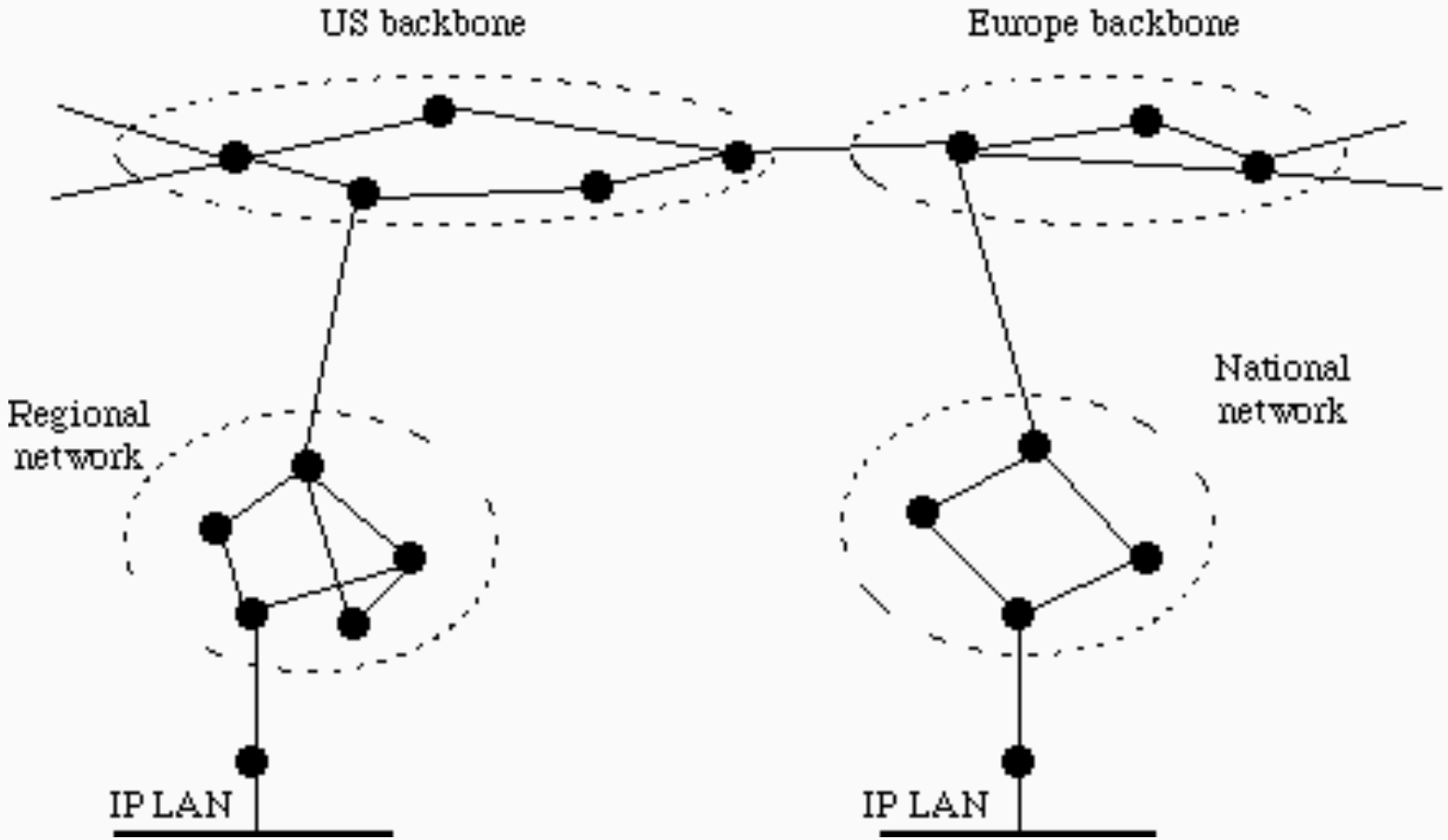
Livello di rete in Internet

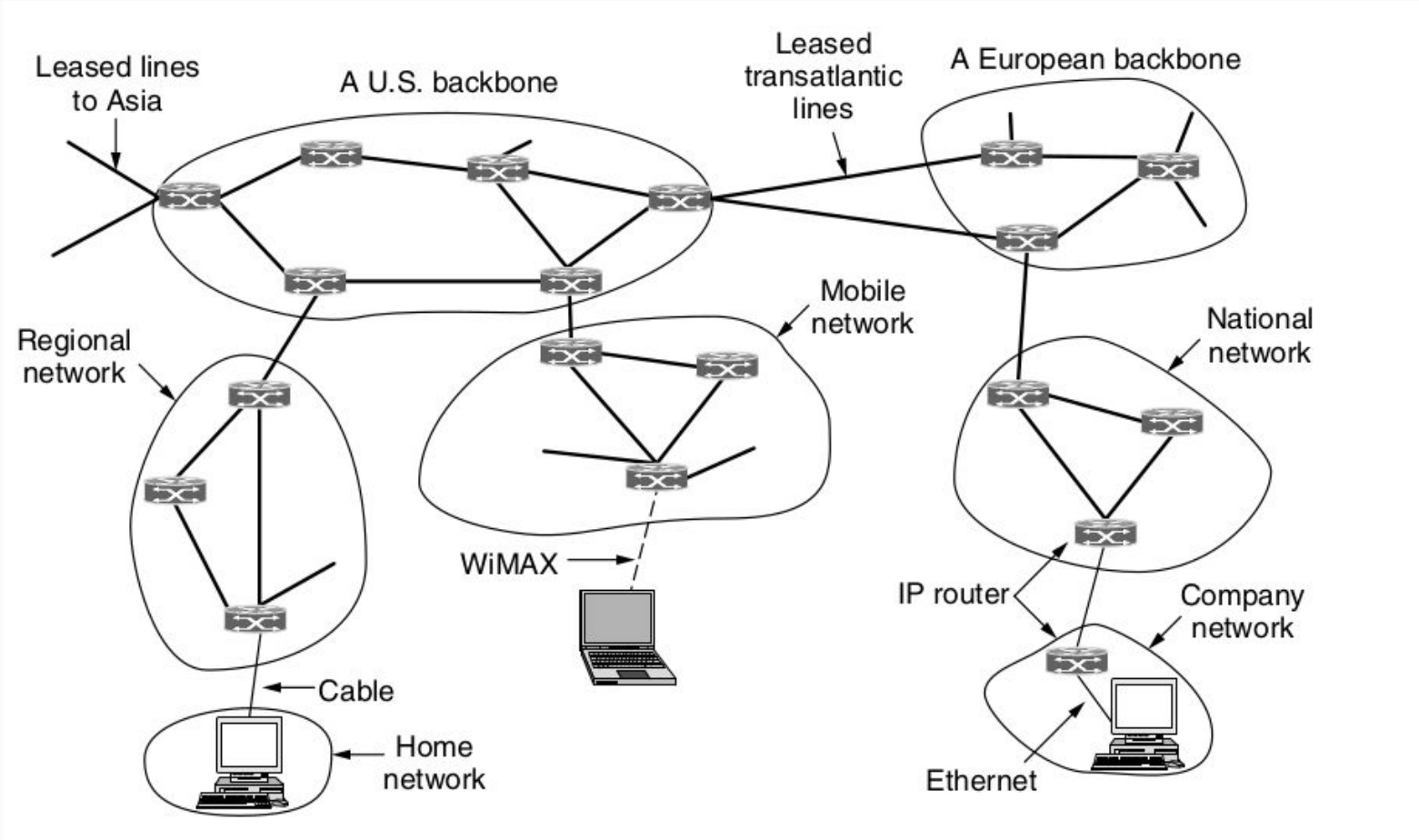
Livello di rete in Internet

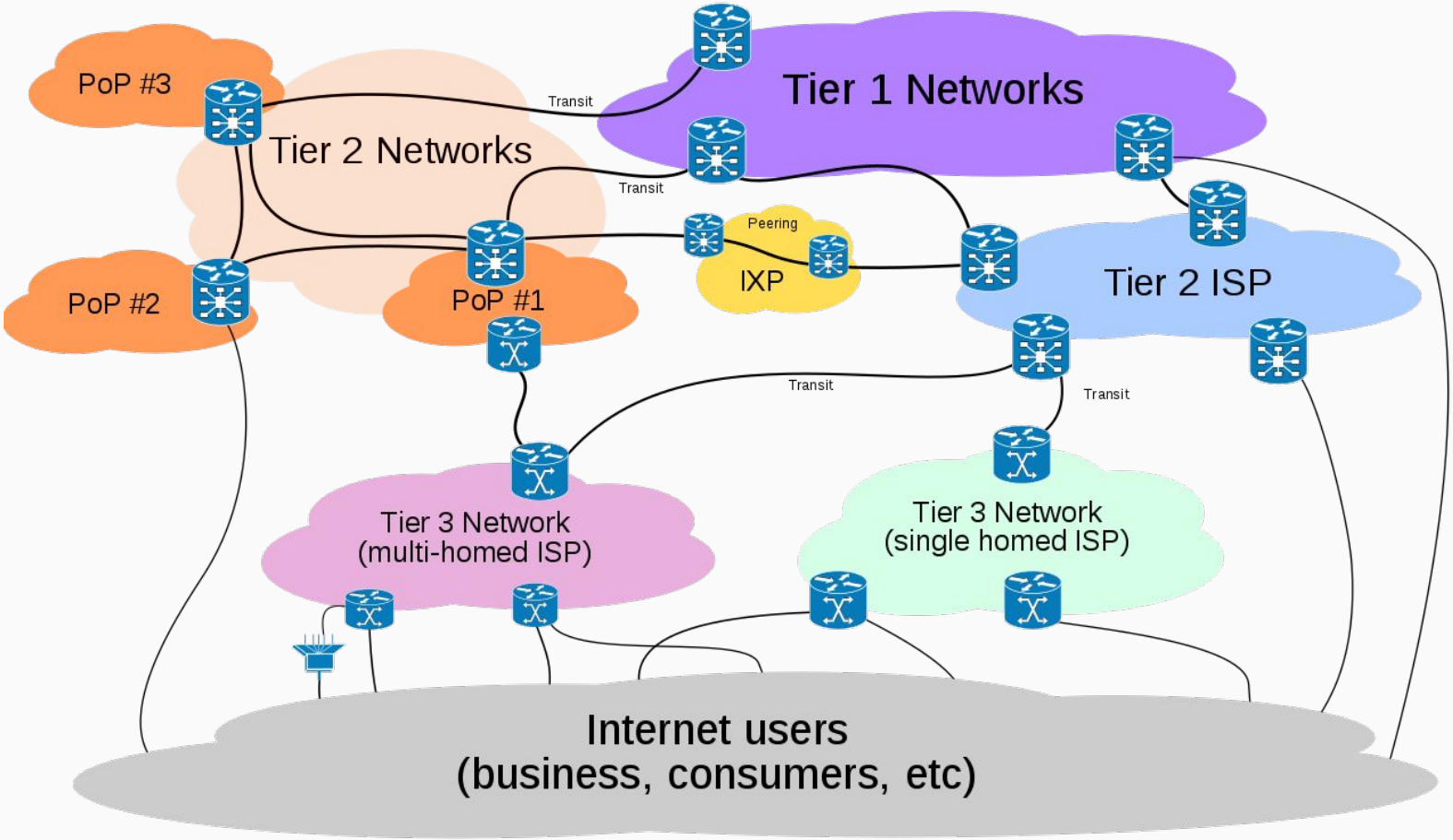
Internet è una collezione di sistemi autonomi (AS) connessi gli uni con gli altri, in cui possiamo distinguere alcune componenti:

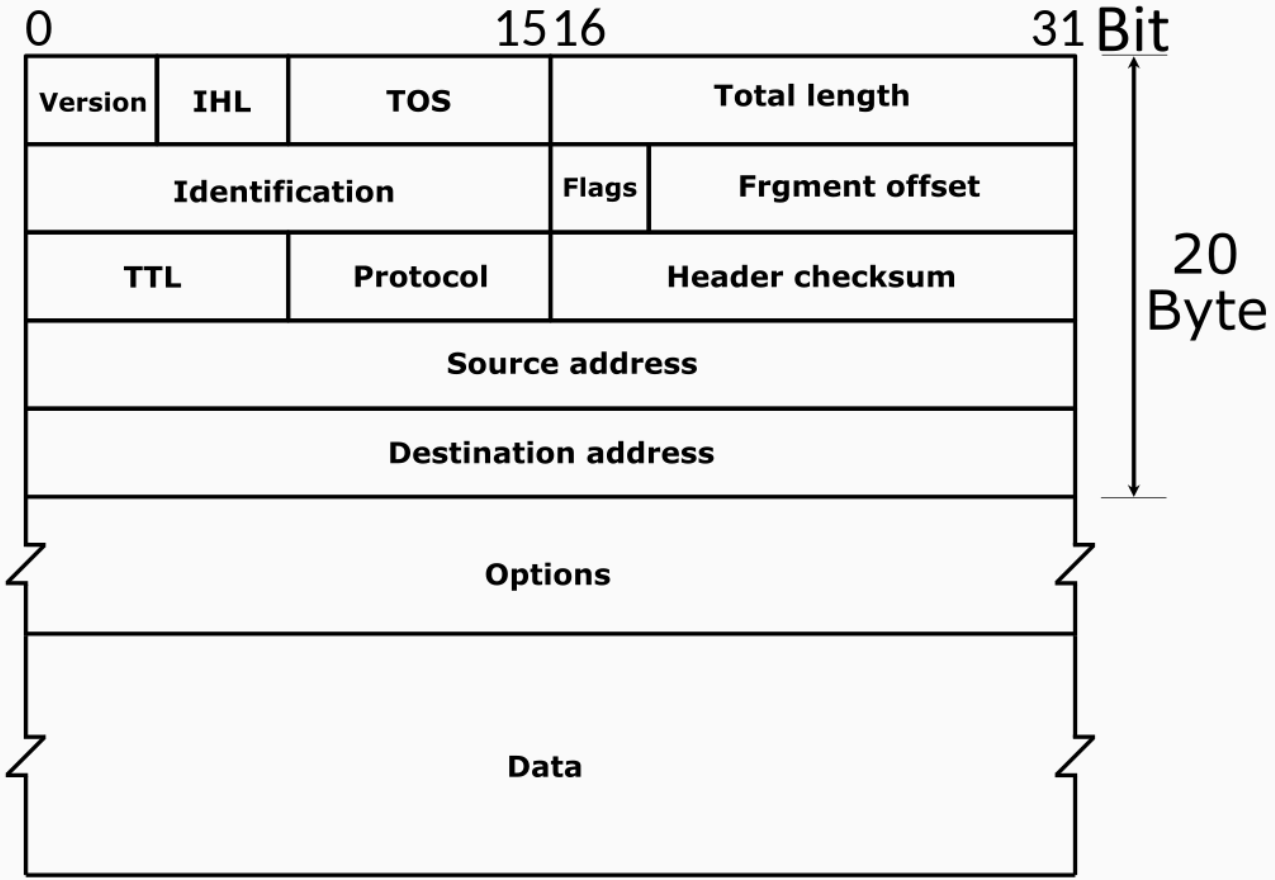
- dorsali (backbone) principali (Tier 1 networks), realizzate con linee ad alta velocità;
- collegati alle dorsali ci sono:
  - ISP, che forniscono l'accesso a aziende, abitazioni, data center….;
  - reti regionali di medio livello (Tier 2 networks);
- collegati alle reti regionali ci sono altri ISP, reti di Università, aziende altre reti di confine



