Università degli Studi di Bergamo

DIP. DI INGEGNERIA DELL'INFORMAZIONE E METODI MATEMATICI

RETI INTERNET MULTIMEDIALI

Concetti Propedeutici

IPv4

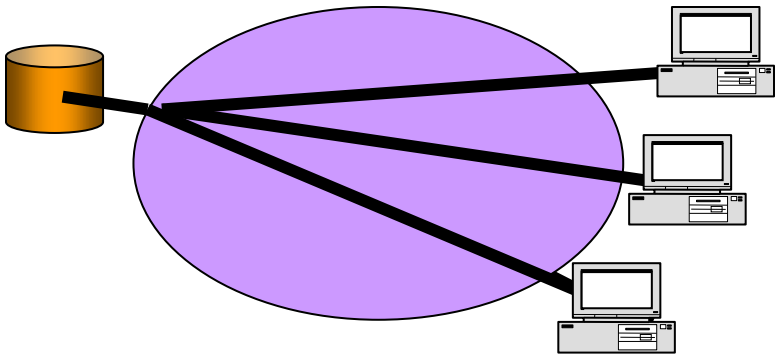
Internet Protocol (version 4)

Reti TCP/IP

- La suite di protocolli di Internet definisce un'architettura di internetworking
- Mediante quest'insieme di protocolli è possibile collegare reti diverse e calcolatori diversi per il trasferimento di informazioni e per la creazione di servizi avanzati di comunicazione
- Il protocollo base è l'Internet Protocol (IP)

IP: le funzionalità locali richieste

- IP aggiunge delle funzionalità di comunicazione che si basano su funzionalità disponibili a livello di rete locale
- Si assume un insieme minimo di funzionalità di trasferimento locale:
  - indirizzamento locale (indirizzo fisico)
  - trasferimento di pacchetti a destinazione in ambito locale (anche non garantito)
  - capacità di indirizzamento broadcast

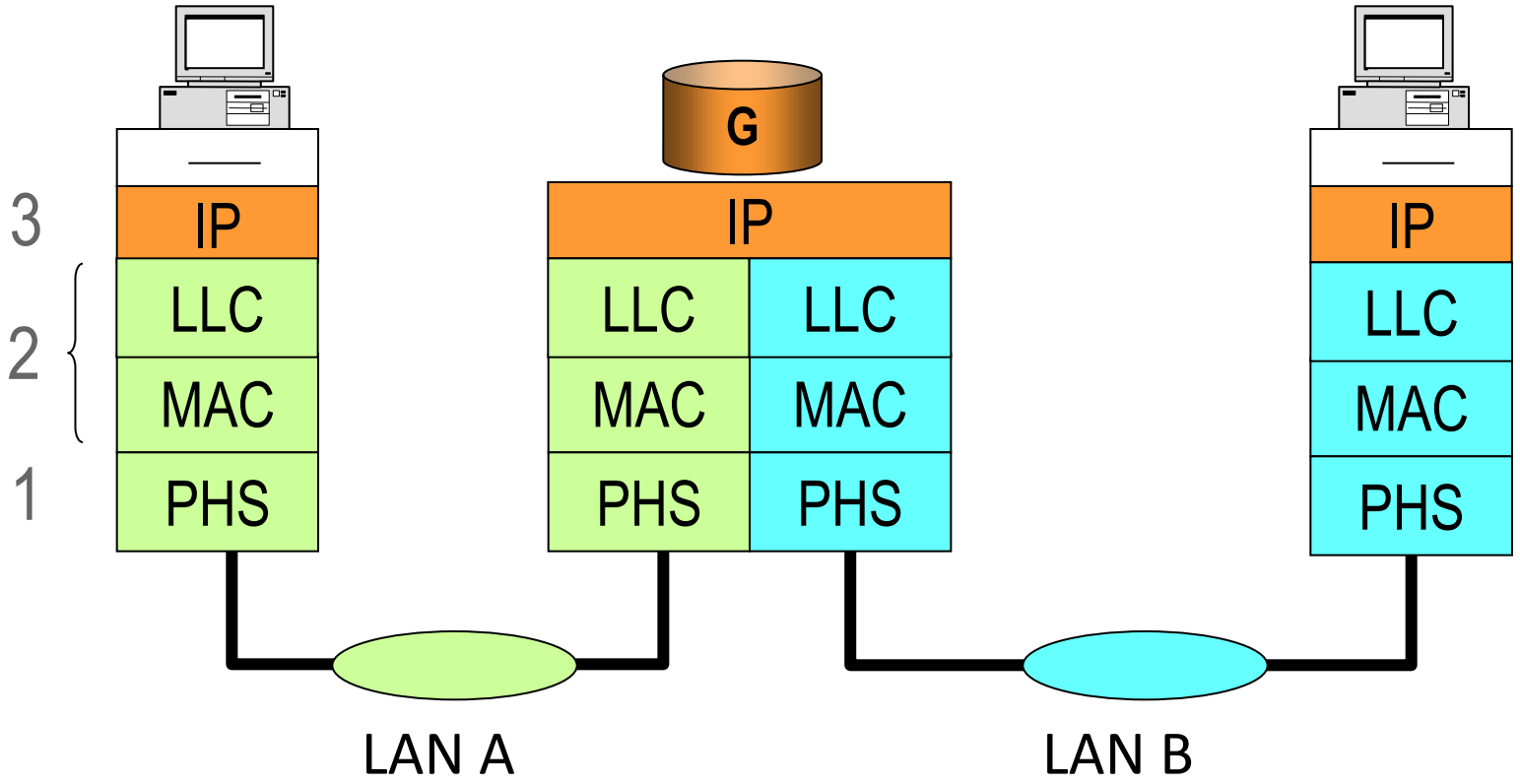


IP: le funzionalità base

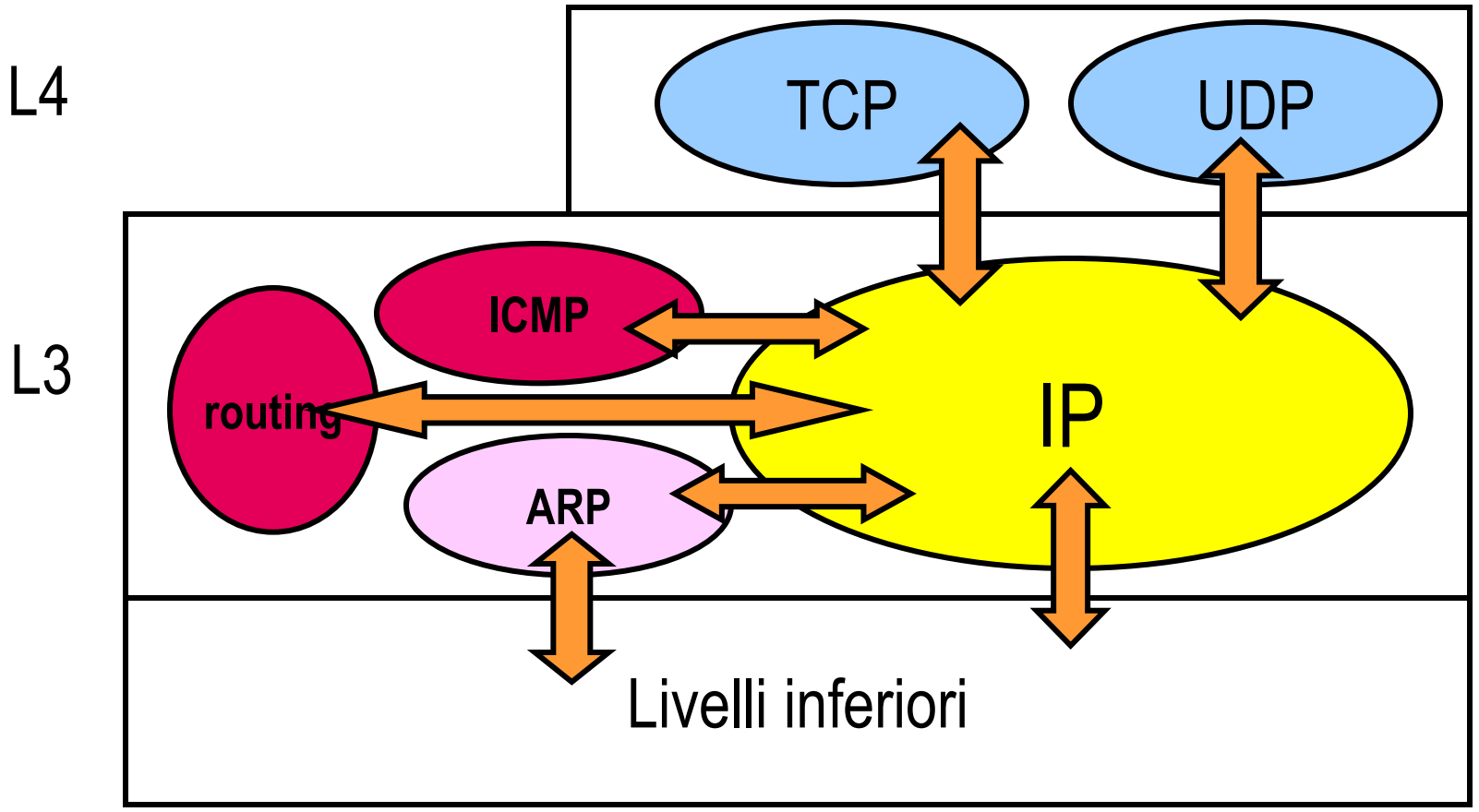
- Assegna un indirizzamento universale
- Trasferisce pacchetti in modo “datagram”
- Non garantisce né l’integrità né la consegna dei pacchetti
- Consegna “best effort” dei pacchetti
- Frammenta i pacchetti se il livello locale lo richiede
- Ricostruisce i frammenti solo in ricezione

L’architettura IP

- Il protocollo IP ha le funzionalità di un protocollo di livello 3 (rete) e si appoggia sopra i livelli delle reti che serve
- Tipico l’esempio delle reti locali (LAN):

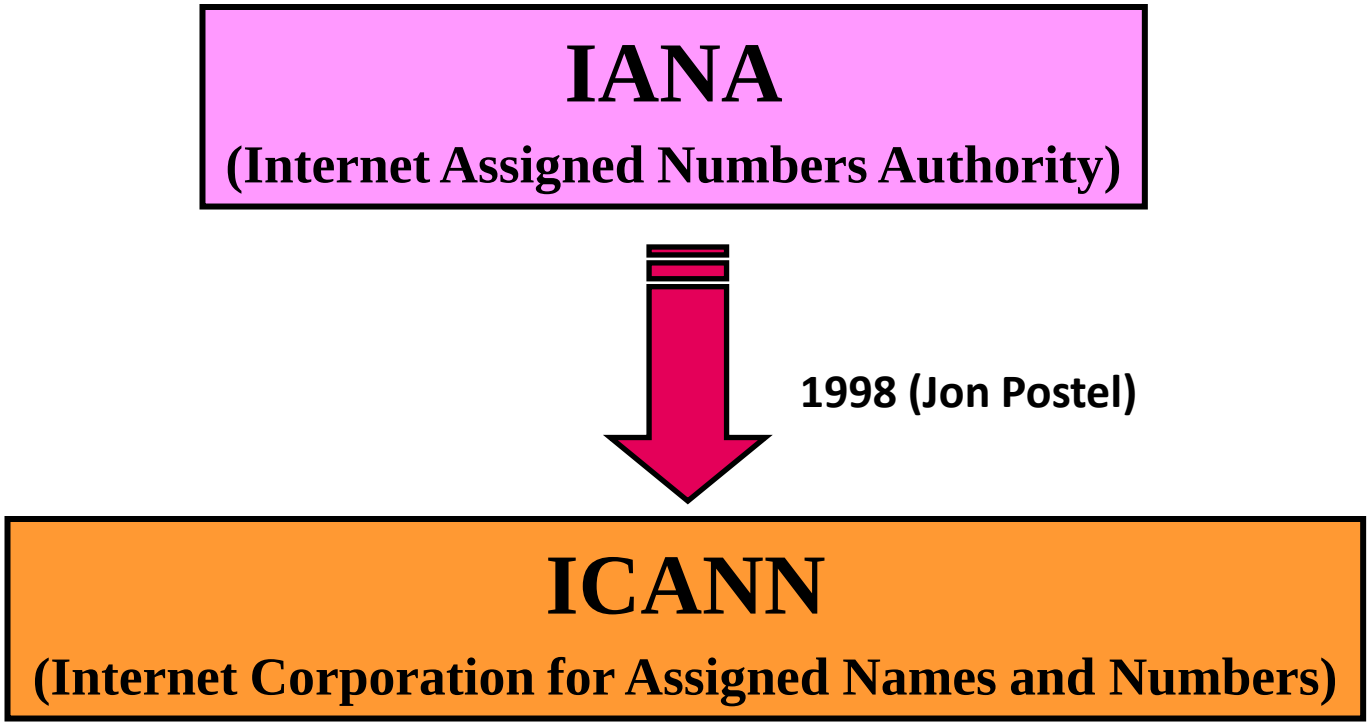


Lo stack TCP/IP base



Indirizzi e nomi

- Gli indirizzi IP sono assegnati su base globale
- Internet fa uso anche di nomi simbolici che sono anch'essi assegnati su base globale



