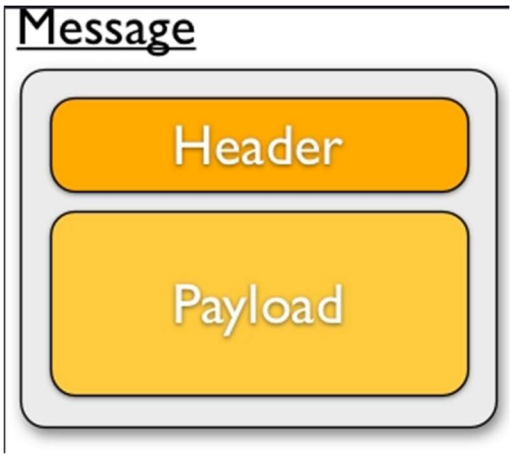
Network

Un rete è un insieme di dispositivi connessi in modo da poter comunicare tra loro tramite vari protocolli che non sono altro che un insieme di regole atte a definire il metodo di comunicazione.
La comunicazione avviene tramite uno scambio di "pacchetti" (ProtocolDataUnit, PDU) che sono una sequenza di bit che vengono scambiati attraverso un mezzo fisico (es. cavo ethernet).
I dati vengono inviati in byte, che sono una sequenza di 8 bit.

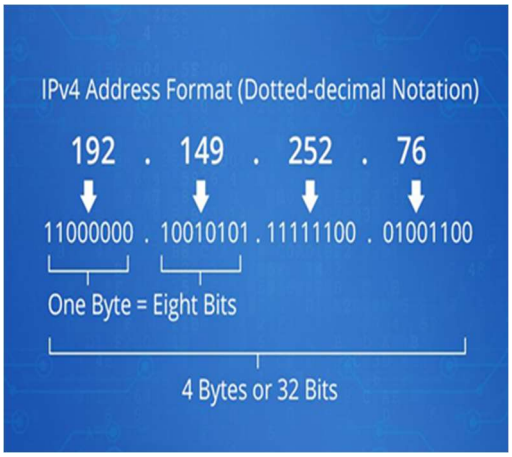
Un **pacchetto** è formato da:
Header ha il compito di assicurare che il dispositivo destinatario sia in grado di interpretare il payload e gestire la comunicazione.
Payload è ciò che realmente inviamo, quindi l'informazione vera e propria (viene anche chiamato carico utile).
L'Header è gestito dal Internet Protocol (IP) e al suo interno ha un dato chiamato Lifespan (o TimeToLive TTL) che indica quanti salti deve fare il pacchetto prima di essere scartato.
Ogni volta che il pacchetto passa attraverso un router, viene decrementato il valore del TTL fino a quando non viene scartato quando arriva a 0.
Questo è importante per evitare che un pacchetto giri all'infinito all'interno di una rete e per poter effettuare una diagnosi della rete analizzando la rotta che fa il pacchetto (traceroute).
Attualmente il TTL è di 128.



Suddivisione delle reti
Le reti vengono suddivise in due categorie:
GEOGRAFICHE sono categorie che si basano sulla distanza tra i dispositivi connessi e possono essere di tipo
-LAN (LocalAreaNetwork) é una rete privata creata con cavi
-WLAN (WirelessLocalAreaNetwork) come la rete LAN ma wireless
-WAN (WideAreaNetwork) comprendere l'area pubblica di una città e serve un provider
-MAN (MetropolitanAreaNetwork) più grande di una LAN ma più piccola di una WAN
-PAN (PersonalAreaNetwork) es. tra smartphone e smartwatch

TOPOLOGICHE sono categorie che si basano sulla configurazione fisica dei collegamenti tra i dispositivi:
-BUS dove tutti i dispositivi sono connessi a un unico cavo di comunicazione
-ANELLO dove ogni dispositivo è connesso a un precedente e a un successivo in sequenza
-STELLA dove tutti i dispositivi sono collegati ad un dispositivo centrale

Indirizzi IP
Il protocollo IP si occupa della consegna dei datagrammi (pacchetti a livello di rete).
La maggior parte delle reti utilizza la versione 4 del protocollo IP (IPv4) che è una sequenza di 32 bit.
I bit vengono convertiti in decimali per poterli rendere leggibili da noi esseri umani.



Esiste anche la versione 6 del protocollo IP (IPv6). Esso è progettato per soddisfare la costante crescita dei dispositivi che comporta l'esaurimento degli indirizzi IPv4.
IPv6 è espresso in esadecimale ed è lungo 128 bit dando così un'enorme possibilità di combinazioni per poter creare degli indirizzi univoci.