http://wwwusers.di.uniroma1.it/Reti1/Cap5.pdf


Leased lines to Asia
A U.S. backbone
Leased transatlantic lines
A European backbone
Mobile network
National network
Regional network
WiMAX
IP router
Company network
Cable
Home network
Ethernet





Intestazione IPv4

Version:

il numero di versione del protocollo (4).

IHL:

lunghezza dell'header in parole di 32 bit (minimo 5, massimo 15).

Differentiated services:

caratterizza affidabilità e velocità richieste, nel caso sia implementata la qualità del servizio.

Intestazione IPv4

Total length
: lunghezza del pacchetto (inclusi dati), massimo 65.535 byte.

Time to live
: contatore (inizializzato a 255) che viene decrementato di uno a ogni hop. Quando arriva a zero, il pacchetto viene scartato.

Protocol
: codice del protocollo di livello di trasporto a cui consegnare i dati (i codici sono definiti in RFC 1700).

Intestazione IPv4

Header checksum

checksum per verificare l'integrità dell'intestazione, viene ricalcolato ad ogni hop perché time to live cambia.

Source address:

indirizzo del mittente.

Destination address

indirizzi del destinatario.

Options

opzioni, in pratica non è più utilizzato.

IPv4: frammentazione

Ogni rete è caratterizzata da una MTU (Maximun Trasmission Unit), che è la dimensione massima dei pacchetti che la possono attraversare.

Nelle reti IPv4 se un pacchetto è più grande della MTU di un router che incontra durante il percorso, viene frammentato in frammenti di 576 byte (minima MTU ammessa in Internet).

I frammenti di un datagram viaggiano in pacchetti separati, frammenti dello stesso datagram potrebbero seguire percorsi diversi.

IPv4: frammentazione

La ricostruzione del datagram originale a partire dai frammenti viene fatta dall'entità IP del router di destinazione.

Ci si basa sui valori dei campi dell'header:

Identification

tutti i frammenti di uno stesso pacchetto hanno lo stesso valore;

IPv4: frammentazione

DF
: don't fragment (se uguale a 1, non si deve frammentare il pacchetto a costo di scegliere una strada meno veloce).

MF
: more fragments (se uguale a 1, il pacchetto non è ancora finito).

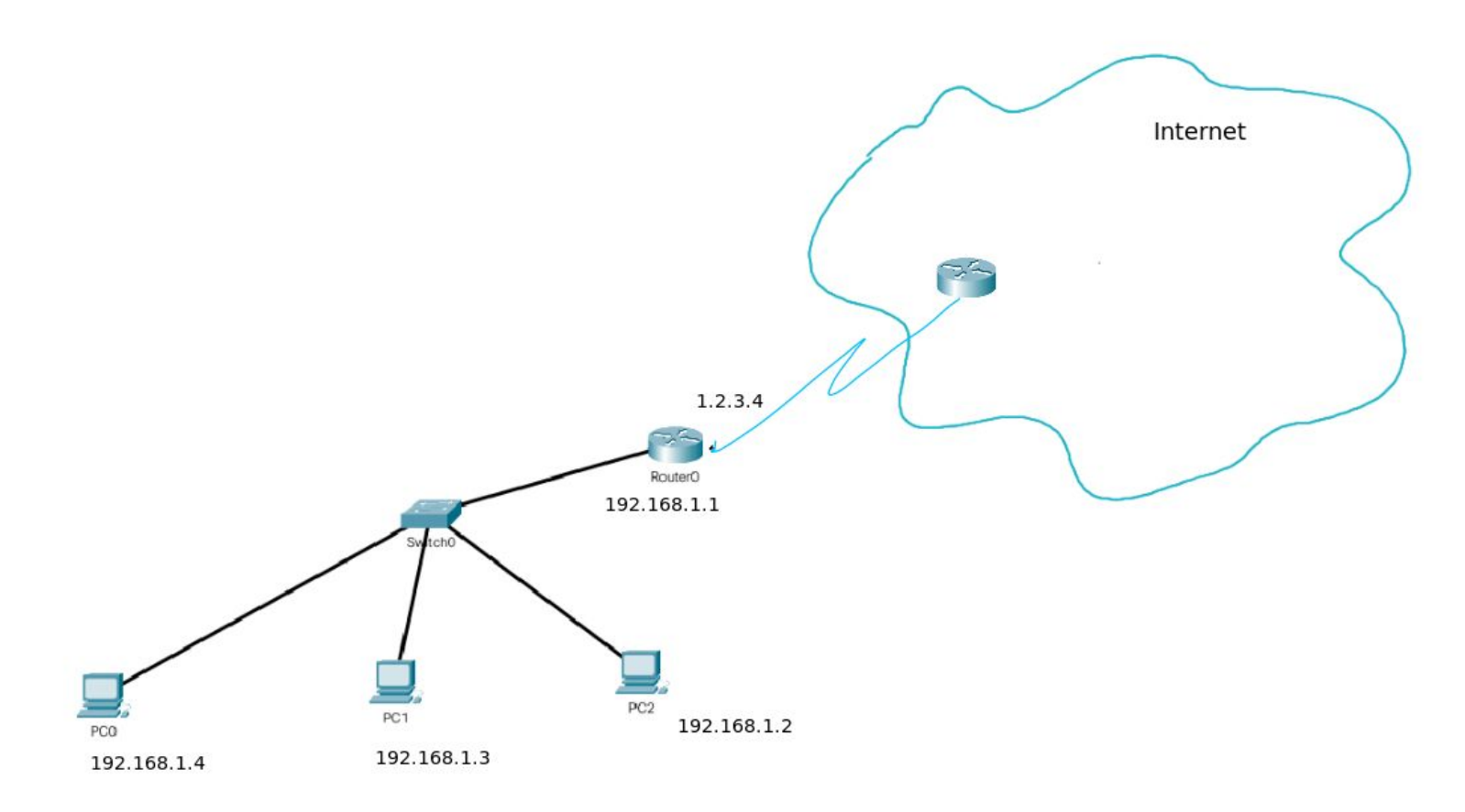
Fragment offset
: posizione del frammento nel pacchetto.

