

Livello di rete

Dopo aver visto il livello di trasporto, possiamo scendere al livello di rete. Il livello di trasporto si occupa della comunicazione logica tra processi applicativi, mentre il livello di rete si occupa di indirizzare e instradare i pacchetti tra host e reti diverse attraverso il percorso di rete più appropriato.

importante specificare che un router, nel suo funzionamento principale, utilizza soprattutto i primi tre livelli della pila di rete: fisico, link e rete.

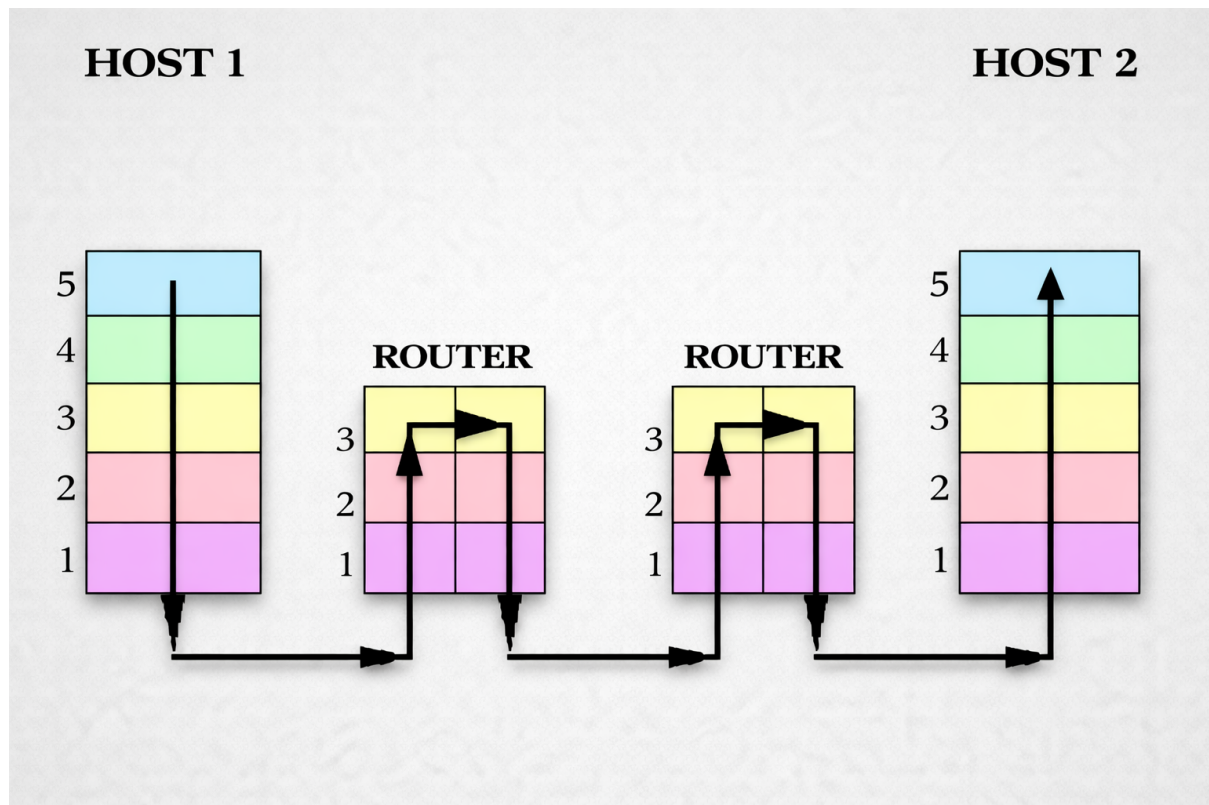
Il motivo è che il router non deve interpretare il contenuto applicativo della comunicazione, per esempio una pagina web, una email o un file. Il suo compito è più limitato: ricevere un pacchetto da un'interfaccia di rete, leggere le informazioni del livello di rete, in particolare l'indirizzo di destinazione, e decidere da quale interfaccia inoltrarlo.

Per svolgere questo compito, il router ha bisogno:

- Del livello fisico, per trasmettere e ricevere segnali sul mezzo di comunicazione.
- Del livello link, per comunicare con i dispositivi direttamente collegati sulla stessa rete locale.
- Del livello di rete, per leggere gli indirizzi e scegliere il percorso verso la destinazione.

