

LABORATORIO DI INFORMATICA

Lezione 31/10/2019


ARPANET

Una rete di computer costituita nel settembre del 1969 negli USA da ARPA (*Advanced Research Projects Agency*)

ARPA fu creata nel 1958 dal Dipartimento della Difesa degli Stati Uniti per dare modo di ampliare e sviluppare la ricerca, soprattutto all'indomani del sorpasso tecnologico dell'Unione Sovietica, che lanciò il primo satellite (Sputnik) nel 1957, conquistando i cieli americani: quando la NASA le subentrò nella gestione dei programmi spaziali l'ARPA assunse il controllo di tutte le ricerche scientifiche a lungo termine in campo militare.

Verso il 1965 l'ARPA cominciò ad avere dei seri problemi di gestione: aveva diversi computer sparsi in varie sedi (tutti molto costosi) che non potevano parlarsi:

Nell'ottobre 1969 Leonard Kleinrock, titolare del laboratorio dell'Università della California di Los Angeles, fu incaricato di creare il primo collegamento telefonico da computer a computer fra la UCLA e lo Stanford Research Institute, che furono così i primi due nodi di Internet.



alle 22:30 del 29 ottobre 1969 il dottorando in informatica Charles Kline prova a inviare un messaggio da un computer dell'Università della California di Los Angeles (UCLA) a uno dello Stanford Research Institute, a oltre 500 km di distanza. Nelle intenzioni di Kline il messaggio doveva essere la parola "LOGIN", ma furono trasmesse solamente le prime due lettere prima che il sistema andasse in crash.

Inizialmente, ARPANET comprendeva soltanto due nodi, il computer di UCLA e quello di Stanford. Più tardi, quell'anno, ne furono aggiunti altri due, nell'Università della California a Santa Barbara, e in quella dello Utah, a Salt Lake City. Nel 1973, ARPANET diventò internazionale, connettendo via satellite due centri, il Norwegian Seismic Array di Kjeller, vicino a Oslo, e l'University College London.



Una comunicazione rapida e condivisa richiedeva un linguaggio comune. Le regole di questa nuova lingua - **protocolli di comunicazione** che definivano le norme di interazione da osservare all'interno della rete - furono formulate, nel 1974, dagli informatici Vint Cerf e Bob Kahn, autori del Transmission Control Protocol (TCP) e dell'Internet Protocol (IP). Questi insiemi di regole definivano, per esempio, il formato standard che dovevano avere i pacchetti di dati, oltre a un sistema uniforme di "indirizzi", in modo che i network potessero trovarsi e comunicare (quelli che oggi conosciamo come indirizzi IP).

ARPANET adottò questi protocolli il 1° gennaio 1983, segnando di fatto la nascita di Internet.

Nei laboratori di ricerca del Cern di Ginevra, nel marzo 1989, Tim Berners-Lee presenta la bozza di un progetto per la condivisione di documenti. Il progetto è giudicato dal suo supervisore "vago ma interessante". Berners-Lee ci lavora e nel 1991 presenta al pubblico [la prima pagina web](#).



I pc connessi alla Rete iniziano ad aumentare esponenzialmente, e nel 1994 raggiungono quota un milione. Di conseguenza aumentano i siti web e uno dei principali problemi è districarsi nella grande offerta e riuscire a individuare il sito desiderato



Motori di ricerca



1995 Yhahoo!

1998 Google

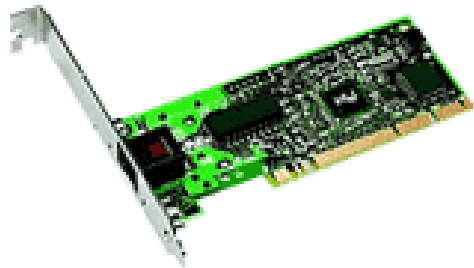


Il modello generale di un sistema di comunicazione è costituito dai seguenti componenti:

- un chiamante, o sorgente, che costituisce il punto di generazione di un messaggio (per esempio una persona che vuole inviare un messaggio telefonico a un'altra persona).
- un trasmettitore che trasforma il messaggio adattandolo al mezzo di comunicazione utilizzato (per esempio il telefono).
- un canale di trasmissione che garantisce il trasferimento del messaggio (per esempio la rete telefonica).
- un ricevitore che trasforma il messaggio adattandolo al ricevente, o destinatario (per esempio la persona che riceve il messaggio telefonico).



- Per poter collegare più computer tra loro, serve anzitutto una **scheda di rete** che viene installata all'interno del computer.
 - Tale scheda funziona da vero e proprio ricetrasmittitore:
 - in **trasmissione trasforma le** sequenze binarie di zeri ed uno, in segnali elettrici che vengono inviati lungo la rete;
 - in **ricezione trasforma i segnali** elettrici della rete in sequenze binarie intelligibili per il computer.
- Oltre alla scheda di rete, è poi presente il **cavo di connessione**.
- La scheda di rete ed il cavo di connessione costituiscono l'**hardware di rete**.



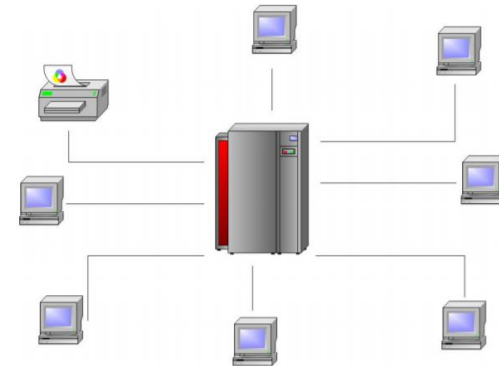
A differenza del doppino telefonico composto solo da due cavi, all'interno sono presenti 8 cavi colorati



