare al sito e agli archivi registrati sul disco del server.

## I nomi di dominio

Un dominio è un nome alfabetico che identifica un server Internet al quale è abbinato un indirizzi IP numerico utilizzato per il trasferimento dei dati, la cui traduzione è affidata al **DNS** (**Domain Name System**)

Il dominio di I° livello è la parte a destra dell’ URL e identifica la nazione del dominio( .it italia, .uk Regno Unito, etc… )o la destinazione d’uso (.com commerciale, .org organizzazione, o.edu educativo, etc…).

I domini di secondo livello sono composti da un’ estensione (il dominio di primo livello e da un nome di riconoscimento. La struttura di un dominio di secondo livello è :” nomedominio.estensione”

I domini di terzo livello, che prendono anche il nome di sottodomini, sono dipendenti da un dominio di secondo livello. I domini di terzo livello hanno una struttura così composta : ”nomesottodominio.nomedominio.estensione”

## Il www

Il WWW è l’acronimo di World Wide Web abbreviata con Web ed è una tecnologia prodotta alla fine degli anni ’80 presso il CERN (Centro Europeo per le Ricerche Nucleari) di Ginevra, con lo scopo originario di fornire uno strumento di lavoro per gli ambienti di ricerca di tutto il mondo.

Esso è uno spazio di Internet destinato alla pubblicazione di contenuti multimediali (testi,immagini,video,etc…).

Tale spazio elettronico e tali servizi sono resi disponibili attraverso particolari computer chiamati server Web.

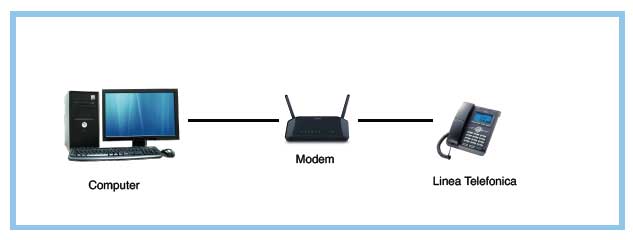
I contenuti del Web sono organizzati nei siti Web a loro volta strutturati in pagine Web le quali si presentano come composizioni di testo visualizzate sullo schermo del computer dal browser Web.

Le pagine Web sono collegate fra loro attraverso i link.( salto da un documento all’altro sul web, essi possono essere attivati grazie a parole sottolineate con colori diversi, immagini, icone etc…).

## Utilizzare la rete

### Il Modem

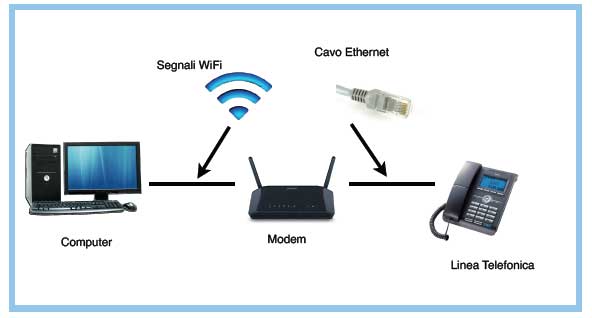
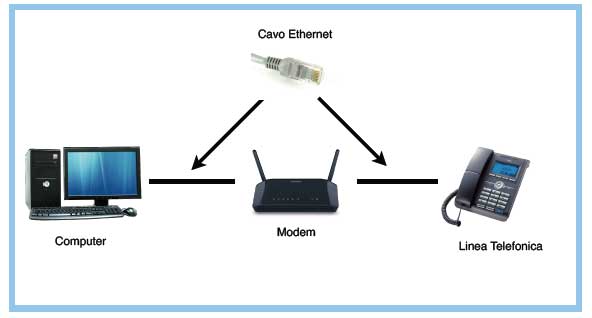
Il modem è un dispositivo che attraverso una linea telefonica, la quale usa un linguaggio analogico, riceve e invia dei dati. La sua funzione tipica infatti è di convertire i segnali di tipo analogico della linea telefonica in segnali di tipo digitale per potere connettersi alla rete Internet. Una caratteristica importante del modem è la sua velocità di trasferimento dei dati. Essa viene espressa in bps, cioè in bit per secondo, e più è alta la sua velocità, più sono veloci le comunicazioni. La velocità di trasferimento è importante perché diminuisce sia i tempi di comunicazione che i costi telefonici.