I livelli superiori, cioè trasporto e applicazione, sono invece necessari soprattutto negli host finali, perché lì si trovano i programmi che comunicano tra loro, come browser, server web, app di messaggistica o client email.

Nota: alcuni router moderni possono analizzare anche informazioni più 'in alto' (porte, protocolli applicativi) per sicurezza e gestione.



La rete Internet è basata di fatto su un protocollo non affidabile e connectionless, **Internet Protocol** (abbreviato *IP*).

Esso è un protocollo a pacchetti di tipo **best effort** che indica un servizio per il quale non esistono garanzie sulla consegna, sul tempo impiegato tra invio e ricezione, né sulla qualità e l'integrità del servizio stesso durante la fase di trasmissione (questi attributi di qualità vengono implementati nel livello di trasporto come abbiamo visto).

Il fatto che *IP* sia best effort non significa che sia inutile o progettato male. Significa che *IP* svolge un compito preciso: provare a consegnare i pacchetti alla destinazione. Se servono affidabilità, riordino o ritrasmissione, questi aspetti vengono gestiti da altri protocolli, come *TCP*, oppure direttamente dall'applicazione.

Come appena detto, il principale compito di *IP* è l'indirizzamento e l'instradamento tra sottoreti eterogenee, che a livello locale utilizzano invece un indirizzamento proprio, tipicamente basato sull'indirizzo *MAC*.

Per permettere a reti diverse di comunicare tra loro, è necessario usare un sistema di indirizzamento comune. Questo sistema è fornito dal **protocollo IP**.

Ogni dispositivo collegato a una **rete IP** (una rete che usa il protocollo *IP*) deve avere un **indirizzo IP**, cioè un identificatore logico usato per raggiungerlo nella rete.

L'indirizzo *IP* permette di indicare il mittente e il destinatario di un pacchetto, anche quando si trovano in reti diverse.

L'indirizzo *IP* ha quindi un ruolo diverso dall'indirizzo *MAC*:

- L'indirizzo *MAC* viene usato nella comunicazione locale, cioè all'interno della stessa rete fisica o locale.

- L'indirizzo IP, invece, viene usato per instradare i pacchetti tra reti diverse.

Quando un pacchetto deve raggiungere una destinazione lontana, attraversa diversi router. Ogni router legge l'indirizzo *IP* di destinazione e decide verso quale rete o verso quale router successivo inoltrare il pacchetto.

Questa procedura prende il nome di **routing**, o instradamento. Il routing è l'insieme delle regole e dei meccanismi che permettono ai pacchetti di trovare un percorso attraverso reti diverse fino alla destinazione.

Il pacchetto che si forma con il protocollo *IP* si chiama **pacchetto IP**.

Esempio

Quando un computer della rete di casa vuole raggiungere un server web su Internet, il pacchetto IP contiene l'indirizzo IP del mittente e l'indirizzo IP del destinatario.

Il router di casa inoltra il pacchetto verso la rete dell'operatore. Da lì, altri router leggono l'indirizzo IP di destinazione e decidono, passo dopo passo, quale percorso far seguire al pacchetto.

Internet si chiama anche **rete TCP/IP** perché si basa principalmente su questi due protocolli fondamentali: *TCP* e *IP*:

- *IP* si occupa di indirizzare i pacchetti e farli arrivare da un dispositivo all'altro attraverso la rete.
- *TCP* si occupa di rendere la comunicazione affidabile, controllando che i dati arrivino correttamente e nell'ordine giusto.

Il nome *TCP/IP* indica quindi l'insieme di protocolli che permette ai computer di comunicare su Internet e su molte reti locali moderne.

Indirizzo IP

Un **indirizzo IP**, acronimo di "Indirizzo Protocollo Internet" (Internet Protocol address), è un numero univoco assegnato a ogni dispositivo collegato alla rete Internet.

Questo indirizzo consente di identificare in modo univoco l'interfaccia di rete su Internet e permette il corretto instradamento dei dati da e verso il dispositivo.

