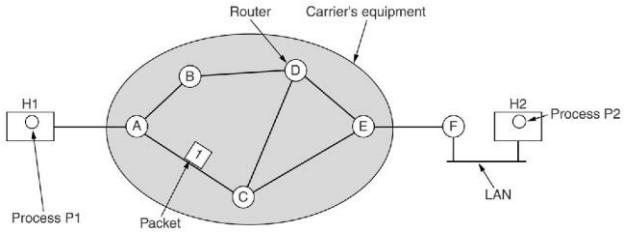
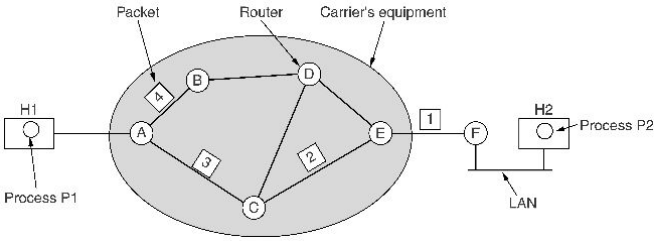
Livello Rete / Network

Sappiamo che ***due host*** sono ***separati da un certo numero di nodi intermedi***, separati a loro volta (ma non per forza) da reti funzionanti con tecnologie diverse, e che tra tali nodi è possibile intraprendere molteplici percorsi. Lo ***strato di rete permette di determinare quale tragitto*** (***path***) ***dovranno seguire i dati*** (***instradamento***), deve evitare di sovraccaricare le linee quando sono disponibili percorsi alternativi (***congestione***) e deve risolvere i problemi connessi al transito attraverso reti differenti (***internetworking***).

Inizialmente si prevedeva solamente l'utilizzo del servizio ***Connection Oriented***, mentre in seguito si è sentita la necessità di introdurre nello standard anche il servizio ***Connectionless***. Il servizio senza connessione (***Connectionless***) richiede che i ***pacchetti*** vengano ***instradati indipendentemente*** uno dall'altro.



Sostanzialmente, l'idea di base è quella di stabilire un ***path***, il quale è ***costituito da*** una serie di ***router che il pacchetto dovrà attraversare***. Ovviamente i pacchetti con la stessa connessione seguiranno lo stesso path; di conseguenza, i pacchetti seguiranno un determinato path non in base alla destinazione, bensì in base alla connessione instaurata, la quale è identificata tramite un ***id*** nell'***header*** del ***pacchetto***.



La funzione principale dello ***strato di rete*** è ***l'instradamento*** (***routing***): tale processo permette al router di scegliere, tramite un certo algoritmo, la linea di uscita verso cui instradare i dati. Tale operazione, ovviamente, verrà ripetuta per ogni pacchetto nel caso la connessione sia ***Connectionless***; nel caso della ***Connection Oriented*** viene effettuata una sola volta. Precisamente, possiamo distinguere due operazioni:

- ***Inoltro*** (***forwarding***): definisce le regole con le quali un pacchetto viene inoltrato a livello fisico verso l'uscita (normalmente sulla base della lettura di una tabella di instradamento);
- ***Instradamento***: definisce le regole con le quali viene scelto un percorso in rete tra sorgente e destinazione (sulla base delle quali vengono scritte le tabelle di instradamento).

È importante sapere che un algoritmo di routing deve essere corretto, meno soggetto ad errori, stabile e ottimizzato.

Livello Rete / Network: protocollo, indirizzi e pacchetti IP (Internet Protocol)

Il protocollo IP ha la funzione di ***recapitare dati*** dalla ***sorgente*** alla ***destinazione*** tramite reti interconnesse tra loro. Il recapito viene effettuato in maniera ***diretta*** se **sender** e **receiver** fanno parte della ***stessa rete***, altrimenti in maniera ***indiretta*** nel caso viaggi tramite dei ***router***. Se possibile il pacchetto viaggia per intero, altrimenti viene spezzettato in più parti trasportate individualmente: in tal caso il pacchetto viene riassemblato a destinazione. Tale protocollo fornisce un servizio ***Connectionless*** inaffidabile.

Ogni ***interfaccia di rete*** (cioè ogni connessione ad una rete) deve ***avere un indirizzo IP***: i computer generalmente ne hanno affiliato uno solo, mentre i ***server*** ne ***hanno molteplici***.

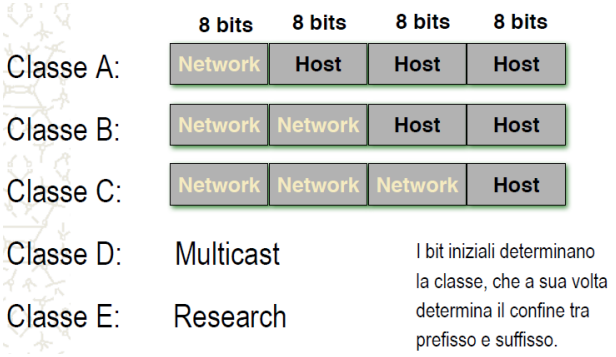
L'***indirizzo IP*** è formato da ***32 bit*** rappresentati da ***4 numeri decimali*** separati da un punto che possono assumere un valore nel range [0 to 255]. Ogni indirizzo IP contiene una parte che ***specifica la rete*** (***prefisso***) ed una parte che ***identifica l'host*** all'interno della rete (***suffisso***). Prefisso e suffisso dipendono dalla classe dell'indirizzo IP, la quale vedremo tra poco.