Gli indirizzi IP

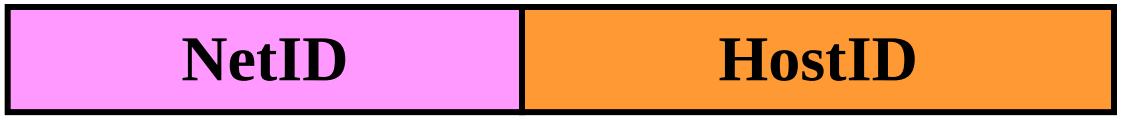
- Sono costituiti da 32 bit solitamente raggruppati in gruppi di 8 bit (byte)

- I byte sono usualmente riportati in notazione decimale divisi da punti (**dotted decimal notation**) e possono assumere valori compresi tra 0 e 255

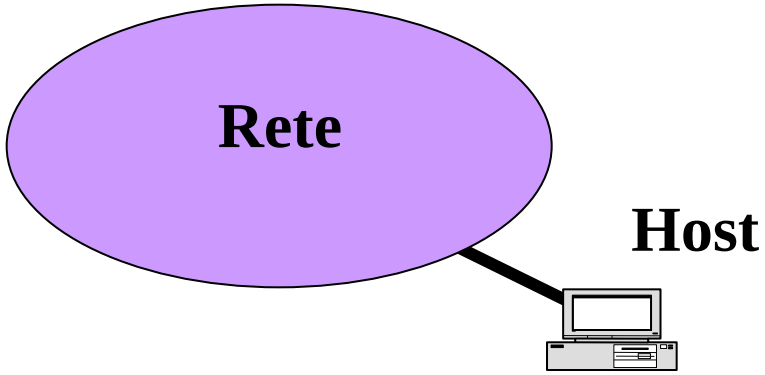
131.175.21.1

Gli indirizzi IP

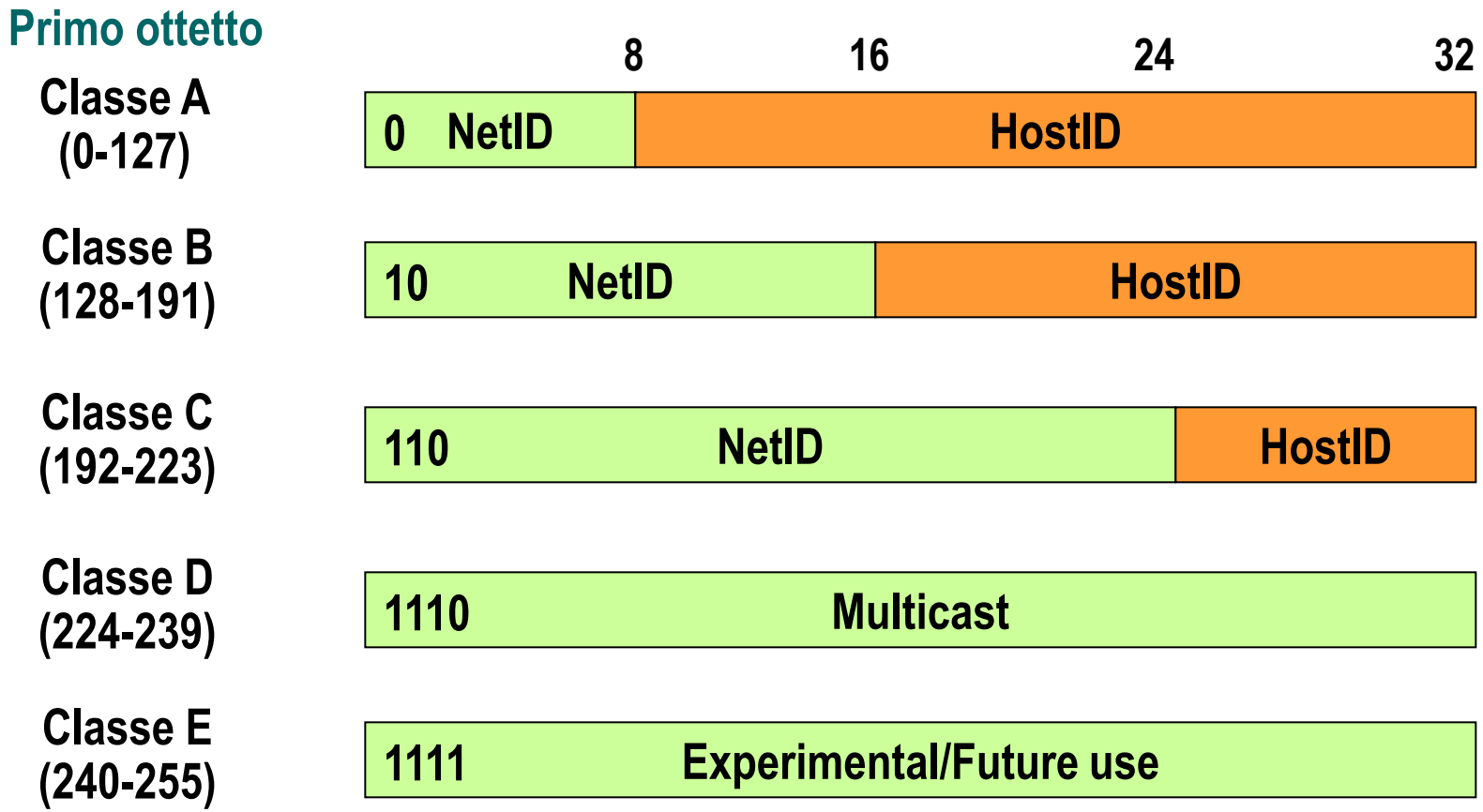
- L'indirizzo è diviso in due parti



- La NetID (indirizzo di rete) identifica la rete
- La HostID (indirizzo di host) identifica l'host nella rete
  - Tutti gli host all'interno della stessa rete hanno lo stesso indirizzo di rete (NetID)

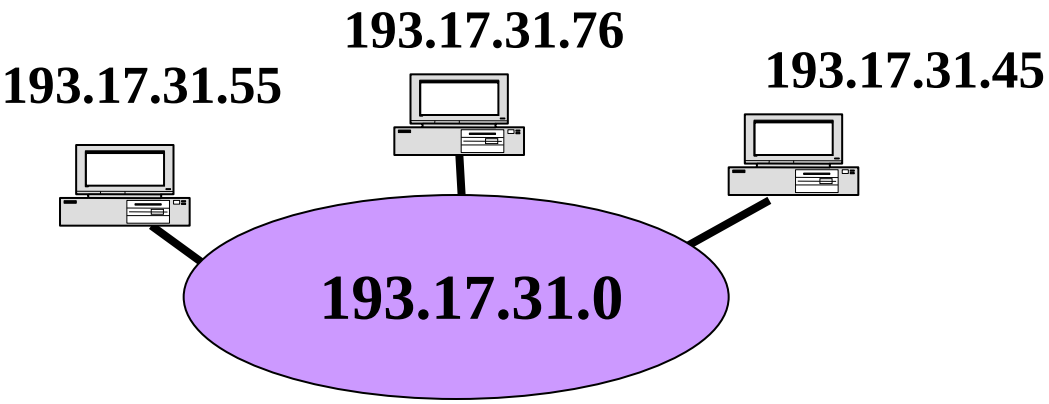


Le classi


Primo ottetto
8
16
24
32
Classe A
(0-127)
0 NetID
HostID
Classe B
(128-191)
10 NetID
HostID
Classe C
(192-223)
110 NetID
HostID
Classe D
(224-239)
1110 Multicast
Classe E
(240-255)
1111 Experimental/Future use

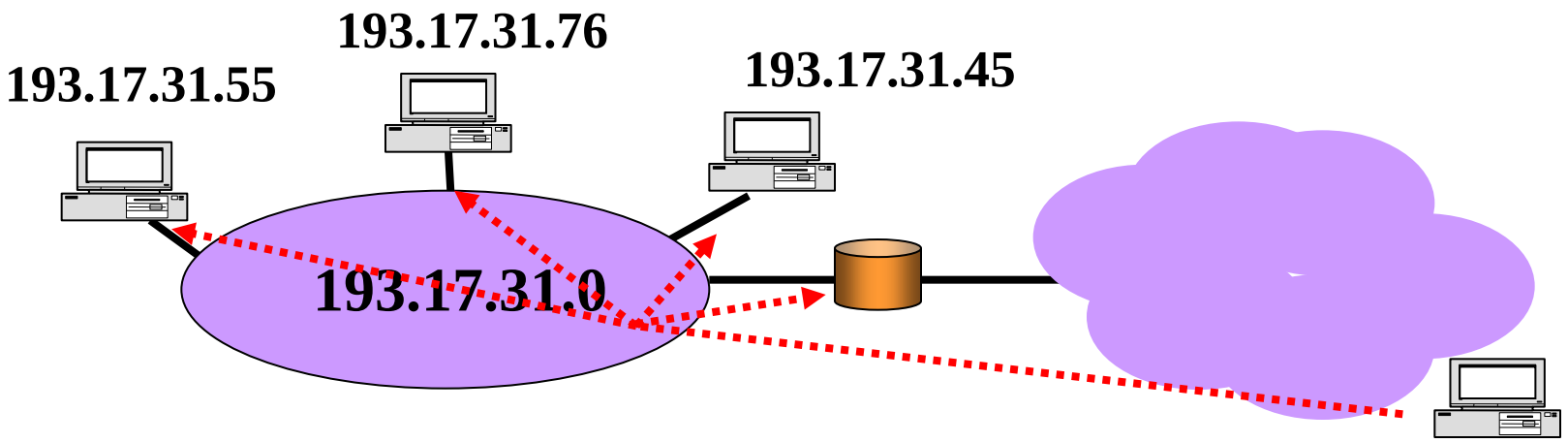
Indirizzi speciali

- Indirizzo di rete
  - L'indirizzo con il campo HostID posto a 0 serve ad indicare la rete il cui indirizzo è contenuto nel campo NetID (usato solo nelle tabelle di instradamento)
  - Esempio:
    - rete in classe B: 131.175.0.0
    - rete in classe C: 193.17.31.0



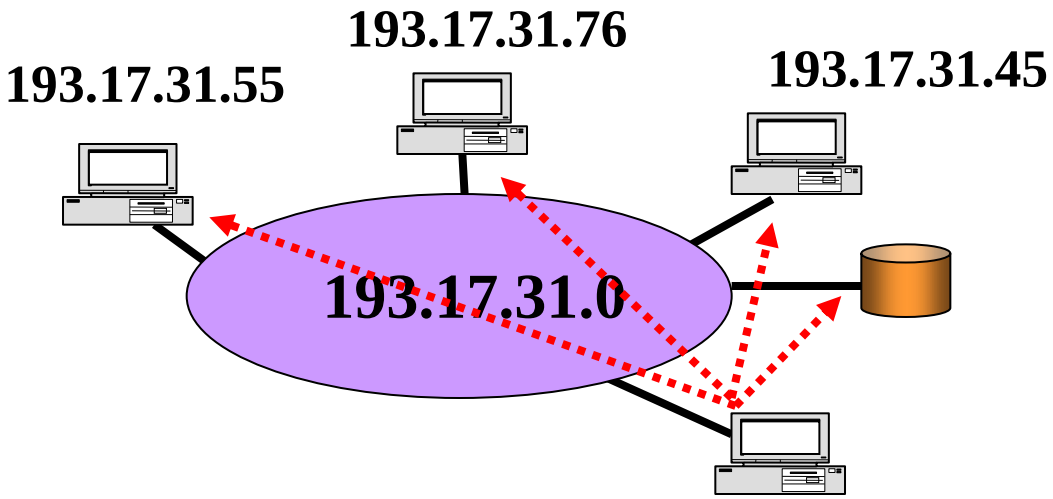
Indirizzi speciali

- Indirizzo **broadcast diretto**:
  - Un indirizzo con il campo HostID di soli 1 assume il significato di indirizzo broadcast della rete indicata nel campo NetID.
  - Esempio: 193.17.31.255