Il modem è un dispositivo che permette al computer, che usa segnali digitali, di interfacciare con la rete telefonica, che usa segnali di tipo analogico.

#### Come si collega alla rete?

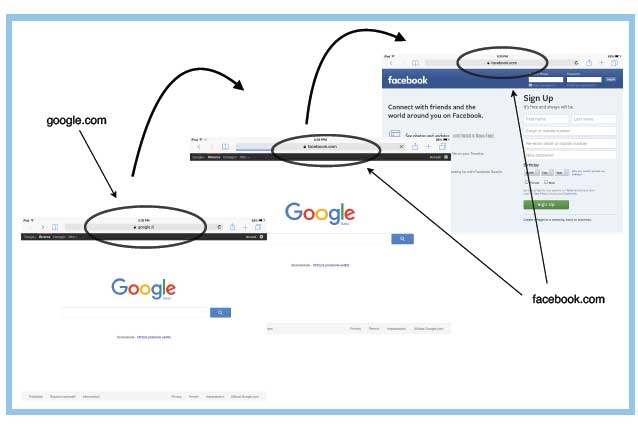
Il modem si connette principalmente in due modi: si collega con il cavo ethernet, mettendo in connessione il modem da un lato con il computer dall'altro lato, o si collega senza cavi, cioè il computer si connette utilizzando i segnali wifi, usando un modem wireless che usa segnali radio.



### I browser

Il browser è un programma che visualizza i testi ipertestuali. Esso interpreta i dati inseriti nella casella dell'indirizzo, cioè l'URL (Uniform Resource Locator), e vengono scritti in codice HTML, che è il linguaggio di formattazione degli ipertesti, per potere visualizzare le pagine Web. Il browser installato sul computer dell'utente ha il compito di interagire con i browser dei Web servers sparsi nel mondo, i quali contengono le informazioni necessarie per potere caricare una pagina Web. Una volta inserito l'URL nella casella dell'indirizzo, i dati vengono scritti in HTML. Il browser identifica quali Web servers hanno le informazioni richieste e quando trovati li invia la richieste delle informazioni. I Web servers rispondono alle richieste mandandogli le informazioni, le quali vengono gestite dal browser e visualizzate graficamente. A man mano che arrivano le informazioni, la pagina viene costruita.

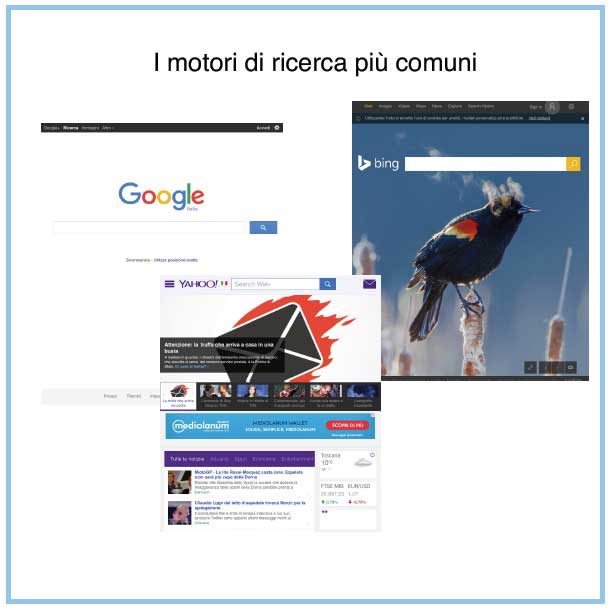
Il browser è un programma che visualizza i testi ipertestuali. Ha il compito di trovare le informazioni richieste e di ottenerle per farle visualizzare all' utente.