Gli indirizzi *IP* possono essere di due versioni principali:

- **IPv4** (Versione 4)
- **IPv6** (Versione 6)

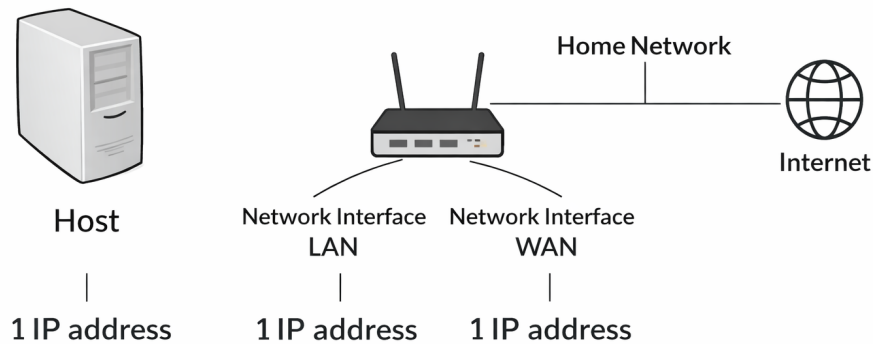
La versione storicamente più diffusa è *IPv4*, che usa indirizzi di 32 bit. A causa della crescita di Internet, lo spazio degli indirizzi *IPv4* si è progressivamente esaurito.

Per questo è stato introdotto *IPv6*, che usa indirizzi di 128 bit e offre uno spazio di indirizzamento enormemente più ampio.

E' importante specificare che l'indirizzo *IP* non si riferisce all'host ma alla sua interfaccia di rete. Per esempio:

- Un host con una sola scheda di rete (ad esempio solo Wi-Fi) avrà un solo *IP*.

- I router che collegano più linee (per esempio un router domestico ha di solito almeno due interfacce logiche: una verso la rete locale di casa e una verso la rete dell'operatore Internet) hanno due interfacce di rete e quindi due *IP*.



Ma perchè esistono gli indirizzi *IP* se esistono gli indirizzi *MAC*?

Gli indirizzi *IP* sono necessari per l'instradamento globale, mentre i *MAC* sono limitati alla rete locale.

Sotto le motivazioni:

- Scalabilità e organizzazione: Gli indirizzi *IP* sono organizzati in gerarchie, il che li rende scalabili e adatti a grandi reti come Internet. Gli indirizzi *MAC*, d'altra parte, sono assegnati ai singoli dispositivi dai produttori e non seguono una struttura gerarchica, il che li rende meno adatti per organizzare una rete su larga scala.
- Indipendenza dalla rete fisica: il protocollo *IP* può funzionare sopra tecnologie diverse, come Ethernet, Wi-Fi, fibra o rete mobile.
- Flessibilità: Gli indirizzi *IP* possono essere assegnati dinamicamente il che semplifica la gestione delle reti in cui i dispositivi si uniscono e lasciano la rete. Gli indirizzi *MAC* sono assegnati staticamente dai produttori dei dispositivi.

Gli indirizzi *IP* possono essere:

- statici
- dinamici

Indirizzo *IP* statico

Un indirizzo *IP* statico è un indirizzo configurato in modo stabile su un dispositivo o assegnato in modo fisso da un amministratore di rete o da un ISP.

Questo tipo di indirizzo è fisso e costante, il che significa che il dispositivo avrà sempre lo stesso indirizzo *IP* ogni volta che si connette alla rete. Gli indirizzi *IP* statici sono spesso

utilizzati per server, dispositivi di rete critici e dispositivi che devono essere sempre raggiungibili tramite lo stesso indirizzo.

Indirizzo IP dinamico

Un indirizzo *IP* dinamico è un indirizzo assegnato temporaneamente a un dispositivo ogni volta che si connette alla rete.

Gli indirizzi *IP* dinamici sono gestiti da un server *DHCP* (Dynamic Host Configuration Protocol), che assegna automaticamente indirizzi *IP* ai dispositivi in base a una insieme di indirizzi disponibili.

Questi indirizzi possono cambiare ogni volta che il dispositivo si ricollega alla rete o dopo un certo periodo di tempo.

Gli indirizzi *IP* dinamici sono spesso utilizzati per dispositivi domestici e utenti comuni, poiché permettono di usare in modo più efficiente gli indirizzi disponibili: se un dispositivo non è collegato alla rete, il suo indirizzo può tornare disponibile ed essere assegnato ad altri dispositivi.

Da questo [sito](#) si può vedere l'indirizzo IP del vostro dispositivo e se notate che in giornate diverse il vostro *IP* cambia è perché il vostro *IP* è dinamico.