Indirizzi speciali

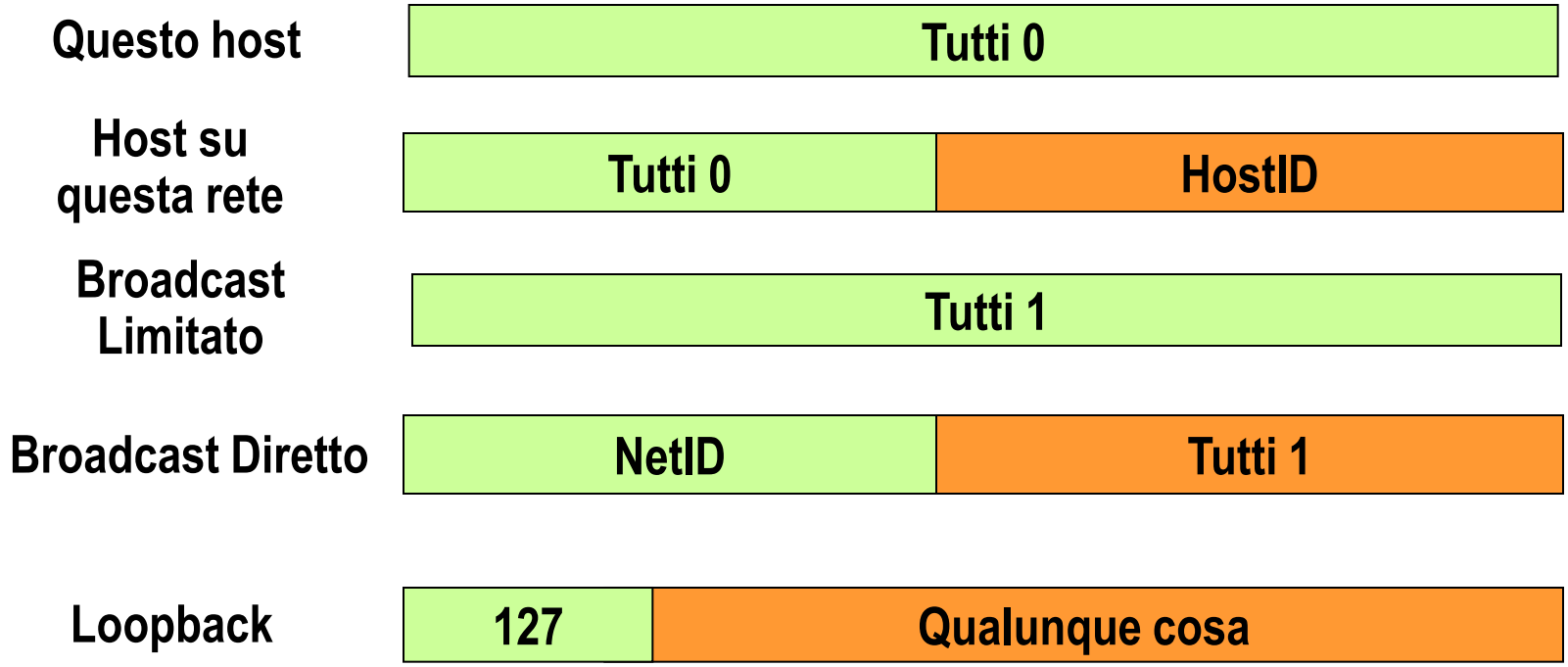
- Indirizzo **broadcasting limitato**:
  - Un indirizzo di tutti 1 (255.255.255.255) assume il significato di indirizzo broadcast nella stessa rete di chi invia il pacchetto. Il pacchetto non può oltrepassare dei router



Indirizzi speciali

- Quando il campo NetID è posto a zero, l'indirizzo indica l'host il cui indirizzo è contenuto nel campo host sulla stessa rete del mittente.
  - Esempio: 0.0.21.173 (in una rete in classe B)
- Se anche il campo host è posto a zero l'indirizzo indica il mittente stesso del pacchetto (usato quando l'host non conosce il proprio indirizzo).
  - Esempio: 0.0.0.0
- Infine, l'indirizzo con il primo ottetto pari a 127 e gli altri campi qualsivoglia indica il loopback sullo stesso host (usato nei sistemi operativi per testare le funzionalità di rete).
  - Esempio: 127.0.0.0

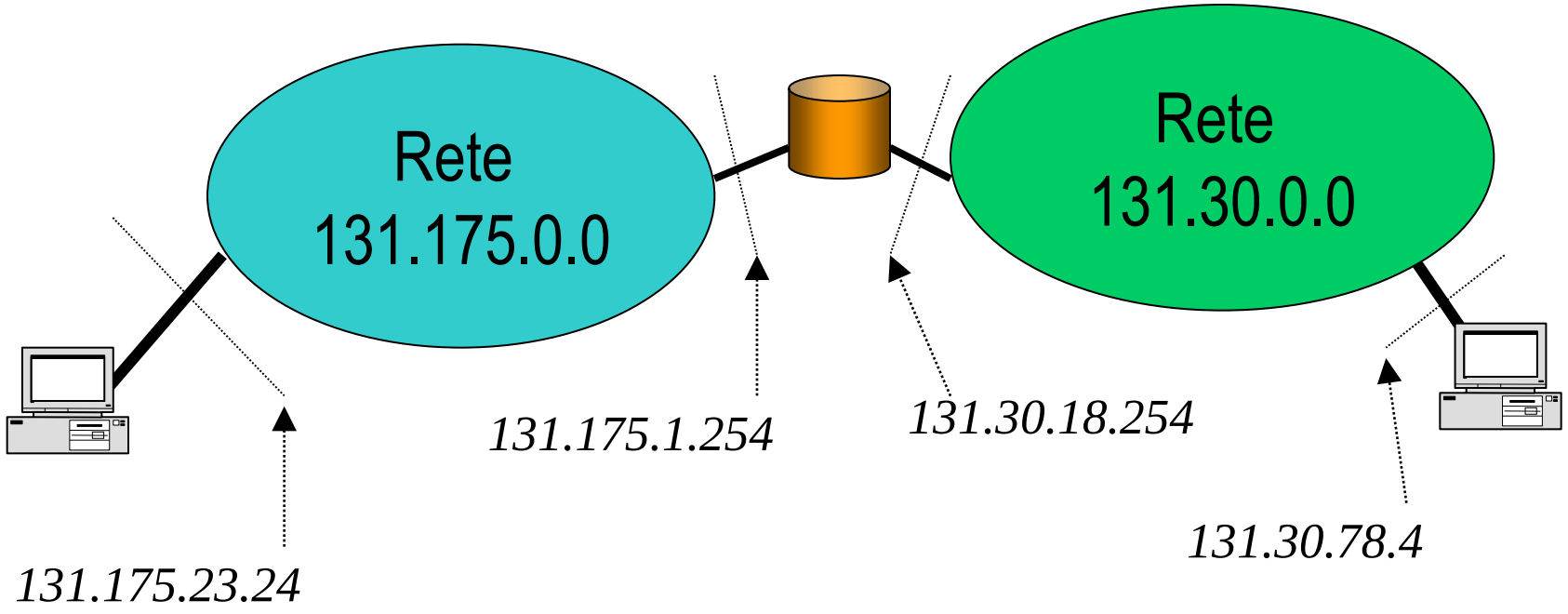
Indirizzi Speciali: riassunto



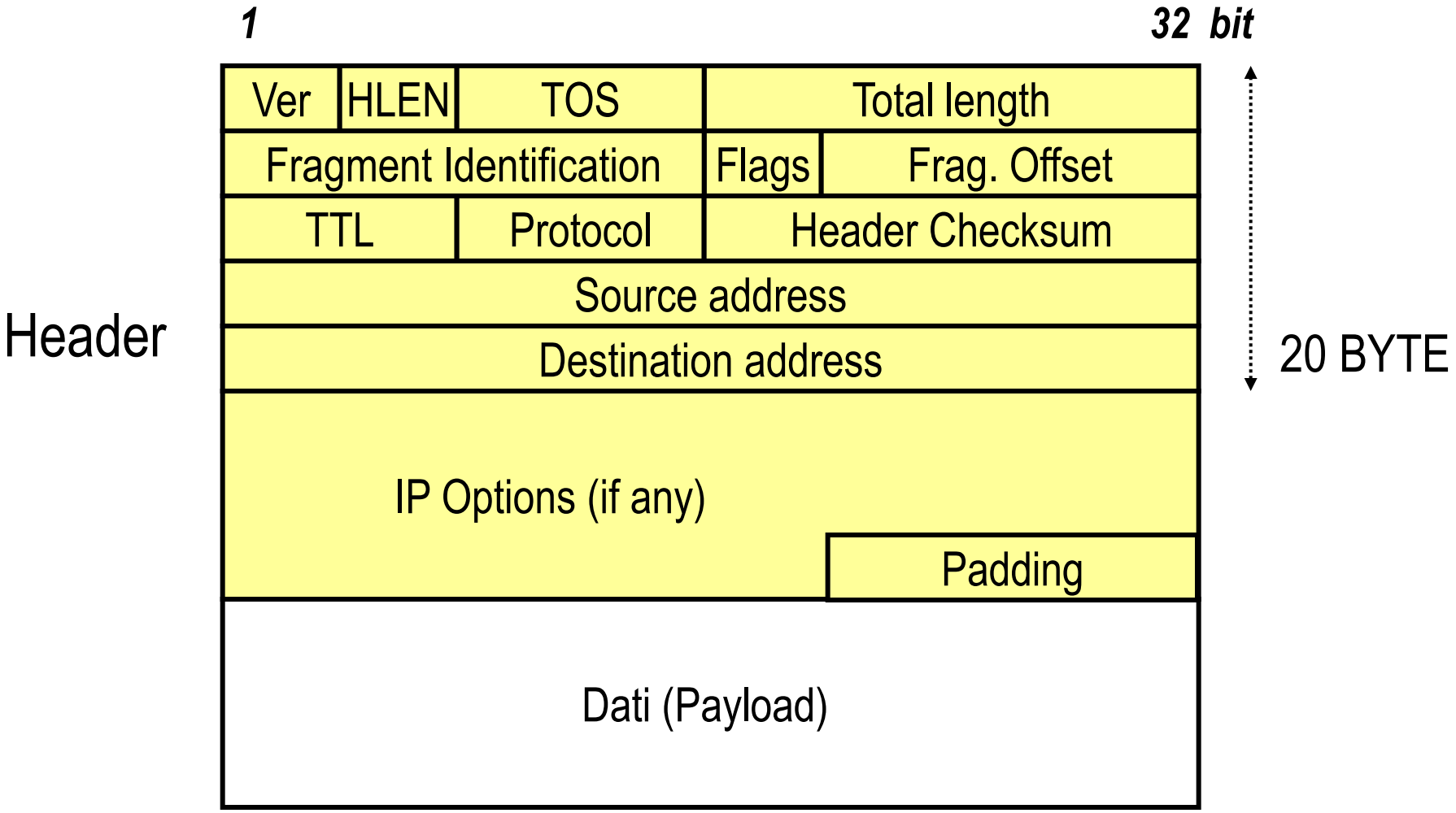
- Primi due indirizzi possono essere usati solo durante lo startup di sistema, e non rappresentano mai un indirizzo di destinazione valido
- Il 3° e 4° indirizzo non rappresentano mai un indirizzo sorgente valido
- Il 5° indirizzo non dovrebbe mai comparire in rete

Indirizzamento IP

- L'indirizzo IP indica l'interfaccia (ovvero il collegamento) di un dispositivo con la rete
- Se un dispositivo ha più interfacce su più reti deve avere un indirizzo per ciascuna interfaccia



Il pacchetto/datagramma IP (RFC 791)



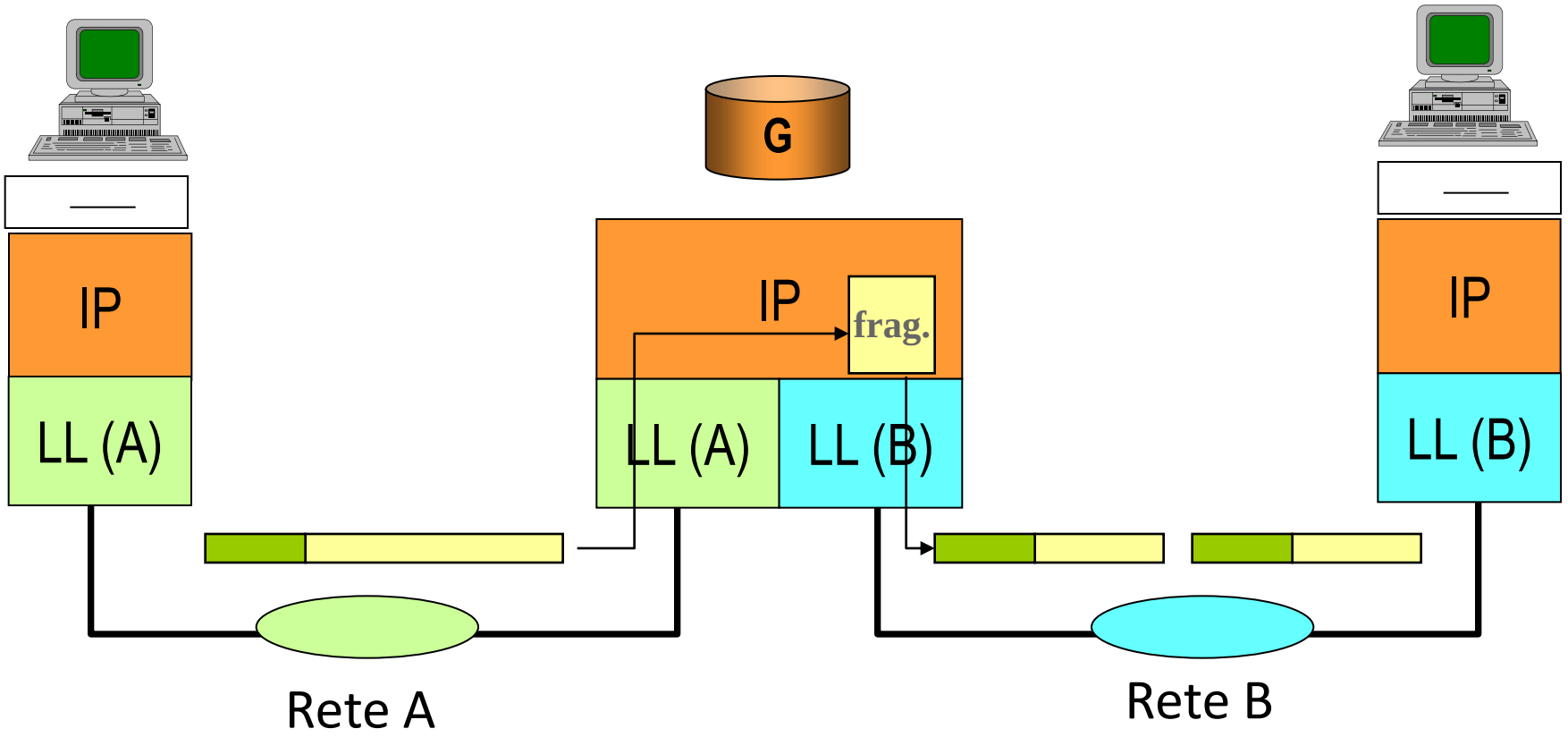
Il pacchetto IP

- **Ver (4 bit)**
  - Version: indica la versione del protocollo; quella che noi studiamo è la versione 4
- **HLEN (4 bit)**
  - Header length: indica la lunghezza dell'header del pacchetto (comprese opzioni e padding) espressa in parole da 32 bit (4 byte). Minimo valore valido: 5
- **TOS (8 bit)**
  - Type Of Service: un campo che adesso prende il nome di DS field (RFC 2474) e può essere utilizzato per la gestione delle priorità nelle code dei router
- **Total length (16 bit)**
  - Indica la lunghezza totale del pacchetto in byte: valore massimo 2^{16}=65536; una volta sottratta la dimensione dell'header, si ha la lunghezza del payload

