Livello di rete

Scritto da Febogamedev

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 (Baker, 1995; Postel, 1981).

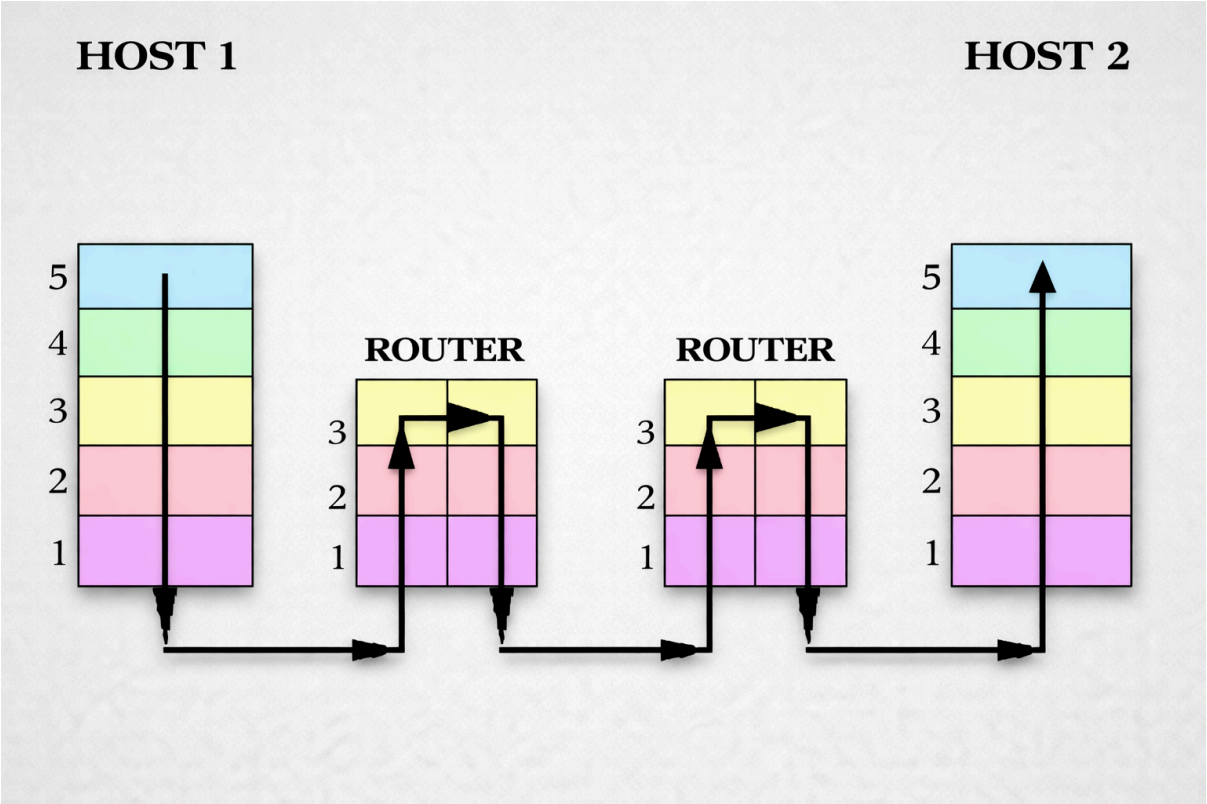
È importante specificare che un router, nel suo funzionamento principale, utilizza soprattutto i primi tre livelli della pila di rete: fisico, link e rete.
Il motivo è che il router non deve interpretare il contenuto applicativo della comunicazione, per esempio una pagina web, un'email o un file. Il 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 (Baker, 1995).

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 (*IP*)** (Postel, 1981).

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) (Postel, 1981).
Il fatto che *IP* sia best effort non significa che sia inutile o progettato male. Significa che I*P* 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 (Postel, 1981).

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* (Postel, 1981).

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 (Hinden & Deering, 2006; Postel, 1981).
L'indirizzo I*P* 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 (Baker, 1995).

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 sui protocolli *TCP* e *IP* (Deering & Hinden, 2017; Postel, 1981):
- *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.