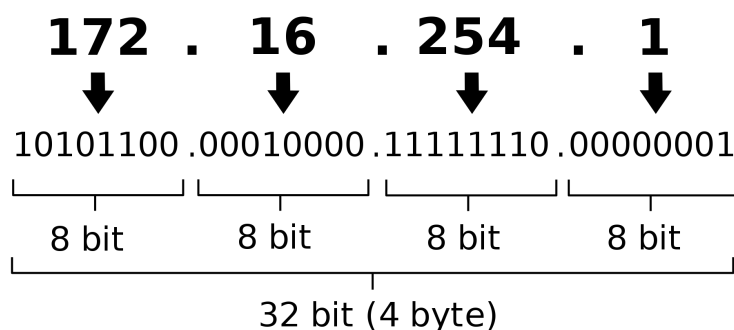
Gli indirizzi *IP* pubblici sono assegnati in blocchi dai **RIR** (Regional Internet Registries). Gli *ISP* ottengono questi blocchi e li distribuiscono ai propri clienti, siano essi aziende, organizzazioni o utenti domestici.

Per ottimizzare l'uso degli indirizzi disponibili, gli *ISP* assegnano spesso *IP* dinamici.

IPV4

L'indirizzo IPv4 è costituito da 32 bit (quattro byte) suddiviso in quattro gruppi da 8 bit (un byte), separati ciascuno da un punto (esempio: 11001001.00100100.10101111.00001111). Ciascuno di questi quattro byte può essere convertito in formato decimale per rendere più facile l'identificazione.

Indirizzo IPv4 in notazione decimale puntata



Ogni byte varia tra 0 e 255 essendo $2^8 = 256$, ovvero le combinazioni disponibili di un numero di 8 bit

Per questo un indirizzo IPv4 viene scritto come quattro numeri decimali separati da punti, per esempio 192.168.1.10.

Nello standard *IPv4*, essendo costituito interamente da 32 bit, le combinazioni utilizzabili sono 2^{32} pari a circa 4 miliardi.

All'inizio questo numero sembrava enorme, ma con la crescita di Internet gli indirizzi *IPv4* pubblici sono diventati insufficienti.

Oggi ogni persona può usare molti dispositivi connessi, come smartphone, computer, tablet, smart TV e dispositivi IoT.

Per ridurre il consumo di indirizzi pubblici sono state introdotte soluzioni come gli indirizzi privati, mentre *IPv6* nasce per offrire uno spazio di indirizzamento molto più ampio.

Indirizzo privato e pubblico

Un **indirizzo IP privato** è un indirizzo *IP* assegnato a un dispositivo all'interno di una rete locale, come una rete domestica o aziendale, e non è direttamente accessibile o indirizzabile su Internet.

Un **indirizzo IP pubblico** è un indirizzo instradabile su Internet. Questo significa che può essere usato per identificare un dispositivo o un router nella rete globale e può essere raggiunto da altri host su Internet, se firewall e configurazioni lo permettono.

Gli indirizzi IP privati funzionano all'interno delle reti locali.

Quando un dispositivo deve comunicare con Internet, il router traduce il suo indirizzo IP privato in un indirizzo IP pubblico. In questo modo, più dispositivi della stessa rete locale possono condividere un unico indirizzo IP pubblico, senza bisogno di avere un indirizzo pubblico diverso per ciascuno.

Quindi, avere indirizzi privati porta questi vantaggi:

- Risparmio di indirizzi IP pubblici: Gli indirizzi *IP* pubblici sono limitati e costosi. Utilizzando indirizzi *IP* privati all'interno di una rete locale, si può ridurre la necessità di richiedere un gran numero di indirizzi *IP* pubblici per un'unica sottorete. Questo è particolarmente utile nelle reti in cui molti dispositivi sono solo utilizzati all'interno dell'ambito locale e non necessitano di una connessione diretta a Internet.
- Sicurezza: L'uso di indirizzi privati offre anche una forma di isolamento, perché i dispositivi interni non sono direttamente raggiungibili da Internet.

Grazie a questa tecnica gli *ISP* solitamente assegnano un solo indirizzo *IP* pubblico per ogni utente anche se egli ha decine di device che si collegano a Internet.

Quindi ricapitoliamo:

- Io, utente, ricevo dal mio *ISP* un indirizzo *IP* pubblico (probabilmente dinamico).
- Invece i miei dispositivi usano tanti indirizzi *IP* privati che poi quando dovranno comunicare in Internet verranno convertiti nel mio *IP* pubblico.