La frammentazione

- Identification, Flags, Fragment Offset
  - Alcuni protocolli di livello inferiore a cui IP si appoggia richiedono una dimensione massima del pacchetto (MTU) inferiore a 65536 bytes (tipico l'esempio di Ethernet che accetta pacchetti fino a 1500 bytes)
  - Prima di passare il pacchetto al livello inferiore, IP divide il pacchetto in frammenti, ciascuno con il proprio header
  - I frammenti verranno ricomposti dall'entità IP del destinatario
  - I campi Identification, Flags e Frag. Offset sono usati per questo scopo

La frammentazione



La frammentazione

- **Identification (16 bit)**
  - Campo che identifica tutti i frammenti di uno stesso pacchetto in modo univoco. E' scelto dall'IP Sender
- **Frag. Offset (13 bit)**
  - I byte del pacchetto originale sono numerati da 0 al valore della lunghezza totale. Il campo Frag. Offset identifica la posizione del frammento nel datagramma IP originale (in multipli di 8 byte). Il primo frammento ha Offset pari a 0.
  - Ad esempio: se un pacchetto di 2000 byte viene diviso in due da 1000 il primo frammento avrà un offset pari a 0 e il secondo pari a 1000 (ovvero: nel campo Frag. Offset del secondo troveremo scritto 1000/8=125)

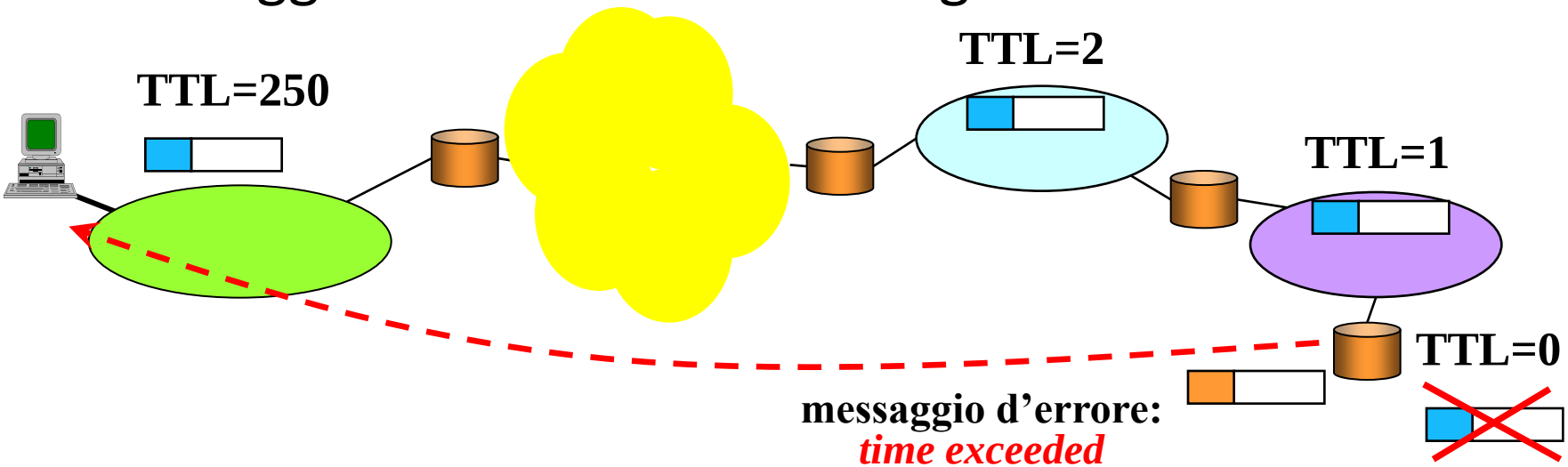
La frammentazione

- **Flags (3 bit)**

  - Il primo bit è riservato e deve contenere 0
  - il bit M (More) è pari a 0 solo nell'ultimo frammento (last fragment), ad 1 negli altri (more fragments)
  - il bit D viene posto a 1 quando non si vuole che lungo il percorso venga applicata la frammentazione
    - in questo caso se la frammentazione fosse necessaria non viene applicata ma viene generato un messaggio di errore

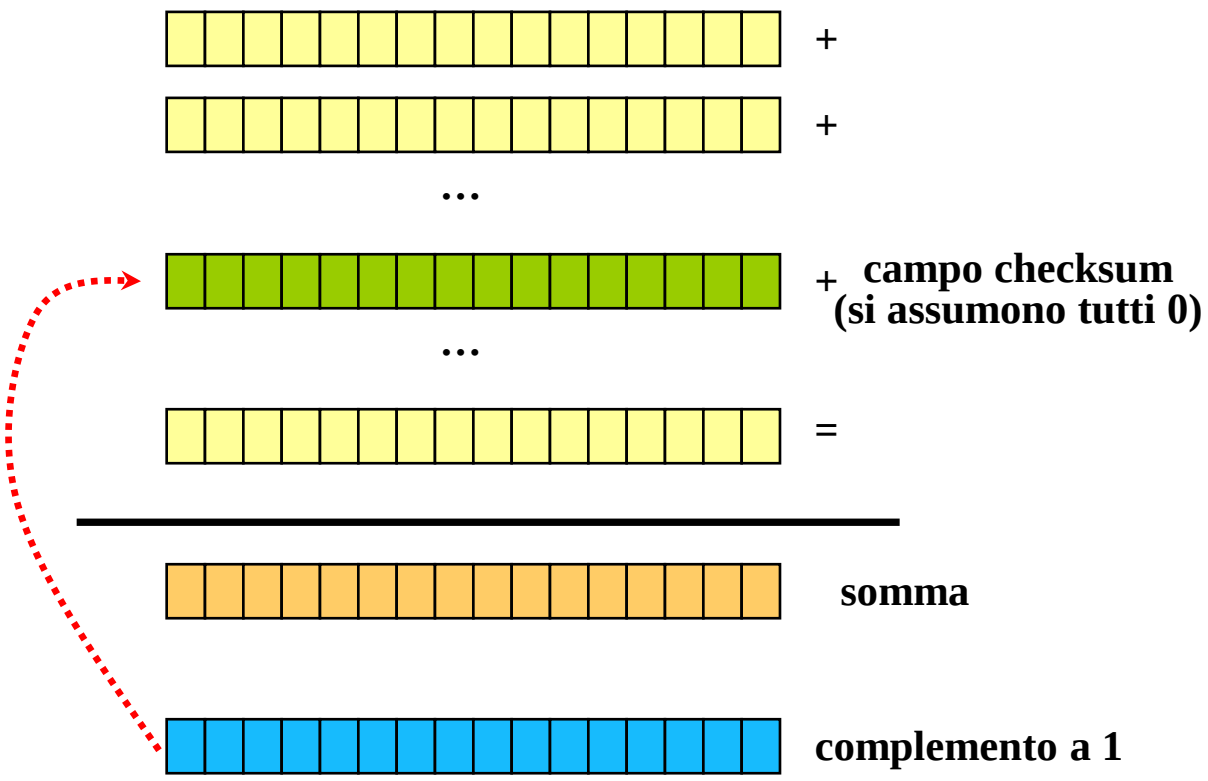
TTL (Time To Live) (8 bit)

- Il campo TTL viene settato ad un valore elevato da chi genera il pacchetto e viene decrementato da ogni router attraversato
- Se un router decrementa il valore e questo va a zero, il pacchetto viene scartato e viene generato un messaggio di errore verso la sorgente



Checksum (16 bit)

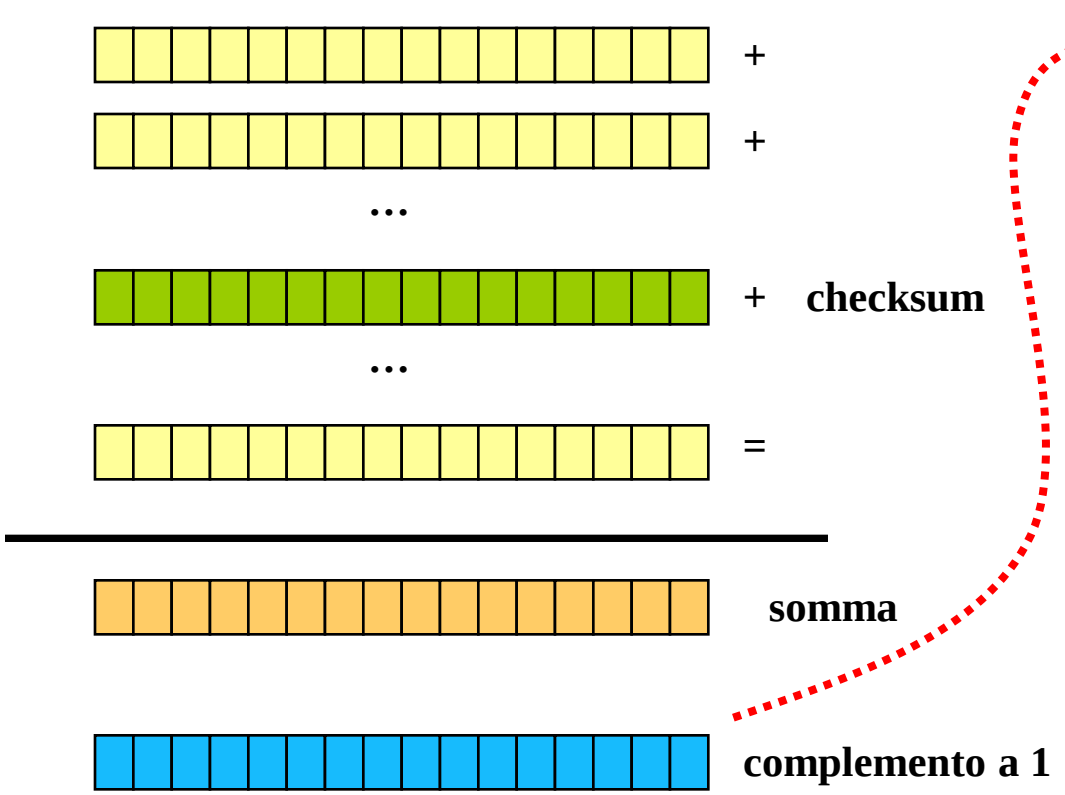
- Serve per individuare eventuali errori nell'header (e solo nell'header)
- Viene calcolato dal mittente e controllato dal destinatario (ad ogni hop)



- L'**header** viene diviso in blocchi di 16 bit
- Viene fatta la somma modulo 2 dei bit corrispondenti in ciascun blocco
- Il risultato viene complementato e quindi inserito nel campo checksum

Checksum

- In ricezione si calcola la somma e si verifica il complemento:



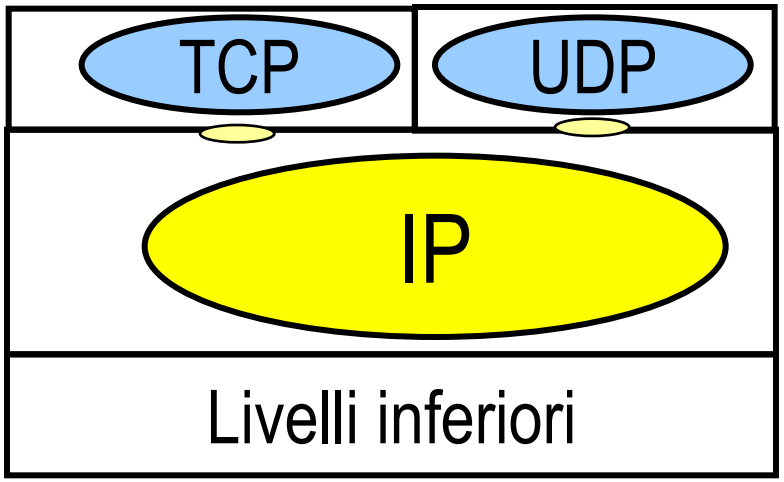
- **se sono tutti 0 il pacchetto viene accettato**
- **altrimenti viene scartato!**

Checksum

- Nota: poiché esistono campi dell'header IP che cambiano a mano a mano che il pacchetto viene inoltrato (es. Time To Live, TTL), ogni entità IP lungo il percorso ricalcola il checksum
- L'entità IP del nodo successivo può così verificare l'integrità dell'header ed accettare o meno il pacchetto IP