Esempio di indirizzo IP: XX.XX.XX.XX

È importante sapere una cosa: mentre ***l'indirizzo MAC identifica univocamente il dispositivo***, ***l'indirizzo IP identifica univocamente la connessione dispositivo-rete***: da ciò consegue che se un computer ha molteplici connessioni di rete, allora avrà assegnato un indirizzo IP per ogni connessione.

Gli indirizzi IP sono raggruppati in diverse categorie, dette ***classi***:

- Gli indirizzi di ***classe A*** hanno il primo campo che assume un valore nel range [0 to 127]: il ***primo*** campo è dedicato al prefisso, i restanti al suffisso; la sequenza di bit comincia con 0;
- Gli indirizzi di ***classe B*** hanno il primo campo che assume un valore nel range [128 to 191]: i primi ***due*** campi sono dedicati al prefisso, i restanti al suffisso; la sequenza di bit comincia con 10;
- Gli indirizzi di ***classe C*** hanno il primo campo che assume un valore nel range [192 to 223]: i primi ***tre*** campi sono dedicati al prefisso, l'ultimo al suffisso; la sequenza di bit comincia con 110;
- Gli indirizzi di ***classe D*** hanno il primo campo che assume un valore nel range [224 to 239]: sono indirizzi dedicati al ***multicasting***; la sequenza di bit comincia con 1110;
- Gli indirizzi di ***classe E*** hanno il primo campo che assume un valore nel range [240 to 255]: sono indirizzi dedicati ad utilizzi sperimentali; la sequenza di bit comincia con 1111.



Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
256.241.20.10	Nonexistent		

- Nel caso un indirizzo IP contenga tutti i ***bit pari a 0*** nel campo di host (***suffisso***), allora si sta indicando la rete.
- L'indirizzo IP contenente tutti i ***bit pari a 0*** nel campo di rete (***prefisso***) indica "***questa rete***".
- L'indirizzo IP contenente tutti i ***bit pari a 0*** sia nel campo di rete che nel campo di host indica "***questo host di questa rete***".
- L'indirizzo IP contenente tutti i ***bit pari ad 1*** sia nel campo di ***rete*** che nel campo di ***host*** indica l'indirizzo ***broadcast della rete locale***, quindi viene utilizzato per mandare un pacchetto IP ad ogni host sulla propria rete.
- L'indirizzo contenente tutti i ***bit pari ad 1*** nel campo ***host*** indica il ***broadcast nella rete specificata nel campo rete***, quindi viene utilizzato per mandare un pacchetto IP ad ogni host appartenente ad una certa rete remota.

L'indirizzo ***127.0.0.0*** indica l'interfaccia di ***loopback***, la quale identifica la macchina locale detta ***localhost***.

Affinché tutto funzioni correttamente, gli indirizzi IP devono essere assegnati da una ***autorità centrale*** che garantisca l'unicità delle assegnazioni (siccome ogni indirizzo IP deve essere unico in tutta la rete). Per internet gli indirizzi sono assegnati dalla ***ICANN***, la quale ha poi delegato organizzazioni regionali assegnando loro gruppi di indirizzi da riassegnare al loro interno.

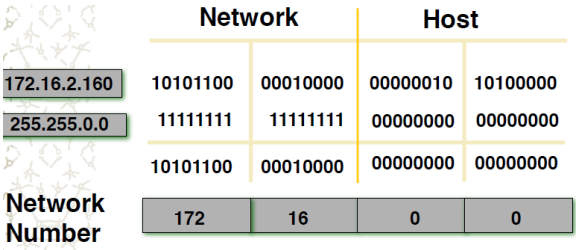
Lo spazio di assegnamento equivale a circa due miliardi di indirizzi, ma con il passare degli anni ci si è accorti di una certa ***carenza di indirizzi***. Per risolvere tale problema, è stata sviluppata una tecnica detta ***subnetting***, la quale permette di suddividere un campo di indirizzi in gruppi più piccoli, trattando un sottogruppo come se fosse una rete a sé stante.

Esempio: un campus ha rete associata 100.0.0.0 (***classe A***) e si vuole suddividere il suo campo di indirizzi: è possibile associare 100.1.0.0 ad un dipartimento, 100.2.0.0 ad un altro dipartimento e così via, in modo da considerare le reti dei dipartimenti come reti a sé stanti e di classe più piccola, il tale ***classe B***. Qualsiasi rete può essere subnettata.