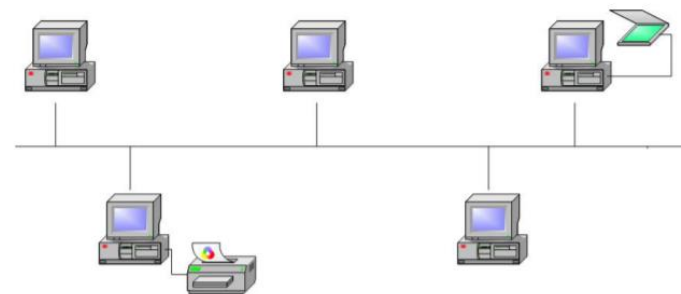


In una rete di comunicazione vengono trasferite informazioni da un nodo all'altro

Prima dell'avvento del PC, l'architettura dominante era quella costituita da un computer centrale – l'unico con capacità elaborativa – a cui ci si collegava con terminali



Più personal computer collegati tra di loro in reti, dotati di capacità elaborativa autonoma, che condividono tra loro risorse e forniscono servizi



Una rete informatica è un insieme di computer connessi tra di loro per mezzo di cavi o antenne che colloquiano scambiandosi dati e condividendo risorse attraverso una serie di protocolli e servizi.



Gli scopi principali di una rete

sono:

La condivisione di risorse

Servizi di comunicazione



In informatica, il **client** indica una determinata componente hardware o software che accede alle risorse o ai servizi erogati da un'altra componente, detta **server**. Ad esempio, un computer che, tramite una rete informatica, richiede uno o più servizi ad un server mediante uno o più protocolli di rete, è un *client hardware*. Un programma di posta elettronica, tipo Outlook, che interroga un server di posta elettronica è invece un esempio di *client software* (più precisamente, è un client di posta elettronica).

In poche parole, un client può essere considerato sia un dispositivo hardware, come un computer, uno smartphone o un tablet, sia un classico software, come un browser o un programma di posta elettronica.

In informatica, il server indica una componente hardware o software che fornisce i dati richiesti da una o più altre componenti, dette client.

In altre parole, un server non è altro che un computer e/o un programma in grado di rispondere alle richieste fatte da altri computer e/o da altri programmi. Ad esempio, un server di posta elettronica potrebbe essere visto come una sorta di ufficio postale dove i vari utenti, ossia i client, si recano per svolgere le proprie mansioni.

A differenza di un client, un server deve però essere capace di gestire tutti gli accessi, le risorse e i dati che gli vengono chiesti, per cui deve avere sia la potenza necessaria per assolvere a questi compiti, sia essere sempre in funzione, in modo tale da poter soddisfare di volta in volta le varie richieste dei client.



In una rete client/server dei computer, detti **server**, mettono a disposizione risorse e offrono servizi ad altri computer, detti **client**, mentre nelle reti **peer to peer**, i computer svolgono contemporaneamente sia il ruolo di client che di server. Quando la distinzione nella prima tipologia di rete è netta, ovvero il client non può diventare server e viceversa, si parla di **server dedicato**. In reti di grandi dimensioni, come server vengono utilizzate macchine dall'alto potere computazionale, in grado di offrire numerosi servizi contemporaneamente. Si usa spesso il termine **host**, per definire server dalle grandi prestazioni.

Nel modello **client/server**, la comunicazione avviene attraverso lo scambio di messaggi. Un **messaggio** altro non è che un insieme di dati che va a costituire un'entità completa. I messaggi solitamente sono suddivisi in **pacchetti**, di una certa dimensione massima.



- Le reti di comunicazione (Network) possono essere catalogate in base alle seguenti caratteristiche:

1) Tipologie di Reti *f*

LAN (Local Area Network) si definisce così una rete limitata ad un zona circoscritta come potrebbe essere una stanza di un ufficio fino ad arrivare alle dimensioni di un campus (1m – 2km). *f*

MAN (Metropolitan Area Network) si definisce così un gruppo di dispositivi o di LAN collegate nell'ambito di una vasta area geografica, come potrebbe essere una città, mediante linea telefonica o altro tipo di cablaggio (ad es. linea dedicata, fibre ottiche, collegamento wireless, ecc..) (2km - 10Km). *f*

WAN (Wide Area Network) si definisce così l'insieme dei dispositivi che permettono la connessione delle reti locali e delle reti metropolitane connesse al livello nazionale, continentale, mondiale (10km – 10.000km).

2) Topologia di Reti:

È la disposizione geometrica del sistema informatico (Bus, Stella, anello)

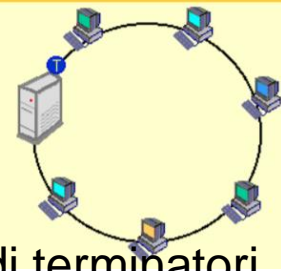


RETE A STELLA

- I computer sono connessi ad un componente centrale chiamato Hub.
- I dati sono inviati dal computer trasmittente attraverso l'Hub a tutti i computer della rete.
- In caso di interruzione di uno dei cavi di connessione di un computer all'Hub, solo quel computer verrà isolato dalla rete.
- In caso di mancato funzionamento dell'Hub tutte le attività di rete saranno interrotte.
- tra i vantaggi dell'hub ci sono l'espandibilità (basta collegare un altro Hub all'Hub iniziale), controllo centralizzato del traffico sulla rete in base a led luminosi che permettono la diagnostica di ogni ramo della rete.



RETE AD ANELLO



• I computer sono connessi tramite un unico cavo circolare privo di terminatori. I segnali sono inviati in senso orario lungo il circuito chiuso passando attraverso ciascun computer che funge da ripetitore e ritrasmette il segnale potenziato al computer successivo: si tratta quindi di una tipologia attiva, a differenza di quella a bus.

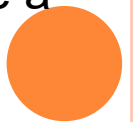
Uno dei metodi usati per la trasmissione dei dati lungo l'anello è detto Token Passing, e si parla infatti di reti Token Ring.

Il token (gettone) viene trasferito da un computer al successivo finché non raggiunge quello su cui sono disponibili dati da trasmettere. Il token viene modificato dal computer trasmittente che aggiunge al dato l'indirizzo del destinatario e quello del mittente e lo rinvia lungo l'anello.