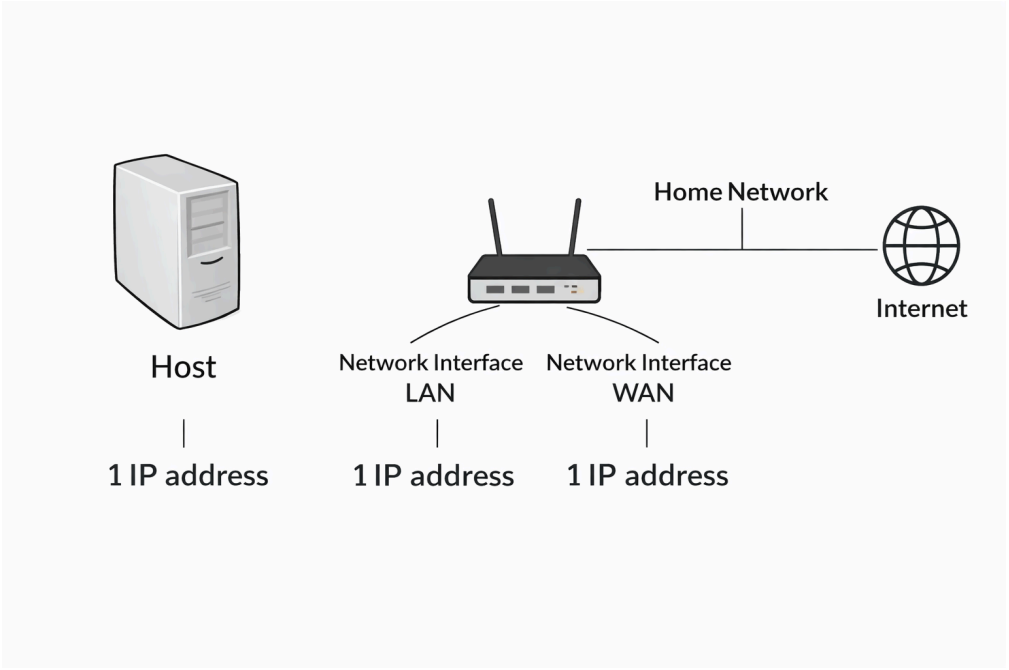
Indirizzo IP

Un **indirizzo *IP***, acronimo di "Indirizzo Protocollo Internet" (Internet Protocol address), è un numero univoco assegnato a ogni dispositivo collegato alla rete Internet (Hinden & Deering, 2006; Postel, 1981).
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 appartenere a 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 (Internet Corporation for Assigned Names and Numbers [ICANN], 2011).
Per questo è stato introdotto *IPv6*, che usa indirizzi di *128* bit e offre uno spazio di indirizzamento enormemente più ampio (Deering & Hinden, 2017).

È importante specificare che l'indirizzo *IP* non si riferisce all'host ma alla sua interfaccia di rete. Per esempio (Hinden & Deering, 2006):

- Un host con una sola scheda di rete (ad esempio solo Wi-Fi) avrà un solo *IP*.
- I router che collegano più linee hanno più interfacce di rete e quindi più indirizzi *IP* (un router domestico ne ha di solito almeno due: una verso la rete locale e una verso la rete dell'operatore).



Ma perché 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.

Le motivazioni sono le seguenti:

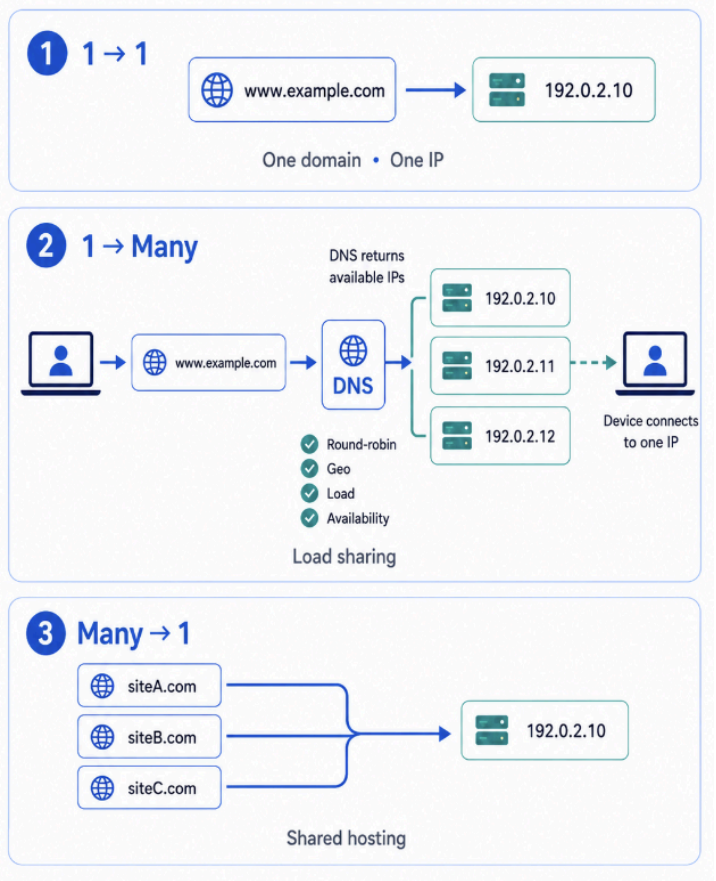
- Scalabilità e organizzazione: gli indirizzi *IP* sono organizzati in gerarchie, il che li rende scalabili e adatti a grandi reti come Internet. Gli indirizzi *MAC*, d'altra parte, sono assegnati ai singoli dispositivi dai produttori e non seguono una struttura gerarchica, il che li rende meno adatti per organizzare una rete su larga scala (Fuller & Li, 2006).
- 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 (Droms, 1997).