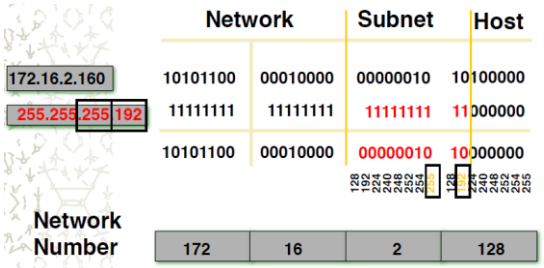
Altro esempio: sia 172.16.0.0 una rete, eventuali subnet possono essere 172.16.1.0, 172.16.2.0, 172.16.3.0 e così via.

Il processo di ***subnetting*** è la ***divisione di una singola rete in sottoreti*** i cui dispositivi avranno l'indirizzo di rete identico. Per svolgere le proprie funzioni, il ***subnetting*** fa uso della ***network mask*** (o ***subnet mask***), la quale permette di suddividere la parte prefisso dalla parte suffisso.

La network mask raffigurerà con i bit 1 il prefisso, con i bit 0 il suffisso. Per capire a quale rete appartiene un indirizzo IP, si mette in AND bit a bit l'indirizzo IP con la network mask.



- Subnets non in uso — schema di default

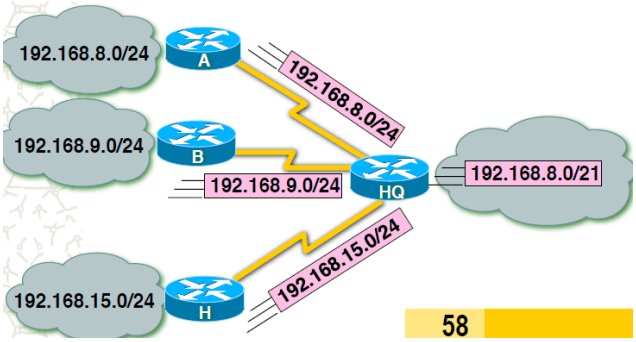


- L'indirizzo di rete viene esteso di 10 bit a discapito degli hosts

Esempio: 193.206.144.64***/26*** -> sono necessari 26 bit per rappresentare l'indirizzo di rete.

Livello Rete / Network: Classless InterDomain Routing

Già diversi anni fa Internet cresceva più velocemente di quanto si potesse pensare. Era, dunque, necessario adottare una soluzione: abbandonare le classi di rete. Si decide quindi di adottare un sistema che consente una migliore gestione degli indirizzi di rete evitando sprechi: il ***CIDR***. Tale sistema permette la ***suddivisione dell'indirizzo IP in prefisso e suffisso senza la suddivisione in classi***. Secondo questo standard ogni record della ***tabella di routing*** specifica la destinazione con la sua maschera, causando però un grave problema: l'aumento delle reti indirizzabili può far esplodere le dimensioni della tabella di routing. Per ovviare a questo problema, gli indirizzi vengono assegnati alle varie organizzazioni regionali e locali che risultano verso l'esterno solo come una rete.



Livello Rete / Network: IPv6 (IP version 6)

Agli inizi degli anni 90 si iniziò la ricerca di un successore di IPv4 siccome si sentiva la necessità di ampliare lo spazio degli indirizzi. Fu così sviluppato un protocollo progettato sul modello dell'IPv4, ampliando e migliorando le sue caratteristiche: ***IPv6***. Tale protocollo offre ***indirizzamento illimitato***, ***riduce*** i ***tempi*** di ***elaborazione*** del router e ***supporta pacchetti*** di ***grosse dimensioni***.

L'IPv6 prevede indirizzi a 16 byte (128 bit), con 8 campi composti da 4 cifre esadecimali e separati tra loro da " : ".

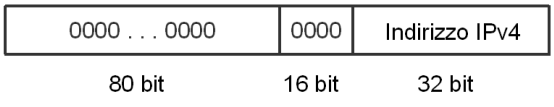
Esempio: 8000:0000:0000:0000:0123:4567:89AB:CDEF

Gli ***indirizzi IPv6*** sono soggetti ad ottimizzazioni riguardo la loro rappresentazione: si possono omettere gli zeri all'inizio di un gruppo e si possono omettere gruppi di zeri consecutivi, rappresentandoli con la seguente sequenza " :: ".

Esempio: 8000::123:4567:89AB:CDEF

Come l'IPv4, anche l'IPv6 definisce ***campi*** appartenenti alla ***rete*** e ***campi*** appartenenti all'***host***. Il formato dell'intestazione (***header***) dell'IPv6 è stato notevolmente semplificato rimuovendo e modificando molteplici campi; anzi, alle volte è possibile attribuire anche molteplici header.

È importante sapere che partendo da un indirizzo IPv6 è possibile ricavarsi l'IPv4. Gli IPv4 sono rappresentati sottoforma di IPv6 da 6 gruppi di zeri e due gruppi che rappresentano l'effettivo IPv4. Quindi, sostanzialmente, è possibile ricreare un IPv4 partendo da un IPv6.



