

Il protocollo deve essere scalabile, non ci devono essere messaggi inviati in broadcast.

Router

il router deve instradare i pacchetti nella rete da un qualsiasi host ad un qualsiasi host sulla base dell'indirizzo IP.

- i router si passano i pacchetti hop-by-hop
- i router sono dispositivi di livello 3 che collegano almeno 2 reti tra loro. Il router decide solo il prossimo hop, è in grado di accettare pacchetti di livello 3 che hanno come indirizzo IP un indirizzo diverso dal loro, ma devono avere il mac-address di destinazione giusto.

IP forwarding

dato un pacchetto in ingresso decidere a chi inviare il pacchetto

è una operazione effettuata da tutti i router. Gli host e i Router hanno una tabella di **Routing** in cui ciascuna riga fornisce il NEXT-HOP per ogni possibile destinazione. Se non si conosce c'è una regola di **default**: si inoltra il pacchetto ad un **default gateway**. Le dimensioni delle tabelle di routing potrebbero essere un limite, per questo sfruttano delle tecniche di **aggregazione** delle reti.

Sono detti protocolli di routing quei protocolli che servono a popolare le tabelle

Indirizzi IP

Ha una dimensione di **32 bit**, rappresentato ogni byte in maniera decimale; hanno lunghezza fissa e sono gerarchici, quindi sono indirizzi strutturati:

- le parti a sinistra sono più significative
- le parti a destra sono meno significative

La parte a sinistra è detta **NET-ID**: ci dice quale è l'identificativo della rete di cui si fa parte. La parte destra è detta **HOST-ID** identifica l'host all'interno della rete

Classi di indirizzamento

Esistevano 3 classi di indirizzamento utilizzabili dagli HOST ed erano **A, B, C**, una classe per multicast e una classe reserved.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

	First byte	Second byte	Third byte	Fourth byte
Class A	0 to 127			
Class B	128 to 191			
Class C	192 to 223			
Class D	224 to 239			
Class E	240 to 255			

Si è introdotto poi un meccanismo di tipo **classless**, ovvero si indica in una informazione apposita (**Netmask**) che specifica quanti bit del NETID sono fissi, in generale quanti sono di net-id e quanti sono di host-id.

a.b.c.d/n

- il /n è il CIDR e indica quanti bit sono fissi

Indirizzi speciali

Esistono degli indirizzi che non possono essere utilizzati:

- Loopback** (localhost) è una classe di indirizzamento di tipo A `127.0.0.0/8`, sono tutti indirizzi di localhost.
- Network address**: quando la parte di HOST-ID è tutta a 0, è l'indirizzo IP di RETE (ovvero identifica la rete)
- Broadcast**: in IP non esiste un broadcast che riguarda l'intera rete globale:
 - LIMITED: tutti i bit a 1 --> broadcast alla rete locale, non inoltrato dai router
 - DIRECTED: host-id tutto a 1 --> broadcast della rete (di uno specifico NET-ID)
- Nessun indirizzo**: tutti i bit a 0 --> usato per il boot o per configurazioni particolari

Indirizzi non routable

Sono indirizzi che non possono essere assegnati per accedere a internet, non vengono inoltrati dai router che gestiscono reti globali --> sono quindi PRIVATI

- `10.0.0.0/8`
- `172.16.0.0/12`

- 192.168.0.0/16

Subnetting

Data una rete di partenza, riesco a creare delle sotto-reti aventi lo stesso HOST-ID del padre

Gestione degli indirizzi pubblici

Ci sono organizzazioni che gestiscono l'assegnamento degli indirizzi IP pubblici --> ICANN (IANA, INTERNIC) e altre sotto-organizzazioni che gestiscono l'assegnamento degli indirizzi in base alle località. Questo fa in modo che gli indirizzi IP siano localizzati geograficamente.