### I motori di ricerca

Il motore di ricerca è un sito Internet che aiuta gli utenti a trovare i siti di loro interesse. Quando un utente inserisce le parole chiave, cioè le parole necessarie per trovare le pagine Web che si riferiscono ad un determinato argomento, e clicca il bottone Cerca per avviare la ricerca, il motore di ricerca cataloga le pagine Web presenti in Internet e cerca all'interno di questi cataloghi ciò che è stato richiesto. Una volta trovate le pagine Web pertinenti all'argomento, il motore di ricerca presenta all'utente un elenco di siti Internet che gli possono andare bene. Il motore d ricerca tuttavia, non trova solo siti Internet, ma anche immagini, video, mappe, libri e news collegati ad un determinato argomento.



Il motore di ricerca è un sito Internet che aiuta gli utenti a trovare i siti a loro interessanti.

Spesso il browser e il motore di ricerca vengono confusi e si crede che abbiano le stesse funzioni. La maggior differenza tra le due è che il browser è un programma, cioè l'utente lo scarica sul computer, mentre il motore di ricerca è un sito Internet che l'utente cerca tramite il browser, quindi per potere usare il motore di ricerca bisogna utilizzare un browser. Il compito del browser è di potere visualizzare i testi ipertestuali, mentre quello del motore di ricerca è di aiutare gli utenti a trovare i siti di loro interesse.

# Il dns

Il Dns (Domain Name System) è un registro universale dove si associa un nome di un indirizzo Internet con il suo indirizzo IP.

Tramite un sistema di replica, le modifiche fatte su un determinato segmento di rete da parte degli amministratori incaricati vengono “copiate” e distribuite pubblicamente nella totalità dei computer collegati.

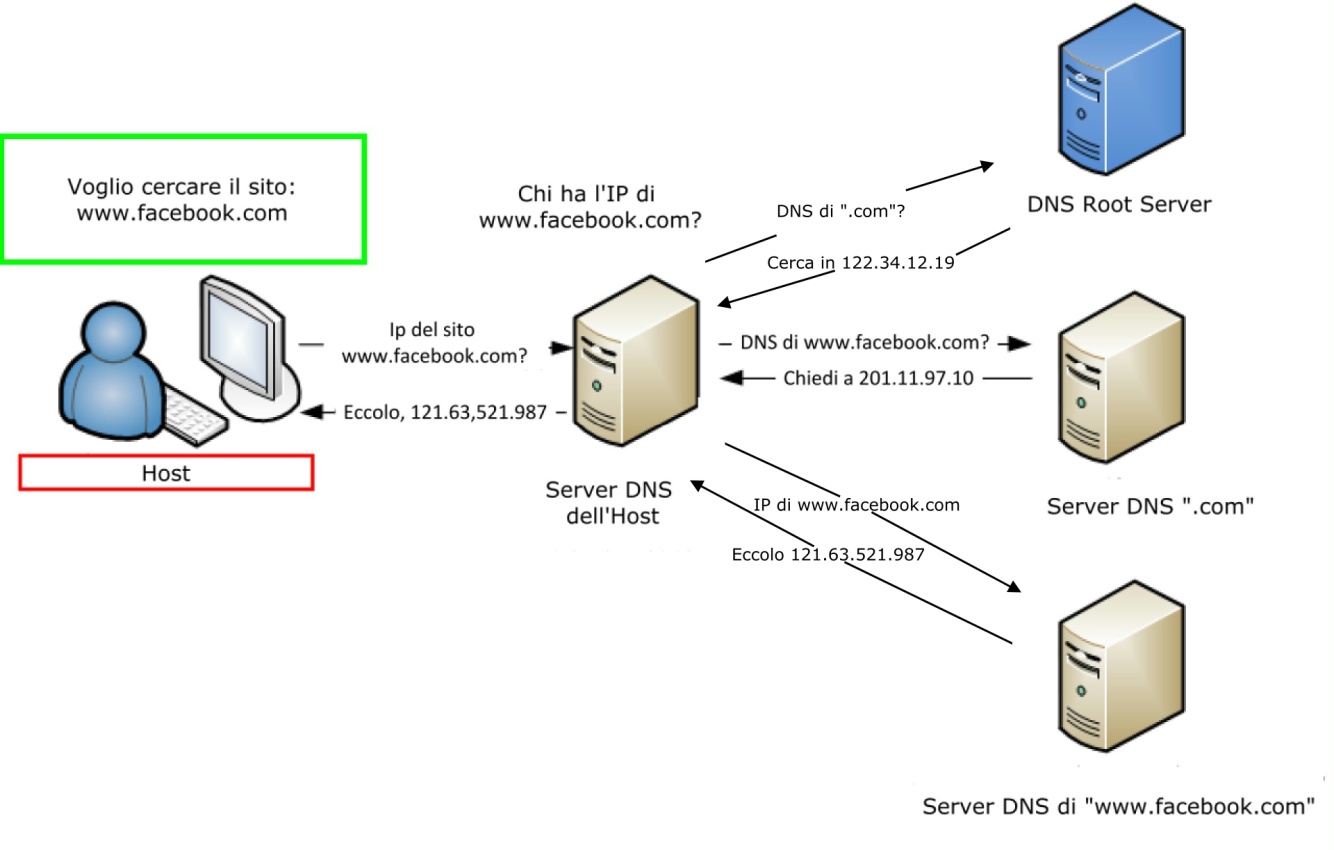
I programmi che gestiscono tuttora questi segmenti di rete sono denominati “Name Server” mentre sono “Resolver” i programmi che interrogano quest’ultimi per la risoluzione di un nome di dominio in rete.