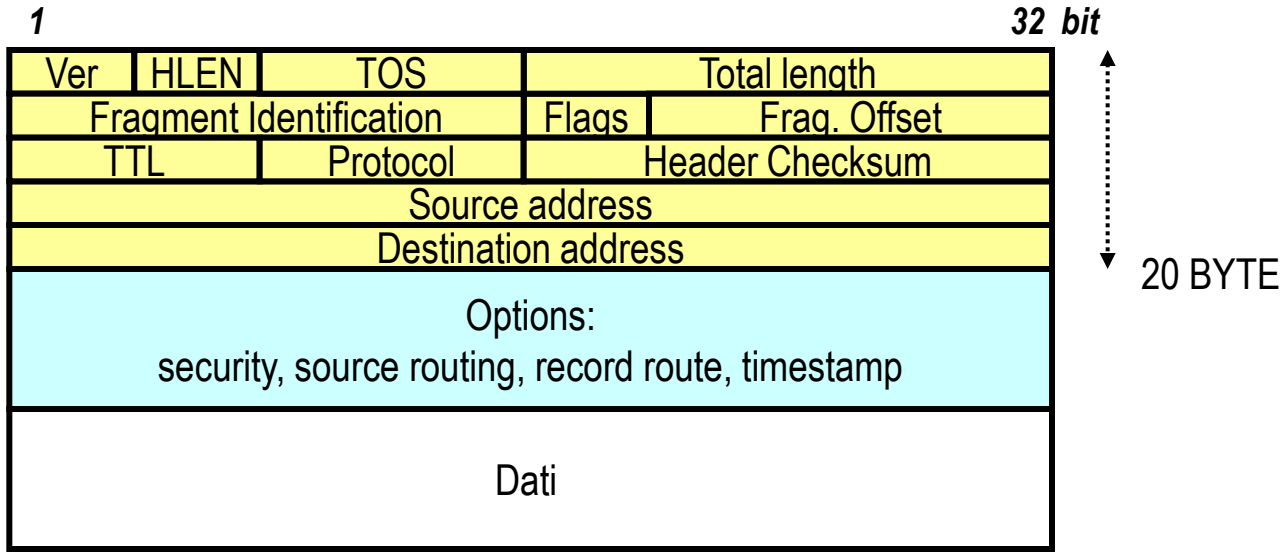
Protocol (8 bit)

- E’ un codice che indica il protocollo di livello superiore (RFC 790)
- Esempio: ICMP=1, TCP=6 …
- più protocolli di livello superiore possono usare IP (multiplazione)
- il codice identifica il SAP (Service Access Point) tra IP e il protocollo di livello superiore

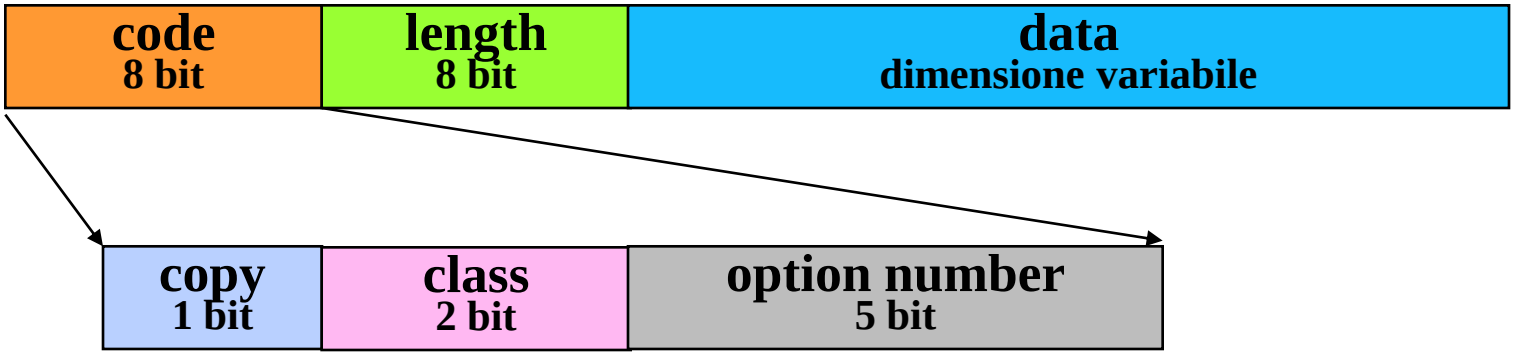


Le opzioni

- La parte iniziale dell'header IP è di 20 byte ed è sempre presente
- In aggiunta è possibile la presenza di campi aggiuntivi (le opzioni) che possono allungare l'header fino ad un massimo di 60 byte



Le opzioni



Copy:
0 nel primo o unico frammento
1 negli altri (copied)

Class:
00 controllo del datagram
10 debugging and measurement

Option number:
00000 end of option (1 byte)
00001 no operation (1 byte)
00011 loose source routing
00100 time stamp
00111 record route
01001 strict source routing

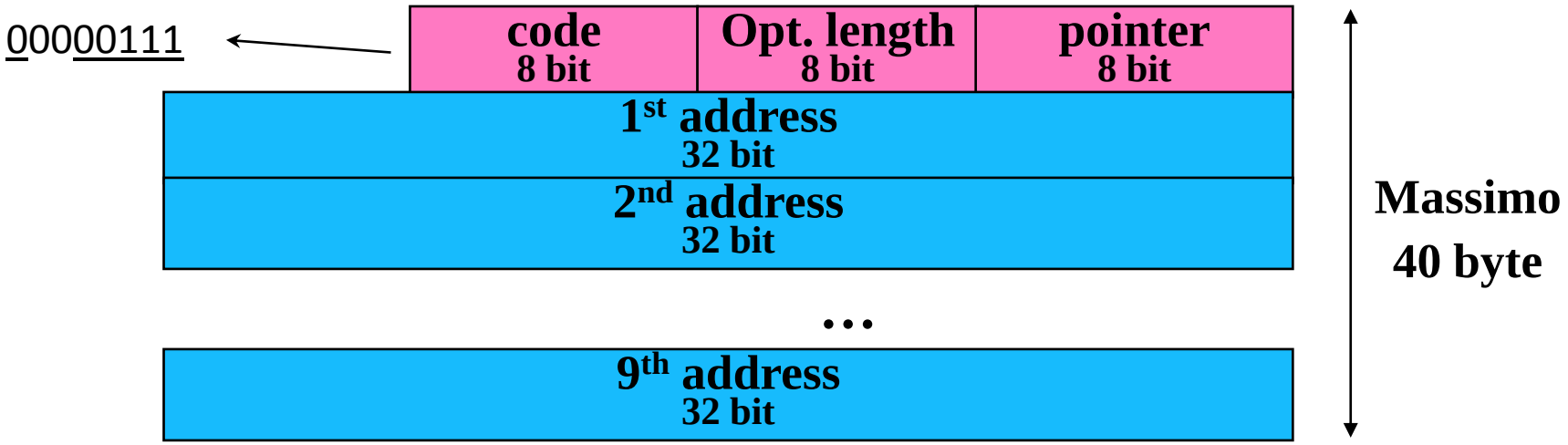
01 e 11 sono riservate per usi futuri

Le opzioni

CLASS	NUMBER	LENGTH	DESCRIPTION
0	0	-	End of Option list. This option occupies only 1 octet; it has no length octet.
0	1	-	No Operation. This option occupies only 1 octet; it has no length octet.
0	2	11	Security. Used to carry Security, Compartmentation, User Group (TCC), and Handling Restriction Codes compatible with DOD requirements.
0	3	var.	Loose Source Routing. Used to route the internet datagram based on information supplied by the source.
0	9	var.	Strict Source Routing. Used to route the internet datagram based on information supplied by the source.
0	7	var.	Record Route. Used to trace the route an internet datagram takes.
0	8	4	Stream ID. Used to carry the stream identifier.
2	4	var.	Internet Timestamp.

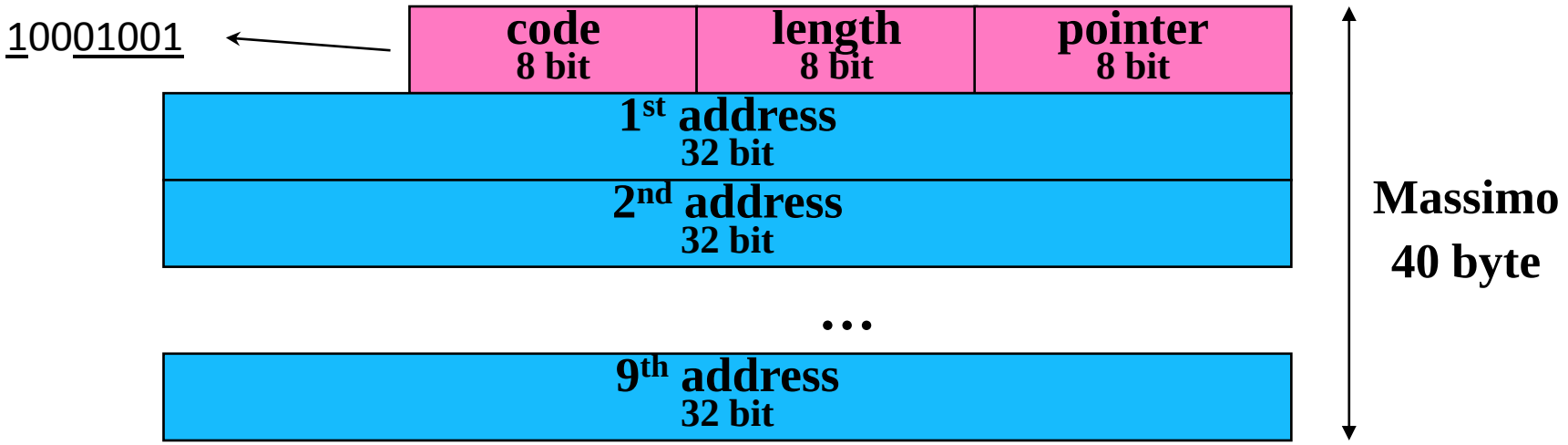
Record Route

- Il pointer indica l'ottetto con cui comincia la prossima area in cui registrare un indirizzo. Il puntatore è relativo a questa opzione.
- Tutti i campi address sono inizialmente vuoti e il pointer vale 4 (ovvero punta al primo campo address, che comincia appunto al 4o ottetto dall'inizio dell'opzione)
- ogni volta che viene attraversato un router viene registrato l'indirizzo nel campo puntato e il puntatore viene aumentato di 4, fino all'eventuale riempimento di tutti i campi address
- (per conoscere il percorso verso una destinazione esiste la possibilità di usare pacchetti ICMP come vedremo in seguito)



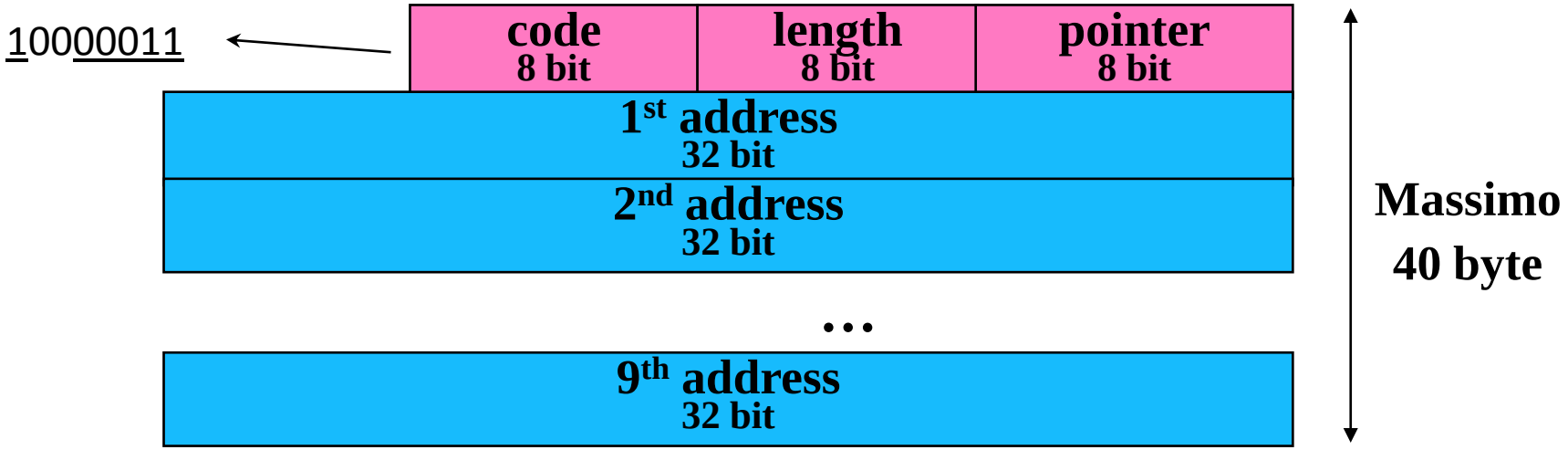
Strict Source Routing

- Implementa un meccanismo di source routing (percorso scelto dalla sorgente)
- Tutti i campi address sono inizialmente pieni e indicano i router che l'IP sender vuole vengano attraversati
- il puntatore viene incrementato di 4 ad ogni hop
- se viene raggiunto un router non previsto il pacchetto viene scartato e viene generato un messaggio di errore
- (usata molto raramente!!!)