Per ridurre l'esaurimento degli indirizzi IPv4, si è ricorsi alla **Classificazione delle reti** (Classful Networking).
Essa consiste nel suddividere le reti in 4 classi:
Classe A è composta dagli indirizzi IP che usano il primo ottetto per identificare la rete dando la possibilità di poter utilizzare gli altri 3 per identificare gli host riuscendo a identificare un gran numero di host.
Classe B è composta dagli indirizzi IP che usano i primi 2 ottetti per la rete e gli altri 2 per gli host. Questa classe viene spesso utilizzata da università o aziende di medie direzioni.
Classe C è composta dagli indirizzi IP che usano i primi 3 ottetti per la rete e l'ultimo per gli host. Questa classe è adatta per uso domestico dato che sono spesso presenti pochi host.
Classe D è una classe utilizzata per l'invio di pacchetti a più dispositivi contemporaneamente senza doverli duplicare (Multicast)
Classe E viene riservata per esperimenti di ricerca e non viene utilizzata su internet.

Classe	Primo otteto	Subnet Mask Default
A	1-126	255.0.0.0
B	128-192	255.255.0.0
C	192-223	255.255.255.0
D	224-239	N/A
E	240-255	N/A

La differenza tra Multicast, Broadcast, e Unicast è che con il Multicast i pacchetti vengono inviati a un gruppo di dispositivi, con il Broadcast i pacchetti vengono inviati a tutti i dispositivi all'interno di una rete e con Unicast i pacchetti vengono inviati ad un solo dispositivo nella rete.
Esiste anche un'altra categoria chiamata Anycast che invia il pacchetto al primo dispositivo che lo richiede.
Anycast (il primo che mi risposte)

Le porte
Una porta è un particolare codice che serve per indentificare le applicazioni specifiche o servizi in esecuzione su un particolare server.
Mentre l'indirizzo IP identifica la macchina di destinazione, la porta fornisce informazioni sul servizio specifico.
Categorie di porte
Well-Known: da 0 a 1023 e sono riservate per i server (http 80, https 443, FTP 21)
Registered: da 1024 a 49151 utilizzate per applicazioni e servizi registrati.
Dynamic or Private: da 49152 a 65535 utilizzate temporaneamente da applicazioni per comunicazioni private e dinamiche.

Subnet mask
La Subnet mask è un valore che indica quali bit di un indirizzo IP sono riservati alla rete e quali sono riservati agli host.
Nella Subnet Mask gli ottetti che hanno 255 sono quelli che non possono essere utilizzati per l'assegnazione degli host dato che vengono utilizzati per identificare in quale rete si trova.
La Subnet mask può essere scritta i tre modi:
-Decimale: 255.255.255.0
-CIDR: /24 (o sider)
-Binario: 11111111.11111111.11111111.00000000

Subnetting
Il Subnetting è una pratica usata per gestire meglio le reti creando delle sottoreti.
Questo permette di avere un migliore utilizzo di tutti gli indirizzi IP disponibili, facilita l'assegnazione degli indirizzi IP e migliora la sicurezza della rete isolando i segmenti di rete.
Per eseguire il Subnetting i bit utilizzati della Subnet non devono essere più di 32, dev'essere scelta una Subnet mask appropriata per gestire al meglio le sottoreti e successivamente si può eseguire il Subnetting della rete.

Come prima cosa dobbiamo convertire indirizzo IP da decimale a binario:
es.172.16.0.0 /22
172=10101100
16=00010000
0=00000000
0=00000000
Successivamente mettiamo "/22" numeri 1 partendo da sinistra e scopriremo la Sub. Mask:
11111111.11111111.11111100.00000000
Per trovare indirizzo di network dobbiamo fare un'operazione di AND logico tra i bit dell'indirizzo IP e i bit della Sub. mask:
10101100. 00010000.00000000.00000000 **(AND)** 11111111.11111111.11111100.00000000
10101100.00010000.00000000.00000000
Che riconvertendo in decimale avremo 172.16.0.0
Per l'indirizzo di gateway dobbiamo prendere indirizzo successivo a quello dell'indirizzo network:
172.16.0.1
Mentre per l'indirizzo di broadcast dobbiamo fare un'operazione di OR logico tra i bit dell'indirizzo IP e i bit della Sub. mask:
10101100. 00010000.00000000.00000000 **(AND)** 00000000. 00000000. 00000011.11111111
10101100.00010000.00000011.11111111
Che riconvertendo in decimale avremo 172.16.252.255
Quindi avremo 2 ottetti+6 bit per gli indirizzi network e 1 ottetto+2bit per gli indirizzi di host

VLAN
Le VLAN (Virtual Local Area Network) é una segmentazione virtuale di una rete in modo tale da avere diverse sottoreti senza però cambiare la configurazione fisica di tutta la rete. Questa configurazione è interamente gestita dagli switch di rete.
Le VLAN hanno molti benefici, tra cui la sicurezza, diminuzione del carico del traffico, gestione più semplice e flessibilità nella configurazione.