Il DNS è quello che si occupa proprio del lavoro di transcodifica. Esso deve contenere una tabella di corrispondenza tra nome di dominio e “IP address” e deve essere capace di rispondere alle richieste di transcodifica che gli arrivano.

## Com’è fatto

Il DNS è strutturato ad albero. La radice dell’albero è il “dominio vuoto”; vengono poi i domini di livello superiore e gli altri sotto domini:

Ogni nodo ha un'etichetta di lunghezza massima 63 caratteri. La radice e' un nodo speciale senza etichetta e non vi è differenza nelle etichette tra maiuscole e minuscole. Il nome di dominio è la successione di etichette a partire dal nodo verso la radice, usando il carattere punto "." come separatore di etichetta. Ogni nodo dell'albero DNS deve avere un nome di dominio univoco.

## Come lavora

Quando un Host ha necessità di comunicare con un altro Host, chiede al DNS di effettuare la risoluzione di tale nome. Quando riceve una richiesta il DNS effettua una ricerca all'interno del suo database al fine di trovare l'indirizzo IP corrispondente al nome Host richiesto. Se il server interrogato possiede l'informazione richiesta la ricerca termina con l'invio dell'indirizzo IP al richiedente. Se la ricerca ha esito negativo il server effettua una richiesta detta ricorsiva al suo server DNS. Ogni server DNS infatti ha a sua volta un server DNS a cui richiedere le informazioni mancanti.

# Il protocollo http

## L’ipertesto

Per descrivere meglio un ipertesto voglio confrontarlo con un libro, un testo editoriale. Quando prendo un libro sono obbligata ad una lettura sequenziale, lineare dalla prima all'ultima pagina, obbligata a seguire ciò  che l'autore ha scritto secondo la sua logica. Diversamente l'ipertesto è capace di lasciarmi un  libero collegamento fra le informazioni poste in diversi punti dello stesso documento e, così, mi permette una consultazione personalizzata, guidata soltanto dalla logica del mio pensiero. Nell'ipertesto si nota la presenza di nodi, parole chiave, che connettono tra loro vari elementi sia di testo che multimediali ( un immagine, una traccia sonora, un filmato) con un semplice clik del mouse. Per navigare in queste interconnessioni ho a mia disposizione una mappa, cioè l'indice generale degli argomenti trattati, che si trova sempre nella prima pagina del documento.

Per navigare all'interno di questa rete ogni contenuto è composto da bottoni di tipo testuale o iconico. Attivando uno di questi bottoni passerò all'informazione che cerco o accederò ad un sottoindice, strutturato più o meno come il generale.

