Livello di rete

Il livello di rete riguarda tutti i dispositivi intermedi presenti nella comunicazione end-to-end. Finora abbiamo parlato di livello applicativo e livello di trasporto, che erano incentrati esclusivamente nella macchina mittente e nella macchina destinazione, il livello di rete è il primo che si occupa invece della comunicazione verso tutti i dispositivi intermedi presenti nella rete.

Forwarding e Routing

Il forwarding è il processo di invio dei pacchetti di dati da un nodo della rete a un altro. In pratica, il forwarding viene effettuato dai dispositivi di rete come switch e router, che sono in grado di analizzare l'intestazione dei pacchetti e inoltrarli al nodo successivo nella catena di nodi intermedi . Il forwarding è un'operazione di tipo locale, in quanto viene eseguito solo tra i dispositivi adiacenti e non richiede una conoscenza completa della topologia della rete.

Il routing, al contrario, è il processo di determinazione del percorso migliore per i pacchetti attraverso la rete. Questo processo coinvolge l'analisi della topologia della rete, la valutazione di diverse metriche (ad esempio, la larghezza di banda disponibile, la congestione della rete e la qualità del servizio richiesta) e l'utilizzo di algoritmi di routing per determinare il percorso ottimale per i pacchetti. Il routing è un'operazione di tipo globale, in quanto richiede una conoscenza completa della topologia della rete e delle capacità di instradamento dei singoli dispositivi.

Data plane (Forwarding)

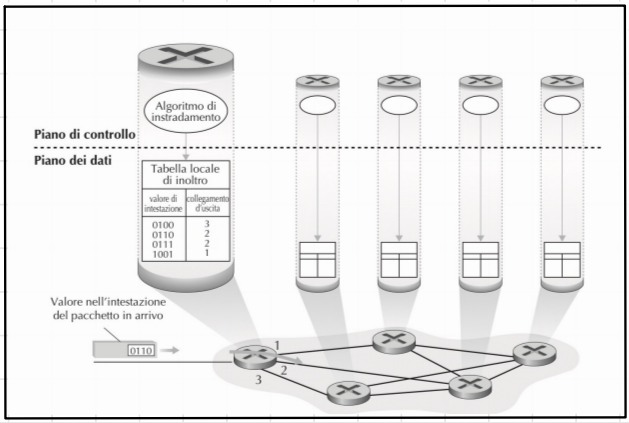
Il data plane viene eseguito dai dispositivi di rete come switch e router, che analizzano l'intestazione dei pacchetti e le informazioni contenute nella tabella di routing , ed inoltra i pacchetti attraverso la rete. Quando un pacchetto arriva in un dispositivo di rete, il data plane utilizza le informazioni nella tabella di routing per determinare il percorso migliore per inoltrare il pacchetto al nodo successivo nella catena di nodi intermedi. Il data plane è quindi responsabile dell'elaborazione e dell'inoltro dei pacchetti di dati attraverso la rete utilizzando il percorso più efficiente possibile.

Control plane (Routing)

Il control plane, invece, utilizza le regole di funzionamento generale della rete per determinare le configurazioni dei dispositivi di rete. Queste regole consentono al control plane di vedere la rete in senso globale, e di determinare il modo migliore per instradare i pacchetti attraverso la rete sulla base delle risorse disponibili.
Il control plane utilizza **algoritmi di routing** per analizzare la topologia della rete, le metriche di rete e le informazioni sullo stato della rete per determinare il percorso ottimale per i pacchetti attraverso la rete. In base a queste informazioni, il control plane determina le configurazioni dei dispositivi e le regole di funzionamento generale della rete, che vengono semplificate e inserite nella tabella di forwarding utilizzata dal data plane per inoltrare i pacchetti attraverso la rete. Il control plane utilizza informazioni come la disponibilità delle risorse (ad esempio, preferendo una scheda cablata rispetto a una wireless) per determinare l'uscita migliore per i pacchetti.