I dati passano attraverso ciascun computer finché raggiungono quello il cui indirizzo corrisponde a quello indicato sui dati. Questo computer restituisce un messaggio di conferma al computer trasmittente il quale crea un nuovo token e lo immette nella rete.

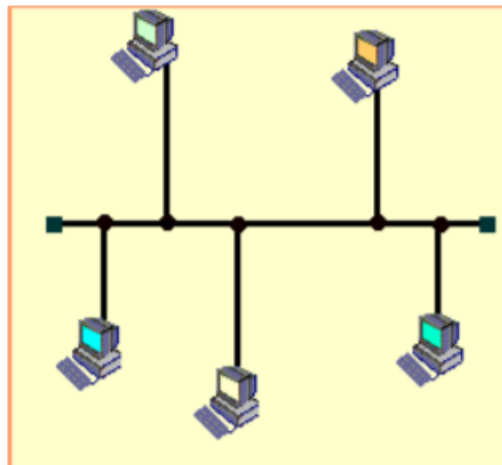
Nelle reti Token Ring, a differenza di altre, un computer malfunzionante viene automaticamente escluso dall'anello consentendo agli altri di continuare a funzionare regolarmente in rete.

In altri tipi di reti ad anello, un computer che non funziona può provocare la caduta di tutta la rete.



Topologia a BUS

- Consiste in un singolo cavo (dorsale) che connette in modo lineare tutti i computer.
- I dati sono inviati a tutti i computer e vengono accettati solo dal computer il cui indirizzo è contenuto nel segnale di origine.
- Un solo computer alla volta può inviare i dati, quindi maggiore è il numero dei computer connessi, più saranno lunghi i tempi di trasmissione.
- A ciascuna estremità del cavo viene applicato un componente chiamato terminatore che assorbe i dati liberi rendendo disponibile il cavo.
- Se un computer si disconnette o se uno dei capi è privo di terminatore, i dati rimbalzeranno interrompendo l'attività su tutta la rete.



Protocolli:

Affinché una rete funzioni è necessario stabilire delle regole in base a cui vengono condotte le attività di rete. Tali regole sono dette appunto protocolli.

Fino agli anni '70, ad esempio, il metodo usato per comunicare usando i fili del telefono si chiamava **commutazione di circuito.**

Il protocollo di comunicazione usato su Internet, invece, è basato su un altro principio: la **commutazione di pacchetto.**



Negli anni 70 i dispositivi di rete erano costruiti da aziende diverse che realizzavano hardware e software con l'obiettivo di far comunicare esclusivamente i prodotti dell'azienda produttrice senza curarsi della comunicazione con sistemi diversi: si realizzarono quelli che furono in seguito identificati come sistemi chiusi (closed system). Con il passare del tempo nacque la necessità di collegare tra loro dispositivi anche a media distanza, per esempio tra due sedi della stessa azienda poste in città differenti, e quindi i sistemi chiusi dovettero connettersi a sistemi e impianti di comunicazione, sia privati che pubblici, di altri produttori. L'ISO (International Organization for Standardization) iniziò a dare le basi per la coordinazione dello sviluppo di standard per l'interconnessione dei sistemi di elaborazione, mettendo a punto lo standard OSI (Open System Interconnection) così facendo creò un protocollo di comunicazione che fosse in grado di far comunicare sistemi con caratteristiche diverse tra loro, passando dai sistemi chiusi ai sistemi aperti (Open System) .



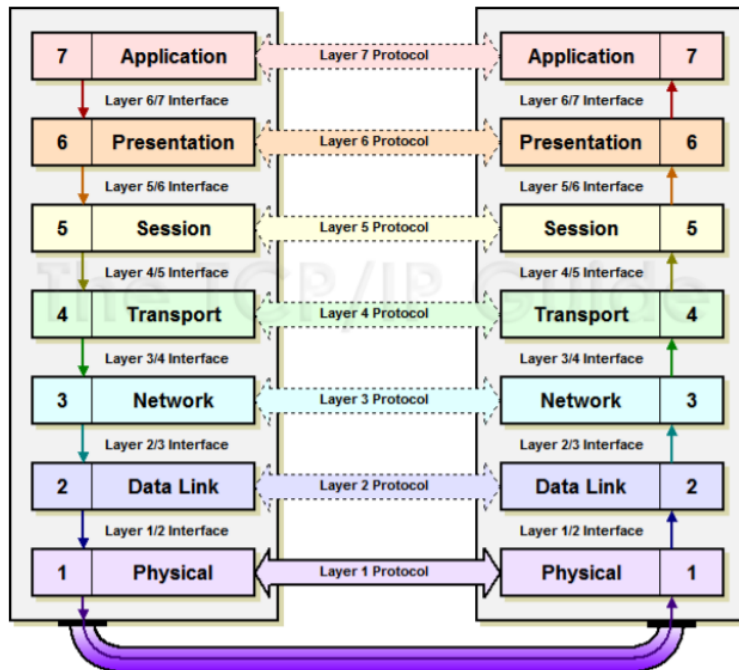
OSI il modello a strati.

Per far comunicare due sistemi diversi, c'è bisogno che questi parlino la stessa "lingua", nel caso dei sistemi di elaborazione serve che utilizzino le stesse regole procedurali per effettuare il trasferimento delle informazioni. Utilizzando un modello a livelli (o strati) si può ridurre la complessità della comunicazione in funzioni elementari e assegnarle a diversi strati. Il modello a strati permette inoltre la modularità degli strati, ovvero si potrebbero modificare le funzionalità di un singolo strato senza dover cambiare tutti gli altri.

