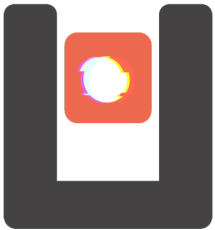


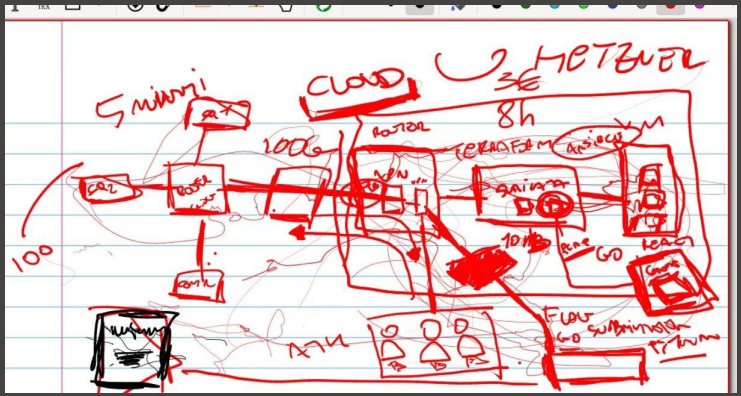
Network Security – Basi e cenni teorici

Karina Chichifoi (@TryKatChup)

April 3, 2022

La sicurezza della rete consiste nell'insieme di strategie, procedure e tecnologie finalizzate a proteggere la rete dagli accessi non autorizzati da potenziali danni. Una delle principali priorità della sicurezza di rete consiste nel controllare l'accesso e impedire che queste minacce riescano a penetrare e a diffondersi al suo interno.

Nel nostro particolare caso sarà molto utile per le competizioni di tipo A/D, dato che dovremmo mantenere sicura la nostra infrastruttura, capire il tipo di traffico in ingresso e uscita, ed evitare intrusioni e il propagarsi di eventuali attacchi.



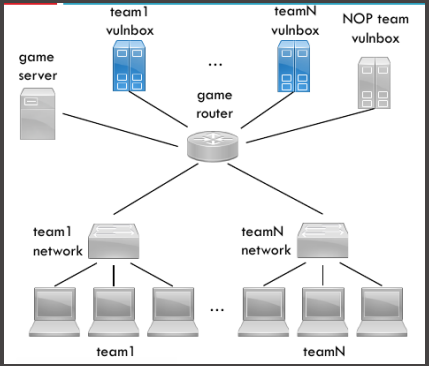


Figure: Infrastruttura CC

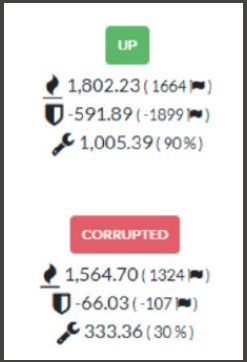


Figure: Stato dei servizi

Suddivisione in base alla dimensione:

- PAN (Personal Area Network): rete ristretta a pochi pc
- LAN (Local Area Network): rete locale la cui dimensione può essere relativa a un edificio o a un campus
- MAN (Metropolitan Area Network): rete che copre un'intera città
- WAN (Wide Area Network): rete che copre uno stato
- Internet: copre l'intero pianeta

Per sistemi aperti intendiamo una rete di calcolatori in cui qualunque calcolatore o applicazione comunica con qualunque calcolatore o applicazione mediante qualunque rete. È importante quindi:

- introdurre regole comuni per lo scambio delle informazioni
- utilizzare standard → dispositivi diversi riescono a comunicare

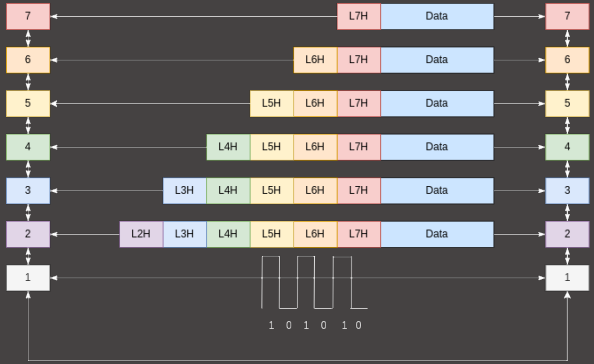
Da qui nasce OSI (1978), un'architettura a strati.