Una altra caratteristica dell'ipertesto, oltre la sua non linearità, è che i testi in esso contenuti sono testi aperti, espandibili. Mentre un libro non cambia nel tempo, un ipertesto al contrario è un libro mai compiuto, in quanto lo posso integrare, posso aggiungere altri elementi, cambiare la sua struttura o la sua veste grafica.

L'ipertesto è anche un valido aiuto nel lavoro interdisciplinare, perché costringe alla collaborazione. Infatti, per creare un ipertesto è necessario l'aiuto di più persone che interagiscono tra loro e forniscono le proprie competenze specifiche.

Infine l'ipertesto è incentrato sul lettore, perché è lui che decide cosa vuole leggere, come vuole usare l'informazione, e questo lo motiva e lo invoglia all'apprendimento.

Un esempio di ipertesto è un **sito web**.

L'**http**, ovvero Hyper Text Transfer Protocol, protocollo di trasferimento di un ipertesto, è usato come principale sistema per la trasmissione di informazioni sul web.

L'http funziona su un meccanismo richiesta/risposta ( client/server) : il client esegue una richiesta e il server restituisce la risposta. Nell'uso comune il client corrisponde al browser e il server al sito web.

L'http è usato per trasmettere risorse non solo files.

Un esempio di http è : <http://www.google.it/>

# La sicurezza in Internet

## Informazioni sensibili, quali sono, perché proteggersi

Nell’ambito della sicurezza informatica i rischi che corre un utente, soprattutto quando il suo computer è connesso a Internet, sono essenzialmente di due tipi: la modifica ed il furto dei dati.

Questi dati sono chiamati dati sensibili e secondo il Codice sulla protezione dei dati personali, sono considerati i dati personali idonei a rivelare: il nome e il cognome, il numero della carta di credito, l'origine razziale ed etnica,le convinzioni religiose,filosofiche o di altro genere,le opinioni politiche,l'adesione a partiti, sindacati,associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,lo stato di salute e la vita sessuale.

Spesso i mezzi d’informazione utilizzano il termine hacker come sinonimo di “criminale informatico”, in realtà hackering indica l’insieme dei metodi, delle tecniche e delle operazioni informatiche che un hacker utilizza per accedere a un sistema hardware o software e per esplorarlo e modificarlo, adattandolo alle proprie esigenze.

Il termine inglese cracker indica colui che si ingegna per eludere blocchi imposti da qualsiasi software al fine di trarne guadagno. Il cracking può essere usato per diversi scopi secondari, ad esempio poter accedere come root nel sistema desiderato o dopo rimuovere le limitazioni di un qualsiasi programma.

I cracker possono essere spinti da varie motivazioni, dal guadagno economico (tipicamente coinvolti in operazioni di spionaggio industriale o in frodi) all'approvazione all'interno di un gruppo di cracker .

Il termine cracker viene spesso confuso con quello di hacker, il cui significato è tuttavia notevolmente diverso. Alcune tecniche sono simili, ma hacker è colui che sfrutta le proprie capacità per esplorare, divertirsi, apprendere, senza creare reali danni. Al contrario, cracker è colui che sfrutta le proprie capacità (o in certi casi quelle degli altri) al fine di distruggere, ingannare e guadagnare.

## Vari tipi di attacchi

Esistono diversi tipi di attacchi in rete, che vengono suddivisi in passivi eattivi.

Gli attacchi passivi servono a ottenere informazioni sul vostro computer e stimare le modalità possibili dell'intrusione remota e si dividono in:

* Sniffing: E' un modo di intercettazione dei dati trasferiti;
* Scansione della porta e della vulnerabilità del sistema operativo: In genere la scansione della porta è una tecnica utilizzata per raccogliere informazioni sui processi del sistema operativo di un computer remoto attivi e in ascolto dei dati e dei comandi tramite le porte associate. La scansione della vulnerabilità del sistema operativo viene finalizzata a definire se un processo con la sua porta aperta è soggetto all'attacco.