Esempio

Immagina di avere una rete domestica con più dispositivi, tra cui computer, telefoni cellulari, stampanti e smart TV. Tutti questi dispositivi si collegano a un router *Wi-Fi* per accedere a Internet.

In questa situazione, il router assegnerà a ciascun dispositivo un indirizzo *IP* privato dall'intervallo di indirizzi *IP* privati (ad esempio, 192.168.1.2, 192.168.1.3, ecc.).

Quando uno di questi dispositivi accede a Internet, il router traduce l'indirizzo *IP* privato del dispositivo in un singolo indirizzo *IP* pubblico assegnato dall'*ISP*.

Questo indirizzo *IP* pubblico è ciò che i server su Internet vedono quando il dispositivo invia richieste.

Esempio pratico:

- Un computer nella tua rete domestica tenta di accedere a un sito web.
- Il computer utilizza il suo indirizzo *IP* privato (ad esempio, 192.168.1.2) per comunicare con il router.
- Il router traduce l'indirizzo *IP* privato del computer in un indirizzo *IP* pubblico assegnato dal tuo *ISP* (ad esempio, 203.45.67.89).
- La richiesta del computer raggiunge il server del sito web con l'indirizzo *IP* pubblico 203.45.67.89.
- Il server invia la risposta al router, che utilizza le informazioni per tradurre l'indirizzo pubblico all'indirizzo privato corretto per inoltrare la risposta al computer all'interno della rete locale.

Ma come fa esattamente il router a trasformare un *IP* privato in pubblico (o viceversa)?

Il NAT (Network Address Translation) è una tecnica che consente a più dispositivi di una *LAN* di condividere un unico indirizzo *IP* pubblico quando si collegano a Internet.

Quando un dispositivo della *LAN* invia una richiesta verso Internet usando il suo *IP* privato, il *NAT* del router interviene in questo modo:

- Sostituisce l'*IP* privato con l'*IP* pubblico del router, perché un *IP* privato non è instradabile su Internet.
- Cambia anche la porta sorgente con una porta temporanea scelta dal router (per distinguere le varie connessioni).
- Salva queste informazioni in una "tabella NAT", dove associa la nuova porta pubblica alla connessione originaria (*IP* privato + porta privata dell'host).
- Inoltra il pacchetto al server destinatario, usando l'*IP* pubblico e la porta appena generata.

Quando il server risponde, invia il pacchetto all'*IP* pubblico del router e alla porta usata dal *NAT*. A questo punto:

- Il router consulta la tabella *NAT*: trova quale host interno aveva avviato quella connessione.
- Traduce l'indirizzo di destinazione, sostituendo l'*IP* pubblico e la porta con i valori originali dell'host (*IP* privato + porta privata).
- Inoltra la risposta al dispositivo corretto all'interno della *LAN*.

Nota: Nel linguaggio comune si parla spesso semplicemente di *NAT*. Però ora abbiamo descritto una variante evoluta del *NAT*: questa variante è chiamata più precisamente *PAT* o *NAPT*, ed è quella usata comunemente nelle reti domestiche.

Esempio

Immagina questa situazione:

- Tu sei sul PC con *IP* privato 192.168.1.100
- Vuoi accedere ad un sito che ha *IP* pubblico 93.184.216.34 e porta 80
- Il tuo router ha un *IP* pubblico assegnato, es: 203.0.113.1

1. Invio della richiesta

Il tuo PC manda un pacchetto a 93.184.216.34 (porta 80), ma non può uscire su Internet con un *IP* privato, quindi:

Il router, tramite il NAT, modifica il pacchetto:

- Cambia il mittente da 192.168.1.100 con porta 54321 a 203.0.113.1 con porta 60001 (scelta arbitraria: 54321 era la porta del PC, 60001 è una porta del router)
- Salva la traduzione in una tabella NAT:

Porta pubblica	IP interno	Porta interna
60001	192.168.1.100	54321

2. Ricezione della risposta

- Il server example.com risponde a 203.0.113.1:60001.
- Il router controlla la sua tabella NAT, trova che 60001 corrisponde a 192.168.1.100 con porta 54321
- Cambia il destinatario del pacchetto da 203.0.113.1 con porta 60001 a 192.168.1.100 con porta 54321
- Lo invia al tuo PC

IPV6

IPv6 è una versione più recente del protocollo *IP*, introdotta soprattutto per risolvere il problema della scarsità degli indirizzi *IPv4*.