Control plane : approccio distribuito tradizionale

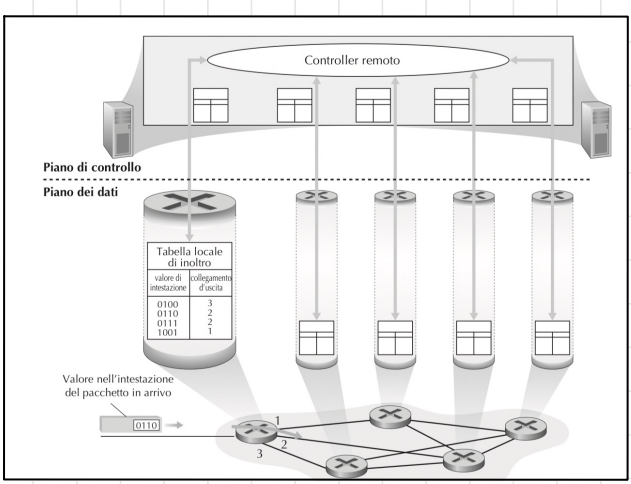
In questo approccio, l'algoritmo di routing è implementato in ogni router, che quindi svolge sia la funzione di inoltro che quella di instradamento internamente (non vi è una netta separazione tra piano dati e di controllo). In pratica, ogni dispositivo di rete (router, switch, etc.) ha il compito di prendere autonomamente le decisioni di instradamento del traffico sulla base dell'informazione di routing che ha a disposizione.
L'approccio a controllo distribuito prevede l'uso di protocolli di routing che consentono ai dispositivi di rete di scambiarsi informazioni sulle rotte disponibili. In questo modo, ogni dispositivo di rete può determinare autonomamente ed in modo decentralizzato il percorso migliore per instradare il traffico verso la destinazione desiderata.



Control plane : approccio SDN(softare defined network)

Questo approccio prevede una separazione tra il controllo della rete (control plane) e il trasferimento dei dati (data plane). SDN adotta un approccio a controllo centralizzato per il control plane, che consente di gestire la rete in modo più flessibile e dinamico rispetto ai tradizionali approcci a controllo distribuito.

Nell'approccio SDN, il control plane è centralizzato in un'entità software chiamata **controller**. Il controller gestisce la topologia della rete, raccogliendo informazioni dai dispositivi di rete (switch, router, etc.) attraverso un protocollo di comunicazione e decidendo come instradare il traffico sulla base delle politiche di rete definite dall'amministratore.
Il data plane, invece, è costituito dai dispositivi di rete (switch, router, etc.) che instradano il traffico sulla base delle istruzioni ricevute dal controller. I dispositivi di rete non devono avere funzionalità avanzate di routing, poiché la maggior parte delle decisioni di routing sono prese dal controller.



Servizio datagram e a circuito virtuale

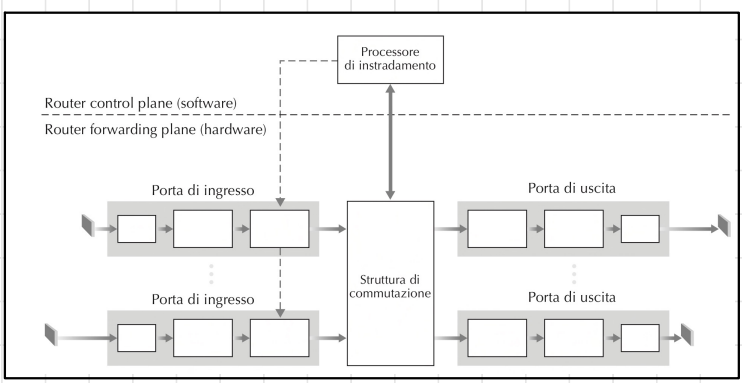
Il servizio datagram e il servizio a circuito virtuale rappresentano due approcci differenti per la gestione della comunicazione dati all'interno di una rete.

Il servizio datagram, utilizzato a livello di rete di Internet, mette a disposizione un servizio noto come **best-effort**, ossia "col massimo impegno possibile". Con questo servizio, non c'è garanzia che i pacchetti vengano ricevuti nell'ordine in cui sono stati inviati, così come non è garantita la loro eventuale consegna. Non c'è garanzia sul ritardo end- to-end, così come non c'è garanzia su una larghezza di banda minima. In questo caso, i pacchetti dati vengono inviati attraverso la rete senza un percorso prestabilito, e ogni nodo di rete prende le proprie decisioni di routing in base alle informazioni contenute nella tabella di instradamento. Tuttavia, questo approccio è facile da implementare e funziona bene se la probabilità di insuccesso nella trasmissione è bassa, cosa che viene garantita dall'hardware.