Gli attacchi attivi sono finalizzati alla penetrazione remota nel vostro computer, al furto dei dati o all'esecuzione di attacchi allo scopo della perturbazione difunzionamento del sistema operativo e si dividono in:

* IP Spoofing: E' un tipo di attacco informatico che consiste nel falsificare l'indirizzo IP del computer da cui viene eseguito l'attacco;
* Denial of Service (DoS): E' un attacco contro un computer particolare per esaurire le sue risorse e rende il computer inaccessibile agli altri computer della rete.

## Gli antivirus

Gli antivirus sono software per la gestione della sicurezza informatica; servono infatti a prevenire, rilevare e spesso eliminare software dannosi, i cosiddetti malware, categoria nella quale rientrano i virus informatici, i dialer(un programma per computer di pochi kilobyte che crea una connessione ad Internet, a un'altra rete di calcolatori o semplicemente a un altro computer tramite la comune linea telefonica o un collegamento), gli spyware(un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso), i trojan(un tipo di [malware](https://it.wikipedia.org/wiki/Malware), le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto), i worm (è una particolare categoria di [malware](https://it.wikipedia.org/wiki/Malware) in grado di autoreplicarsi. È simile ad un virus ma, a differenza di questo, non necessita di legarsi ad altri eseguibili per diffondersi ma si diffonde spedendosi direttamente agli altri computer, ad esempio tramite e-mail o una rete di computer), i rootkit(un programma software prodotto per avere il controllo sul sistema senza bisogno di autorizzazione da parte di un utente o di un amministratore), ecc.

## La crittografia

Se si vuole garantire la riservatezza dei messaggi, è possibile cifrarli con un codice segreto usando la tecnica della crittografia.

Per crittografia si intende quella tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario.

Ogni sistema di crittografia ha due parti essenziali: un algoritmo (per codificare e decodificare) e una "chiave", la quale consiste di informazioni che, combinate con il testo passato attraverso l'algoritmo, darà poi il testo codificato. In ogni moderno sistema di crittografia si assume che l'algoritmo sia conosciuto dai potenziali "nemici", quindi la sicurezza di un sistema risiede solo ed esclusivamente nella segretezza della chiave.

## Il protocollo https

I siti che sono protetti dalla crittografia si riconoscono dal fatto che il loro indirizzo inizia con https:// (HyperText Transfer ProtocolSecure) e sulla barra degli indirizzi del browser compare il simbolo di un lucchetto.

Grazie all’HTTPS viene creato un canale di comunicazione criptato tra il client e il server attraverso uno 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.

## I certificati

Per garantire l’autenticità di un sito o per verificare l’identità di un utente esiste anche il certificato digitale, uno speciale attestato emesso da un’autorità di certificazione riconosciuta che conferma l’associazione tra una chiave pubblica e un soggetto che dichiara tale chiave come propria.

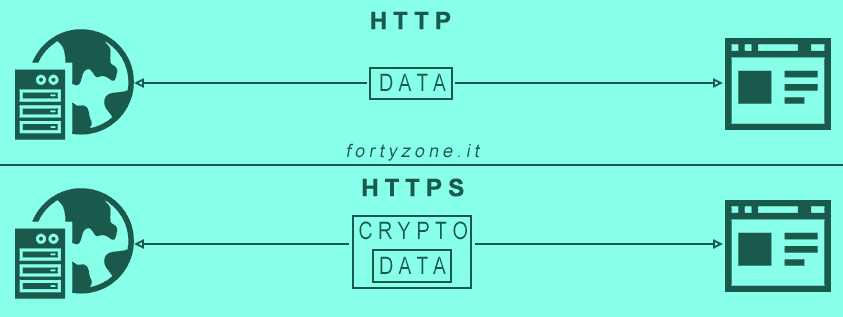
Un certificato è composto da:

* una chiave pubblica;
* dei dati identificativi, che possono riferirsi ad una persona, un computer o un'organizzazione;
* un periodo di validità;
* l'URL della lista dei certificati revocati.

Il tutto è firmato da una terza parte fidata.

## Differenza tra http e https

HTTP e HTTPS sono due varianti dello stesso protocollo utilizzato per il trasferimento delle pagine web in internet.