Negli ultimi anni si è andati in contro all'esaurimento di indirizzi IP, ci sono stati 3 soluzioni:

- utilizzo di indirizzi classless
- uso di indirizzi privati per poi fare NATTING
- Passare al protocollo IPV6

Natting

Un router che fa non natting inoltra solamente i pacchetti. Uno che fa natting, invece, modifica l'indirizzo IP sorgente per poterlo far girare su internet. Il nat viene utilizzato anche per questioni di sicurezza: dall'esterno non si vedono gli indirizzi IP privati

- Indirizzo pubblico --> accessibile by default
- Indirizzo privato --> NON accessibile by default

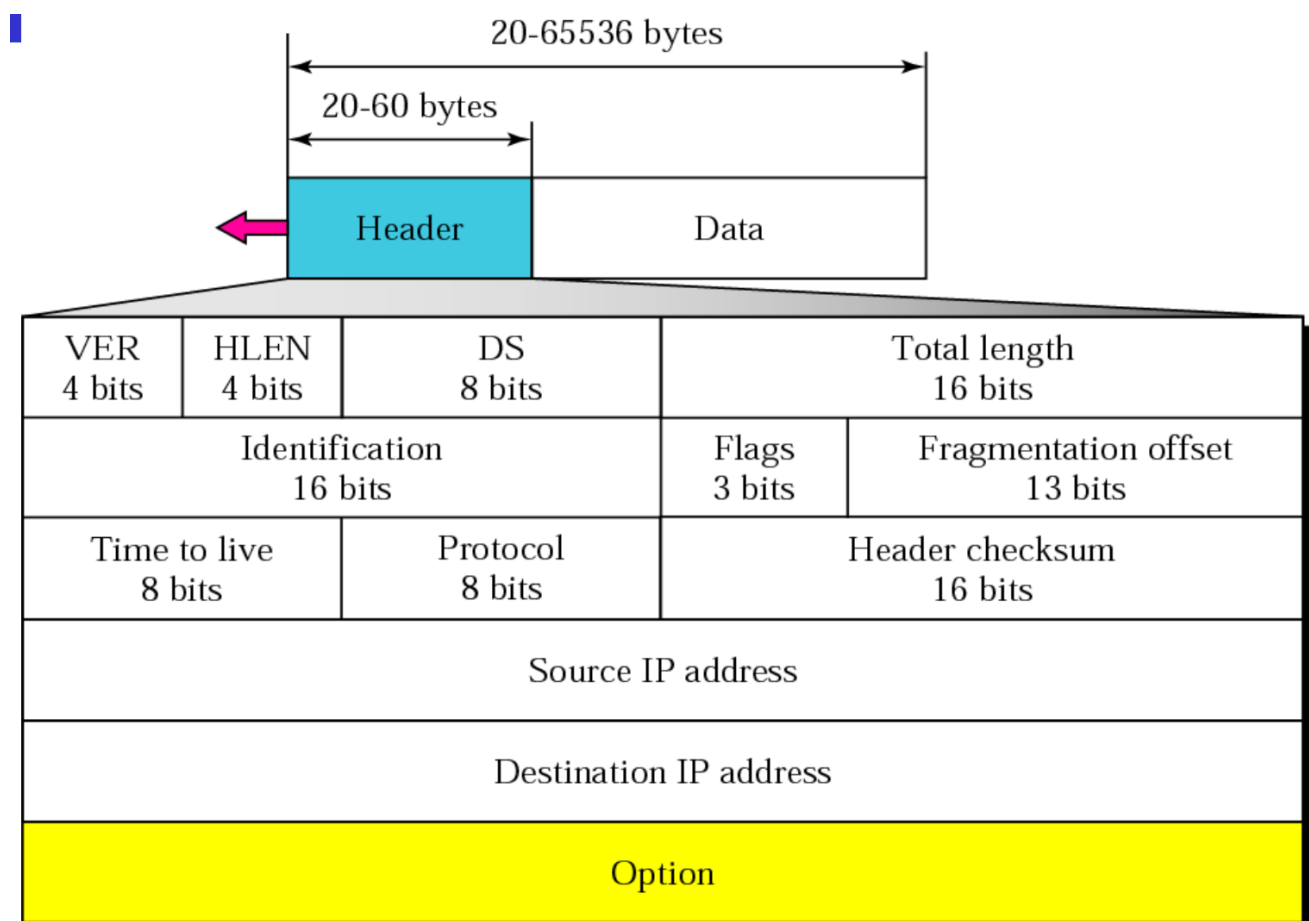
Alcuni protocolli applicativi sono limitati dal NATTING, rompe la comunicazione END-TO-END

Datagramma IP

Il pacchetto IP è lungo fino a 64 Kbyte ed è formato da HEADER e PAYLOAD.