Il servizio a circuito virtuale è un approccio che prevede l'individuazione esatta delle macchine da attraversare per la comunicazione dati, e la riservazione di una porzione di banda per la durata della comunicazione stessa. In questo caso, un percorso prestabilito viene creato prima dell'inizio della comunicazione, e la banda viene divisa tra i vari utenti che utilizzano il circuito virtuale. Ciò garantisce un livello di affidabilità e prestazioni elevate, oltre alla possibilità di controllare la congestione della rete. Tuttavia, questo approccio richiede una maggiore complessità operativa e di gestione della rete.

Router

Un router è un dispositivo di rete che consente di instradare i pacchetti di dati tra diverse reti, utilizzando una tabella di routing per determinare il percorso migliore. Esso è fondamentale per il funzionamento di internet e delle reti aziendali, e può offrire anche funzionalità di sicurezza.



- **porte di ingresso**

Le porte di ingresso di un router rappresentano una parte fondamentale del dispositivo, in quanto consentono di ricevere i pacchetti di dati provenienti dalle diverse reti e instradarli verso la destinazione desiderata.
Nelle porte di input di un router, si ha un componente che lavora a livello data-link e che si occupa di ricevere i pacchetti di dati provenienti dalle diverse interfacce di rete. Successivamente, i dati ricevuti vengono bufferizzati per consentire una gestione efficiente del traffico, in quanto non è detto che i pacchetti vengano inoltrati con la stessa velocità con cui vengono ricevuti. Per instradare i pacchetti di dati verso la destinazione desiderata, i router utilizzano delle tabelle di routing, che suddividono i gruppi di pacchetti in base alla destinazione e assegnano loro le uscite predefinite.

Per assegnare un'uscita a un pacchetto in ingresso, si cerca una voce della tabella di inoltro con il prefisso di indirizzo più lungo che matcha all'indirizzo di destinazione.

Le porte di ingresso di un router quindi sono fondamentali per il funzionamento del dispositivo, poiché consentono di ricevere i pacchetti di dati dalle diverse interfacce di rete, bufferizzarli e instradarli verso la destinazione desiderata utilizzando le tabelle di routing.

Memorie associative CAM e TCAM

Le memorie associative CAM e TCAM (Content-Addressable Memory e Ternary Content-Addressable Memory) sono importanti componenti utilizzati nei router per la ricerca di informazioni all'interno delle tabelle di routing, in quanto consentono di effettuare ricerche molto rapide all'interno delle tabelle di routing, poiché sono in grado di confrontare l'intero indirizzo IP di un pacchetto di dati con gli indirizzi presenti nella tabella di routing in modo simultaneo.
Le CAM sono utilizzate per la ricerca di informazioni esatte all'interno della tabella di routing, mentre le TCAM consentono di effettuare ricerche parziali utilizzando maschere di bit, permettendo di individuare i percorsi di routing per più destinazioni contemporaneamente. Le memorie associative rendono possibile l'elaborazione di un alto volume di pacchetti di dati in tempo costante.

- **struttura di commutazione**

Dopo l'arrivo dei pacchetti nella parte di input del router, segue un meccanismo che sposta i pacchetti nella coda di uscita corretta, precedentemente identificata. Questo meccanismo di commutazione può utilizzare diverse architetture, tra cui la memoria condivisa, il bus condiviso e la rete di interconnessione.

Nella architettura della **memoria condivisa**, i pacchetti di dati che arrivano in ingresso al router vengono salvati in memoria e successivamente letti dalla memoria per essere instradati verso la porta di uscita corretta. Tuttavia, questa architettura può essere molto lenta in quanto richiede molti accessi alla memoria, ma è facile da implementare.