Come funziona? L'informazione che un mittente vuole inviare a un destinatario passa da un livello superiore a quello inferiore e subisce man mano delle trasformazioni che consentono alla fine di trasmetterla su un canale fisico



Ogni livello (strato) del mittente comunica (logicamente) con il suo pari del destinatario, chiamato: peer level. Ogni livello ha degli elementi attivi chiamate entità, che sono in grado di inviare e ricevere informazioni. Le entità che formano gli strati di pari livello sui diversi computer sono chiamati peer entity, e possono essere: processi o dispositivi hardware. Le modalità con cui ogni livello realizza le sue funzionalità sono mascherate agli altri livelli, ovvero un livello non conoscerà le funzioni degli altri livelli



Peer level

ogni livello può comunicare con il suo superiore e con il suo inferiore ovvero con i livelli a lui adiacenti, per far comunicare i livelli fra di loro c'è bisogno di stabilire dei protocolli di comunicazione: le interfacce. Le interfacce o SAP (Service Access Point) sono necessarie ai livelli per scambiarsi informazioni.



Il principio che sta alla base delle architetture di rete che utilizzano il modello a strati, è l'incapsulamento (encapsulation). Questo processo si verifica nel momento in cui un Computer (Host A) vuole inviare dati all'Host B, e l'informazione (PDU) passa da un livello superiore a quello inferiore, e ogni livello aggiunge a quest'ultimo un pacchetto di dati chiamato header.



TCP/IP: (*Transmission Control Protocol - Internet Protocol*) Insieme dei protocolli usato da internet per implementare la gerarchia a 4 livelli che eseguono operazioni analoghe a quelle vostre, nel caso di spedizione di un pacco fino alla ricezione.

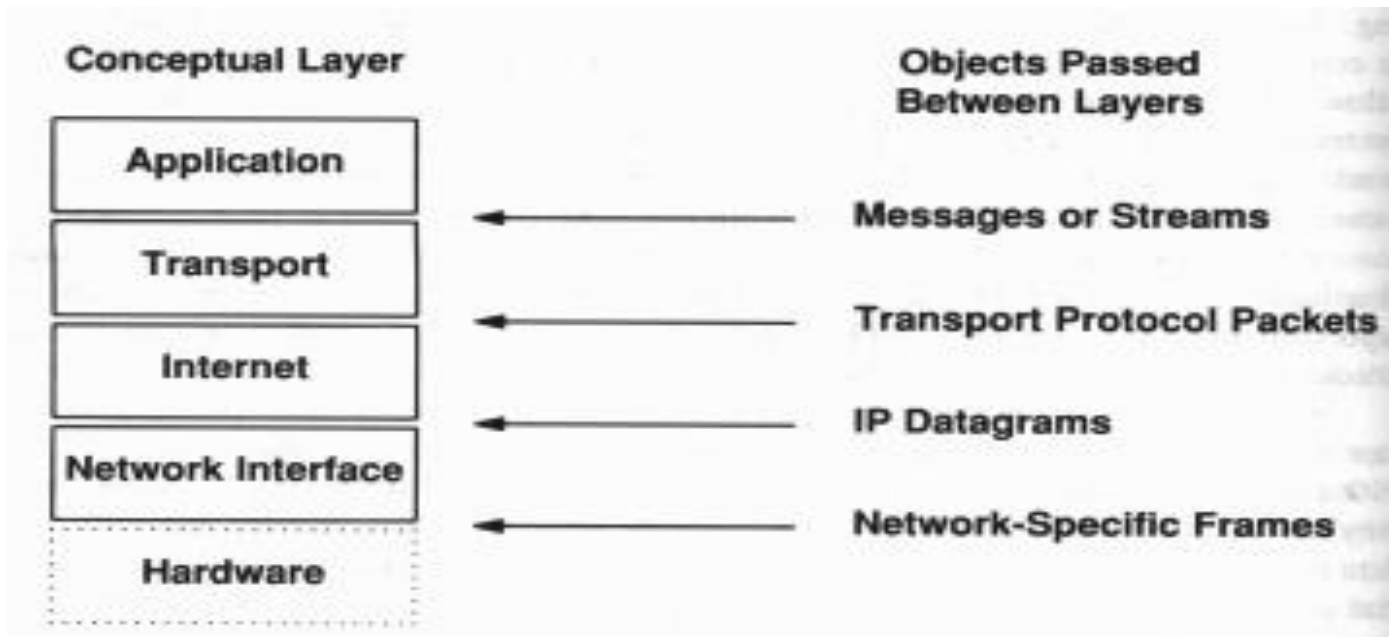
Il modello a strati è una comoda rappresentazione dei sistemi di rete che permette concettualmente di separare le diverse funzionalità in strati di protocolli, permettendo così di studiare più facilmente i protocolli di rete. L'idea della stratificazione è fondamentale per poter disegnare l'architettura software strutturata in livelli, ognuno dei quali con i suoi vari protocolli, tratta una parte specifica dei problemi di trasmissione. Il concetto di stratificazione poggia su un principio basilare il quale, in sostanza, afferma che lo strato *n*-esimo alla stazione destinazione deve ricevere un pacchetto identico a quello che è uscito dal medesimo livello alla stazione sorgente.



Concettualmente, mandare un messaggio da un programma su una macchina ad un programma su un'altra, significa trasferire tale messaggio giù attraverso tutti i vari strati fino al livello di rete e, tramite l'hardware, raggiungere l'altra macchina, risalire gli strati software in successione fino al livello di applicazione dell'utente destinazione.

In particolare il software TCP/IP è organizzato concettualmente in quattro livelli più un quinto costituito dal supporto fisico vero e proprio. La figura mostra i quattro livelli:





Application Layer : A livello più alto, l'utente invoca i programmi applicativi che permettono di accedere ai servizi disponibili attraverso Internet; tale livello riguarda tutte le possibili opzioni, chiamate, necessità dei vari programmi. **In pratica gestisce l'interattività tra l'utente e la macchina.**

Un programma applicativo interagisce con uno dei protocolli di livello trasporto per inviare o ricevere dati e li passa al livello trasporto nella forma richiesta.

Transport Layer :

Lo scopo primario del livello trasporto è consentire la connessione in rete fra due utenti ovvero permettere la comunicazione tra un livello applicativo ed un altro; una comunicazione di questo tipo è spesso detta "end-to-end".