Lo scopo di OSI è:

- Scomporre il problema in sottoproblemi più semplici da trattare
- Rendere i vari moduli indipendenti tra loro
- Potere consentire a diversi costruttori di realizzare servizi e interfacce

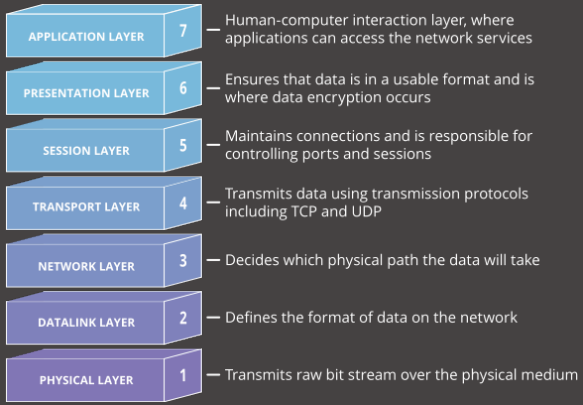
- I servizi sono ciò che viene fornito da uno specifico strato
- I protocolli sono il come un certo servizio viene fornito da uno strato. Un protocollo consente a due entità dello stesso livello di potere comunicare tra loro, comprendendo quello che si sta trasmettendo
- Un'interfaccia consente di avere regole di dialogo tra entità di livelli adiacenti
- L'unità dell'informazione di ciascun livello viene chiamata Protocol Data Unit (PDU)

Ciascun livello inoltre aggiunge all'unità di informazione un header o un footer. Quando l'informazione arriva a destinazione, ciascun livello estrae l'header utile per il suo livello, e passa il resto dell'informazione ai livelli superiori.



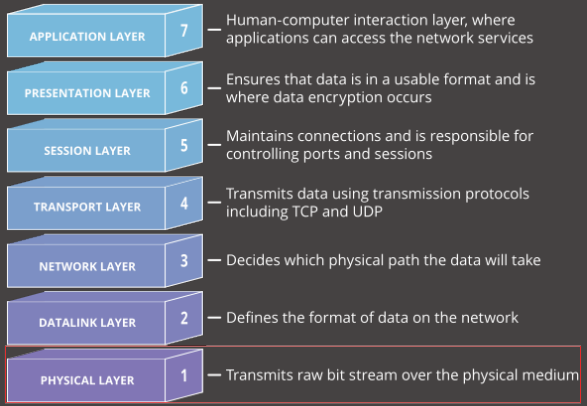
In ISO/OSI si hanno 7 strati:

- I primi 3 sono detti lower, o network oriented layers
- Gli strati 5,6,7 sono detti upper o application oriented layers
- Lo strato 4 fa da raccordo tra upper e lower layers
- Gli strati dal 4 in su operano invece solo end-to-end



Consente di trasmettere un flusso di dati attraverso un collegamento fisico, occupandosi della forma e dei livelli di tensione del segnale.

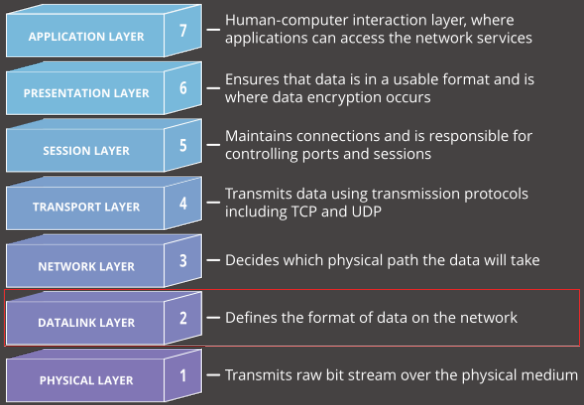
- Unità dati: bit
- Tecnologie: bluetooth, fibra ottica, cavo di rame



Consente un trasferimento affidabile di dati a livello fisico.

Effettua anche un controllo degli errori e perdite di segnale.

- Unità dati: frame
- Protocolli: Ethernet, Wi-Fi

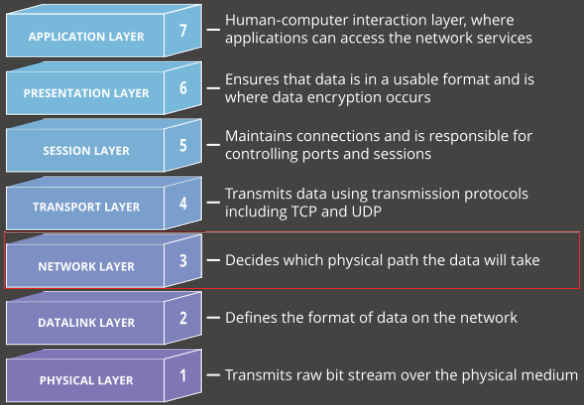


Rende i livelli indipendenti dai meccanismi e dalle tecnologie usate per la connessione.