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 (Internet Assigned Numbers Authority [IANA], n.d.).
Per ottimizzare l'uso degli indirizzi disponibili, gli *ISP* assegnano spesso *IP* dinamici.

Un nome di dominio può essere associato a uno o più indirizzi *IP*, e allo stesso modo un indirizzo *IP* può essere associato a uno o più domini.

- La relazione più semplice è uno a uno, in cui un dominio corrisponde a un solo indirizzo *IP*, per esempio `www.esempio.it → 192.0.2.10`.
- Esiste poi la relazione uno a molti, in cui uno stesso dominio è associato a più indirizzi *IP*: questa configurazione può essere utilizzata per distribuire il traffico tra più server e aumentare disponibilità e prestazioni.
- È possibile anche una relazione molti a uno, nella quale più domini diversi puntano allo stesso indirizzo *IP*; è una situazione molto comune nei servizi di hosting, dove uno stesso server ospita numerosi siti web. Il *DNS* permette quindi di gestire associazioni flessibili tra nomi di dominio e indirizzi *IP*, che non devono necessariamente avere una corrispondenza univoca.

Quando un dominio è associato a più indirizzi *IP,* il *DNS* non dirige direttamente il traffico, ma restituisce al dispositivo uno o più indirizzi disponibili.
La scelta può avvenire in modi diversi: il server *DNS* può alternare gli indirizzi restituiti, come nel ***DNS* round-robin** (il server *DNS* restituisce gli IP cambiando l'ordine in modo ciclico per dividere le visite), oppure selezionarli in base a criteri come la posizione geografica dell'utente, il carico dei server o la loro disponibilità. Una volta ricevuta la risposta *DNS*, sarà poi il dispositivo dell'utente a stabilire la connessione verso uno degli indirizzi *IP* ottenuti.



Gli indirizzi *IP* possono essere:

- Statici

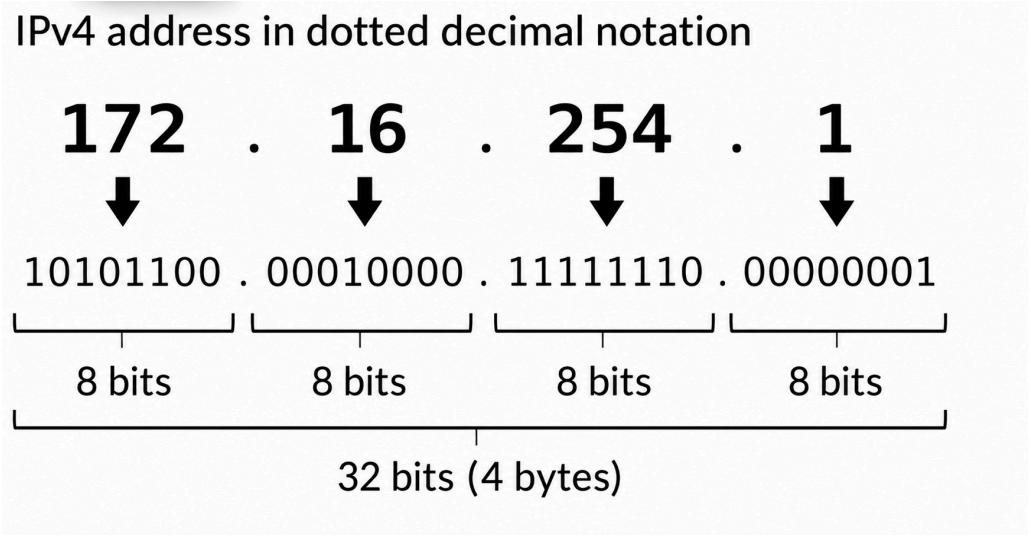
- Dinamici

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 (Droms, 1997).
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 un insieme di indirizzi disponibili (Droms, 1997).
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.

IPV4

L'indirizzo IPv4 è costituito da 32 bit (quattro byte) suddivisi in quattro gruppi da 8 bit (un byte), separati ciascuno da un punto (esempio: 11001001.00100100.10101111.00001111) (Postel, 1981).
Ciascuno di questi quattro byte può essere convertito in formato decimale per rendere più facile l'identificazione.