NAT: Network Address Translation (RFC 1631)

È una tecnica utilizzata per collegare a Internet una rete LAN che utilizza indirizzi interni privati. Ciò avviene utilizzando l'indirizzo IP pubblico che il router ha verso l'esterno.

Tutti i pacchetti in uscita dalla LAN quindi avranno lo stesso indirizzo IP (pubblico) sorgente, il problema è determinare a quale nodo interno inoltrare le eventuali risposte, che avranno tutte come indirizzo di destinazione il router.

Source NAT esempio



Source NAT - esempio

Indirizzo privato	Porta privata	Indirizzo esterno	Porta esterna	Porta NAT
192.168.1.2	21023	128.10.19.20	80	14003
192.168.1.4	386	128.10.19.20	80	14010
192.168.1.2	26600	207.200.75.12	21	14012
192.168.1.3	1274	128.210.1.5	80	14007

In uscita il NAT sostituisce nell'intestazione IP l'indirizzo sorgente con il proprio indirizzo IP pubblico e nel segmento TCP in numero di porta sorgente con un nuovo numero (porta NAT) che serve a garantire l'univocità delle TSAP utilizzate.
In ricezione si confrontano nel pacchetto in ingresso:

- porta di destinazione con porta NAT
- indirizzo e porta sorgente con indirizzo e porta esterna

se si trova una riga che corrisponde, nel pacchetto la porta destinazione e l'indirizzo di destinazione vengono sostituiti con porta e indirizzo privato corrispondenti.

NAT

Il NAT offre anche una (minima) protezione alla rete interna, perché le tabelle vengono costruite sulla base di richieste di connessione che client interni fanno verso server esterni.

Pacchetti in arrivo che non trovano riscontro nelle tabelle NAT vengono scartati e non è possibile attivare dall’esterno connessioni verso server interni.

Destination NAT

È usato per rendere accessibili dall’esterno i server in esecuzione in reti con indirizzo IP privato.

Serve una configurazione statica in cui si specifica a quale indirizzo IP locale destinare tutti i pacchetti in arrivo all’indirizzo IP pubblico del server su una determinata porta (es. porta 80 per il server Web).

ARP (Address Resolution Protocol, RFC 826)

Serve per derivare, dall'indirizzo IP dell'host di destinazione, l'indirizzo di livello data link necessario per inviare il frame contenenente il pacchetto da inoltrare.

Opera a livello due: con un broadcast di livello due viene inviata una ARP Request con cui si chiede chi ha un determinato indirizzo IP.

La stazione con quell'indirizzo IP risponde, inserendo nella risposta il proprio indirizzo data link.

ICMP (Internet Control Message Protocol, RFC 792)

È il protocollo utilizzato nelle reti IP per la segnalazione di eventuali errori e per la generazione di messaggi amministrativi e di stato.

È incluso in tutte le implementazioni di IP e quindi risiede in ogni computer host o router che utilizza l'IP.

ICMP (Internet Control Message Protocol, RFC 792)

Viene utilizzato ad esempio quando:

- i pacchetti non possono essere consegnati;
- un router non ha sufficienti buffer per conservare ed inoltrare i pacchetti;
- una destinazione non è raggiungibile;
- un pacchetto ha superato il TTL;
- l'header non è corretto;
- ….

ICMP (Internet Control Message Protocol, RFC 792)

I messaggi ICMP sono inseriti nel payload di un pacchetto e vengono generati/gestiti direttamente dall'entità IP sorgente/destinazione.

Il formato del pacchetto ICMP prevede:

- tipo, indica un particolare messaggio ICMP;
- codice, viene usato in alcuni messaggi ICMP per specificare alcune condizioni;
- checksum , per il controllo di errore; viene calcolato su tutto il pacchetto ICMP.

Nel pacchetto inoltre possono esserci dei dati legati al particolare messaggio ICMP.

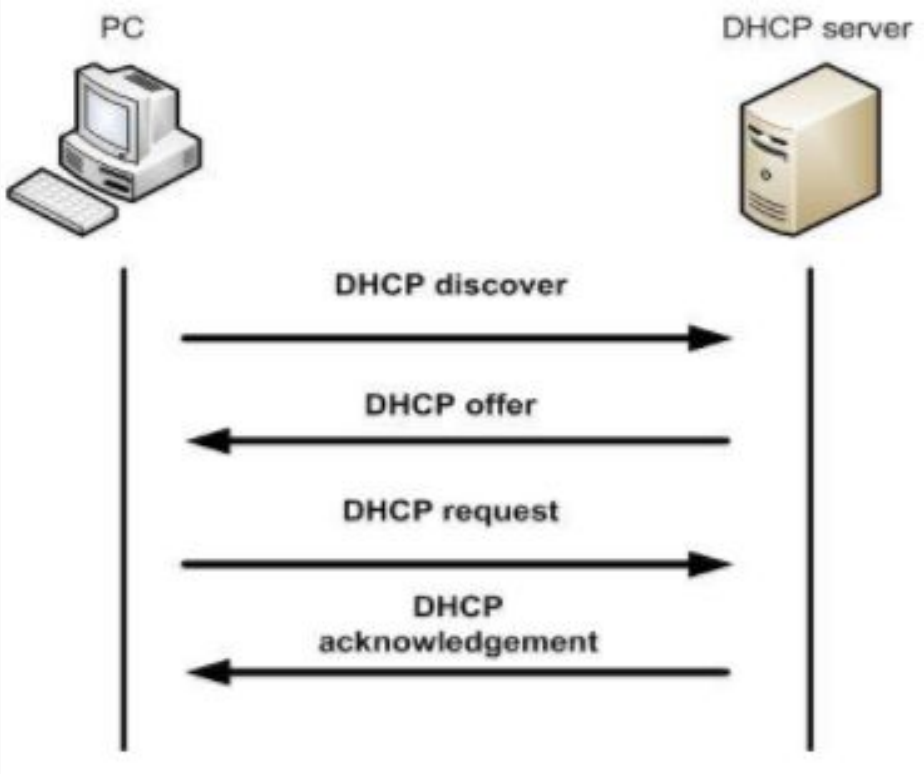
ICMP (Internet Control Message Protocol, RFC 792)