Lo scopo di questo livello è di far giungere le unità di informazioni (pacchetti) al destinatario, scegliendo il percorso attraverso la rete.

Si occupa del routing, consentendo il corretto instradamento dei pacchetti verso la giusta destinazione.

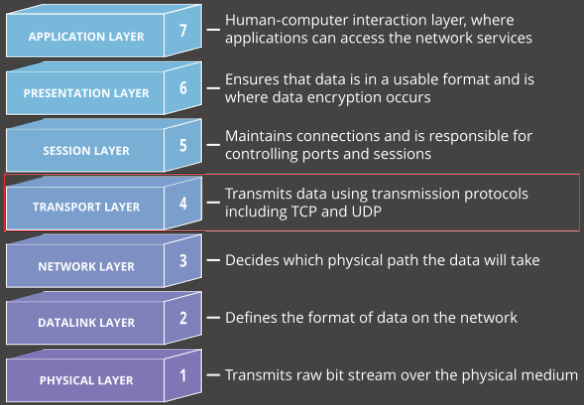
- Unità dati: pacchetto
- Protocolli: IP



Consente un trasferimento dati trasparente e affidabile, effettuando un controllo degli errori e flusso tra due host.

Il suo scopo è di fornire un canale sicuro end-to-end, svincolando gli strati superiori dai problemi di rete.

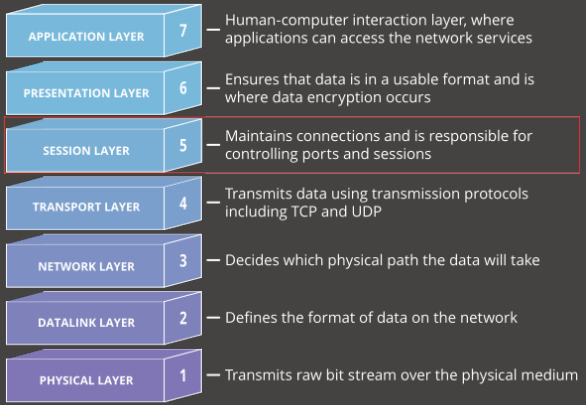
- Unità dati: segmenti
- Protocolli: TCP, UDP



Consente di stabilire, gestire e terminare sessioni di comunicazione tra applicazioni.

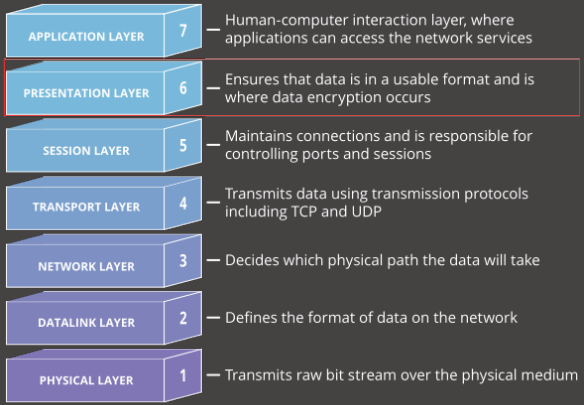
Vengono introdotti anche dei punti di sincronizzazione (token) e vengono inseriti checkpoint, in modo da ridurre la quantità di dati da ritrasmettere in caso di gravi malfunzionamenti.

- Protocolli: SOCKS, NetBIOS



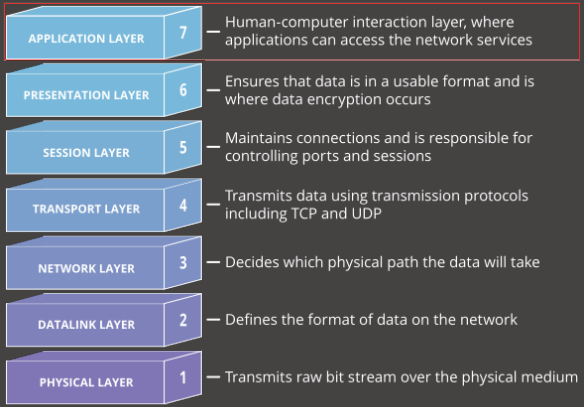
Si occupa della trasformazione dei dati in un formato standard, e offre servizi come la compressione e cifratura.