Header IP

L'header del pacchetto IP è di lunghezza variabile.



- **VERS** (4 bit) --> Versione del protocollo
- **HLEN** (4 bit) --> Lunghezza dell'header, scritto in **word**, ovvero ti dice quante word da 32 bit è grande l'header
- **TOTAL LENGHT** (16 bit) --> dimensioni del pacchetto (compreso header) espresso in byte, quindi al massimo 64Kbyte
- **TOS** (type of service) --> impiego originale: si potevano settare dei bit per maneggiare il pacchetto in diversi modi. Attualmente diviso in 6 bit chiamati DSCP che vengono interpretati secondo classi di servizio (imitando l'utilizzo originale) e 2 bit di ECN: per la gestione della congestione dei router. (*rimane opzionale*)
- **Time to Live** (8 bit) --> contatore che conta quanti router ancora potrà attraversare il pacchetto prima di essere scartato (ogni router decrementa di 1 il TTL) serve ad eliminare il pacchetto in caso di Loop
- **Protocol** (8 bit) --> Serve per gestire il protocollo di livello 4
- **IP option** --> serve per fare test e debugging (sempre scritto in multipli di 4 byte se no viene aggiunto un PADDING)

Campi della frammentazione del pacchetto

IP è il payload di un protocollo H2N, non è detto che il pacchetto ci stia (spesso per via dell'MTU). La suddivisione è logica, basta suddividere il pacchetto in più pacchetti più piccoli e questi campi servono per la ricostruzione:

- **Identification** (16 bit) --> numero intero che rappresenta e identifica il pacchetto all'interno della connessione
- **Flag** (3 bit) --> bitmask che serve per gestire la frammentazione

- **Fragment offset** --> posizione del pacchetto fisico in base alla posizione del pacchetto originale

Non tutti i byte "costano" uguale: anche solo 1 byte in più può far sì che il pacchetto venga frammentato. La frammentazione può avvenire sul router che conosce gli MTU, ma c'è un problema:

- non si può frammentare un pacchetto già frammentato e ricostruirlo è costoso. La soluzione è mandare un pacchetto indietro che dice *packet too big* con allegato il nuovo MTU supportato.

C'è un bit di FLAG che se settato non fa frammentare il pacchetto. Questo tipo di flag è utilizzato per quello che viene detto **Path MTU discovery**, per capire qual'è il percorso più efficace per raggiungere una determinata destinazione.

È possibile anche che livelli superiori abbiano una logica loro di FRAMMENTAZIONE, l'importante è che questa logica venga implementata una sola volta nello stack.

Routing e AS

Esistono due tipi di routing

- INTERIOR --> stesso AS
- EXTERIOR --> fra diversi AS --> che parlano una lingua "comune"

Gli AS sono identificati da un ASN (Autonomous System Number), un numero di 2/4 byte univoco. Nessun AS gestisce più del 5% del traffico:

- un **Internet exchange point** è un punto di incontro tra tanti AS
 - Transit: un AS pagante paga un AS venditore per avere accesso o la possibilità di transito
 - Peering: scambio alla pari, non si paga
- un **Peering point** può essere un luogo fisico, più piccolo perché mette in comunicazioni piccoli ISP. Esistono diversi tipi di AS:
 - Transit
 - Multi-homed --> per quanto collegato a diversi AS, non permette il transito, ma solo connettività verso le sue gestioni
 - STUB --> AS connesso con una sola connessione ad un altro AS

Protocolli di Routing

Esistono diversi protocolli di routing dipendentemente dal contesto in cui ci si trova:

- protocolli di routing inter-AS (BGP) --> distribuito, non centralizzato
- protocolli di routing intra-AS
 - **Routing Information Protocol** (RIP) --> Distribuito
 - **Open Shortest path first** (OSPF) --> Centralizzato


Tutti questi protocolli servono per un motivo: dato un grafo che rappresenta la rete, trovare il percorso minimo:

- in internal i nodi sono dei router
- in external i nodi sono degli AS

La logica su cui si basa internet è a due livelli, dato che gli AS hanno in gestione dei blocchi di indirizzi (IP-PREFIX) il traffico si sviluppa nel seguente modo:

1. se Dest-IP è nell'AS allora faccio routing INTRA-AS
2. altrimenti invio il pacchetto a router di confine (che parlano tra AS) che mantengono mappe fra IP-PREFIX e AS.