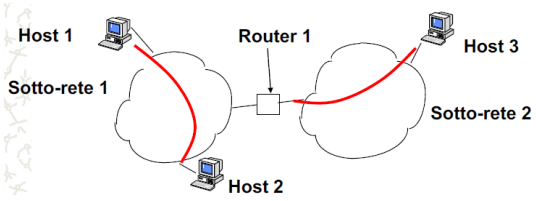
Esempio: ::89AB:CDEF oppure ::137.171.205.239

C'è un problema: l'IPv6 può spedire, instradare e ricevere pacchetti IPv4, ma IPv4 non è in grado di gestire pacchetti IPv6. Una soluzione sono i ***DNS (Domain Name System)***, i quali ***permettono di creare indirizzi IPv6 partendo da un IPv4***: il kernel capisce che si tratta di un indirizzo speciale ed usa la comunicazione IPv4.

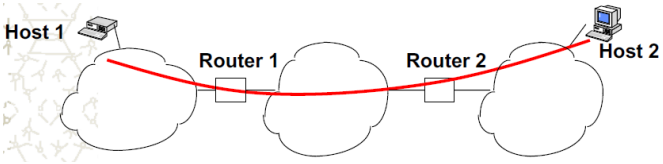
Livello Rete / Network: routing e forwarding

Riguardo il ***routing IPv6***, può essere ***diretto*** o ***indiretto***.

- ***Instradamento diretto***: la trasmissione di un pacchetto avviene tra ***due stazioni connesse nella stessa sottorete*** senza coinvolgere alcun router intermedio.



- ***Instradamento indiretto***: la trasmissione di un pacchetto avviene tra ***due stazioni non situate nella stessa sottorete***, quindi la sottorete del mittente sarà diversa dalla sottorete del destinatario, coinvolgendo ***router intermedi***: il router esamina il pacchetto ricevuto e, se l'host di destinazione non si trova in una sottorete a cui il router è direttamente connesso, ***inoltrerà*** il pacchetto ***al router successivo***, il cui ripeterà tali controlli. Nel caso, invece, il destinatario si trovi nella stessa sottorete del router che sta esaminando il pacchetto, si individua l'indirizzo ***MAC del destinatario*** tramite procedura ***ARP (Address Resolution Protocol).***



Riassumendo, dato un pacchetto:

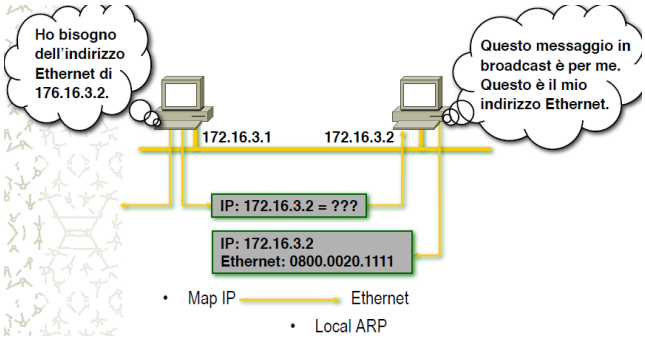
- Viene ***estratto*** il campo ***destinazione***;
- Si cerca la ***destinazione*** nella ***routing table***;
- Si trova la ***prossima destinazione*** Z (***hop***), la quale può essere il dispositivo ***destinatario*** o il prossimo ***router***;
- Il ***pacchetto*** viene ***spedito*** a Z.

Ad ogni "***hop***" viene ***ricalcolata la strada*** da seguire per tutti i pacchetti in transito, nel caso di ***Connection Oriented***.

Il problema sta nel come fare a sapere a quale indirizzo MAC inviare il pacchetto, contando che l'host conosce solo l'indirizzo IP del destinatario. IP si appoggia, quindi, ad un protocollo chiamato ***ARP(Address Resolution Protocol)***.

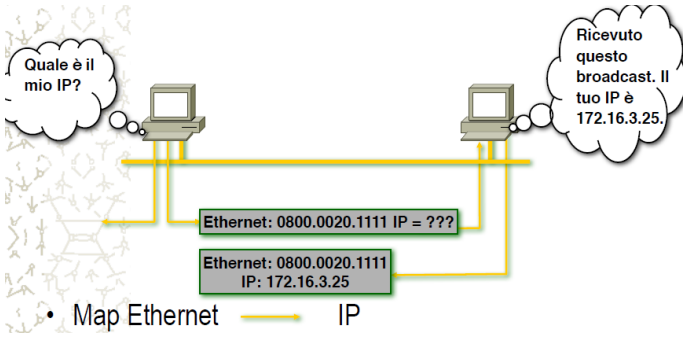
Vediamo come funziona ***ARP***: poniamo di avere un host con indirizzo IP A1 e con indirizzo MAC MA1 il quale deve inviare un pacchetto IP ad un host con indirizzo IP A2 sulla stessa rete. ARP si procura le informazioni necessarie nel seguente modo:

- Viene ***costruito un pacchetto data-link*** (chiamato ***ARP Request***) contenente A1, MA1, A2 e MA2, quest'ultimo contrassegnato da una serie di 0;
- Tale ***pacchetto*** viene ***inviato in broadcast*** sulla ***rete locale***;
- ***Tutti ricevono*** tale pacchetto ***ARP***, ***ma solo l'host*** con MAC MA2 ***lo processerà***;
- ***L'host*** di ***destinazione creerà*** un ***pacchetto data-link*** (chiamato ***ARP Response***) nella quale inserirà il campo mancante. Tale pacchetto verrà trasmesso in maniera diretta e non in broadcast;
- Viene quindi ***acquisito*** il ***MAC*** MA2 rilegato ***all'indirizzo IP*** A2.