- Protocolli: PGP, MIME, ASCII

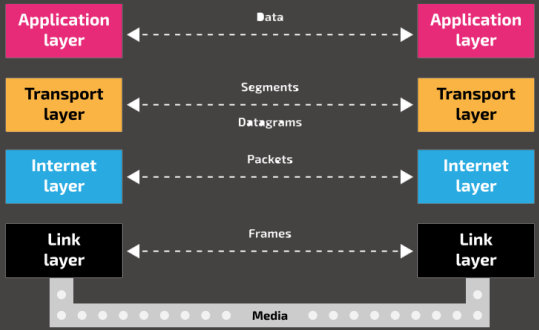


Fornisce servizi per i processi delle applicazioni.

- Protocolli: DHCP, DNS, LDAP, SSH, HTTP



ISO/OSI è stato creato nel 1978
è evoluto come modello teorico;
al contrario TCP/IP risulta un modello pratico, utilizzato normalmente per le implementazioni delle funzioni di rete.

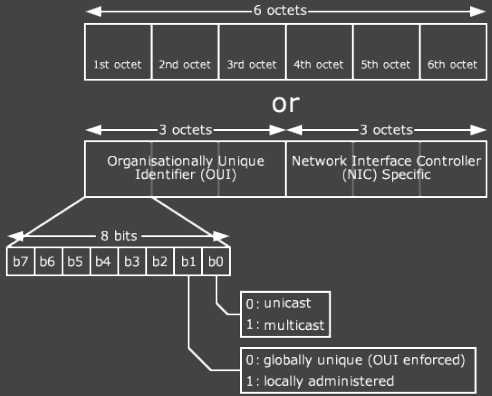


Ciascuna scheda di rete di un dispositivo è identificata da un MAC Address, ovvero un indirizzo a 6 byte strutturato nel seguente modo:

00:50:FC:A0:67:2C

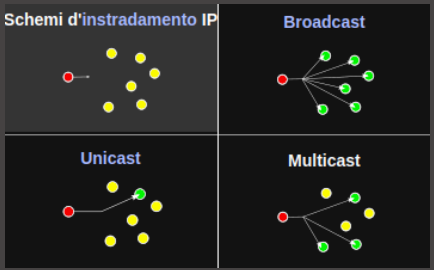
Dove:

- I primi 3 ottetti (ovvero i primi 24 bit) dipendono unicamente dal produttore della scheda di rete. In particolare, se si considera il primo byte e si guarda l'ultimo bit si ha:
  - Multicast se bit $= 1$
  - Unicast se bit $= 0$
- I successivi 3 ottetti dipendono dal numero di serie della scheda di rete stessa:
  - Si hanno 2^{48} (cioè 281.474.976.710.656) indirizzi MAC possibili, che è un numero che è impossibile raggiungere prima che le schede di rete cambino standard


6 octets
1st octet
2nd octet
3rd octet
4th octet
5th octet
6th octet
or
3 octets
3 octets
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b7
b6
b5
b4
b3
b2
b1
b0
0 : unicast
1 : multicast
0 : globally unique (OUI enforced)
1 : locally administered

Normalmente un messaggio può essere inviato in:

- Unicast: un dispositivo invia l'informazione a un solo dispositivo
- Multicast: un' informazione viene inviata a più dispositivi finali
- Broadcast: l'informazione viene inviata contemporaneamente a tutti i dispositivi presenti nella rete (`FF:FF:FF:FF:FF:FF`)



Utile per motivi di:

- Privacy
- Interoperabilità

La randomizzazione dell'indirizzo MAC della scheda WIFI è abilitata di default su:

- Android >=8
- iOS >=14

Per abilitarla su Arch: link
Per abilitarla su Windows: link

Protocollo a livello di rete:

- Connectionless: assenza di richiesta di connessione → non c'è garanzia che il singolo pacchetto sia stato consegnato, né che sia stato consegnato nell'ordine corretto.
- Non affidabile: i datagram possono essere persi o danneggiati durante il tragitto oppure potrebbero arrivare in ordine sparso a destinazione.