Nella architettura del **bus condiviso**, i pacchetti di dati vengono bufferizzati nelle code di ingresso e uscita, eliminando la necessità di accedere alla memoria. In questo modo, il router può gestire un traffico di dati più elevato rispetto alla memoria condivisa. Tuttavia, questa architettura richiede un bus più robusto per garantire la corretta gestione del traffico.

Nella architettura della **rete di interconnessione**, i pacchetti di dati possono essere instradati verso diverse porte di uscita selezionate per gestire l'inoltro dei pacchetti. In questo modo, si possono selezionare diverse porte di ingresso e uscita per gestire l'inoltro dei pacchetti. Tuttavia, questa architettura può essere più complicata da implementare e richiedere costi maggiori. Inoltre, non è possibile instradare pacchetti di diverse porte di input sulla stessa uscita.

Organizzando molti più piani di commutazione parallelamente, è possibile organizzare le connessioni su più porte in ingresso e instradarle con una velocità molto più elevata, ma a fronte di un maggiore costo. La scelta dell'architettura dipende dalle specifiche esigenze di prestazioni, costi e scalabilità del router.

- **Porte di uscita** : memorizzano i pacchetti che provengono dalla struttura di commutazione e li trasmettono sul collegamento in uscita, operando le funzionalità necessarie del livello di collegamento e fisico.

- **Processore di instradamento** (routing processor) : segue le funzioni del piano di controllo. Nei router tradizionali, esegue i protocolli di instradamento, gestisce le tabelle di inoltro e le informazioni sui collegamenti attivi, ed elabora la tabella di inoltro per il router. Nei router SDN, il processore di instradamento è responsabile della comunicazione con il controller remoto, in modo da ricevere le occorrenze della tabella di inoltro e installarle alle porte di ingresso.

Se la memoria del router è eccessiva rispetto al traffico di dati gestito, i pacchetti di dati molto probabilmente non andranno persi, ma potrebbero subire un aumento dei tempi di attesa e creare congestione. Inoltre, aumentando la capacità della memoria del router, i pacchetti di dati vengono bufferizzati per un periodo di tempo più lungo.

La formula che spiega quanto bufferizzare in relazione alla capacità di rete è :

$$\text{Buffering} = \frac{RTT \cdot C}{\sqrt{N}} \rightarrow bit/s$$

- **RTT** rappresenta il ritardo di andata e ritorno (Round Trip Time), ovvero il tempo necessario per un pacchetto di dati per viaggiare dalla sorgente alla destinazione e ritornare indietro.
- **C** rappresenta la capacità del link di rete, ovvero la quantità massima di dati che il link può trasferire in un'unità di tempo (ad esempio, in bit al secondo).
- **N** rappresenta il numero di flussi di dati presenti nella rete.

La formula indica che il buffering necessario per gestire correttamente i flussi di dati dipende dal prodotto tra il RTT e la capacità del link di rete, diviso per la radice quadrata del numero di flussi presenti nella rete. In altre parole, maggiore è il RTT e la capacità del link, maggiore sarà il buffering necessario per gestire i flussi di dati.

Tuttavia, è importante notare che troppo buffering può causare congestione di rete e aumentare i ritardi, in particolare per le applicazioni in tempo reale. Pertanto, la scelta del valore di buffering dipende dalle specifiche esigenze della rete e del tipo di applicazioni che viaggiano sulla rete stessa.

Smaltimento dei buffer

Dato che la porta di uscita può trasmettere un solo pacchetto in un intervallo prestabilito (tempo di trasmissione del pacchetto), i pacchetti in arrivo dovranno mettersi in coda per la trasmissione sul collegamento in uscita. In assenza di sufficiente memoria per inserire nel buffer il nuovo pacchetto in ingresso, occorrerà stabilire se scartarlo o se rimuoverne uno o più, fra quelli già in coda, per far posto al nuovo arrivato.

Si utilizzano degli algoritmi per prendere la scelta sul pacchetto da scartare :

FCFS (First-Come, First-Served) è un altro algoritmo utilizzato per la gestione dei pacchetti in una rete. Questo algoritmo gestisce i pacchetti in ordine di arrivo, ovvero il primo pacchetto che arriva viene trasmesso per primo. L'algoritmo FCFS è molto semplice ed efficiente, poiché non richiede alcun tipo di ordinamento dei pacchetti. Tuttavia, questa politica di gestione dei pacchetti può portare a problemi di congestione di rete in situazioni di traffico intenso.