Ogni byte può assumere valori compresi tra 0 e 255, poiché $2^8 = 256$, ovvero il numero di combinazioni disponibili con 8 bit.
Per questo un indirizzo IPv4 viene scritto come quattro numeri decimali separati da punti, per esempio 192.168.1.10.

Poiché un indirizzo *IPv4* è costituito da 32 bit, le combinazioni disponibili sono 2^{32}, pari a circa 4 miliardi (Postel, 1981).

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 (Deering & Hinden, 2017; Rekhter et al., 1996).

Approfondimento
Gli indirizzi *IP* sono adatti a reti molto grandi come Internet perché possiedono una struttura gerarchica, che permette di organizzare i dispositivi in reti e sottoreti.
Un indirizzo *IP*, infatti, non identifica soltanto un dispositivo, ma contiene anche informazioni sulla rete alla quale esso appartiene.

Questo permette ai router di gestire il traffico senza dover conoscere individualmente ogni dispositivo connesso a Internet.
Per esempio, immaginiamo che un operatore possieda un'intera rete identificata dal prefisso:
203.0.112.0/20
Dove

- La parte /20 indica che i primi 20 bit dell'indirizzo identificano la rete, mentre i bit rimanenti possono essere utilizzati per distinguere gli indirizzi al suo interno. In questo modo il prefisso rappresenta non un singolo indirizzo, ma un intero blocco di indirizzi *IP*.

All'interno di questa rete possono essere presenti migliaia di dispositivi, ciascuno con un proprio indirizzo *IP*.
Un router esterno, però, non deve memorizzare una rotta diversa per ciascuno di essi: può semplicemente sapere che tutti gli indirizzi appartenenti a quel prefisso devono essere inviati verso quell'operatore.

Il processo può quindi avvenire progressivamente:
Internet → *ISP* → sottorete → dispositivo

Man mano che il pacchetto si avvicina alla destinazione, i router utilizzano informazioni sempre più specifiche.
Questo principio prende il nome di **aggregazione delle rotte** e consente di ridurre enormemente la quantità di informazioni che i router devono conservare.

Gli indirizzi *MAC* funzionano diversamente.
Un indirizzo come:
3C:52:82:A1:43:11
identifica un'interfaccia di rete, ma non indica in quale rete essa si trovi. Due dispositivi

con indirizzi *MAC* simili possono trovarsi in parti completamente diverse del mondo. Il *MAC* non possiede quindi una struttura che permetta ai router di raggruppare facilmente i dispositivi in base alla loro posizione nella rete.

Se Internet utilizzasse direttamente gli indirizzi *MAC* per l'instradamento, i router dovrebbero teoricamente mantenere informazioni molto più dettagliate sui singoli dispositivi e sulla loro posizione.
Con gli indirizzi *IP*, invece, è possibile rappresentare interi gruppi di dispositivi attraverso pochi prefissi di rete.

Un'analogia utile è quella del sistema postale. Un indirizzo postale è organizzato gerarchicamente:
Italia → Lombardia → Milano → Via Roma → numero 15

Un centro postale nazionale non ha bisogno di conoscere direttamente la posizione della singola abitazione: deve inizialmente sapere soltanto che una lettera destinata a Milano deve essere inviata verso Milano.
Saranno poi i centri di smistamento successivi a individuare progressivamente la zona, la via e infine il numero civico.
Un indirizzo *MAC* sarebbe invece più simile a un codice identificativo personale privo di indicazioni geografiche. Conoscere il codice permetterebbe di sapere chi è il destinatario, ma non dove inviare la lettera.

Per questo i due indirizzi hanno funzioni differenti e complementari: l'indirizzo *IP* permette di individuare una destinazione all'interno di una rete gerarchica e di instradare i pacchetti su larga scala, mentre l'indirizzo *MAC* viene utilizzato principalmente per identificare le interfacce e consegnare i pacchetti all'interno del collegamento locale.

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 (Rekhter et al., 1996).
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 (Srisuresh & Egevang, 2001).
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 utilizzati solo in 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).
- I miei dispositivi, invece, usano indirizzi *IP* privati che, quando dovranno comunicare su 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 nell'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 (Srisuresh & Egevang, 2001; Srisuresh & Holdrege, 1999).
Quando un dispositivo della *LAN* invia una richiesta verso Internet usando il suo *IP* privato, il *NAT* del router interviene in questo modo (Srisuresh & Egevang, 2001):
- 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’I*P* pubblico del router e alla porta usata dal *NAT*.
A questo punto:

- Il router consulta la tabella *NAT* per trovare 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 (Srisuresh & Holdrege, 1999).

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, ad esempio: 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* (Deering & Hinden, 2017).
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, rappresentati in forma esadecimale per motivi di leggibilità, si possono generare molti più indirizzi *IP* unici rispetto a quelli che utilizzano 32 bit (Hinden & Deering, 2006).