Il router è il principale attore del compito di instradamento dei dati. È un vero e proprio calcolatore con una CPU e una RAM.

La tabella di routing contiene le rotte verso altri router e il loro costo.
Il costo, o metrica, sono informazioni basate sulla larghezza di banda, numero di hop (nodi della rete), il ritardo, carico, Maximum Transmission Unit, affidabilità della comunicazione.

I protocolli di routing sono un insieme di norme che regolamentano la comunicazione tra due router. Forniscono informazioni utili sulle rotte più comode da utilizzare attraverso le quali inviare i pacchetti.

`137.204.150.24`

- Indirizzi composti da 32 bit
- Si hanno pertanto 2^{32} indirizzi IPv4 possibili (4,294,967,296)
- Un indirizzo IP definisce in modo univoco un'interfaccia di rete connessa ad un LAN o WAN
- Esistono anche i multi-homed host, ovvero host con due o più interfacce di rete che usa più indirizzi IP
- Un router che collega N reti ha almeno N distinti indirizzi IP, uno per ogni interfaccia di rete

Abbiamo ben 5 classi di indirizzi IP:

- Classe A: da `0.0.0.0` a `127.255.255.255`
- Classe B: da `128.0.0.0` a `191.255.255.255`
- Classe C: da `192.0.0.0` a `223.255.255.255`
- Classe D: da `224.0.0.0` a `239.255.255.255`
- Classe E: da `240.0.0.0` a `255.255.255.255`

Esistono anche una serie di indirizzi riservati (RFC 1700, 3927)

- `0.0.0.0` indica l'host corrente senza specificarne l'indirizzo
- `0.x.y.z` indica un certo Host-ID sulla rete corrente senza specificare il Net-ID
- `255.255.255.255` è l'indirizzo di limited broadcast
- `127.x.y.z` è il loopback, che redirige i datagrammi agli strati superiori
- `169.254.x.y` riservati per l'autoconfigurazione degli host

In molti casi una rete di classe `A` o `B` è troppo grande (molti indirizzi inutilizzati) e una di classe `C` troppo piccola.

Indirizzamento IP più flessibile senza l'uso delle classi: pertanto adesso si utilizza CIDR (Classless Inter-Domain Routing)

Un indirizzo IP è diviso in due parti:

- Network-ID che identifica la rete (prefisso)
- Host-ID che identifica l'host all'interno della rete (suffisso)

La suddivisione è indicata dalla netmask, una sequenza di 4 byte associata all'indirizzo, in cui

- i bit a 1 corrispondono ai bit dedicati al Network-ID
- i bit a 0 corrispondono ai bit dedicati al Host-ID

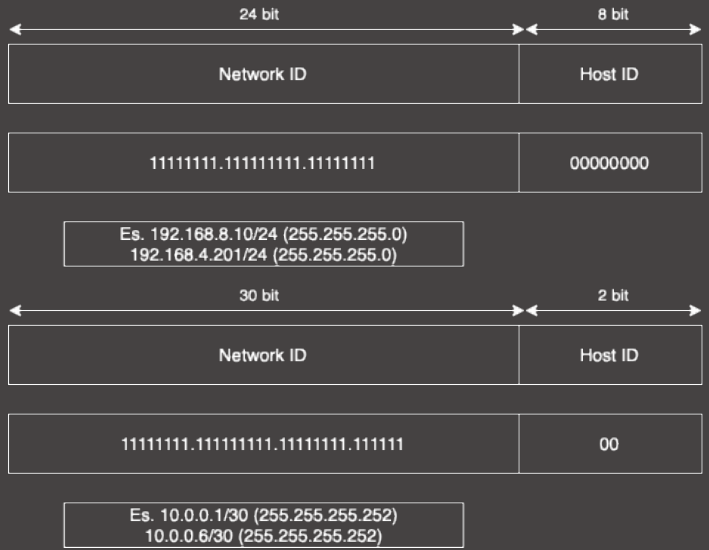
- Composta da 32 bit
- Specifica il numero massimo di host disponibili in una rete
- Può indicare per quali dispositivi si applica una specifica regola (ad esempio con iptables)

Per definizione, una netmask ha sempre tutti i bit a 1 a sinistra e tutti quelli a 0 a destra.
Non esistono netmask con degli 0 tra gli 1.

- `11111011.11011111.11100000.00010000` non è valida!