RED (Random Early Detection) prevede la gestione delle code di I/O sui router con un modello FIFO. Quando il buffer di una coda raggiunge il 75% della sua capienza, alcuni pacchetti vengono eliminati in modo "casuale" per prevenire la saturazione del buffer e i pacchetti vengono quindi trasmessi nello stesso ordine con cui sono arrivati in coda.
In questo modo, si evita che TCP saturi i buffer e rallenti l'invio dei pacchetti, utilizzando strategie di controllo congestione messe in atto da TCP Tahoe o Reno. La politica RED è particolarmente utile per evitare la congestione di rete in situazioni di traffico intenso.

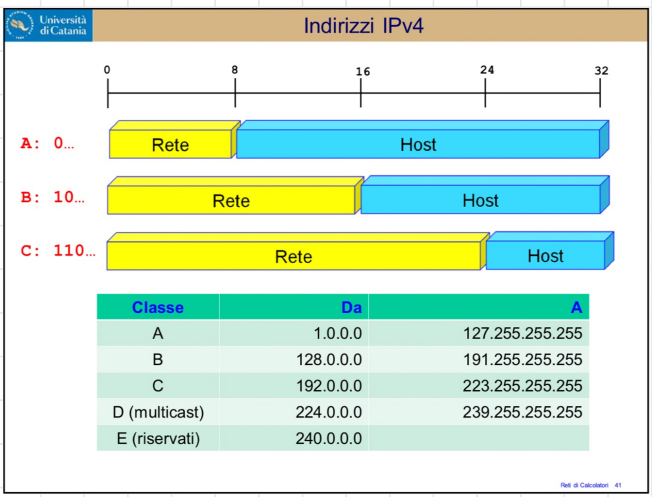
RR (Round Robin), invece, scandisce le code di bufferizzazione e le gestisce tutte in parallelo, inviando un pacchetto per ciascuna coda. Questa politica permette di gestire in modo più efficiente il traffico di dati e prevenire la congestione di rete, garantendo una distribuzione equa del traffico su tutte le code di bufferizzazione. Tuttavia, la politica RR richiede una maggiore complessità nell'implementazione rispetto alla politica RED.

IPv4 (internet protocol versione 4)

Il pacchetto a livello di rete è noto come datagramma. IPv4 è un protocollo di rete utilizzato per l'instradamento dei pacchetti di dati su Internet. Gli indirizzi IPv4 sono composti da 32 bit, divisi in quattro ottetti da 8 bit ciascuno. Questi indirizzi sono suddivisi in classi di indirizzi, che sono gruppi di indirizzi utilizzati nelle tabelle di routing.

- **Classi di indirizzi IP**

Le classi di indirizzi IPv4 sono A, B, C, D ed E. Ogni classe di indirizzi ha una diversa lunghezza della parte di rete e della parte di host. La parte esplicita dell'indirizzo identifica la rete, mentre la parte con gli asterischi identifica l'host. Nella classe A, il primo ottetto identifica la rete, mentre gli ultimi tre ottetti identificano l'host. Nella classe B, i primi due ottetti identificano la rete, mentre gli ultimi due ottetti identificano l'host. Nella classe C, i primi tre ottetti identificano la rete, mentre l'ultimo ottetto identifica l'host. Le classi di indirizzi D e E, utilizzate per scopi speciali come la multicast e la sperimentazione.