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

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 (Hinden & Deering, 2006).
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

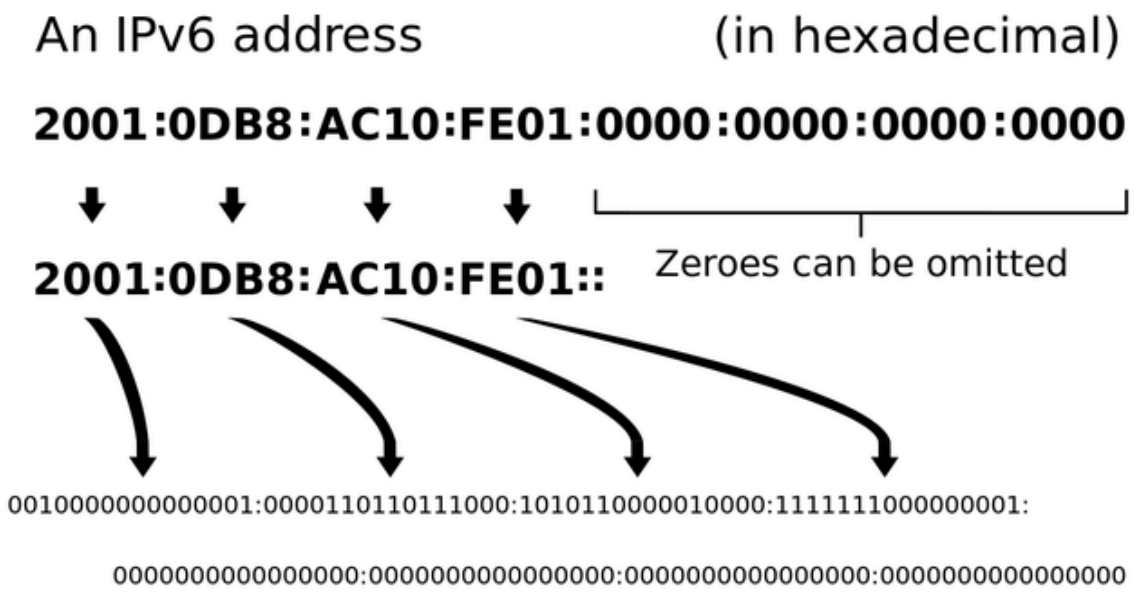
Per strutturare l'indirizzo IPv6 in un modo più agevole, si è affermata una forma di scrittura più breve (Kawamura & Kawashima, 2010):

- 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 consecutivi composti interamente da zeri lasciando al loro posto il simbolo "::" (Kawamura & Kawashima, 2010).
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 (Kawamura & Kawashima, 2010).

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



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)** (Hinden & Haberman, 2005).
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 comunicare all'interno della propria LAN, non con l'intera rete 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 (Deering & Hinden, 2017).

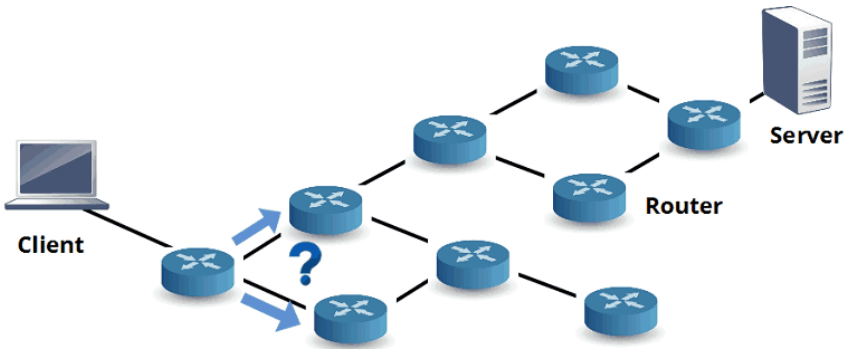
Routing

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

Il routing è il processo mediante il quale viene determinato 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 (Baker, 1995).

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 (Baker, 1995).
Le rotte possono essere apprese e aggiornate dinamicamente dai router in risposta a cambiamenti nella topologia di rete o nelle 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 I*P* 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 (Baker, 1995).