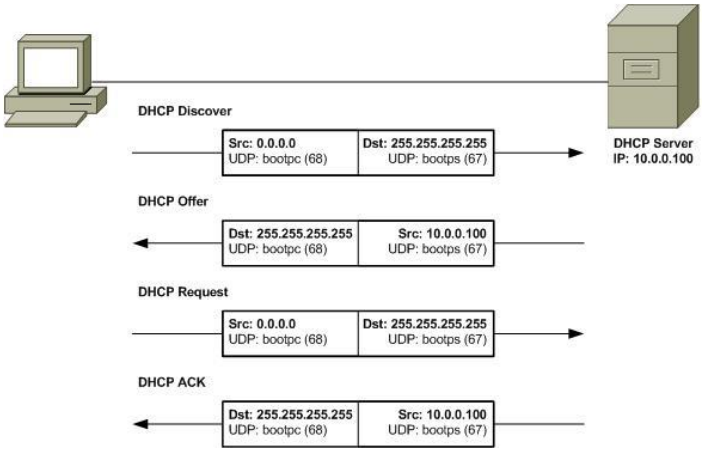
Ogni volta che viene rilevata una nuova associazione, essa viene memorizzata nella ***cache***. Quando ARP rileva un indirizzo MAC, controlla la cache: se l'associazione è già presente, viene utilizzata senza mandare alcuna ***ARP Request*** o ***Response***. Le ***entry*** nella cache di ARP hanno un ***timer***, il quale alla scadenza eliminerà la entry. È possibile impostare anche delle entry senza una scadenza.

Nel caso fosse necessario, esiste una tecnica chiamata ***ARP Reverse***, quale serve a trovare l'IP associato ad un indirizzo MAC.



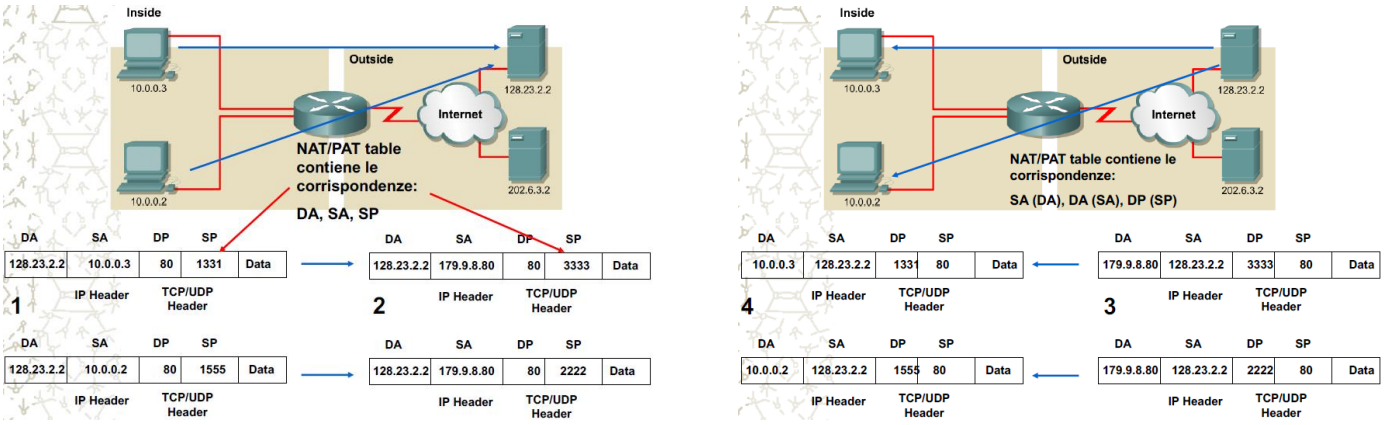
Livello Rete / Network: DHCP(Dynamic Host Configuration Protocol)

Il ***DHCP*** permette agli host, dopo lo startup, di ottenere un indirizzo IP da un server, evitando configurazioni manuali.



Livello Rete / Network: NAT

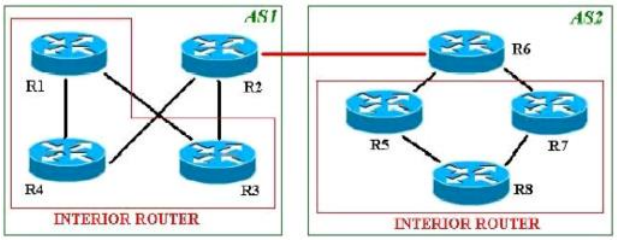
Il ***Network Address Translation (NAT)*** è un meccanismo che permette di mappare un indirizzo IP in un altro indirizzo IP. Le reti locali hanno diversi indirizzi ***IP privati*** che riguardano precisi dispositivi connessi alla rete. Attraverso il NAT, questi indirizzi privati vengono tradotti in un indirizzo ***IP pubblico*** quando le richieste in uscita vengono inviate ad Internet. Il processo inverso si verifica nel caso i dati siano in entrata.