Il software di tale livello divide il flusso di dati in pacchetti (di solito di circa 500 byte) che vengono passati insieme all'indirizzo di destinazione allo strato sottostante. Il livello di trasporto deve accettare dati da molti utenti contemporaneamente e, viceversa, deve smistare i pacchetti che gli arrivano dal sotto ai vari specifici programmi; deve quindi usare dei codici appositi per indicare le cosiddette porte.

Il livello di trasporto può regolare il flusso di informazioni e può, nel caso del TCP, fornire un trasporto affidabile assicurando che i dati giungano a destinazione senza errori ed in sequenza mediante un meccanismo di acknowledgement e ritrasmissione.

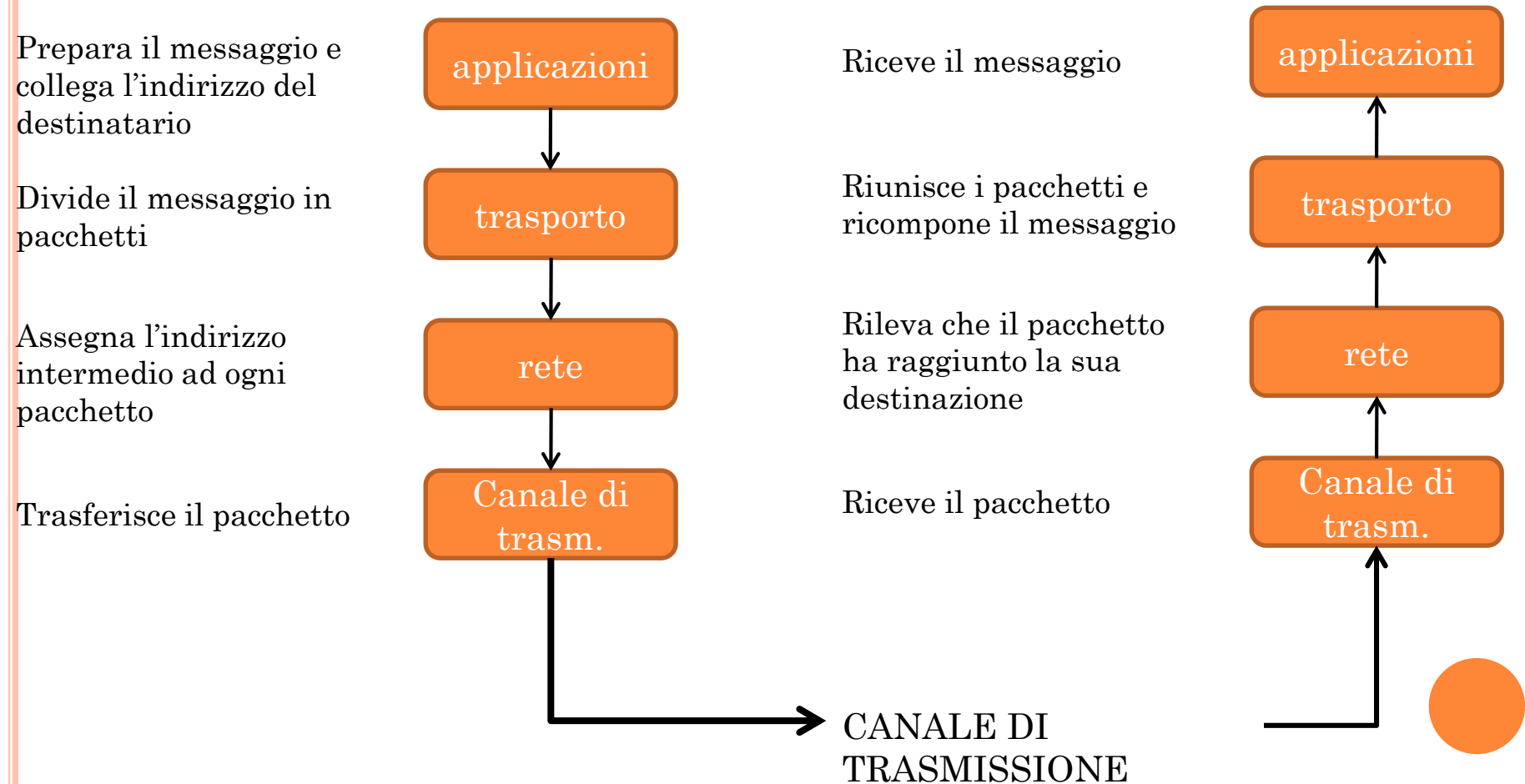


Internet Layer (IP) : Questo livello gestisce la comunicazione tra una macchina ed un'altra; accetta una richiesta di inoltrare di un pacchetto da un livello di trasporto insieme all'identificazione della macchina alla quale il pacchetto deve essere inviato.

È il livello più caratteristico della internet, detto appunto IP (internet protocol) che crea il datagramma di base della rete, sostanzialmente, riceve e trasferisce senza garanzie i pacchetti, che gli arrivano da sopra, verso la macchina destinataria.



Network Interface Layer : Il quarto ed ultimo strato è costituito da una interfaccia di rete che accetta il datagramma IP



Riassumendo, la comunicazione su Internet implica l'interazione di quattro livelli di software:

- Il livello di applicazione: si occupa di messaggi e indirizzi dal punto di vista delle applicazioni;
- il livello di trasporto: converte i messaggi in pacchetti compatibili con Internet e assembla di nuovo i messaggi prima di inoltrarli all'applicazione;
- il livello di rete: si occupa di recapitare i pacchetti attraverso Internet;
- il livello di collegamento: gestisce le trasmissioni di un pacchetto da un computer ad un altro;



Le persone hanno molteplici "identificatori": nome, codice fiscale, matricola universitaria...



I telefoni sono identificati da un unico numero.



I dispositivi collegati ad Internet (host, router) hanno due identificatori (il dispositivo conosce solo il proprio identificatore numerico):

Indirizzo IP (numero di 32 bit): utilizzato per instradare i pacchetti nella rete.

Hostname (stringa alfanumerica): è la traduzione del numero in nome logico utilizzato dalle persone.