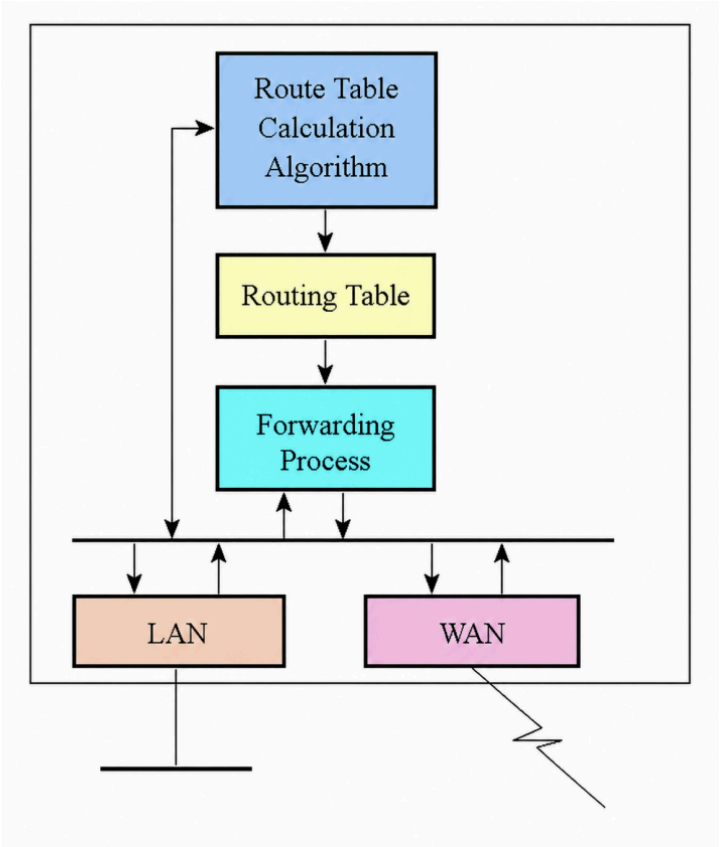


Ecco come funziona il processo di forwarding in un router:

- 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 sulle 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 verificarsi 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 (Baker, 1995).


Route Table
Calculation
Algorithm
Routing Table
Forwarding
Process
LAN
WAN

Materiale di supporto

Esercizi

Che cosa deve fare il router?
Un computer della rete domestica deve inviare un pacchetto a un server web presente su Internet.
Il pacchetto attraversa il router di casa e successivamente diversi router della rete dell'ISP.

Rispondi alle seguenti domande:

- Spiega quale compito svolge il livello di rete durante questa comunicazione.
- Indica quali informazioni deve leggere principalmente un router per decidere dove inoltrare il pacchetto.
- Spiega perché, nel suo funzionamento principale, il router non ha bisogno di interpretare il contenuto della pagina web richiesta.
- Indica quali tre livelli della pila vengono utilizzati principalmente dal router e quale funzione svolge ciascuno.
- Spiega perché i livelli di trasporto e applicazione sono invece particolarmente importanti negli host finali.
- Descrivi cosa significa che il protocollo IP fornisce un servizio best effort.
- Se un pacchetto viene perso durante il percorso, spiega perché non è necessariamente IP a occuparsi della sua ritrasmissione.
- Spiega infine perché il fatto che IP non garantisca la consegna non significa che il protocollo sia progettato male.

IP o MAC?
Una scuola possiede due LAN differenti collegate attraverso un router.
Il computer A si trova nella LAN 1 e deve comunicare con il computer B situato nella LAN 2.
Entrambi i computer possiedono un indirizzo MAC e un indirizzo IP.

Analizza la comunicazione.

- Spiega quale funzione svolge l'indirizzo MAC.
- Spiega quale funzione svolge invece l'indirizzo IP.
- Indica quale dei due indirizzi è necessario per instradare il pacchetto tra le due LAN.
- Spiega perché il solo indirizzo MAC non sarebbe adatto per organizzare l'instradamento su una rete globale come Internet.
- Spiega in che senso gli indirizzi IP sono indipendenti dalla tecnologia fisica utilizzata, come Ethernet, Wi-Fi, fibra o rete mobile.
- Il router possiede un'interfaccia collegata alla LAN 1 e una collegata alla LAN 2. Spiega perché deve possedere almeno due indirizzi IP.
- Uno studente afferma: «Ogni computer possiede sempre esattamente un indirizzo IP». Valuta l'affermazione e correggila utilizzando il concetto di interfaccia di rete.

Assegnare gli indirizzi di una rete
Un'azienda possiede:

- 80 computer dei dipendenti.

- 30 smartphone aziendali.
- 6 stampanti di rete.
- 3 server che devono essere sempre raggiungibili allo stesso indirizzo.
- Alcuni dispositivi che entrano ed escono frequentemente dalla rete.

L'amministratore deve decidere quali dispositivi utilizzare con indirizzi IP statici e quali con indirizzi dinamici.

Rispondi alle seguenti domande:
- Individua quali dispositivi potrebbero beneficiare maggiormente di un indirizzo IP statico e motiva la scelta.
- Individua quali dispositivi potrebbero utilizzare normalmente indirizzi dinamici.
- Spiega quale funzione svolge un server DHCP.
- Descrivi cosa può accadere all'indirizzo IP dinamico di un dispositivo quando questo si scollega dalla rete.
- Spiega perché l'assegnazione dinamica permette di utilizzare in modo più efficiente l'insieme degli indirizzi disponibili.
- Un server aziendale cambia continuamente indirizzo IP. Spiega quale problema pratico potrebbe creare.
- Proponi quindi una strategia generale di assegnazione degli indirizzi per la rete descritta e motiva le tue scelte.