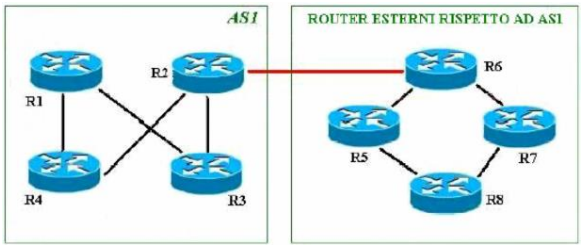
Livello Rete / Network: approfondimento sui router

Un router monta un ***sistema operativo*** nella sua memoria chiamato ***Cisco IOS*** ed è caratterizzato da ***porte di ingresso ed uscita***, un ***blocco di commutazione*** che collega le porte di ingresso con quelle di uscita, un ***processore di instradamento*** che esegue protocolli di routing e aggiorna le tabelle di routing, ***memoria ROM, RAM*** (per le tabelle di routing), ***NVRAM*** (per le configurazioni di avvio), ***Flash*** (immagine IOS).

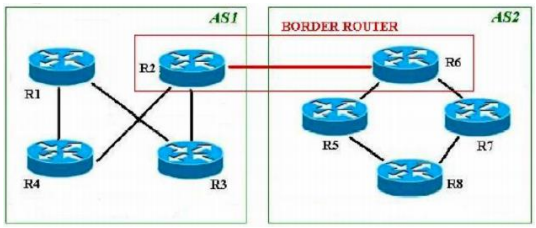
Il collegamento di più ***reti sotto un unico dominio*** prende il nome di ***Autonomous System (AS).*** I router che instradano messaggi nello stesso ***AS*** e che non hanno diretta connessione con i router di altre reti sono detti ***Interior Router***: scambiano informazioni di instradamento tramite un ***Interior Gateway Protocol***;



I router che instradano messaggi tra ***AS diversi*** sono detti ***Exterior Router***: scambiano informazioni utilizzando un ***Exterior Gateway Protocol***.



I router che hanno la funzione di fare da ponte di collegamento tra ***AS diversi*** vengono detti ***Border Router*** (anche router di frontiera).



Livello Rete / Network: matching riguardo il routing

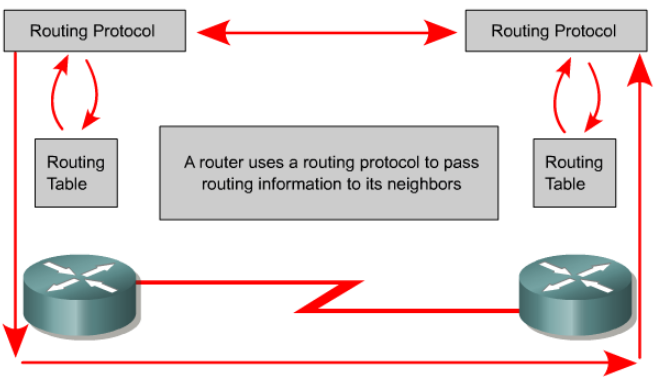
Per poter instradare i vari pacchetti, un router ha bisogno di alcune informazioni fondamentali, quali sono:

1. l'indirizzo IP dell'host di destinazione;
2. l'indirizzo dei router ad esso adiacenti;
3. i possibili percorsi alternativi per poter raggiungere reti remote.

Per valutare se un certo host con indirizzo X appartiene ad una sottorete con indirizzo Y/M, si effettua un'operazione di matching svolgendo X AND M = Y AND M: se il matching darà esito positivo per più righe nella tabella di routing, si attua la regola del ***Longest Prefix Match***, cioè si utilizza la riga con il maggior numero di bit in comune X AND M. Quindi, sostanzialmente, dato un pacchetto con indirizzo di destinazione, viene effettuato il matching con tutti gli indirizzi IP nella tabella di ***routing***: se la destinazione coincide con molteplici indirizzi della tabella di routing, allora tali indirizzi avranno maschere differenti. Verrà, quindi, scelto quello con maschera maggiore grazie al ***Longest Prefix Match*** e si proseguirà con la procedura ***ARP***.

È possibile effettuare ***due tipi di instradamento***:

1. ***routing statico,*** prevede il ***calcolo*** dei ***percorsi offline***, quando la rete non è ancora attiva, a carico dell'operatore;
2. ***routing dinamico,*** permette ai ***percorsi*** di ***cambiare dinamicamente*** in base alle situazioni di traffico ed altre condizioni.