L'**indirizzo IP** è associato in maniera univoca a ciascuna interfaccia.

È composto da 2 parti:

Prefisso: id della rete di appartenenza (network -id);

Suffisso: specifico per l'host.



IPv4 = 32 bits

2^{32} indirizzi totali = 4.294.967.296

IPv6 = 128 bits (Nuova generazione di Internet)

2^{128} indirizzi possibili ($\sim 3,4 \times 10^{38}$).

~ 1030 indirizzi per ogni persona del pianeta

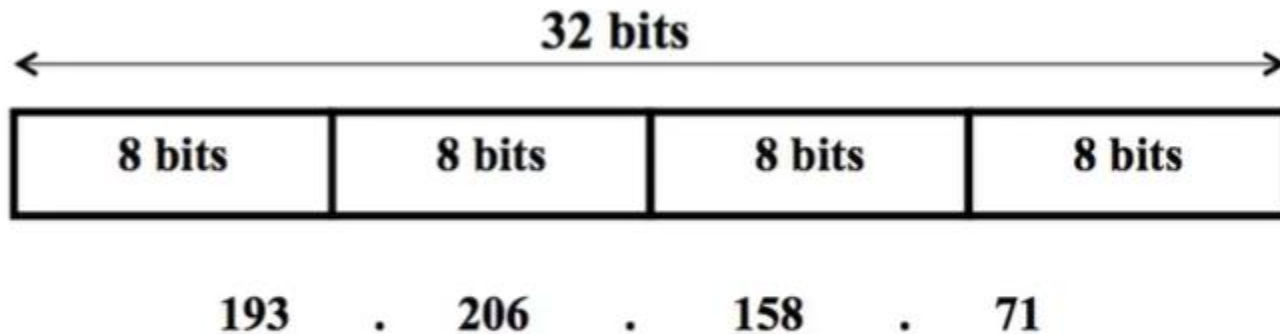


Indirizzo IPv4:

32 bit = 4 byte

Notazione decimale puntata:

0.0.0.0 ÷ 255.255.255.255



Si può leggere dal prompt dei comandi

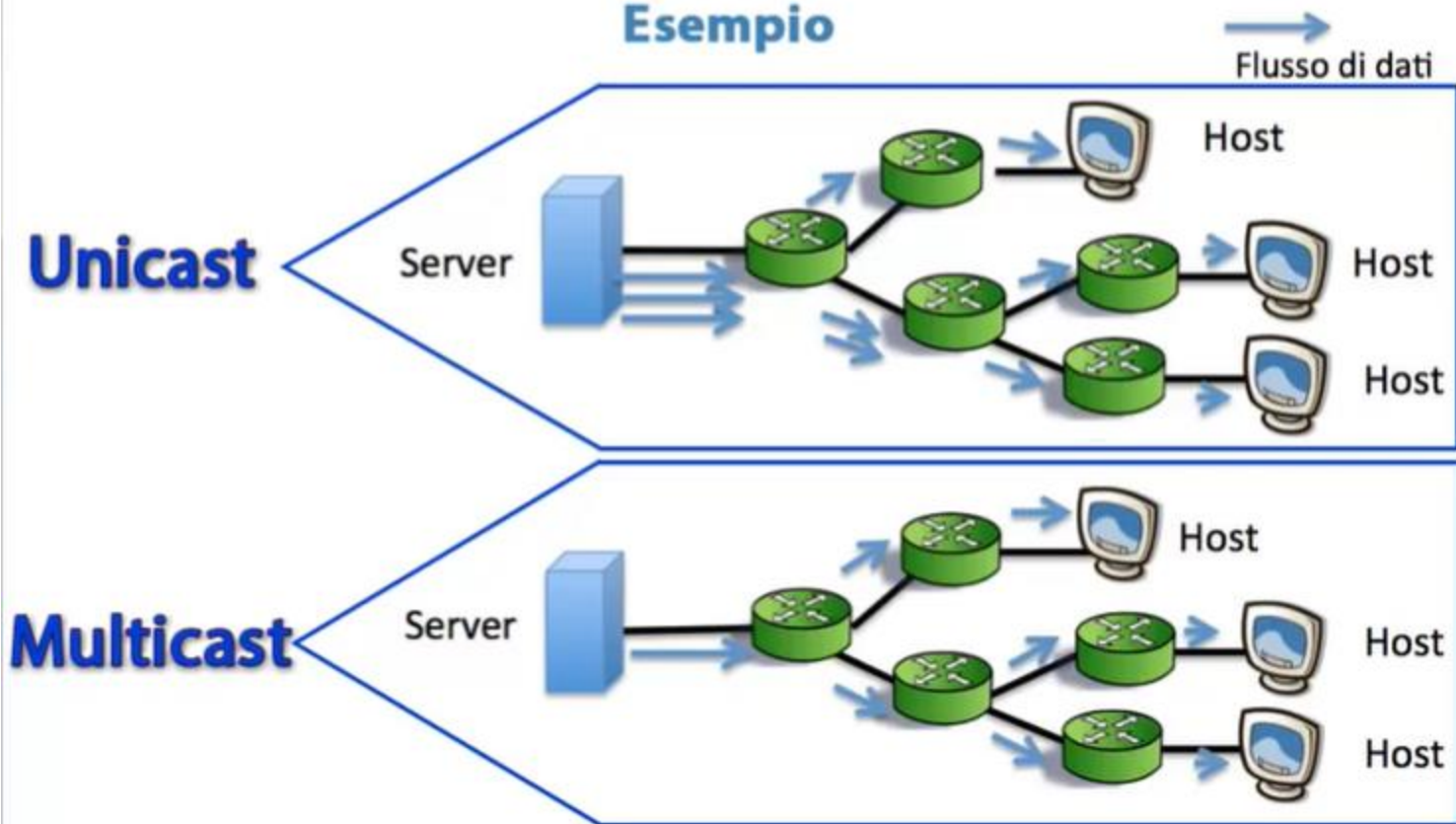


Unicast: indirizzi di nodi

Multicast: indirizzo IP rappresenta gruppi di nodi (uno a tanti)

Anycast: indirizzo unico di più copie identiche di nodi

Esempio





▶ **IP Pubblici**

Sono unici e univoci nel mondo dell'Internet pubblico e sono assegnati dagli enti preposti GARR / RIPE / IANA.