I principali tipi di messaggio ICMP sono:

- destination unreachable: non si trova la destinazione del pacchetto. Viene inviato al mittente del pacchetto;
- time exceeded: il contatore di un pacchetto è arrivato a zero. Viene inviato al mittente del pacchetto;
- redirect: il router ha ragione di pensare che il pacchetto gli è arrivato per errore, ad esempio perché un host mobile si è spostato. Viene inviato al mittente del pacchetto;

ICMP (Internet Control Message Protocol, RFC 792)

- echo request, reply: si vuole sapere se una destinazione è raggiungibile. Si invia request, si aspetta reply. È utilizzato dai protocolli di routing dinamico e per testare il funzionamento della rete (comando ping).
- timestamp request, reply: come il precedente, con in più la registrazione dell'istante di arrivo e di partenza, per misurare le prestazioni della rete.



https://www.greycampus.com/opencampus/ethical-hacking/dhcp-poisoning

DHCP (Dynamic Host Configuration Protocol, RFC 2131)

l protocollo DHCP, che opera al livello applicazione, ha lo scopo di consentire ad un computer che deve connettersi ad una rete locale di configurare automaticamente i parametri necessari:

- indirizzo IP e prefisso;
- indirizzo del default gateway;
- indirizzo del server DNS.

DHCP (Dynamic Host Configuration Protocol, RFC 2131)

La configurazione automatica è particolarmente utile nel caso di dispositivi mobili, che vengono spesso spostati da una LAN ad un'altra.

All'interno della LAN vengono installati uno o più server DHCP che hanno lo scopo di "ascoltare" le richieste e rispondere adeguatamente.

Ciascun server DHCP ha a disposizione un gruppo di indirizzi IP e tiene via via conto di quelli liberi e di quelli già assegnati.

DHCP (Dynamic Host Configuration Protocol, RFC 2131)

Client e server DHCP operano utilizzando l'UDP:

- nel momento in cui ha bisogno di configurarsi, il client invia una DHCPDISCOVER in broadcast di livello 3 (indirizzo IP sorgente 0.0.0.0, e destinazione 255.255.255.255;
- eventuali server DHCP presenti possono rispondere con una DHCPOFFER (indirizzata a livello 2 al client che ha fatto la query) in cui propongono un indirizzo IP e gli altri parametri di configurazione al client.

DHCP (Dynamic Host Configuration Protocol, RFC 2131)

Il client:

- se riceve più offerte, il client ne selezione una;
- in ogni caso il client invia in broadcast una DHCPREQUEST specificando nel campo "server identifier", quale server ha selezionato;
- il server selezionato conferma, sempre in broadcast, l'assegnazione dell'indirizzo con un pacchetto DHCPACK;
- gli altri server vengono automaticamente informati che la loro offerta non è stata scelta dal client.

Routing in Internet

Internet è una collezione di sistemi autonomi (AS) interconnessi.

Il routing è organizzato in maniera gerarchica:

- routing all'interno del sistema autonomo utilizzando un IGP (Interior Gateway Protocol);
- routing tra i diversi sistemi autonomi utilizzando un EGP (Exterior Gateway Protocol).

Routing in Internet

La definizione classica di un sistema autonomo è:

Un insieme di router connessi sotto il controllo di uno o più operatori di rete per conto di una singola entità amministrativa o dominio che presenta una politica di routing comune e chiaramente definita a Internet.

A ogni AS viene assegnato un numero univoco che identifica in modo univoco ogni rete su Internet e che viene utilizzato nel routing esterno.

Routing in Internet

Se un router deve instradare un pacchetto a un altro router appartenente allo stesso AS, avrà nella propria tabella di routing l'informazione di raggiungibilità idonea.

Se al contrario è necessario raggiungere un router che appartiene ad un differente AS il pacchetto viene inviato attraverso una coppia di exterior router, almeno uno per AS.

Ciascun exterior router conosce le reti raggiungibili utilizzando i link che lo collegano agli altri exterior router, ma non conosce il modo in cui queste reti sono di fatto connesse all'interno dei rispettivi AS, secondo un modello tipicamente gerarchico.

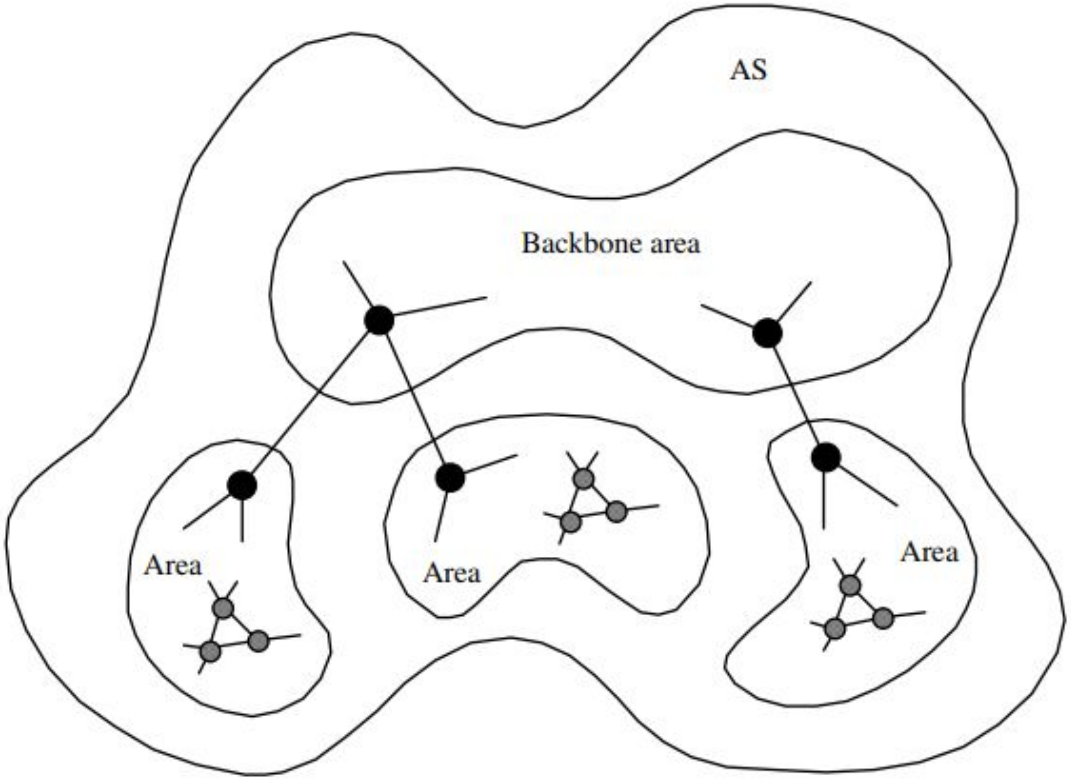
OSPF

OSPF (Open Shortest Path First, RFC 1247) è il protocollo di routing interno di Internet che sta gradualmente sostituendo RIP.

È basato sull'algoritmo link state routing e prevede la possibilità di organizzare gerarchicamente anche il routing interno.