La differenza più evidente è l'aumento dello spazio di indirizzamento: mentre *IPv4* usa indirizzi da 32 bit, *IPv6* usa indirizzi da 128 bit.

La differenza è visibile già dal formato degli indirizzi:

- Indirizzo *IPv4*: 203.0.120.195
- Indirizzo *IPv6*: 2001:0620:0000:0000:0211:24FF:FE80:C12C

Con 128 bit (che si presentano sotto forma di esadecimali per motivi di leggibilità) si possono generare molti più indirizzi *IP* unici rispetto a quelli che utilizzano 32 bit.

- Spazio di indirizzamento dell'*IPv4*:
 $32 \text{ bit} = 2^{32} \text{ di indirizzi} \approx 4,3 \text{ miliardi di indirizzi}$
- Spazio di indirizzamento dell'*IPv6*:
 $128 \text{ bit} = 2^{128} \text{ di indirizzi} \approx 340 \text{ sestilioni di indirizzi}$

Questa differenza di quantità diventa più chiara tramite un confronto: mentre lo spazio di indirizzamento dell'*IPv4* con i suoi 4,3 miliardi di *IP* non basta per dotare tutte le persone sul pianeta di un unico indirizzo, con un sistema a 128 bit teoricamente si potrebbe dotare ogni granello di sabbia sul pianeta di un indirizzo *IP*.

I 128 bit di un indirizzo *IPv6* sono suddivisi in 8 blocchi di 16 bit.

Tramite una scrittura esadecimale si può annotare un blocco di 16 bit con 4 cifre e lettere (i due punti sono utilizzati come elemento di separazione).

Esempio

2001:0620:0000:0000:0211:24FF:FE80:C12C

Per strutturare l'indirizzo IPv6 in un modo più agevole, si è affermata una forma di scrittura più breve:

- Gli zeri iniziali di ogni blocco possono essere omessi. Per esempio, il blocco 0620 può diventare 620 e il blocco 0211 può diventare 211.
- Se un blocco è composto solo da zeri, cioè 0000, può essere scritto semplicemente come 0.

Esempio

2001:0620:0000:0000:0211:24FF:FE80:C12C

diventa

2001:620:0:0:211:24FF:FE80:C12C

Questi indirizzi si possono compattare ancora: per ogni indirizzo IPv6 è possibile omettere i blocchi esadecimali con tutti zero consecutivi lasciando al loro posto il simbolo "::".

La compressione con il simbolo :: può essere usata una sola volta all'interno dello stesso indirizzo IPv6. Se venisse usata più volte, non sarebbe più possibile capire quanti blocchi di zeri sono stati omessi in ciascun punto.

Esempio

2001:0620:0000:0000:0211:24FF:FE80:C12C

diventa

2001:620:0:0:211:24FF:FE80:C12C

diventa

2001:620::211:24FF:FE80:C12C

An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ |-----|

2001:0DB8:AC10:FE01:: Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

Con *IPv6*, grazie all'enorme quantità di indirizzi disponibili, diventa meno necessario usare *NAT* per far condividere a molti dispositivi lo stesso indirizzo pubblico. L'obiettivo di *IPv6* è permettere a molti dispositivi di avere un indirizzo globale univoco.

Esistono comunque indirizzi *IPv6* pensati per l'uso interno alle reti locali, chiamati Unique Local Address, **ULA**.

Questi indirizzi non sono destinati a essere instradati sulla rete Internet globale.

Gli ULA servono per dare indirizzi IPv6 stabili e utilizzabili solo internamente, senza esporre quei dispositivi alla rete Internet globale (per esempio una stampante ha bisogno di collegarsi con la sua LAN locale, non certamente con tutto Internet).

Nonostante *IPv6* risolva molti limiti di *IPv4*, gli indirizzi *IPv4* sono ancora molto usati.

Il motivo principale è che Internet è nata e si è sviluppata per molti anni usando *IPv4*, quindi una grande quantità di reti, dispositivi, server, software e configurazioni continua a supportarlo.

Passare completamente a *IPv6* richiede tempo, aggiornamenti tecnici e compatibilità tra sistemi diversi.