Loose Source Routing

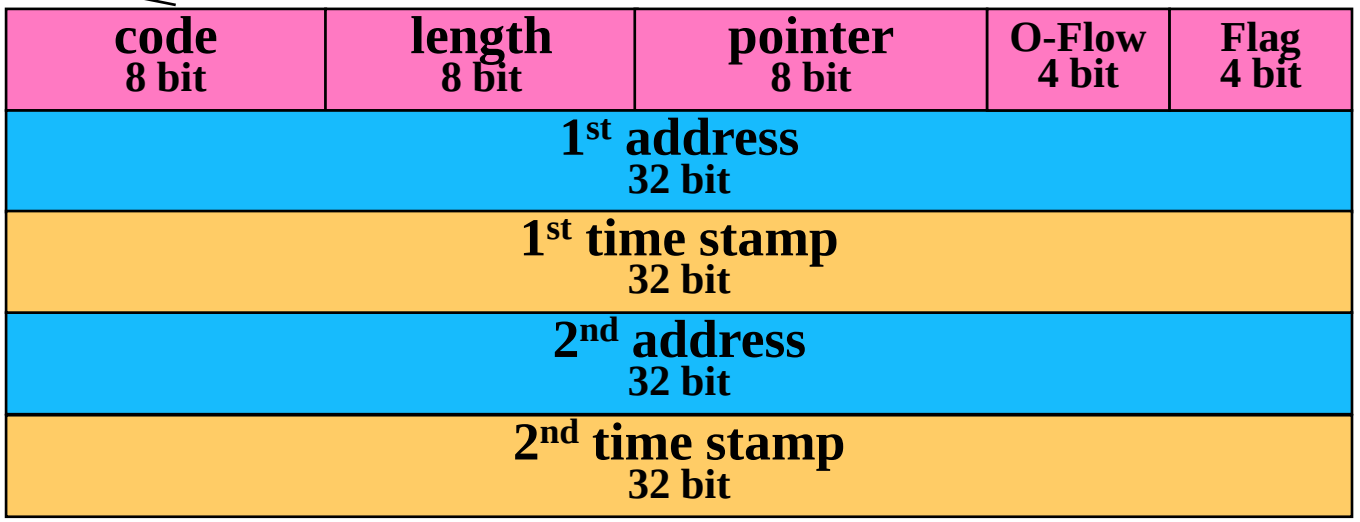
- Come la precedente, ma è possibile visitare anche altri router (il pacchetto non viene scartato)
- (usata molto raramente!!!)



Timestamp

- Misura il tempo assoluto di uscita del pacchetto in un router
- Il campo Over-Flow indica il numero di router sul percorso che non hanno potuto aggiungere il timestamp (per mancanza di spazio nell'opzione, che al massimo può raggiungere i 40 byte)
- Il campo Flag indica la modalità operativa stabilita dal mittente (address riempiti dal mittente o dai router, ecc.)

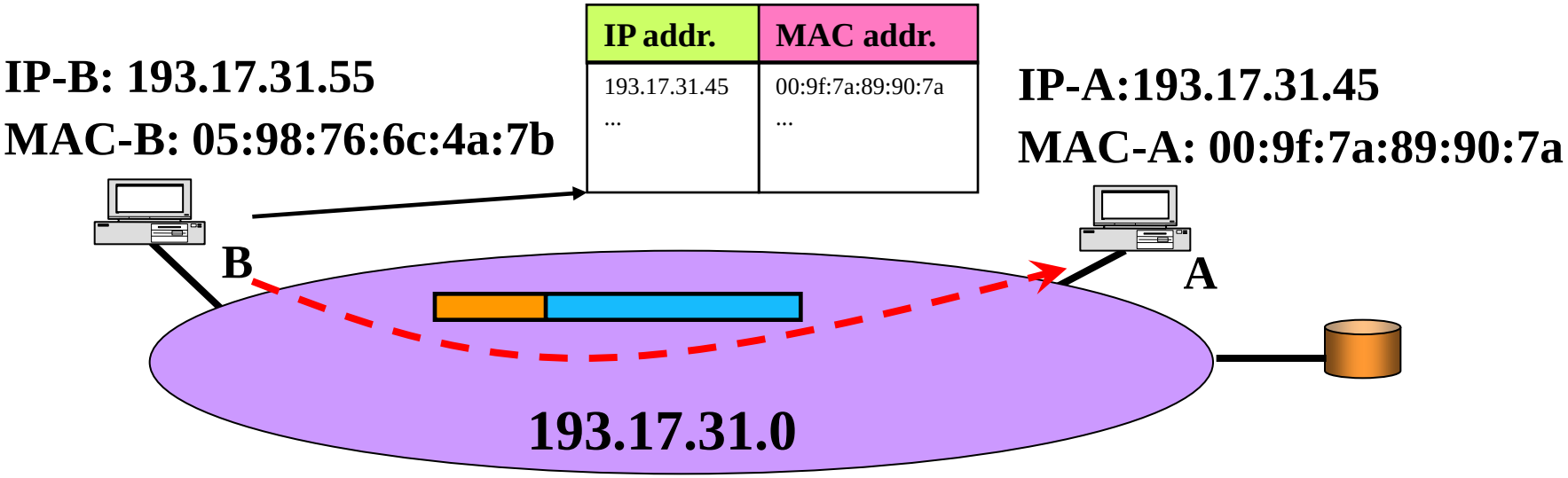
01000100



…

Corrispondenza tra indirizzi IP e indirizzi fisici

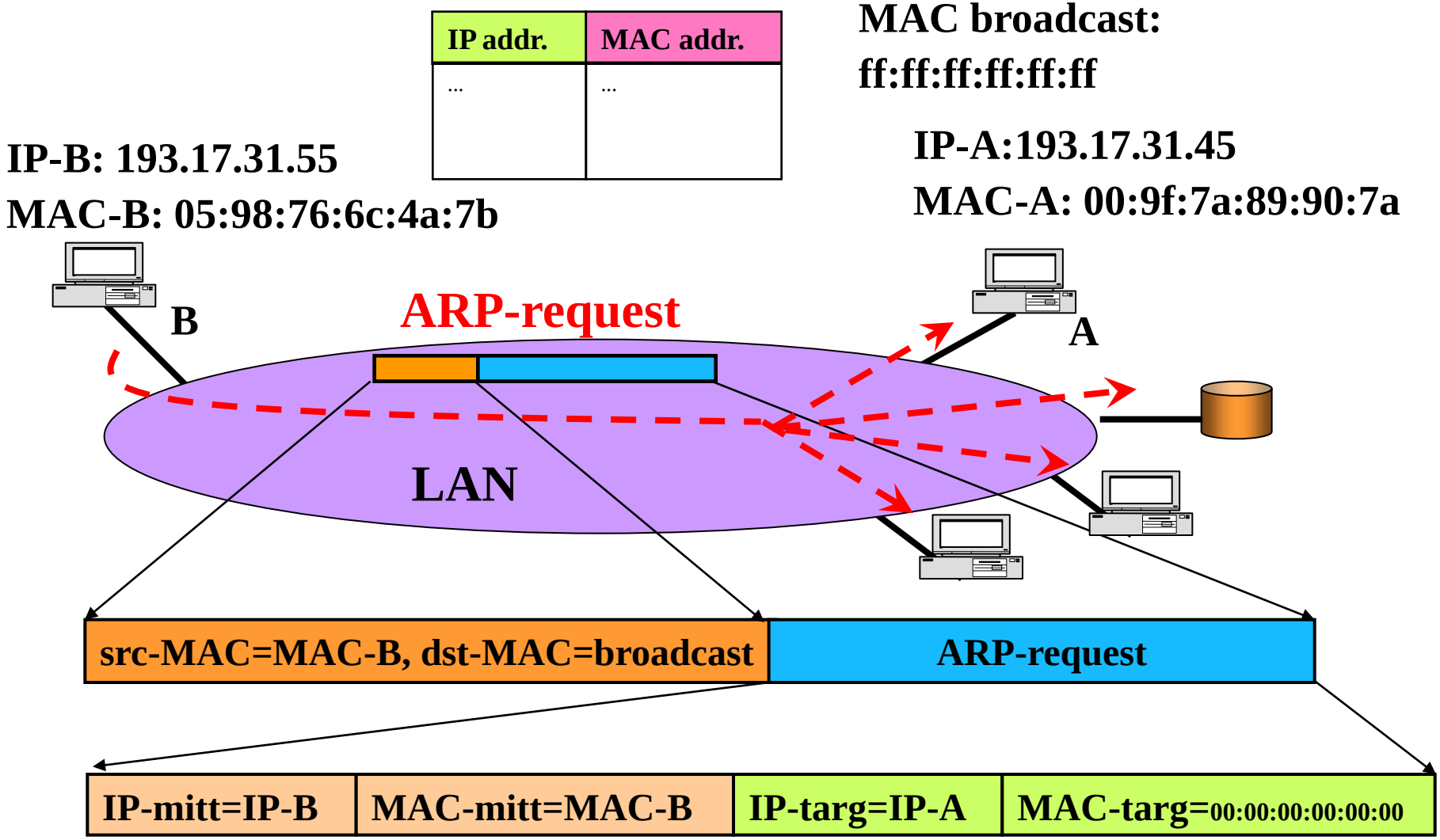
- Illustrando le tecniche di inoltro abbiamo ipotizzato la presenza di una tabella di corrispondenza tra indirizzi IP e indirizzi di livello inferiore (indirizzi fisici)
- Queste tabelle vengono create dinamicamente da ciascun host mediante il protocollo ARP



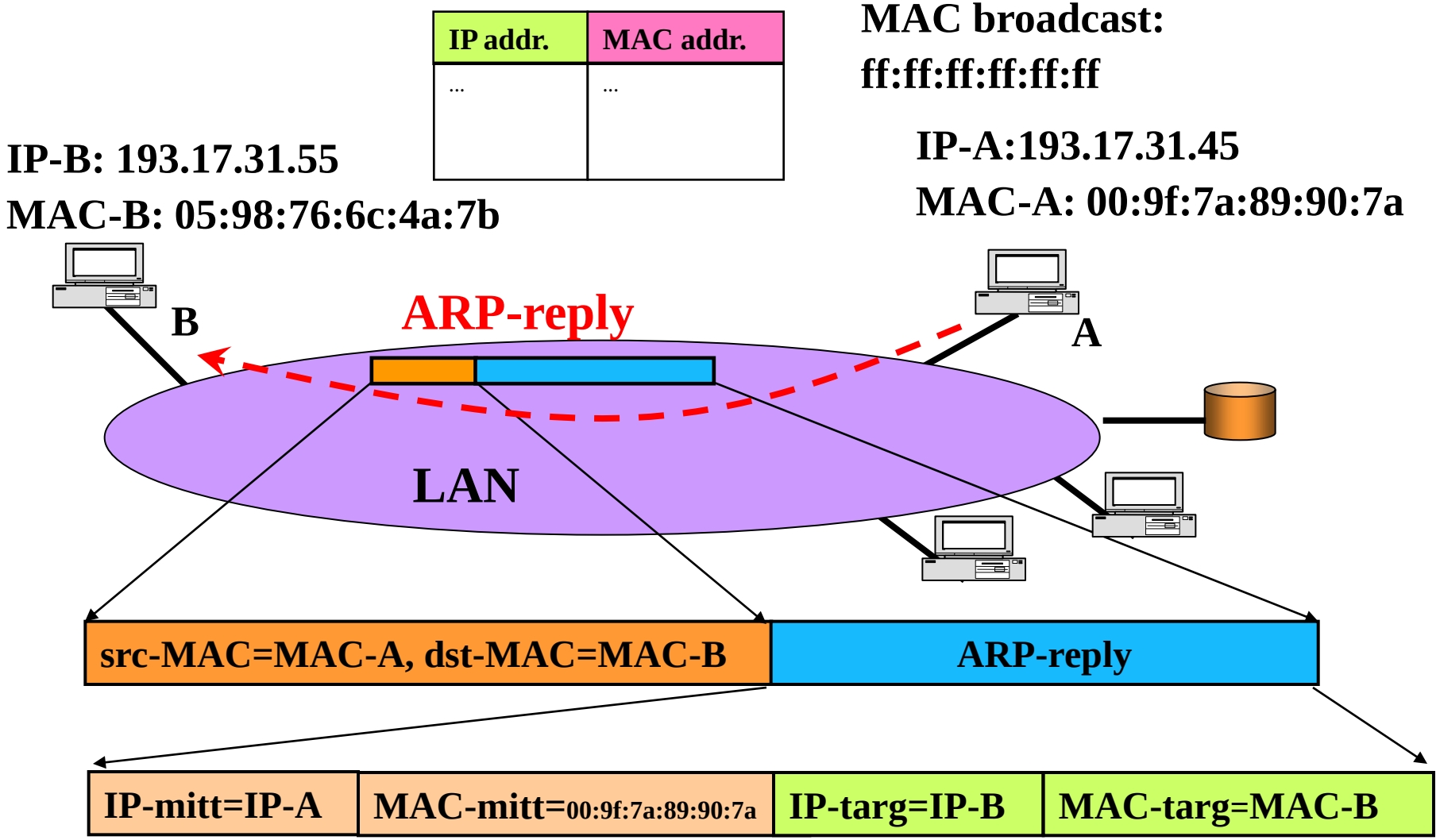
ARP (Address Resolution Protocol)