L'AS in questo caso viene suddiviso in diverse aree, di cui una è l'area di backbone ed è connessa a tutte le altre aree

OSPF (Open Shortest Path First, RFC 1247)



http://wwwusers.di.uniroma1.it/Reti1/Cap5.pdf

BGP (Border Gateway Protocol, RFC 1654)

È basato sul distance vector routing, con due differenze:

- può gestire politiche di instradamento non necessariamente legate ai costi, ma derivanti da considerazioni di carattere geopolitico (ad esempio, da leggi nazionali) che vengono configurate manualmente nei router;
- mantiene (e scambia con gli altri router) non solo il costo per raggiungere le altre destinazioni, ma anche il cammino completo, risolvendo così il problema del conteggio all'infinito.

IP versione 6

Il progetto di una nuova versione del protocollo IP era stato lanciato nel 1990 IETF (Internet Engineering Task Force) con gli obiettivi di:

- supportare miliardi di nodi;
- ridurre la dimensione delle tabelle di routing;
- semplificare il protocollo, per rendere il funzionamento dei router più veloce;
- introdurre elementi di sicurezza (gestione di autenticazione e privacy);
- gestire il tipo di servizio, in particolare per i dati real time;
- permettere al protocollo di evolvere nel futuro;
- permettere alla versione nuova di coesistere con la vecchia.

IPv6

La nuova versione del protocollo è stata selezionata nel 1998 ed è descritta negli RFC dal 2460 al 2466. Le sue principali caratteristiche sono:

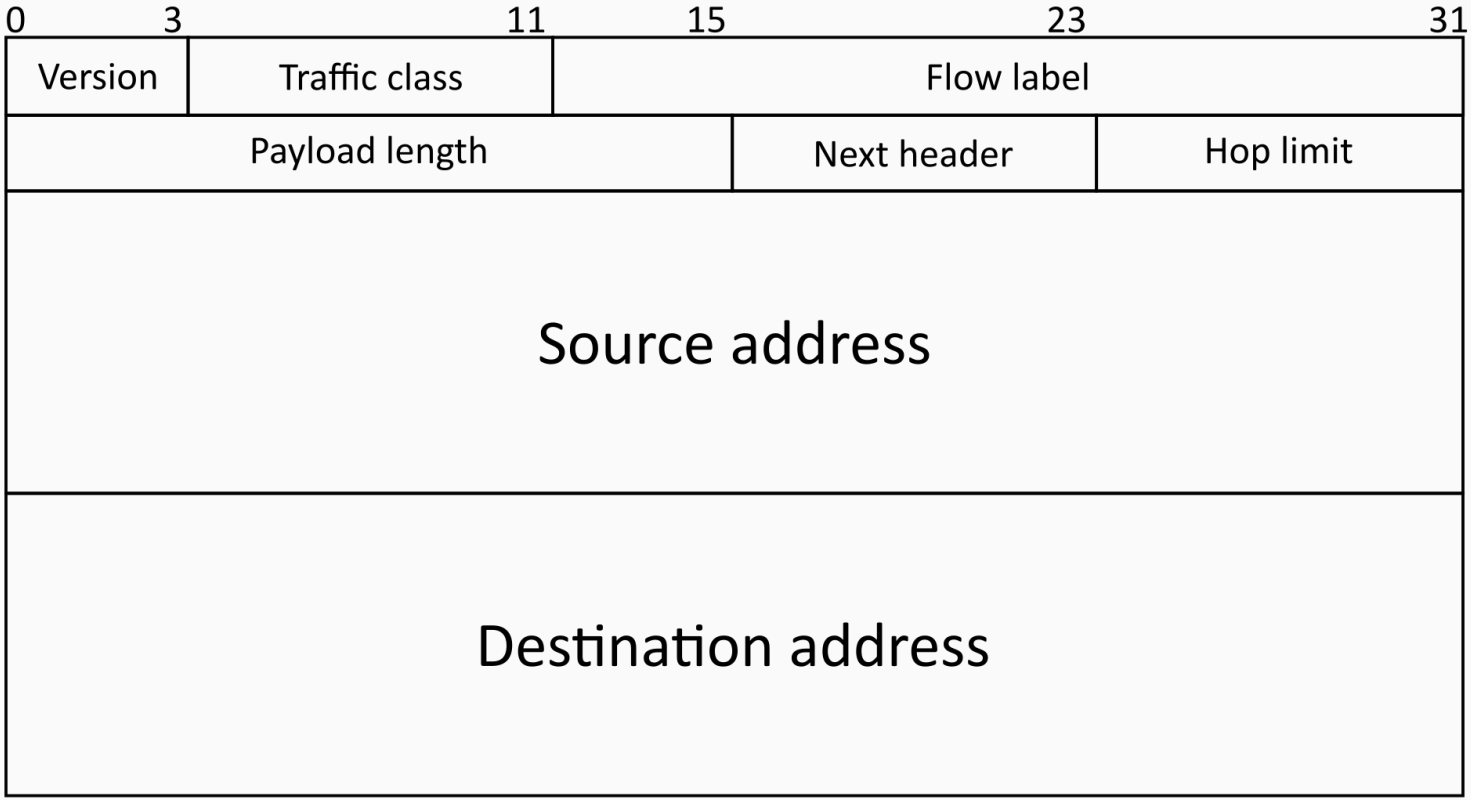
- ★ indirizzi a 128 bit, il che consente di avere un numero di indirizzi(655.570.793.348.866.943.898.599 indirizzi IPv6 per metro quadro della superficie terrestre) sicuramente sufficiente alle esigenze attuali e future per molti anni;

IPv6

- ★ l’header è semplificato (solo sette campi rispetto ai ai tredici di IPv4), e questo permette ai router di sveltire l'inoltro, aumentando il throughput e diminuendo i ritardi;
- ★ è migliorato supporto per le opzioni, e anche questo velocizza il processo di inoltro;
- ★ grazie alla storia precedente, è stato possibile migliorare alcuni aspetti relativi alla sicurezza e alla privacy;
- ★ è stata posta attenzione alla qualità del servizio, in modo da poter trattare diversamente le diverse tipologie di dati trasmessi.

Formato del pacchetto IPv6

Intestazione principale del pacchetto IPv6



Intestazione principale

- Version: la versione del protocollo, in questo caso sei. Analizzando questo campo i router possono distinguere tra i pacchetti Ipv4 e Ipv6 durante il periodo di coesistenza dei due protocolli.

Intestazione principale

- Traffic class: è usato per distinguere la classe di servizio per pacchetti con diverse esigenze di consegna. In pratica identifica i pacchetti che appartengono a una stessa classe di traffico e quindi distinguere tra loro i pacchetti con diversa priorità.

  Ad esempio può essere utilizzato da un ISP per differenziare il traffico immesso nella rete un suo cliente o per assegnare una classe a tutti i pacchetti in uscita verso altre reti, al fine di assegnare una classe di servizio concordata con altri.

Intestazione principale

- Flow label: questo campo è stato previsto per permettere l'utilizzo di pseudoconnessioni.