Nell'HTTP tutte le comunicazioni avvengonosenz'alcun genere di sicurezza, nell'HTTPS viene creato un canale di comunicazione criptato attraverso lo scambio di certificati in modo da garantire l'identità delle parti e la riservatezza dei dati. Mentre il primo é quello di utilizzo più comune, l'HTTPS viene di norma utilizzato in tutte quelle situazioni in cui é richiesto un certo grado di sicurezza come transazioni elettroniche, acquisti online e lettura di messaggi di posta elettronica.

Differenze tra HTTP e HTTPS

# Casi d’uso

## Richiesta di un video al server YouTube

Quando l’utente accede a You Tube, tramite il suo computer locale, inserisce inizialmente nella barra degli indirizzi della home page di un motore di ricerca (come ad esempio Google) l’**URL** di You Tube cioè: [**https://www.youtube.com**](https://www.youtube.com).

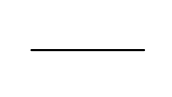
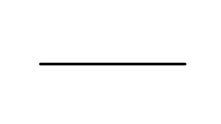
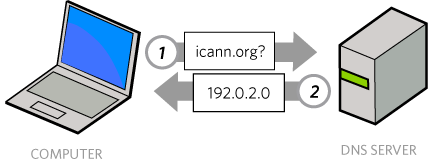
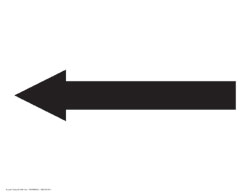
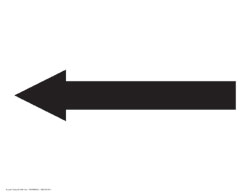
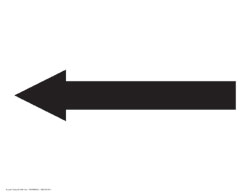
* **HTTPS** indica il **protocollo di trasferimento di pagine web sicuro**, cioè fornisce un certificato che dimostra l’autenticità della pagina web (hyper text transfert protocol secure).
* **www.youtube.com** è detto **dominio** che individua l’azienda o l’organizzazione a cui il computer è collegato. In questo caso il **dominio di alto livello** (top-level domain) **.com** sta per organizzazione commerciale.

Quando poi l’utente cerca un video su You Tube, accanto al dominio verrà indicata la **risorsa**, per esempio: [https://www.youtube.com**/videoautomobili**](https://www.youtube.com/videoautomobili).

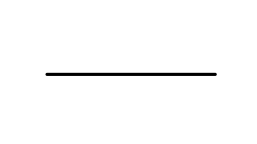
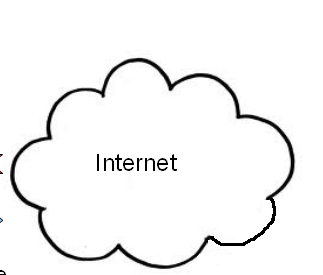
Per prima cosa, l’host locale (dell’utente) contatta il **DNS** (domain name server) per conoscere l’indirizzo IP corrispondente al dominio [www.youtube.com](http://www.youtube.com). Il DNS o conosce direttamente l’IP desiderato, o inoltra la richiesta ad altri DNS. Alla fine ritornerà all’utente l’IP richiesto (oppure un messaggio di errore se l’URL non corrisponde a nessun IP, come ad esempio nel caso di URL digitate male).

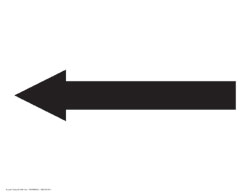
A questo punto l’host locale può contattare il server Youtube, specificando la risorsa desiderata, in questo caso videoautomobili, e il proprio indirizzo IP, in modo tale che il server sappia a quale indirizzo inviare la risorsa.



    **Ritorno ris.**

**Ritorno risorsa**

****  



**Ritorno risorsa**

## DNS:

Il **DNS** (domain name server) è un server distribuito che fornisce un indirizzo **IP** a partire dall’indirizzo URL (www…) ed ha una tabella con tutti i nomi a dominio.

L’architettura del DNS è ad **albero** dove vi è un **server principale** che comanda tutti gli altri server, fino ad arrivare alle **foglie**, cioè tutti gli host collegati ad esso.