Classe	Da	A
A	1.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D (multicast)	224.0.0.0	239.255.255.255
E (riservati)	240.0.0.0	

Reti di Calcolatori 41

Il formato dei datagrammi IPv4 sono formati da un **header di 20byte** a meno di eventuali campi opzionali . La memoria associativa TCAM sfrutta la lunghezza dell'header per cercare match nelle tabelle di inoltro, informazione riportata nel campo "lunghezza dell'intestazione".
L'intestazione di un pacchetto IPv4 contiene diverse informazioni che vengono utilizzate dai nodi intermedi per instradare il pacchetto attraverso la rete. L'intestazione contiene i seguenti campi:

- Versione: indica la versione del protocollo IPv4 utilizzata ("4").
- Lunghezza dell'intestazione: indica la lunghezza dell'intestazione in parole da 32 bit. Questo campo può variare a seconda dei campi opzionali presenti nell'intestazione ma solitamente è di 20 byte a meno di campi opzionali.
- Tipo di servizio: fornisce informazioni sul tipo di servizio richiesto per il pacchetto, ad esempio la priorità e la qualità del servizio (QoS) richiesta.
- Lunghezza totale: indica la lunghezza totale del pacchetto (intestazione e payload) in byte.
- Identificativo, flag e offset di frammentazione: questi campi vengono utilizzati per gestire i pacchetti che sono troppo grandi per essere trasmessi in un'unica volta attraverso la rete e devono essere frammentati in pacchetti più piccoli.
- Tempo di vita (TTL): indica il numero massimo di nodi intermedi attraverso i quali il pacchetto può essere instradato prima di essere scartato.
- Protocollo: indica il protocollo di livello superiore utilizzato dal pacchetto (ad esempio TCP o UDP).
- Checksum dell'intestazione: viene utilizzato per verificare l'integrità dell'intestazione.
- Indirizzo IP di origine e destinazione: indicano gli indirizzi IP del mittente e del destinatario del pacchetto.

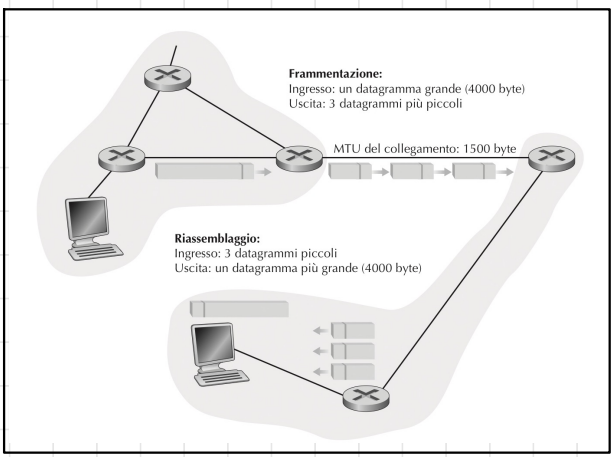
Il carico utile (payload) di un pacchetto IPv4 contiene i dati effettivi che vengono trasmessi dal mittente al destinatario. In generale, i pacchetti IPv4 vengono trasmessi attraverso la rete in modo indipendente gli uni dagli altri e possono seguire percorsi diversi. La loro elaborazione e instradamento sono gestiti dai nodi intermedi della rete, che utilizzano le informazioni contenute nell'intestazione per determinare il percorso migliore per il pacchetto.

Frammentazione

Nella gestione dei pacchetti di dati su Internet, spesso è necessario suddividere un pacchetto grande in unità separate, adattando la loro dimensione all'MTU (Maximum Transmission Unit) del collegamento. Questo processo è noto come frammentazione del pacchetto.

Per effettuare la frammentazione del pacchetto, si suddivide il pacchetto in unità separate, ma aventi lo stesso ID, in modo da identificare che appartengono allo stesso pacchetto originale. Inoltre, si utilizza un campo offset per identificare di quanto è sfasata rispetto all'origine la posizione del pacchetto.Tuttavia, se si perde un frammento di un pacchetto, è necessario reinviare l'intero pacchetto. Ogni frammento ha anche un flag more fragments, che indica se ci sono altri frammenti dopo o se è l'ultimo frammento del pacchetto. Questo sistema fornisce flessibilità, in quanto un frammento può essere a sua volta frammentato. Alcuni pacchetti, tuttavia, non necessitano di essere frammentati, e l'informazione relativa è contenuta in un campo don't fragment.

In IPv4 qualsiasi router di transito può frammentare un pacchetto, ciò non avviene in IPv6.