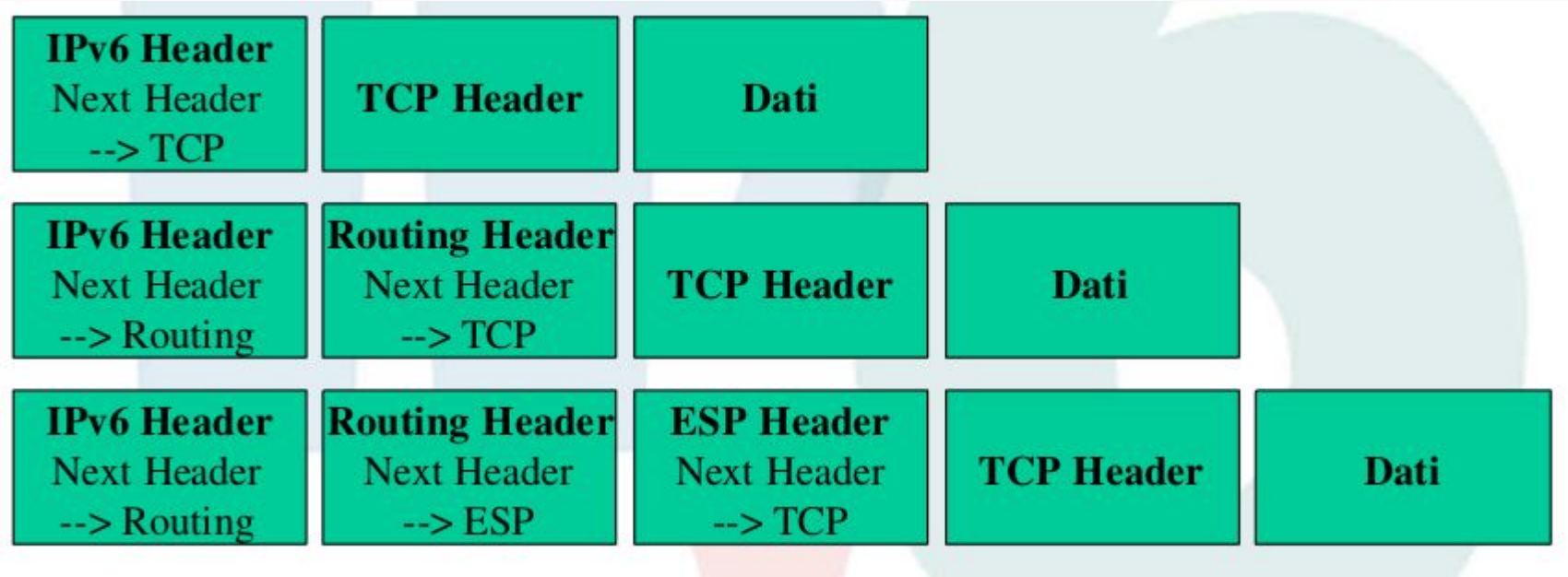
  Se il campo ha un valore diverso da zero, allora tutti i pacchetti di uno stesso flusso (con identica flow label e identici indirizzi IP sorgente e destinazione) devono ricevere lo stesso trattamento da tutti router.

Intestazione principale

- Payload length: indica la lunghezza in byte del payload.

- Next header: questo campo indica quale delle sei intestazioni di estensione (se ce ne sono) segue l'intestazione principale. Se non ci sono altre intestazioni, il campo indica il protocollo a cui va consegnato il payload secondo le codifiche del campo protocol dell'intestazione IPv4.

Campo Next Header e “catena” delle intestazioni

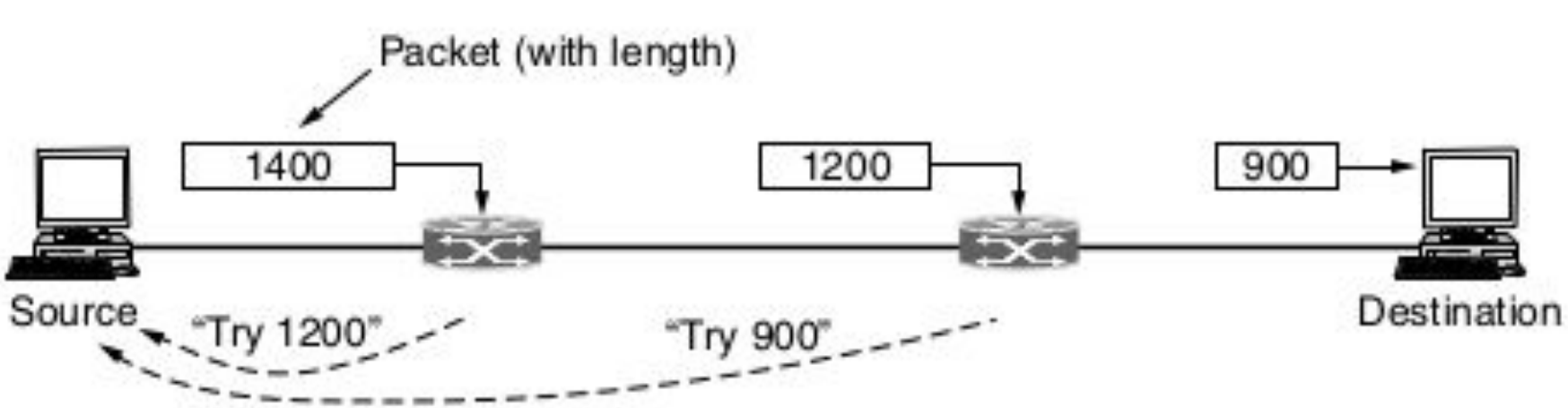


Intestazione principale

- Hop limit: è analogo al time to live di IPv4, è un numero che viene decrementato da ciascun router che inoltra il pacchetto, se arriva a 0 il pacchetto viene scartato.

- Source Address e Destination Address sono i due campi dell'intestazione destinati a contenere rispettivamente l'indirizzo sorgente e destinazione del pacchetto.

Path MTU discovery



Path MTU discovery

Quando un nodo invia un pacchetto troppo grande, il router che non è in grado di trasportarlo lo scarta ed invia al sorgente un messaggio di errore per segnalare la dimensione massima che dovranno avere i futuri pacchetti in quella direzione.

La dimensione minima della MTU dei router è stata portata da 576 a 1280 byte per permettere il passaggio di pacchetti con payload di 1024 byte.

Formato degli indirizzi IPv6

Un indirizzo IPv6 è rappresentato usando 8 quartetti di cifre esadecimali separati dal simbolo ':', ad esempio:

FE80:0000:0000:0000:0001:0800:23E7:F5DB

Per brevità gli 0 iniziali di ogni gruppo possono essere omessi, quindi ad esempio l'indirizzo riportato sopra diventa:

FE80:0:0:0:1:800:23E7:F5DB

Formato degli indirizzi IPv6

Per omettere un gruppo (uno solo) di zeri consecutivi si usa il simbolo '::'

FE80::1:800:23E7:F5DB

L'organizzazione degli indirizzi è gerarchica (rete - host nella rete), a ogni rete fisica è associato un prefisso. Nella configurazione di un nodo si deve specificare la lunghezza del prefisso, che sostituisce definitivamente la maschera di sottorete.