Di conseguenza, i singoli byte di una netmask non possono assumere tutti i 256 valori possibili, ma solo 9:

- $00000000 = 0$
- $10000000 = 128$
- $11000000 = 192$
- $11100000 = 224$
- $11110000 = 240$
- $11111000 = 248$
- $11111100 = 252$
- $11111110 = 254$
- $11111111 = 255$


24 bit
8 bit
Network ID
Host ID
11111111.111111111.11111111
00000000
Es. 192.168.8.10/24 (255.255.255.0)
192.168.4.201/24 (255.255.255.0)
30 bit
2 bit
Network ID
Host ID
11111111.111111111.11111111.111111
00
Es. 10.0.0.1/30 (255.255.255.252)
10.0.0.6/30 (255.255.255.252)

Si hanno quindi 4 byte, ognuno dei quali con i valori visti in precedenza.

La netmask si può specificare alla fine di un indirizzo IP nel seguente modo: `192.168.1.0/24`

Per testare le varie configurazioni:

- comando `ipcalc`
- questo sito: link

Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Rete IP a disposizione: `192.168.1.0/24`
LAN A ha 50 host:

- mi basta una sottorete da 62 indirizzi host
- `192.168.1.0/26` è un Net-ID valido

LAN B ha 100 host:

- mi basta una sottorete da 126 indirizzi host
- `192.168.1.64/25` NON è un Net-ID valido
- `64 = 01000000`
- `192.168.1.128/25` è un Net-ID valido
- `128 = 10000000`

Ci sono diverse problematiche relative a IPv4:

- Se un host viene spostato in un'altra rete, il suo indirizzo IP deve cambiare
- Occorre automatizzare l'assegnazione della configurazione degli indirizzi IP dei diversi client in una intranet → DHCP
- Data l'enorme diffusione di Internet, il numero di indirizzi possibili è troppo basso → utile l'adozione di reti IP private e di tecniche di NAT (Network Address Translation)

Consente a più dispositivi di accedere a internet mediante un solo indirizzo IP. Si occupa della traduzione da indirizzi IP pubblici e privati e viceversa.
Indirizzi riservati a reti IP private:

- da `10.0.0.0` a `10.255.255.255`
- da `172.16.0.0.0` a `172.31.255.255` (rete aziendale)
- da `192.168.0.0` a `192.168.255.255` (rete di casa)

Un server DHCP ha il compito di assegnare ad un dispositivo che si connette alla sua rete il primo indirizzo IP valido disponibile. Quando un host collegato ad una LAN o ad una linea vuole usare il DHCP:

- Invia un messaggio `DHCPDISCOVER` in broadcast
- Uno o più Server se presenti rispondono con `DHCPOFFER`
- L'Host ne sceglie uno e gli invia `DHCPREQUEST` per richiedere la configurazione
- Il Server risponde con `DHCPACK` specificando la configurazione

È necessario un server DHCP (porta 67 UDP).

L'IP spoofing consiste nella creazione di un pacchetto con i source address modificati, in modo da sia nascondere l'identità del mittente, sia eventualmente per impersonificare qualcun altro, o entrambe.
È una tecnica utilizzata solitamente dai malitenzionati per utilizzare attacchi DOS contro uno specifico dispositivo o infrastruttura.

ARP (Address Resolution Protocol) è un protocollo collocato tra il livello 2 e il livello 3 ISO/OSI che consente di ottenere un indirizzo fisico di un nodo, partendo dal suo indirizzo IP.

- Alice vuole sapere l'indirizzo MAC di Bob
- A tal scopo, Alice invia un pacchetto broadcast (ARP Request) per richiedere l'indirizzo fisico corrispondente all'IP di Bob
- Tutti gli host della rete ricevono quel pacchetto e solo chi riconosce il proprio indirizzo IP risponde con il proprio indirizzo fisico, ovvero Bob (ARP Reply)

Viene utilizzata una memoria cache per mantenere le associazioni {indirizzo IP - indirizzo fisico} utilizzate.

Sfrutta il mancato meccanismo di autenticazione del protocollo ARP: qualsiasi dispositivo può rispondere a un ARP Request.
L'attaccante invierà delle opportune ARP request modificate, in modo da popolare l'ARP cache con il proprio indirizzo MAC.