Indirizzamento

Generalmente un host ha un solo collegamento con la rete e quando l'host vuole inviare un datagramma, lo fa su tale collegamento. Il confine tra host e collegamento fisico viene detto interfaccia. Invece, dato che il compito di un router è ricevere datagrammi da un collegamento e inoltrarli su un altro, questo deve necessariamente essere connesso ad almeno due collegamenti e anche il confine tra un router e i suoi collegamenti è chiamato interfaccia. Il router presenta più interfacce, una su ciascuno dei suoi collegamenti. Dato che host e router sono in grado di inviare e ricevere datagrammi, IP richiede che tutte le interfacce abbiano un proprio indirizzo IP. Pertanto, l'indirizzo IP è tecnicamente associato a un'interfaccia, anziché all'host o al router che la contiene.

Gli indirizzi IP sono lunghi 32 bit (4 byte) e quindi ci sono in totale 2^32 indirizzi IP, cioè circa 4 miliardi.
L'indirizzo 193.32.216.9 in notazione binaria diventa :

11000001 00100000 11011000 00001001

Ogni interfaccia di host e router di Internet ha un indirizzo IP globalmente univoco (eccetto quelle gestite da NAT)

Indirizzi Gerarchici (geografici)

Gli indirizzi IPv4 sono composti da 32 bit e sono assegnati in modo gerarchico, fornendo informazioni sulla posizione geografica del dispositivo. Le cifre dell'indirizzo seguono una gerarchia, che identifica la rete e l'host. Questo tipo di indirizzamento è utile per instradare i pacchetti di dati su Internet, in quanto fornisce informazioni sulla strada da seguire per arrivare alla destinazione.

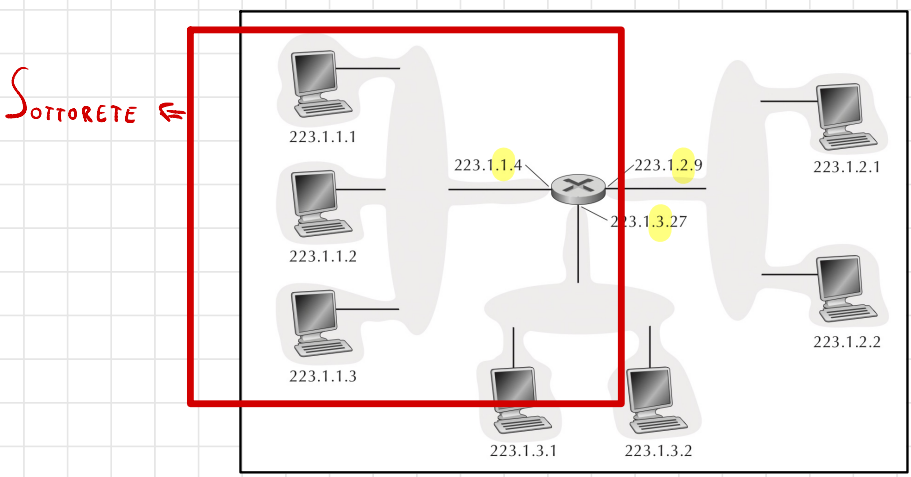
Indirizzi Flat

Sono indirizzi che non forniscono informazioni sulla posizione della destinazione. Questo tipo di indirizzamento è utile in contesti in cui non è necessario conoscere la posizione geografica del dispositivo, come ad esempio in reti locali (MAC).

Classful adressing e CIDR

La strategia di assegnazione degli indirizzi Internet è detta classless interdomain routing CIDR. Prima dell'adozione di CIDR, le parti di rete di un indirizzo IP dovevano essere lunghe 8, 16 o 24 bit. Tale schema di indirizzamento era noto come classful addressing e le sottoreti con indirizzi di sottorete da 8, 16 e 24 bit erano note rispettivamente come reti di classe A, B e C. Il requisito che la parte di sottorete di un indirizzo IP fosse lungo esattamente 1, 2 o 3 byte si rivelò problematico. Una sottorete di classe C (/24) poteva ospitare solo fino a 2^8 – 2 = 254 host (due dei 256 indirizzi sono riservati per usi speciali): troppo pochi per molte organizzazioni.