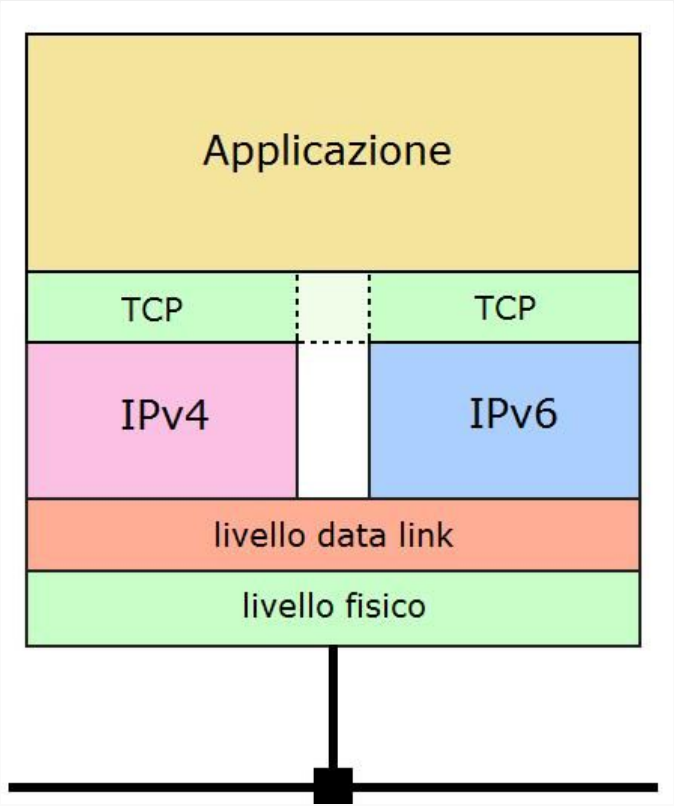
Transizione IPv4 IPv6

Il passaggio dalla versione 4 alla versione 6 di IP è reso particolarmente complicato dal fatto che i due protocolli sono sostanzialmente incompatibili.

L'evoluzione sta avvenendo in tre fasi:

1. si usa principalmente l’infrastruttura IPv4 esistente ,
2. i protocolli coesistono ,
3. i nodi IPv4 restanti usano l’infrastruttura IPv6 e devono poter usare i servizi IPv6 .

Dual stack



Dual stack

I nodi utilizzano entrambi i protocolli.

È semplice da implementare, ma ovviamente aumenta la complessità della rete.

Non risolve il problema della diminuzione degli indirizzi IPv4 poiché ogni interfaccia dev'essere sempre e comunque dotata dei due indirizzi IPv4 e IPv6.

Dual Stack Transition Mechanism (DSTM)

Il DSTM è l'evoluzione della tecnica del dual stack e si pone come obiettivo il minimo utilizzo possibile di indirizzi IPv4. Affinché ciò sia possibile gli indirizzi di versione 4 sono assegnati dinamicamente alle interfacce, risparmiando così un ampio range di indirizzi IPv4.

Da Wikipedia, l'enciclopedia libera, voce Transizione IPv4/IPv6

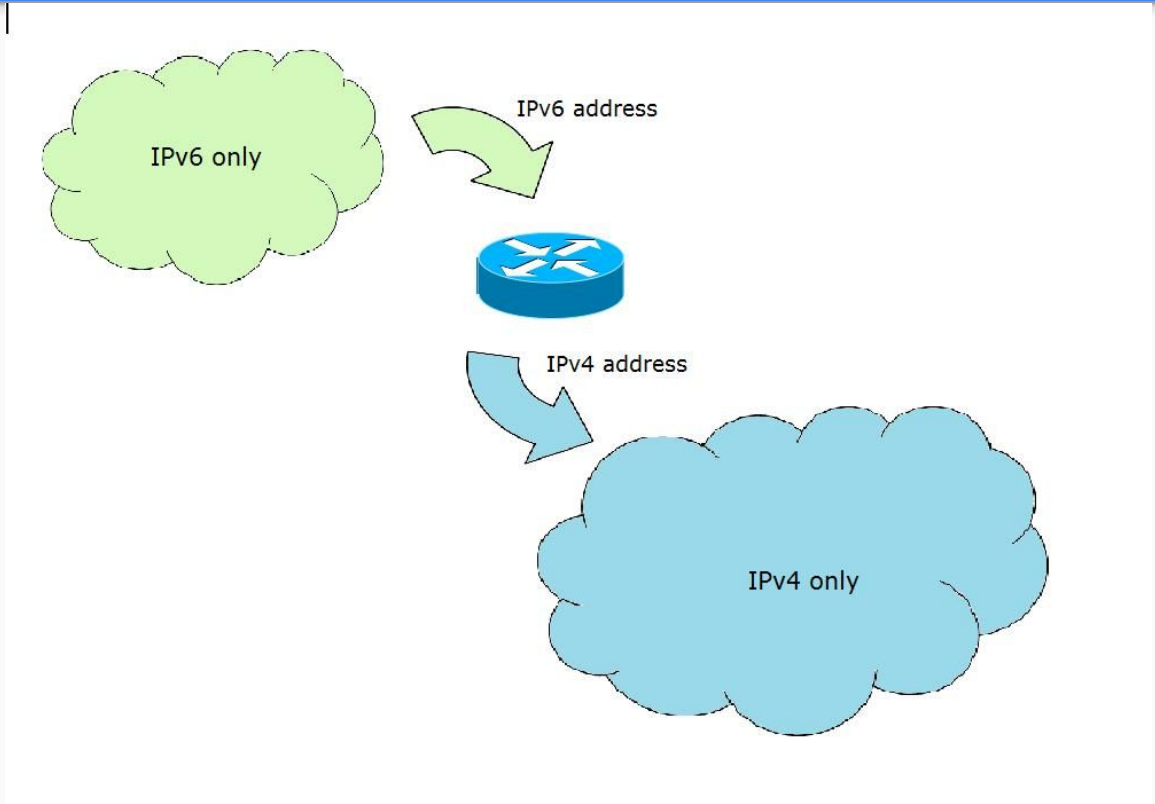
Application Level Gateway (ALG)

La rete interna utilizza IPv6, solo il gateway è dotato di dual stack.

“Il vantaggio della tecnologia ALG consiste nel dotare solo un apparato in tutta la rete del dual stack, non appesantendola ulteriormente. Un limite dei router ALG è che possono operare solamente su alcuni dei servizi di rete, per esempio HTTP. Se invece si vuole dotare la rete di altre funzionalità, lo si fa aggiungendo altri router ALG dotate delle funzionalità desiderate.”

Da Wikipedia, l’enciclopedia libera, voce Transizione IPv4/IPv6

Network Address Translator - Protocol Translator (NAT-PT)



Tunneling