Modalità di attacco:

- Man in the Middle
- Denial of Service

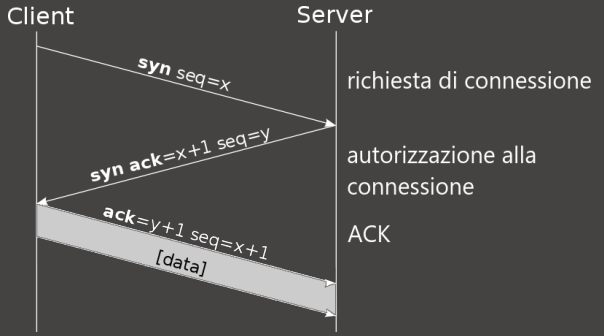
- Tabelle ARP statiche
- Controllo degli accessi alla rete locale
- Suddivisione della rete
- Comunicazione cifrata

TCP è un protocollo connection-oriented utilizzato nel livello di trasporto e, assieme a Internet Protocol, garantisce affidabilità nella trasmissione dei dati, sfruttando un canale di trasmissione bidirezionale.

TCP garantisce:

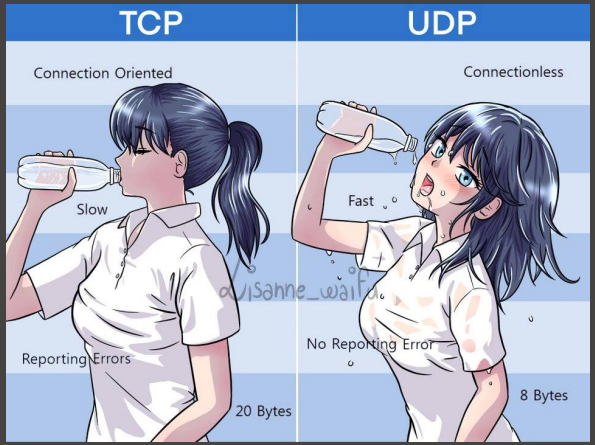
- Comunicazione process to process
- Consegna prioritaria di dati (se specificato) su banda limitata
- Consegna ordinata dei dati
- Controllo di flusso
- Controllo di congestione.

Consente di stabilire una connessione affidabile. Vengono utilizzati dei valori contenuti nel segmento, `seq` e `ack`, che consentono sia a mittente che a destinatario di coordinarsi tra loro e di verificare la corretta ricezione.



UDP è un protocollo di trasporto a pacchetto a basso costo, utilizzato in combinazione con il protocollo del livello di rete IP.
Fornisce un servizio unreliable e connectionless: i datagrammi possono essere persi, duplicati, consegnati fuori ordine o arrivare in ritardo.
Normalmente utilizzato per gli stream video.

- TCP crea una connessione prima di trasmettere i messaggi, mentre UDP no
- TCP consente il recupero e la ritrasmissione dei pacchetti persi
- TCP trasmette i pacchetti in ordine, mentre UDP no
- UDP è più veloce di TCP
- UDP viene normalmente utilizzato per stream video e audio



Dato che la comunicazione è process-to-process, vengono utilizzate delle porte per identificare un servizio o un processo.

Le porte sono suddivise in 3 categorie:

- Well-known ports (0-1023): normalmente utilizzate dai processi di sistema
- Registered ports (1024-49151): assegnate da una autorità centrale (IANA), per specifici servizi
- Ephemeral ports (49152-65535): porte dinamiche o private non registrate da IANA

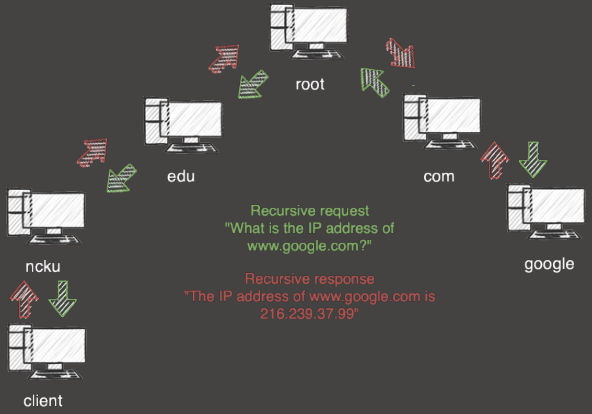
Porte	Servizi
21 e 22	File Transfer Protocol
22	SSH
25	Simple Mail Transfer Protocol
53	Domain Name Server
80	HTTP
443	HTTPS

IL DNS (Domain Name System) è un insieme di gestori di tabella e di indirizzi IP. Il suo compito è quello di attuare corrispondenze tra i nomi dei nodi della rete (host) e gli indirizzi IP; quest'operazione viene detta risoluzione. Il servizio è realizzato tramite un database distribuito, costituito da server DNS.