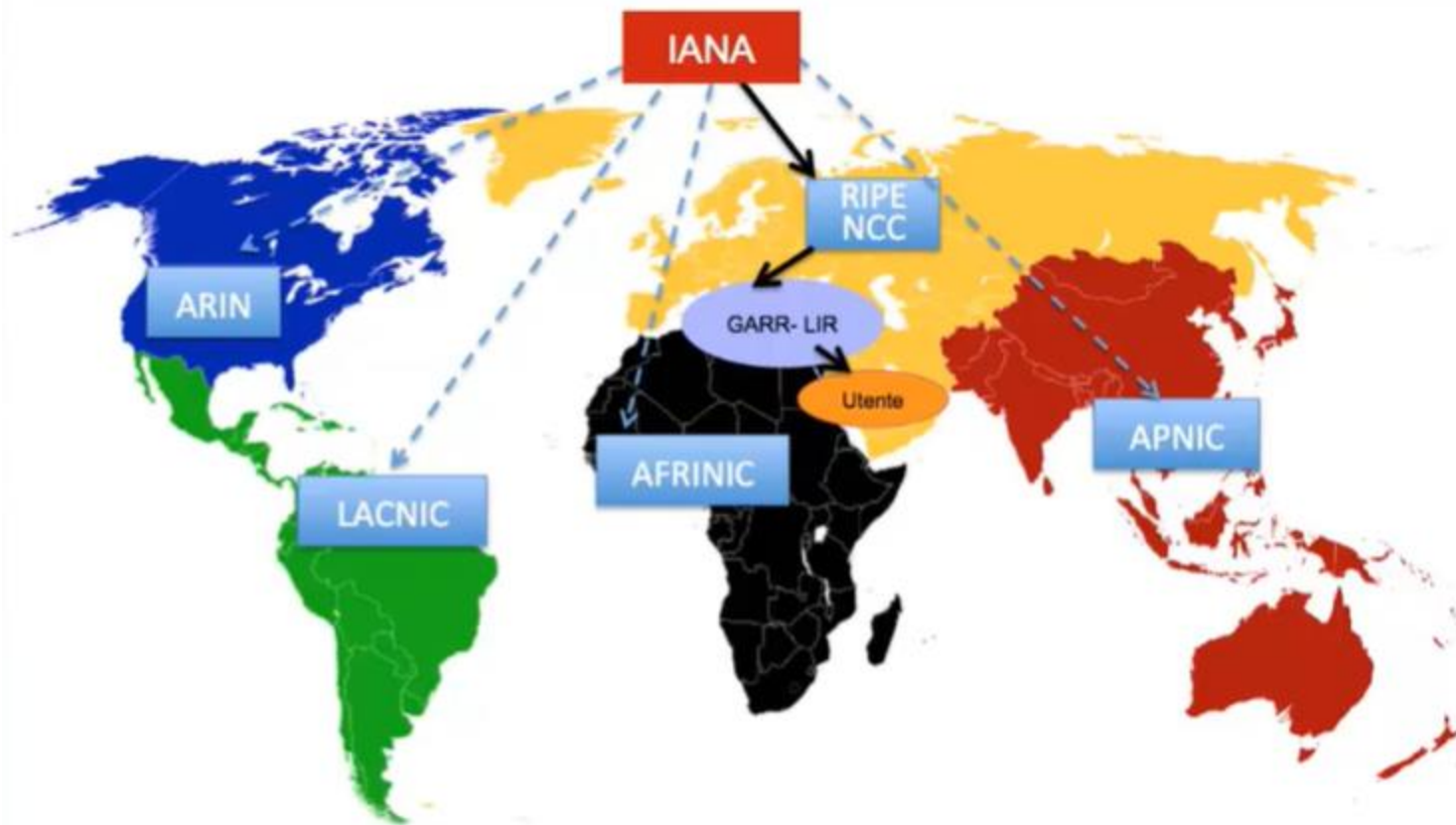
▶ **IP Privati**

Sono indirizzi utilizzati all'interno di reti private ma non vengono trasmessi nell'Internet pubblico globale.



Non sono visibili su internet





IANA - Internet Assigned Numbers Authority
Regional Internet Registry
Local Internet Registry
Utente



Dato lo scopo rivolto verso l'utente, all'**Hostname** si preferiscono attribuire valori mnemonici.

Il **DNS** realizza uno spazio dei nomi gerarchico e permette la traduzione del nome mnemonico di un host in un indirizzo IP.

Per esempio:



Implementa un meccanismo efficiente (mediante **name servers**), distribuito su scala geografica, per convertire un hostname in un indirizzo IP e viceversa.



Un **dominio di primo livello** (conosciuto anche come ***estensione o TLD***) è utilizzato per identificare uno specifico territorio o uno specifico tipo di attività.

Un **dominio di secondo livello** generalmente identifica il soggetto, il prodotto, il brand, l'azienda o il servizio promosso dal dominio

Un **dominio di terzo livello** (anche conosciuto come **sottodominio**) identifica una specifica parte o sezione del dominio stesso. Per esempio in *blog.keliweb.com* o *faq.keliweb.com* "*blog*" e "*faq*" rappresentano un approfondimento di una parte dell'intero dominio.



**Generic
Top Level Domain
- gTLD -**

.com .net .info .org ecc.