Gli algoritmi di Routing globali sono globali, ovvero tutti conoscono la posizione e il percorso per raggiungere tutti. Esistono anche algoritmi di routing detti locali) dove non tutti conoscono la topologia di rete.

#todo  rivedere diff globali e locali, centralizzato e distribuito

Link State

Sono algoritmi globali, prevedono che la topologia e i costi di ogni link siano noti a tutti:

1. ogni nodo calcola lo stato dei link ad esso connesso
2. ciascun nodo periodicamente trasmette identità e costi dei suoi link
3. per trovare il percorso minimo si usa l'algoritmo di **Dijkstra**

L'invio dell'informazione avviene tramite pacchetti che prendono il nome di **LSP** contenenti:

- Node ID
- Lista dei vicini e costo dei link
- informazioni aggiuntive: - Numero di sequenza - TTL L'inoltro di questi pacchetti viene fatto con un algoritmo di FLOODING (inondazione). Quando **i** riceve un pacchetto LSP da **j**:
- se il pacchetto è valido --> salva e inoltra
- altrimenti lo scarta

L'algoritmo di **forward search** viene fatto tramite **Dijkstra**, non si potrebbe utilizzare se non si conoscesse tutta la rete, o se non si è sicuri della rappresentazione di essa

Distance vector protocol

È un calcolo distribuito del net-hop. È adatto a:

- una rete che cambia
- è basato su un algoritmo iterativo
- è asincrono L'unità di scambio è la **distance** ovvero il "costo" delle varie tratte.

A differenza del link state qui si utilizza l'algoritmo di **bellman-ford**: Ogni nodo conosce le info dei nodi adiacenti, al posto di fare flooding si inviano le informazioni solo ai nodi vicini. L'aggiornamento è basato su informazioni locali, il valore percorso ottimo si

otterrà dopo diverse iterazioni. Questa informazione serve per popolare le tabelle di routing

Problemi

1. I link possono cambiare --> in un contesto del genere (decentralizzato) non è detto che si arrivi a una soluzione ottima o è possibile che si creino dei cicli
2. Effetto rimbalzo --> scambiarsi informazioni locali su collegamenti globali introduce una propagazione dell'errore, non converge mai.

Per evitare il COUNT-TO-INFINITY si sceglie una soglia bassa per rappresentare l'infinito (una volta era 16). Oppure si utilizza lo SPLIT-HORIZON --> non invio al next-hop i costi che coinvolgono quel next-hop come passaggio. (su alcune reti complicate non funziona)

L'unico modo per evitare i cicli è mandare un PATH VECTOR --> invece di inviare solo la distanza e di salvarci solo il next-hop, ci salviamo e inviamo l'intero percorso per quella destinazione

Protocollo RIP (intra-AS)

È un protocollo di tipo distance-vector, con alcune semplificazioni:

- il costo deriva dal numero di hop (un grafo con ogni link a costo 1)
 - facendo così sceglie sempre i collegamenti diretti

Limiti

- fattibili su reti solo a 16 hop
- non reagisce molto bene a un cambiamento

Protocollo OSPF

Protocollo centralizzato Link-state con possibilità di aggiungere sicurezza:

Problema del routing

Se un router mi manda informazioni false, in un contesto decentralizzato è molto difficile capirlo. In OSPF esistono funzionalità crittografiche che permettono la certificazione delle informazioni

Protocollo BGP

È un protocollo decentralizzato di tipo distance-vector ampliato a path-vector, è decentralizzato perché lavora sugli AS. In BGP ci si scambiano anche le POLICY --> per via dei rapporti degli AS, non è detto che AS1 permetta il transitare di pacchetti provenienti da AS2. Esistono due tipi di router in BGP:

- Transit Router --> I-BGP (internal)
 - se ho due border router dentro ad un AS se ho un pacchetto che transita in questo AS io metto in collegamento questi due router tramite BGP

- Edge Router --> E-BGP (external) I router di bordo parlano sia in BGP sia nel protocollo interno agli AS. Il protocollo BGP impone che gli AS dichiarino quali prefissi di rete sono di sua competenza.