Per questo oggi *IPv4* e *IPv6* convivono: molte reti usano ancora IPv4, spesso con tecniche come NAT e indirizzi privati, mentre IPv6 viene introdotto progressivamente per permettere una crescita più ampia e moderna della rete.

Routing

Dopo aver visto gli indirizzi IP, possiamo chiederci come un pacchetto riesca a raggiungere una rete lontana.

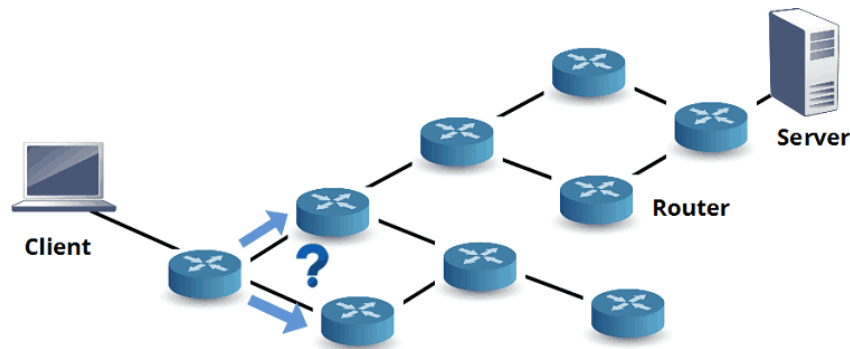
Il routing è il processo di determinare il percorso ottimale (il percorso più adatto secondo le informazioni disponibili e le regole configurate) attraverso il quale i dati vengono instradati da un punto di origine a una destinazione all'interno di una rete o tra diverse reti.

I router mantengono **tabelle di routing** che contengono informazioni sulle reti raggiungibili e sul prossimo passo da seguire per raggiungerle. Questo prossimo passo può essere un altro router, chiamato next hop, oppure una rete direttamente collegata al router.

Le rotte possono essere apprese e aggiornate dinamicamente dai router in risposta a cambiamenti nella topologia di rete o alle condizioni della rete.

Questo permette alle tabelle di routing di adattarsi ai cambiamenti della rete.

Dopo che il routing ha stabilito la rotta ottimale, il **processo di forwarding** (inoltro) è invece l'operazione concreta con cui il router prende un singolo pacchetto, legge il suo indirizzo IP di destinazione, consulta la tabella di routing e lo inoltra attraverso l'interfaccia di uscita corretta. Questo processo assicura che il pacchetto raggiunga la sua destinazione finale attraverso la rete nel miglior modo possibile.



Ecco come funziona il processo di forwarding in un router:

- Ricezione del pacchetto: Il processo di forwarding inizia quando il router riceve un pacchetto da una delle sue interfacce di rete. Questo pacchetto può provenire da una delle reti direttamente connesse al router o essere stato inoltrato da un altro router sulla rete.
- Analisi dell'indirizzo di destinazione: Il router esamina l'indirizzo *IP* di destinazione contenuto nell'intestazione del pacchetto. Questo indirizzo *IP* indica il destinatario finale del pacchetto.
- Ricerca nella tabella di routing: Il router consulta la sua tabella di routing che contiene informazioni sulle reti disponibili e le rotte per raggiungere queste reti. Il router cerca una voce nella tabella che corrisponda all'indirizzo di destinazione del pacchetto.
- Selezione della rotta ottimale: In base alla ricerca possono succedere tre situazioni:
 - Se il router trova una voce nella tabella di instradamento che corrisponde all'indirizzo di destinazione, seleziona la rotta ottimale in base alle informazioni nella voce.
 - Se non trova una rotta specifica, il router verifica se è configurata una **default route** (una rotta di default). Se la trova, inoltra il pacchetto verso il router indicato come percorso predefinito, spesso un router collegato a una rete più ampia, come quella dell'operatore Internet.
 - Se un router non ha una default route e non trova una rotta specifica per l'indirizzo di destinazione, il pacchetto viene scartato.
- Inoltro del pacchetto: Il router inoltra il pacchetto sulla rotta selezionata. Questo può implicare l'invio del pacchetto a un altro router o direttamente all'host di destinazione se si tratta di una rete locale conosciuta.

Le tabelle di routing possono essere configurate manualmente dall'amministratore di rete oppure aggiornate automaticamente tramite **protocolli di routing**. Questi protocolli permettono ai router di scambiarsi informazioni sulle reti raggiungibili e di adattarsi ai cambiamenti della rete.