**Country Code
Top Level Domain
- ccTLD -**

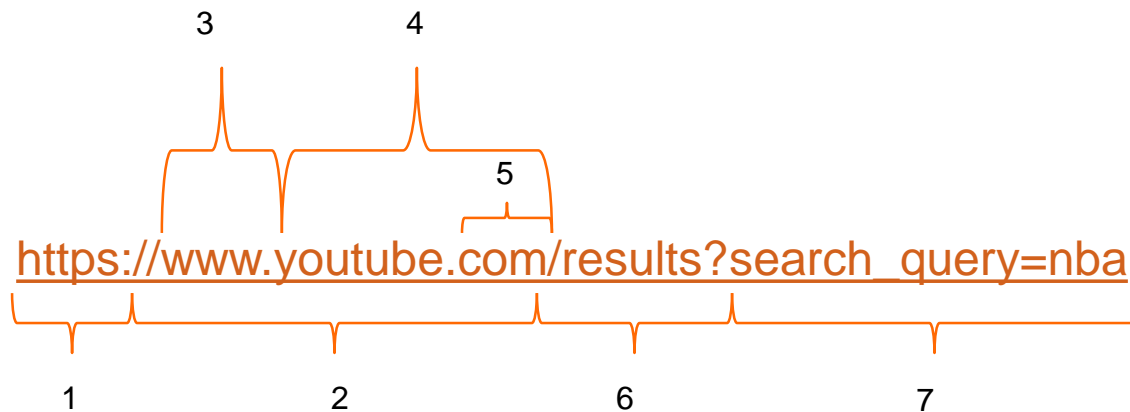
.it .fr .uk .us .jp ecc.

I gTLD si sono evoluti negli anni. All'inizio erano pochi e con un utilizzo specifico, ma adesso con la liberalizzazione possono essere creati TLD con qualsiasi parola o sequenza di caratteri.

Nome del Dominio	Significato
.COM	Organizzazioni commerciali
.EDU	Istituzioni USA per l'istruzione
.GOV	Istituzioni governative USA
.MIL	Istituzioni militari USA
.NET	Organizzazioni commerciali
.ORG	Solitamente organizzazioni senza scopo di lucro
Codice nazionale (IT, CH, DE, FR, UK, ...)	Nomi nazionali (schema geografico)

L'acronimo "URL" sta per "Uniform Resource Locator" o "Localizzatore Uniforme di Risorse", e viene comunemente usato per fare riferimento a un sito o un indirizzo, anche se, in realtà, il suo obiettivo è solitamente una directory o un percorso specifico.

Un URL è comunemente composto da più parti. Per comprendere la sua struttura e i suoi componenti, smantelleremo il seguente URL di esempio:



1. Il *Protocollo* in uso. In questo caso: *HTTP* ("Hypertext Transfer Protocol", Protocollo di Trasferimento di un Ipertesto)
Esistono anche altri protocolli, come *HTTPS*, *FTP* e così via.
2. L' *host* o il *nome host*: `www.youtube.com`
3. Il *sottodominio*: `www`.
4. Il *nome del dominio*(dominio): `youtube.com`
5. Il *dominio di primo livello* (suffisso di un indirizzo web): `.com`
(conosciuto anche con l'abbreviazione *TLD*)
6. Il *Percorso*
Un percorso fa di solito riferimento a un file o a una cartella (directory) presente nel server (per esempio `/folder/file.html`)
7. *Parametro e valore*



HTTP e FTP sono due dei protocolli Internet più comunemente utilizzati. HTTP sta per Hyper text transfer protocol; FTP è il protocollo di trasferimento file.

La differenza principale tra i due protocolli è il loro scopo. HTTP serve come un modo di accesso alle pagine web sul World Wide Web. FTP è destinato a facilitare il trasferimento sicuro dei file su Internet.



ATTACCHI:

Quando un PC è collegato ad una rete, si espone agli accessi autorizzati. I sistemi di computer possono essere attaccati attraverso software dannosi detti **malware**, che può essere trasferito ed eseguito su di un pc o attaccarlo a distanza.

Un virus è un software che infetta un pc inserendosi nei programmi presenti nella macchina. Quando il programma ospite viene eseguito, viene eseguito anche il virus.

Worm (verme) è un programma che si trasferisce attraverso la rete, insinuandosi nei computer e inoltrando copie di se stesso ad altri computer. Una tipica conseguenza è il suo duplicarsi e diffondersi incontrollato.

Cavallo di Troia: entra nel computer sotto forma di applicazione legale, importato dall'utente e rimangono in attesa di un evento come il verificarsi di una data. Si presentano molto spesso sotto forma di allegati ai messaggi e-mail.

Spyware: (software che annusa) ovvero raccoglie le informazioni sulla attività che si svolgono nel computer su cui risiede e le porta al mandante



Phishing (dal greco pesca) è un modo esplicito di ottenere informazioni semplicemente chiedendole es. passw. Username. Il processo implica la diffusione di esche in rete.

Come difendersi

Software antivirus: Utilizzato per riconoscere e rimuovere virus ed altre infezioni. Deve essere sempre aggiornato

Firewall (porta di fuoco) Ferma il traffico proveniente da computer che lanciano un attacco. I filtri antispam sono un esempio di firewall, progettati specificatamente per le e-mail

In alcuni casi, lo scopo del vandalismo informatico è quello di interrompere il corretto funzionamento del sistema, ma in altri casi, l'obiettivo finale è quello di accedere alle informazioni.

Il mezzo tradizionale dei dati è quello di controllarne l'accesso attraverso username e password. Tuttavia servono a poco quando i dati sono trasferiti sulla rete.

Può essere utile allora ricorrere alla crittografia (*La crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma*).

Oggi molte applicazioni internet sono state modificate in modo da incorporare tecniche crittografiche:

FTP → FTPS; HTTP → HTTPS

Internet è una immensa risorsa che offre un'innumerabile quantità di servizi per tutti i gusti. Purtroppo, però, **non tutti i servizi offerti vengono impiegati a fini di bene**. Proprio per questo motivo, quando navighi su Internet, devi essere consapevole dei potenziali rischi che corri.

Il deepfake una nuova minaccia

Si tratta di video falsi, creati grazie alla tecnologia deep learning che permette di sostituire i volti di due persone (face swapping) riproducendone la voce e sincronizzando il labiale.