Il ***routing statico*** è ingestibile in condizioni di reti complesse e le destinazioni non possono cambiare, mentre con il ***routing dinamico*** vengono utilizzati protocolli per costruire le ***tabelle di routing***: per costruire la tabella, ciascun router dovrà scambiare pacchetti informativi con i router ad esso collegati.

Livello Rete / Network: algoritmi basati sul percorso più breve

Una rete è rappresentabile sottoforma di grafo, dove ogni nodo rappresenta un router ed ogni arco rappresenta una linea di comunicazione, detta anche ***canale***. Per scegliere un percorso/cammino tra due router, l'algoritmo cerca il più breve tra essi considerando le ***metriche*** possibili, quindi la distanza geografica, costi e capacità.

Introduciamo, quindi, la ***metrica***, la quale offre una misurazione secondo un certo criterio: minore è la sua misurazione e più corto sarà il percorso. Uno degli algoritmi utilizzati per calcolare il percorso minimo è quello di Dijkstra (***Shorted Path First***): tale ***algoritmo mantiene in una tabella la più piccola distanza conosciuta*** per ogni destinazione e quale canale utilizzare per raggiungerla. Tali tabelle vengono aggiornate scambiando informazioni con i router vicini.

L'algoritmo di Dijkstra utilizza il protocollo ***distance vector***: l'idea è quella di partire dal nodo sorgente e di guardare i nodi adiacenti assegnando loro il valore del costo per raggiungerli.

Facciamo un esempio: B raggiunge A in 5ms, C raggiunge A in 8ms e D raggiunge A in 4ms. Se Z raggiunge B in 2 ms, Z raggiunge C in 3ms e Z raggiunge D in 5ms, allora il percorso più breve sarà il seguente:

Z -> 2ms -> B -> 5ms -> A

Quindi Z -> 7ms -> A

Livello Rete / Network: algoritmi basati sul percorso più breve con "protocollo flooding"

Il ***flooding*** è un protocollo di instradamento usato dal router che ***inoltra un pacchetto in ingresso su tutte le linee ad eccezione di quella da cui proviene*** e viene solitamente usato per trovare il ***percorso migliore***. Tale algoritmo genera un vasto numero di pacchetti duplicati, raggiungendo anche l'infinito, quindi si associa un contatore al fine di evitare ciò: se il contatore raggiunge lo 0, il pacchetto viene eliminato.

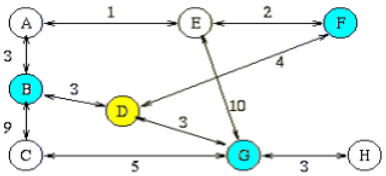
Gli aspetti negativi di questo algoritmo sono legati alla sua inefficienza, siccome manda ogni pacchetto su ogni rete provocando un utilizzo inefficiente della rete. Gli aspetti positivi riguardano il fatto che non c'è bisogno della conoscenza della topologia della rete che il pacchetto attraversa e che ogni pacchetto arriverà nel minor tempo possibile (siccome segue tutte le strade, quindi anche la più veloce).

Tale protocollo viene scarsamente utilizzato per via della sua inefficienza.

Livello Rete / Network: algoritmi di routing link state

Tali algoritmi nascono con l'intenzione di sostituire gli algoritmi ***Distance Vector*** e si basano sull'invio di pacchetti detti ***Link State Packet*** (***LSP***) contenenti le ***informazioni*** di ***costo*** e di ***ritardo*** di ***ogni link uscente dal nodo*** su cui si opera. La propagazione degli ***LSP*** avviene tramite ***flooding***. Ogni nodo utilizza queste informazioni per calcolare il costo minimo verso tutti i nodi. Quindi, sostanzialmente, il router operante associa ad ogni destinazione un costo dipendente dalla linea (***link***) che collega i due nodi adiacenti.

Una volta ottenute le informazioni da tutti gli altri router della rete, si costruisce il grafo di rete e si utilizza ***Dijkstra*** per trovare il cammino minimo.



Gli algoritmi ***LSP*** non possono gestire qualsiasi rete di qualsiasi dimensione, quindi occorre realizzare il routing in modo gerarchico, suddividendo la rete in aree.

Livello Rete / Network: differenze tra link state e distance vector

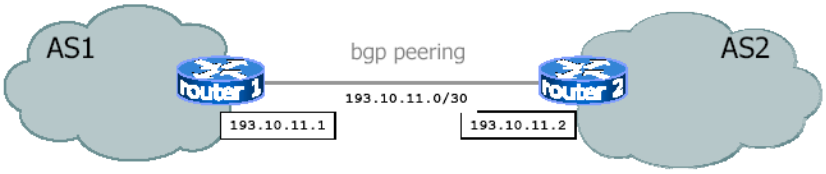
Sostanzialmente, i ***protocolli distance vector*** partono dal nodo sorgente e guardano i nodi adiacenti associando dei valori, quali saranno i costi per raggiungerlo. Si itera il ragionamento su ogni nodo.

I ***protocolli link state***, invece, mandano informazioni in flooding sulla rete.