Una casa con un solo IP pubblico
Una famiglia possiede questi dispositivi:
- Un computer con IP privato 192.168.1.10
- Uno smartphone con IP privato 192.168.1.11
- Una smart TV con IP privato 192.168.1.12
- Il router possiede l'indirizzo IP pubblico 203.0.113.1

Il computer apre una connessione verso un server web utilizzando la propria porta sorgente 52341. Il router traduce temporaneamente la comunicazione utilizzando la porta pubblica 60001.

Analizza cosa accade.
- Spiega la differenza tra indirizzo IP privato e indirizzo IP pubblico.
- Spiega perché 192.168.1.10 non può essere utilizzato direttamente per essere instradato su Internet.
- Descrivi cosa modifica il router quando il computer invia il pacchetto verso Internet.
- Indica quali informazioni deve registrare nella propria tabella NAT.
- Il server risponde a 203.0.113.1:60001. Spiega come il router riesce a capire che la risposta deve essere inoltrata a 192.168.1.10:52341.
- Spiega perché smartphone e smart TV possono utilizzare contemporaneamente lo stesso IP pubblico senza confondere le comunicazioni.
- Spiega perché la tecnica descritta nella dispensa è più precisamente PAT/NAPT, anche se nel linguaggio comune viene spesso chiamata semplicemente NAT.
- Indica due vantaggi dell'utilizzo di indirizzi privati illustrati nella dispensa.

IPv4 e IPv6

Considera questi due indirizzi:

- IPv4: 172.16.254.1.
- IPv6: 2001:0620:0000:0000:0211:24FF:FE80:C12C.

Rispondi alle seguenti domande:

- Indica quanti bit utilizza un indirizzo IPv4 e in quanti gruppi viene suddiviso.
- Spiega perché ciascun numero decimale di un IPv4 può assumere valori compresi tra 0 e 255.
- Indica quanti bit utilizza invece IPv6.
- Spiega perché IPv6 offre uno spazio di indirizzamento enormemente superiore rispetto a IPv4.
- Riscrivi l'indirizzo IPv6 eliminando gli zeri iniziali non necessari nei singoli blocchi.
- Comprimi ulteriormente l'indirizzo utilizzando correttamente il simbolo ::.
- Spiega perché il simbolo :: può essere utilizzato una sola volta nello stesso indirizzo.
- Spiega perché con IPv6 diventa meno necessario utilizzare NAT per far condividere a molti dispositivi lo stesso indirizzo pubblico.
- Spiega che cosa sono gli Unique Local Address (ULA) e perché possono essere comunque utili anche in una rete IPv6.
- Spiega perché IPv4 continua a essere largamente utilizzato nonostante l'esistenza di IPv6.

Routing o forwarding?

Un router riceve un pacchetto destinato all'indirizzo di una rete lontana.
La sua tabella di routing contiene queste informazioni:

- La rete A è direttamente collegata.
- La rete B è raggiungibile attraverso il Router 2.
- La rete C è raggiungibile attraverso il Router 3.

Per tutte le altre destinazioni è configurata una default route verso il Router 4.
Rispondi alle seguenti domande:

- Spiega che cosa si intende per routing.
- Spiega che cosa si intende invece per forwarding.
- Indica quale funzione svolge la tabella di routing.
- Spiega che cosa si intende per next hop.
- Se il pacchetto è destinato alla rete B, descrivi cosa deve fare il router.
- Se il pacchetto è destinato a una rete non presente esplicitamente nella tabella, spiega cosa accade grazie alla default route.
- Immagina che venga rimossa anche la default route e che il router non conosca alcun percorso verso la destinazione. Spiega cosa accade al pacchetto.
- Spiega perché routing e forwarding non sono la stessa operazione, anche se collaborano tra loro.
- Immagina che un collegamento verso Router 2 smetta di funzionare e che il router utilizzi protocolli di routing dinamico. Spiega come la tabella di routing potrebbe adattarsi alla nuova situazione.
- Ricostruisci infine l'intera procedura: ricezione del pacchetto → lettura dell'IP di destinazione → consultazione della tabella → scelta della rotta → inoltro attraverso l'interfaccia corretta.