- Il meccanismo si basa sulla capacità di indirizzamento broadcast della rete locale
- quando nella tabella memorizzata nell'host (denominata *ARP-cache*) non è presente l'indirizzo cercato, viene generato un messaggio di ARP-request
- La ARP-request viene inviata in broadcast e contiene l'indirizzo IP di cui si chiede il corrispondente indirizzo MAC
- L'host che riconosce l'indirizzo IP come proprio invia una ARP-reply direttamente a chi aveva inviato la richiesta, con l'indicazione dell'indirizzo MAC

ARP (Address Resolution Protocol)



ARP (Address Resolution Protocol)



Formato dei pacchetti ARP

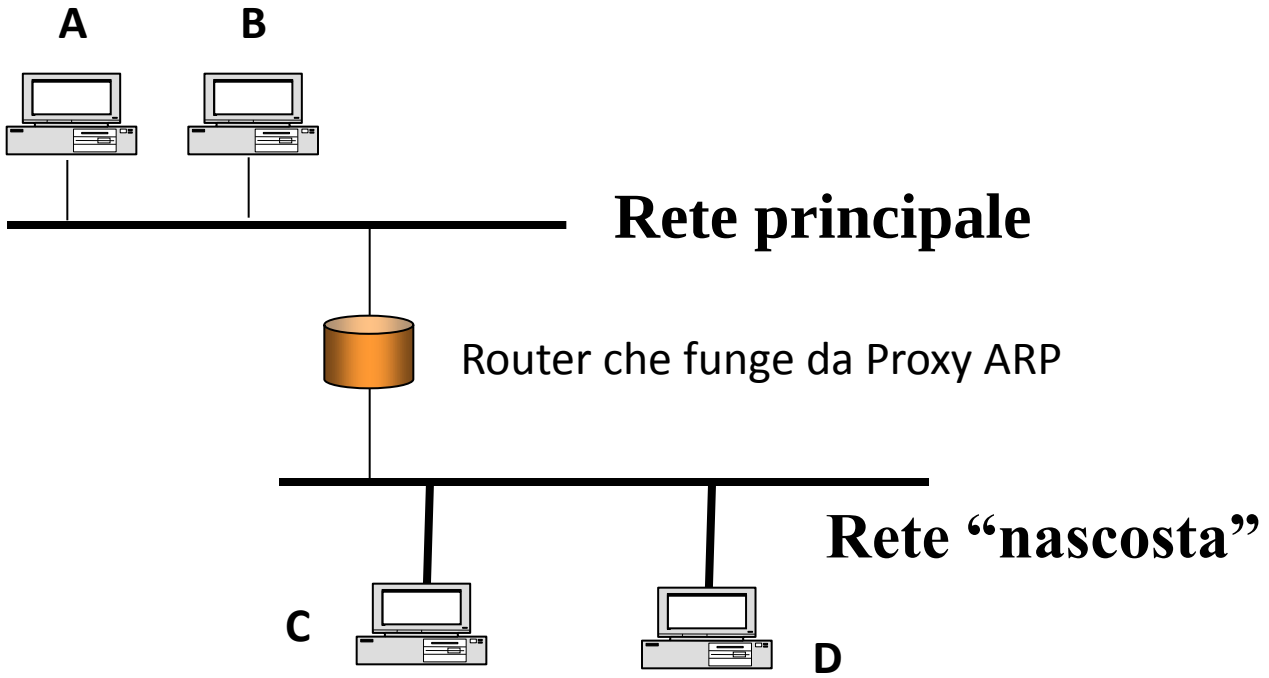
- ARP può essere usato per altri protocolli di livello 2 e livello 3 quindi occorre indicare il tipo di protocollo (IP nel nostro caso) e il tipo di hardware (Ethernet per esempio)
- Ovviamente: il formato di un pacchetto ARP (ovvero la lunghezza dei suoi campi) varia in funzione del tipo di hardware e di protocollo utilizzati!

Domini di broadcast e reti IP

- Per il funzionamento del meccanismo di inoltro e dell'ARP abbiamo fin qui ipotizzato che una sottorete IP corrisponda uno a uno con una rete locale (Dominio di Broadcast)
- In realtà un'unica rete locale può corrispondere a diverse sottoreti IP (per es. perché la numerazione disponibile per una non è sufficiente)
- Non è possibile che più reti locali possano coesistere in un'unica sottorete IP perché non potrebbero comunicare

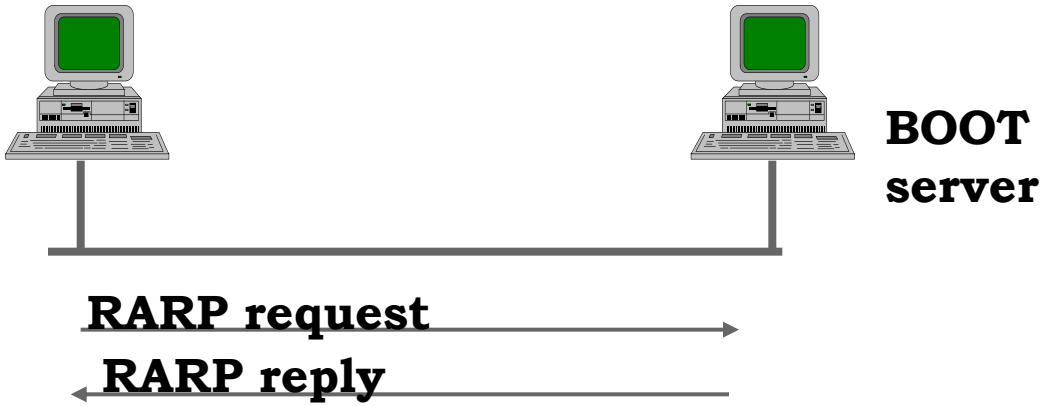
Domini di broadcast e reti IP: proxy ARP

- Un'alternativa è quella dell'installazione di un proxy ARP nel router
- La tecnica del proxy ARP consente a due reti fisicamente distinte di condividere lo stesso indirizzo di rete
- Il router conosce la collocazione fisica dei vari host nelle due reti
- Il router risponde alle richieste ARP su ciascuna delle due reti, "fingendosi" il destinatario. Dopodiché instrada i pacchetti al vero host destinatario



RARP (Reverse ARP)

- Il protocollo ARP consente di associare ad un indirizzo IP noto un indirizzo fisico non noto usando la capacità di broadcast della rete sottostante
- Il protocollo RARP (Reverse ARP) è in grado di effettuare l'operazione inversa:
  - Un host che conosce il proprio indirizzo fisico chiede di sapere il proprio indirizzo IP
  - Utile per macchine diskless che effettuano il bootstrap in rete
  - Ma non è più usato !!!



Indirizzi dinamici

- L'uso di procedure di questo tipo ha suggerito la possibilità di usare procedure per associare in modo flessibile gli indirizzi IP agli indirizzi fisici
- Può essere comodo non configurare i singoli host con l'indirizzo IP, ma usare un server per memorizzare tutte le configurazioni
- In molti casi non è necessario avere un'associazione stabile tra i due indirizzi ma si può usare un'associazione dinamica (più host degli indirizzi disponibili):
  - Host spesso inattivi (es. collegamenti remoti con rete d'accesso telefonica)
  - Host che usano IP solo per rari scambi di informazioni

Indirizzi dinamici

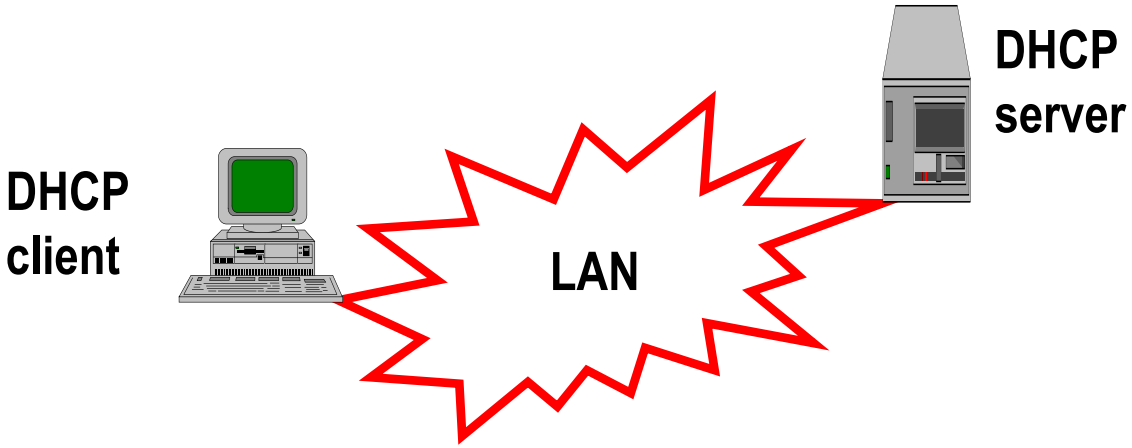
- Supponiamo di avere un server in grado di fornire l'indirizzo IP ad un host su richiesta
- Sono possibili diversi casi:
  - Associazione statica: il server ha una tabella di corrispondenza tra indirizzi fisici e indirizzi IP e all'arrivo di una richiesta consulta la tabella e invia la risposta
  - Associazione automatica: la procedura di corrispondenza nella tabella è automatizzata dal server
  - Associazione dinamica: l'insieme di indirizzi IP è più piccolo del numero di host che possono usarlo

Associazione dinamica

- Il caso dell'allocazione dinamica è utile in situazioni nelle quali gli host non necessitano di avere sempre un indirizzo IP
- L'associazione deve essere temporanea (uso di timeout o procedure di rilascio esplicito)
- E' possibile che all'arrivo di una richiesta non vi siano indirizzi disponili (rifiuto della richiesta)
- Il dimensionamento del numero di indirizzi IP segue gli stessi principi del dimensionamento di un fascio di circuiti in telefonia

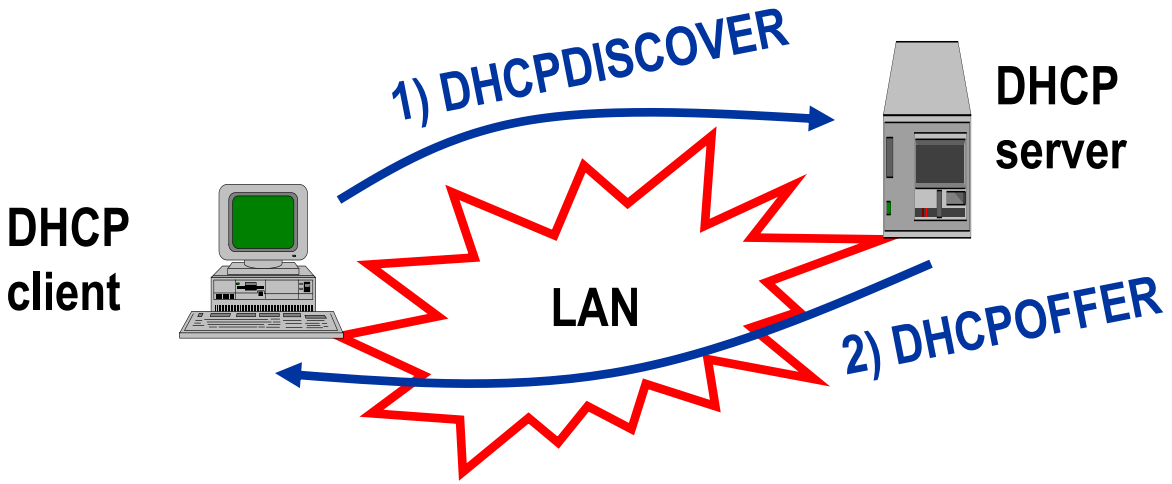
Dynamic Host Configuration Protocol (DHCP)

- Per la configurazione di indirizzi IP non si usa il RARP, ma un protocollo più evoluto derivato dal BOOTP
- E’ un protocollo di tipo client-server



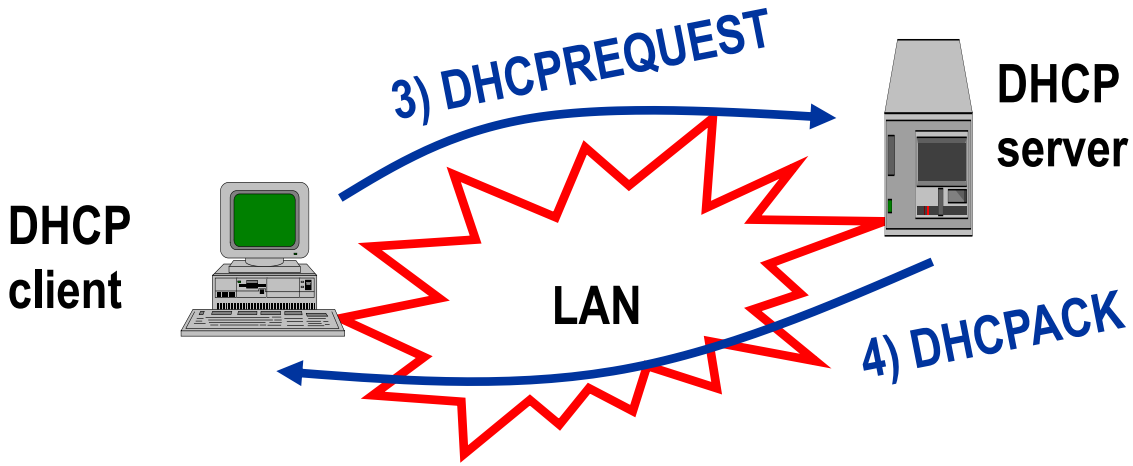
DHCP

- Un client che deve configurare il proprio stack IP invia in broadcast un messaggio di DHCPDISCOVER contenente il proprio indirizzo fisico
- Il server risponde con un messaggio di DHCPOFFER contenente un proprio identificativo e un indirizzo IP proposto