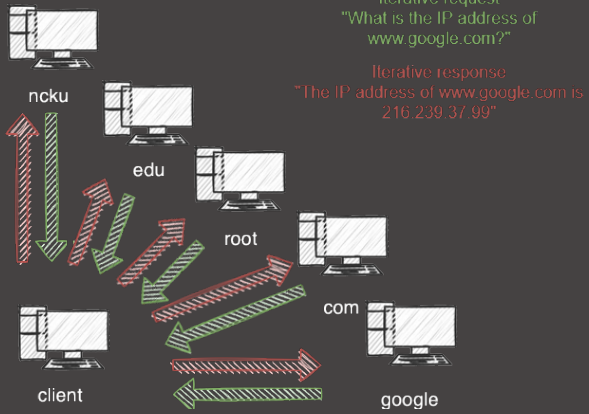
Ogni organizzazione ha un proprio gestore DNS e coordina le richieste dei suoi utenti. Il DNS ha una struttura gerarchica ad albero rovesciato, ed è diviso in domini (com, org, it ecc).

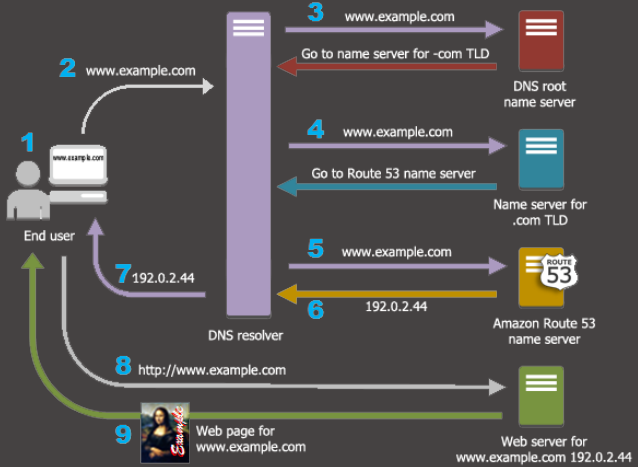
I domini sono logici e non sono collegati alla rete fisica.

Se il server DNS a cui si è fatta la richiesta è responsabile del dominio, risolve l'indirizzo, altrimenti trasmette la richiesta ad un server DNS di livello superiore e aspetta la risposta per il client.
Successivamente il root server inoltra la richiesta al server interessato (passando prima per i server del livello superiore a quello richiesto).
Se non viene trovato il server entro un time out si segnala errore.



Se il server DNS a cui si è fatta la richiesta è responsabile del dominio, risolve l'indirizzo, altrimenti invia al client il nome del server che secondo lui è in grado di rispondere.




1
www.example.com
End user
2 www.example.com
3 www.example.com
Go to name server for -com TLD
DNS root name server
4 www.example.com
Go to Route 53 name server
Name server for .com TLD
5 www.example.com
6 192.0.2.44
ROUTE 53
Amazon Route 53 name server
7 192.0.2.44
DNS resolver
8 http://www.example.com
9 Web page for www.example.com
Web server for www.example.com 192.0.2.44

Un attacco DNS rebinding avviene quando un sito web dannoso finge che gli indirizzi IP facciano parte del suo dominio. In questo modo il sito può aggirare i criteri della stessa origine implementati dai browser e visualizzare i dati di tali indirizzi IP.

Può verificarsi un attacco DNS rebinding se qualcuno visita un sito web dannoso che identifica l' indirizzo IP locale della vittima, deducendone la struttura della sua rete locale.
Il sito web dannoso potrebbe quindi associare i propri domini all'indirizzo IP locale, inviare richieste ai dispositivi sulla rete e leggere le risposte a tali richieste.

La funzione di un firewall è quella di proteggere una o più macchine da accessi indesiderati provenienti dall'esterno.
Vi possono essere 2 tipologie:

- Packet Filter: posto tra rete locale e Internet, filtra i pacchetti e può scartarli in base a provenienza e destinazione, porta, etc
- Proxy Server: filtra i dati sulla base dei protocolli applicativi, non si ferma semplicemente al livello di rete come il packet filter. Tutto il traffico da e verso l'esterno deve passare da esso

Domande?