Esistono due tipi di VLAN
Acces port collegano dispositivi finali e appartengono a una singola VLAN.
Trunk Ports: Collegano gli switch tra lor e possono trasportare il traffico di più VLAN usando il tagging VLAN per identificare il traffico di ciascuna VLAN.
All'interno dei pacchetti di una VLAN viene inserito un tag che serve per riconoscere la VLAN stessa.
Per la configurazione delle VLAN, alcuni switch hanno due tipi di porte:
Access Ports che collegano i dispositivi finali come computer, stampanti, ecc.
Trunk Ports che servono per collegare due switch tra loro permettendogli di trasportare il traffico di più VLAN usando il tagging VLAN

Tipi di vlan
VLAN di default: ogni switch ha una VLAN di default a cui appartengono tutte le porte non configurate per altre VLAN.
VLAN di accesso: sono VLAN standard utilizzate per segmentare il traffico di rete. (reparto vendite/IT)
VLAN di Management: è dedicata alla gestione dei dispositivi di rete
VLAN di voce: specifiche per il traffico VoIP (Voice over IP) e generalmente hanno una priorità più alta per garantire la qualità di servizio
VLAN di Rete: utilizzate per il Routing tra VLAN diverse

VLAN
Le VLAN (Virtual Local Area Network) é una segmentazione virtuale di una rete in modo tale da avere diverse sottoreti senza però cambiare la configurazione fisica di tutta la rete. Questa configurazione è interamente gestita dagli switch di rete.
Le VLAN hanno molti benefici, tra cui la sicurezza, diminuzione del carico del traffico, gestione più semplice e flessibilità nella configurazione.

Esistono due tipi di VLAN
Acces port collegano dispositivi finali e appartengono a una singola VLAN.
Trunk Ports: Collegano gli switch tra lor e possono trasportare il traffico di più VLAN usando il tagging VLAN per identificare il traffico di ciascuna VLAN.
All'interno dei pacchetti di una VLAN viene inserito un tag che serve per riconoscere la VLAN stessa.
Per la configurazione delle VLAN, alcuni switch hanno due tipi di porte:
Access Ports che collegano i dispositivi finali come computer, stampanti, ecc.
Trunk Ports che servono per collegare due switch tra loro permettendogli di trasportare il traffico di più VLAN usando il tagging VLAN

Tipi di vlan
VLAN di default: ogni switch ha una VLAN di default a cui appartengono tutte le porte non configurate per altre VLAN.
VLAN di accesso: sono VLAN standard utilizzate per segmentare il traffico di rete. (reparto vendite/IT)
VLAN di Management: è dedicata alla gestione dei dispositivi di rete
VLAN di voce: specifiche per il traffico VoIP (Voice over IP) e generalmente hanno una priorità più alta per garantire la qualità di servizio
VLAN di Rete: utilizzate per il Routing tra VLAN diverse

NAT e PAT
NAT è una tecnica di traduzione degli indirizzi che va a modificare gli indirizzi IP da indirizzo privato a pubblico nel momento in cui dev'essere effettuata una connessione tra due dispositivi di due reti pubbliche diverse.
Questo é uno dei pochissimi momenti dove l'indirizzo IP viene modificato.
Esistono due tipi di NAT
Static NAT dove l'indirizzo IP di ogni dispositivo viene convertito in un altro IP pubblico sempre fisso.
È un tipo di traduzione 1:1 dove l'indirizzo IP pubblico non cambia mai.
Dynamic NAT mappa un IP privato secondo un range di indirizzi IP pubblici ogni volta che viene effettuata una comunicazione.
Il range di indirizzi si chiama "pool" e quando un dispositivo interno comunica con l'esterno, gli viene assegnato un IP pubblico libero dal pool e se il pool finisce, altri dispositivi non possono comunicare fino a quando un IP si libera.

PAT (Port Address Translation) é una tecnica di traduzione che funziona come il NAT ma viene utilizzato un solo inidirizzo io pubblico per ogni dispositivo presente nella rete interna differenziando le connessioni tramite le porte.

IP Privato	Traduzione in PAT
192.168.1.2	203.0.113.10 : 30001 → Web:80
192.168.1.3	203.0.113.10 : 30002 → Web:80