Se specifico un numero come 25 verranno utilizzati i primi 25 bit dell'indirizzo IP per indicare la subnet mask, mentre i rimanenti 7 bit saranno usati per indicare gli host disponibili (da 0 a 127). Questo schema è un metodo per suddividere gli indirizzi IP allo scopo di allocarli con il minimo spreco possibile, infatti si possono specificare numeri di bit variabili e non interi blocchi da 8 bit . Si ottiene quindi un'ottimizzazione dello spazio di indirizzamento.



Per IP, la rete che interconnette le tre interfacce di host e l'interfaccia di un router forma una sottorete. IP assegna a questa sottorete l'indirizzo 223.1.1.0/24, dove la notazione /24, detta anche maschera di sottorete (subnet mask), indica che i 24 bit più a sinistra dell'indirizzo definiscono l'indirizzo della sottorete. Di conseguenza, la sottorete **223.1.1.0/24** consiste di tre interfacce di host (223.1.1.1, 223.1.1.2, 223.1.1.3) e di un'interfaccia di router (223.1.1.4). Ogni altro host connesso alla sottorete 223.1.1.0/24 deve avere un indirizzo della forma 223.1.1.xxx.

Subnetting

Una subnet mask rappresenta un'organizzazione fisica delle classi di indirizzi all'interno della stessa LAN, che consente di suddividere la rete in sotto-reti. Un indirizzo IPv4 è un campo a 32 bit, che può essere suddiviso in due parti: la parte di rete e la parte di host. La subnet mask identifica quanti bit, di un indirizzo IP, vengono utilizzati per identificare la rete e sono detti bit fissi, in quanto sono uguali per tutti gli host all'interno della stessa rete. Tutti gli altri bit sono detti variabili e servono ad identificare l'host.

La scelta dell'utilizzo di una subnet mask dipende dalle specifiche esigenze della rete e dei dispositivi connessi. La suddivisione della rete in sotto-reti consente di ottimizzare il routing dei pacchetti di dati su Internet, migliorando l'efficienza e la sicurezza della rete.

La subnet mask viene indicata dopo l'indirizzo IP attraverso /N, dove N è il numero di bit che identificano la rete di appartenenza :

192.168.1.7 / 24 - solo i primi 24 bit identificano la rete di appartenenza
- i rimanenti 8 indicano l' host

infatti la traduzione binaria della maschera è la seguente :

01100000 . 01011010 . 00000001 . 00000111 **IP**

11111111 . 11111111 . 11111111 . 00000000 **subnet mask** **host (da 0 a 2^8)**

Indirizzi speciali

Alcuni indirizzi speciali non possono essere utilizzati per configurare host all'interno di una rete :

L'indirizzo **0.0.0.0** viene utilizzato come indirizzo di default o indirizzo di "tutti gli indirizzi" in alcune situazioni. Ad esempio, un dispositivo potrebbe utilizzare l'indirizzo 0.0.0.0 come indirizzo IP sorgente quando invia un pacchetto su una rete se non ha ancora un indirizzo IP assegnato.

L'indirizzo **255.255.255.255**, noto anche come indirizzo di broadcast limitato, viene utilizzato per inviare pacchetti di broadcast a tutti i dispositivi nella stessa rete locale. Quando un dispositivo invia un pacchetto a questo indirizzo, il pacchetto viene trasmesso a tutti i dispositivi nella rete locale.

In alcuni casi particolari, come quando sono presenti solo due router agli estremi di un collegamento senza alcuna macchina intermedia, è possibile utilizzare una subnet mask con **prefisso /31**. In questo caso, non è necessario considerare gli indirizzi di broadcast e l'intera rete, poiché tutti i bit sono utilizzati per identificare gli host.

Configurazione delle reti

Se viene cambiato l'IP ad una macchina questa non farà più parte della rete. Se vengono numerate diversamente un numero di macchine esse possono comunicare tra loro ma non con la rete. Si possono mettere due indirizzi IP alla stessa scheda di rete con lo scopo di far comunicare delle macchine isolate con la rete .

NB un indirizzo IP è associato ad una sola scheda di rete ma ad una scheda di rete posso associare più indirizzi IP.