Riassumendo, i ***link state*** mandano informazioni a ***tutti i router***, mentre i ***distance vector*** solo ai ***nodi adiacenti***.

Livello Rete / Network: approfondimento sugli AS

Il ***peering*** è la connessione tra due ***sistemi autonomi*** (***AS***) appartenenti a ***provider distinti***. L'instradamento tra due AS avviene sempre nello stesso modo che abbiamo discusso finora, con la differenza che esiste un unico algoritmo di instradamento tra organizzazioni adiacenti ed è necessario aggiornare le ***tabelle di routing*** manualmente aggiungendo ***percorsi statici***. Ogni AS ha una topologia strana, composta da molteplici reti locali. Non tutte le reti locali sono connesse ad un ***router di frontiera***, quindi è necessario comunicare all'esterno quali sono le reti raggiungibili. I router di frontiera permettono lo scambio di informazioni con altri router di frontiera, appartenenti ad AS differenti: ciò è possibile grazie al peering, il quale è la connessione tra due sistemi autonomi (AS) appartenenti a provider distinti.



Il ***router di frontiera***, quindi, ***fornisce comunicazione*** tra AS differenti e si occupa dell'***instradamento***. Le informazioni tra due AS possono essere scambiare solo se la sessione ***peering*** è attiva, la quale è una connessione TCP.

Protocolli riguardanti i router presenti negli AS sono i seguenti:

- ***IGP*** (***Interior Gateway Protocol***), protocolli che regolano l'instradamento dei pacchetti tra interior routers;
- ***EGP*** (***Exterior Gateway Protocol***), protocolli che regolano l'instradamento dei pacchetti tra exterior routers;
- ***BGP*** (***Border Gateway Protocol***), protocollo EGP che permette di collegare diversi border routers, quindi permette la comunicazione tra due o più AS differenti.

I protocolli IGP comprendono i protocolli ***distance vector*** e ***link state***.

Protocolli Data-Link per WAN e LAN: IBSS, BSS ed ESS

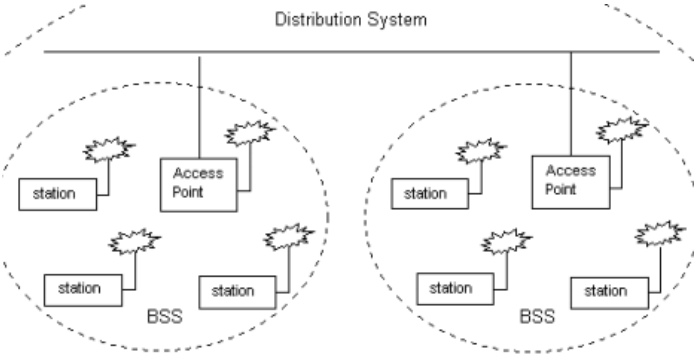
Nelle LAN i computer (o nodi) sono connessi tramite schede di rete e appositi cavi. Tra le reti LAN ci sono le ***Wireless LAN*** (***WLAN***), nel caso si voglia utilizzare una rete senza fili. La WLAN è una rete locale in cui tutti i nodi comunicano tramite il canale radio, quindi senza fili. I vantaggi che offre sono molteplici, quali sono la ***mobilità*** (è possibile spostarsi con i dispositivi entro un certo range senza problemi); l'estensibilità ed il non utilizzo di cavi, in modo da potersi connettere anche dove non riuscirebbero ad arrivare i cavi; i costi sono relativamente bassi rispetto ad una LAN cablata; la configurazione è dinamica e vasta, quindi le WLAN offrono alta scalabilità. Le bande utilizzate nelle ***WLAN*** sono ***2.4GHz*** e ***5GHz***.

Esistono due modalità di funzionamento per le WLAN: Ad ***Hoc Network*** (Independent Basic Service Set - IBSS) e ***Infrastructure Mode*** (Infrastructure Basic Service Set - BSS).

Le ***IBSS*** sono reti wireless in grado di connettere in maniera indipendente molteplici stazioni wireless tra loro senza l'utilizzo di un dispositivo centrale che faccia da tramite. Tale tipologia non è adatta in caso di reti con un gran numero di dispositivi.

Le ***BSS*** si basano su un ***Access Point*** (***AP***) ***cablato*** ad una LAN che funge da tramite per il traffico dei dispositivi wireless. Tale dispositivo permette l'accesso alla rete a dispositivi wireless. Nel caso si parli di AP pubblico, si parla allo stesso tempo di hotspot.

L'***AP*** si interfaccia con il ***Distribution System*** (***DS***), il quale non è altro che un dominio che ***raccoglie molteplici BSS*** che possono comunicare tra loro tramite i loro AP.



Altra tipologia di rete sono le ***Extended Service Set*** (***ESS***), la quale si basa sul collegamento di molteplici ***WLAN BSS*** al fine di generare un'area di copertura notevolmente maggiore. Tale collegamento è dovuto dal DS. Gli elementi di rete al di fuori dell'ESS, vedono l'ESS come una singola rete con molteplici stazioni mobili.