Bibliografia

Baker, F. (1995). *Requirements for IP version 4 routers* (RFC 1812). RFC Editor. https://doi.org/10.17487/RFC1812

Deering, S., & Hinden, R. (2017). *Internet protocol, version 6 (IPv6) specification* (RFC 8200). RFC Editor. https://doi.org/10.17487/RFC8200

Droms, R. (1997). *Dynamic host configuration protocol* (RFC 2131). RFC Editor. https://doi.org/10.17487/RFC2131

Fuller, V., & Li, T. (2006). *Classless inter-domain routing (CIDR): The Internet address assignment and aggregation plan* (RFC 4632). RFC Editor. https://doi.org/10.17487/RFC4632

Hinden, R., & Deering, S. (2006). *IP version 6 addressing architecture* (RFC 4291). RFC Editor. https://doi.org/10.17487/RFC4291

Hinden, R., & Haberman, B. (2005). *Unique local IPv6 unicast addresses* (RFC 4193). RFC Editor. https://doi.org/10.17487/RFC4193

Internet Assigned Numbers Authority. (n.d.). *Number resources*. Retrieved August 17, 2026, from https://www.iana.org/numbers

Internet Corporation for Assigned Names and Numbers. (2011, February 3). *Available pool of unallocated IPv4 Internet addresses now completely emptied*. https://www.icann.org/en/news/releases/release-03feb11-en.pdf

Kawamura, S., & Kawashima, M. (2010). *A recommendation for IPv6 address text representation* (RFC 5952). RFC Editor. https://doi.org/10.17487/RFC5952

Postel, J. (1981). *Internet protocol* (RFC 791). RFC Editor. https://doi.org/10.17487/RFC0791

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). *Address allocation for private internets* (RFC 1918). RFC Editor. https://doi.org/10.17487/RFC1918

Srisuresh, P., & Egevang, K. (2001). *Traditional IP network address translator (Traditional NAT)* (RFC 3022). RFC Editor. https://doi.org/10.17487/RFC3022

Srisuresh, P., & Holdrege, M. (1999). *IP network address translator (NAT) terminology and considerations* (RFC 2663). RFC Editor. https://doi.org/10.17487/RFC2663

Approfondimenti

- James F. Kurose e Keith W. Ross, Reti di calcolatori e Internet. Un approccio top-down, 8ª ed., Pearson, 2022 — Approfondisce il livello di rete, il funzionamento del protocollo IP, il forwarding, le tabelle di inoltro, IPv4 e IPv6 e i principali algoritmi e protocolli di routing.
- Behrouz A. Forouzan e Firouz Mosharraf, Reti di calcolatori, 2ª ed., a cura di Gaia Maselli, McGraw-Hill Education, 2024 — Presenta in modo visuale l'indirizzamento IPv4 e IPv6, il funzionamento dei router, il forwarding, il routing e i principali meccanismi utilizzati per collegare reti differenti.
- Andrew S. Tanenbaum, Nick Feamster e David J. Wetherall, Reti di calcolatori, 6ª ed., Pearson, 2023 — Analizza in modo approfondito il livello di rete, soffermandosi sull'indirizzamento IP, sugli algoritmi di routing, sull'organizzazione delle reti e sul funzionamento dei protocolli di instradamento.

- Douglas E. Comer, Internetworking con TCP/IP. Vol. 1: principi, protocolli e architetture, 5ª ed., Pearson, 2006 — Approfondisce l'architettura TCP/IP con particolare attenzione a IPv4 e IPv6, indirizzamento e subnetting, datagrammi IP, routing, ICMP, ARP e meccanismi che permettono l'interconnessione tra reti.

Nota editoriale

Per la realizzazione di questi materiali ho utilizzato strumenti di intelligenza artificiale generativa come supporto alla scrittura, in particolare per migliorare la forma del testo, riorganizzare i contenuti, correggere la formulazione e velocizzare alcune attività redazionali.

Lavorando autonomamente alla produzione di questi materiali, cerco infatti di automatizzare tutte le attività che possono esserlo, così da poter dedicare più tempo alla ricerca, alla progettazione e allo sviluppo dei contenuti.

L'intelligenza artificiale non determina però i contenuti dell'opera: la scelta degli argomenti, la struttura, le idee, le interpretazioni, gli esempi e l'impostazione didattica sono elaborati da me. L'IA viene quindi utilizzata principalmente come strumento di supporto alla produzione e alla revisione formale, mentre la responsabilità autoriale e progettuale dei contenuti rimane mia.

Salvo diversa indicazione, questo materiale è distribuito con licenza Creative Commons Attribuzione – Non commerciale – Condividi allo stesso modo 4.0 Internazionale (CC BY-NC-SA 4.0).

È quindi possibile condividere, ridistribuire, modificare e creare opere derivate a partire dal materiale, a condizione di attribuirne correttamente la paternità, di non utilizzarlo per scopi commerciali e di distribuire eventuali versioni modificate o derivate con la stessa licenza.