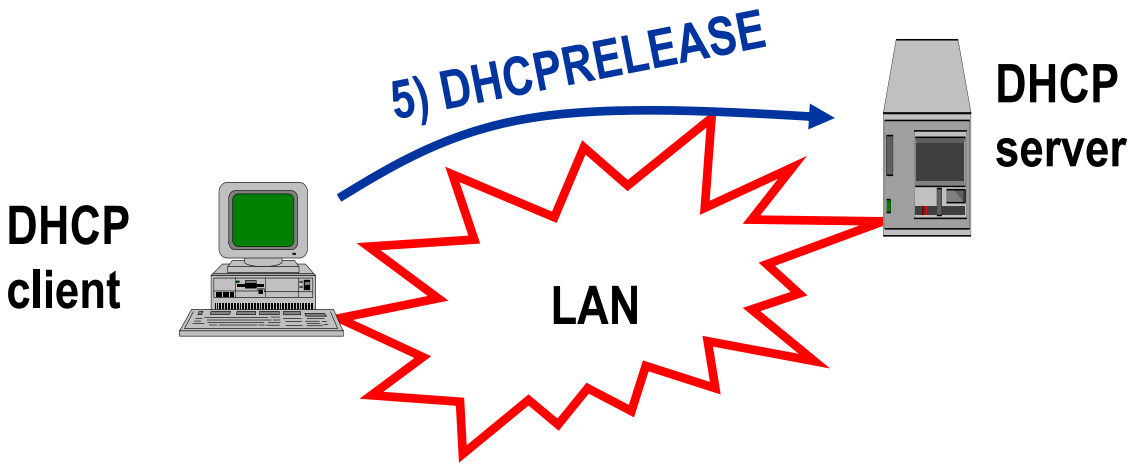
DHCP

- Il client può accettare l'offerta inviando una DHCPREQUEST contenente l'identificativo del server (anche questo messaggio viene inviato in broadcast)
- Il server crea l'associazione con l'indirizzo IP e manda un messaggio di DHCPACK contenente tutte le informazioni di configurazione necessarie



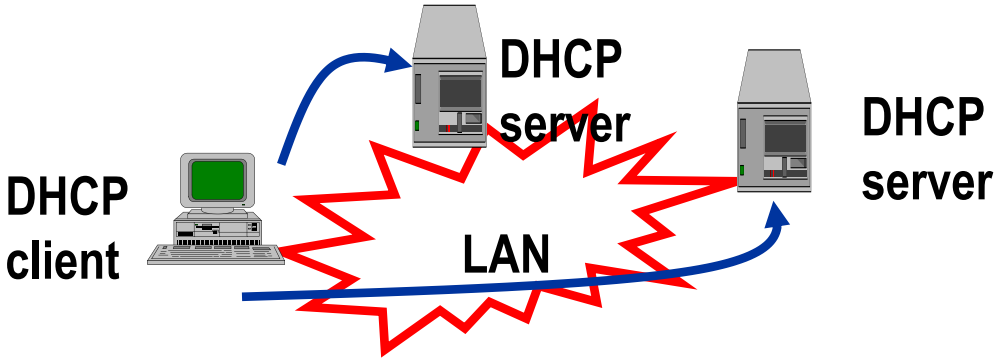
DHCP

- Parametri di configurazione
  - IP address
  - Netmask
  - Default Gateway
  - DNS server
- Il rilascio dell'indirizzo avviene con l'invio di un messaggio di DHCPRELEASE da parte del client

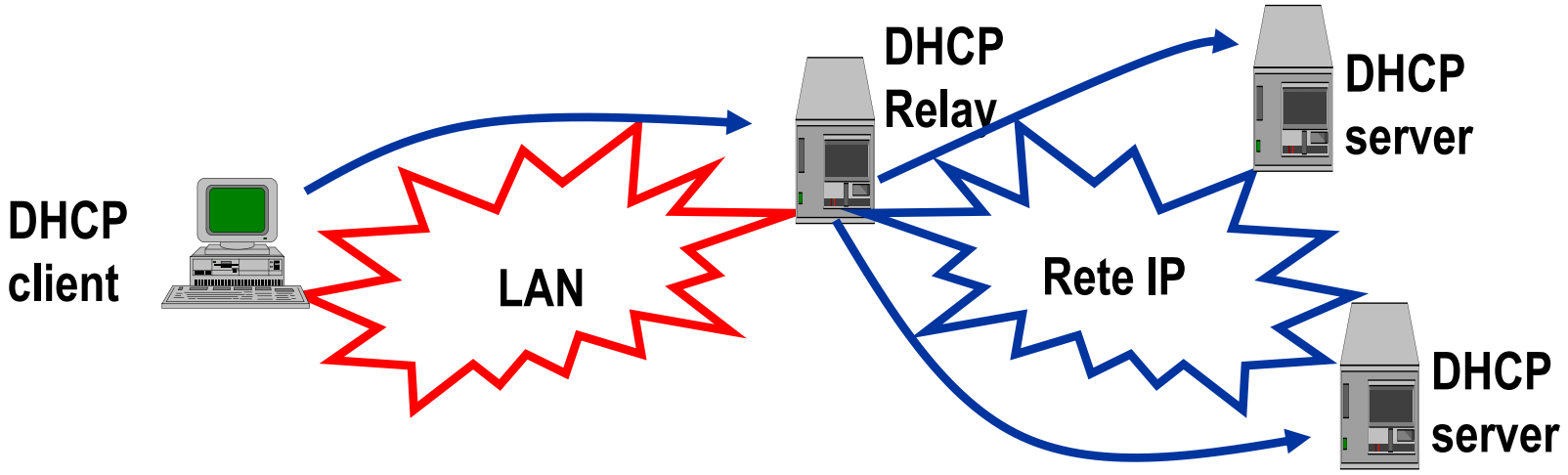


DHCP

- E’ possibile avere più server

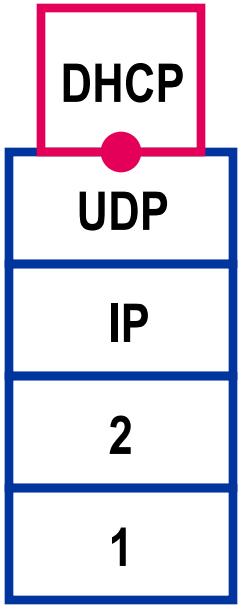


- E’ possibile usare dei DHCP Relay

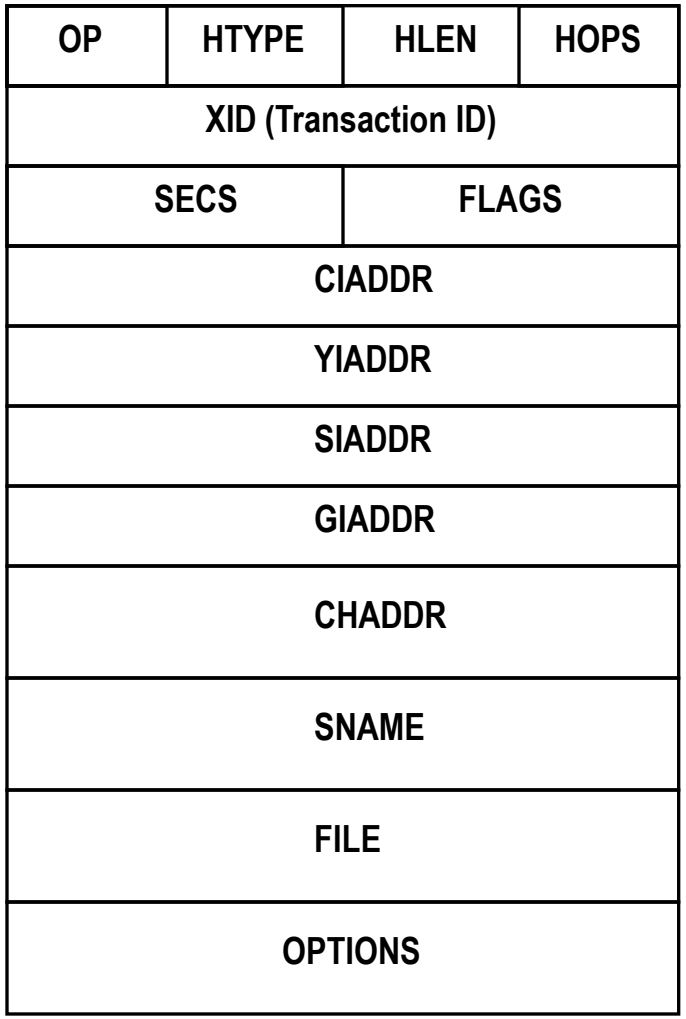


Trasporto dei messaggi

- DHCP si appoggia su UDP per il trasporto dei messaggi
- I messaggi dei client fino all'assegnamento dell'indirizzo IP hanno:
  - ind. IP di sorgente: 0.0.0.0
  - ind. IP di destinazione: 255.255.255.255
  - porta UDP sorgente: 68
  - porta UDP destinazione: 67



Messaggi

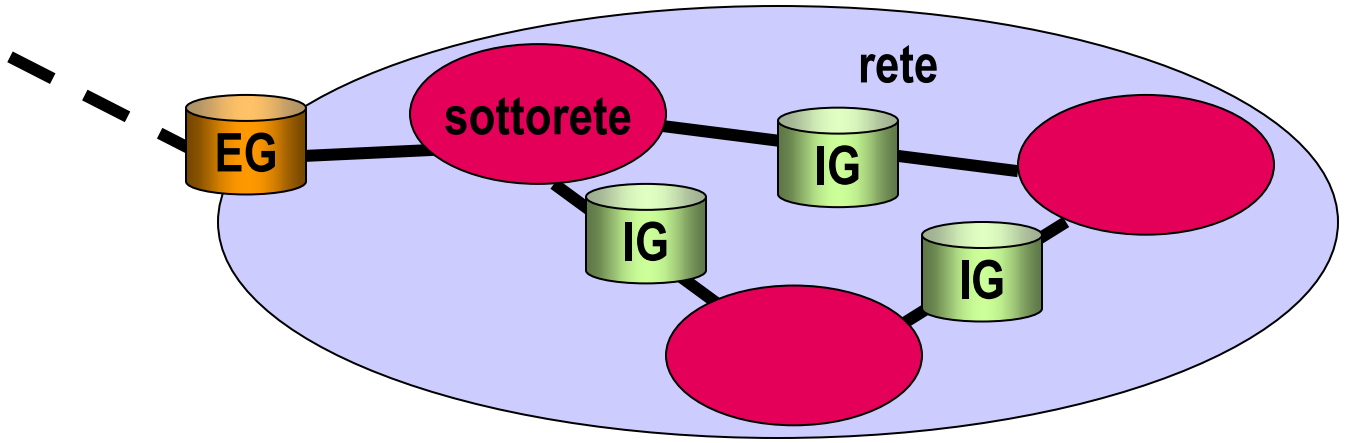


CAMPO	BYTE	DESCRIZIONE
op	1	Tipo di messaggio (1 = BOOTREQUEST, 2 = BOOTREPLY)
htype	1	Tipo di indirizzo fisico (1 = Eth 10Mb)
hlen	1	Lunghezza ind. fisico ('6' per Eth 10Mb)
hops	1	Settato dal client a 0 e incrementato dai relay agests
xid	4	Numero casuale settato dal client e usato per evitare ambiguit\`a
secs	2	Settato dal client, numero di sec dall'inizio della procedura
flags	2	Flags (si usa solo il primo bit per chiedere una risposta multicast o unicast).
ciaddr	4	Indirizzo IP del client (settato dal client, zero se non noto)
yiaddr	4	Indirizzo IP del client (settato dal server)
siaddr	4	Indirizzo IP del server
giaddr	4	Indirizzo del relay agent
chaddr	16	Indirizzo fisico del client
sname	64	Stringa Nome del server (opzionale)
file	128	Stringa nome del file di boot (opzionale)
options	312	Lista di opzioni per il trasferimento di altre informazioni

INTRANET

Indirizzamento Privato, NAT, Tunnelling

Intranet



- Le reti private si sono evolute grazie alla tecnologia IP e sono passate da grandi reti collegate a livello 2 (bridge) a reti collegate con router IP
- Una INTRANET non è altro che una rete privata che utilizza tecnologia di interconnessione IP
- Di solito oggi con INTRANET si intende una rete IP collegata con la rete pubblica INTERNET mediante un ISP e dotata di servizi per gli utenti di Internet come server www, server di posta, ecc.

Intranet

- L’evoluzione di servizi e protocolli ha però reso le Intranet strutturalmente differenti dalle reti pubbliche
  - Problemi di sicurezza
  - Problemi di gestione degli indirizzi
  - Problemi di distinzione tra servizi offerti ai soli utenti della Intranet e servizi offerti anche agli utenti di Intenet

Indirizzi

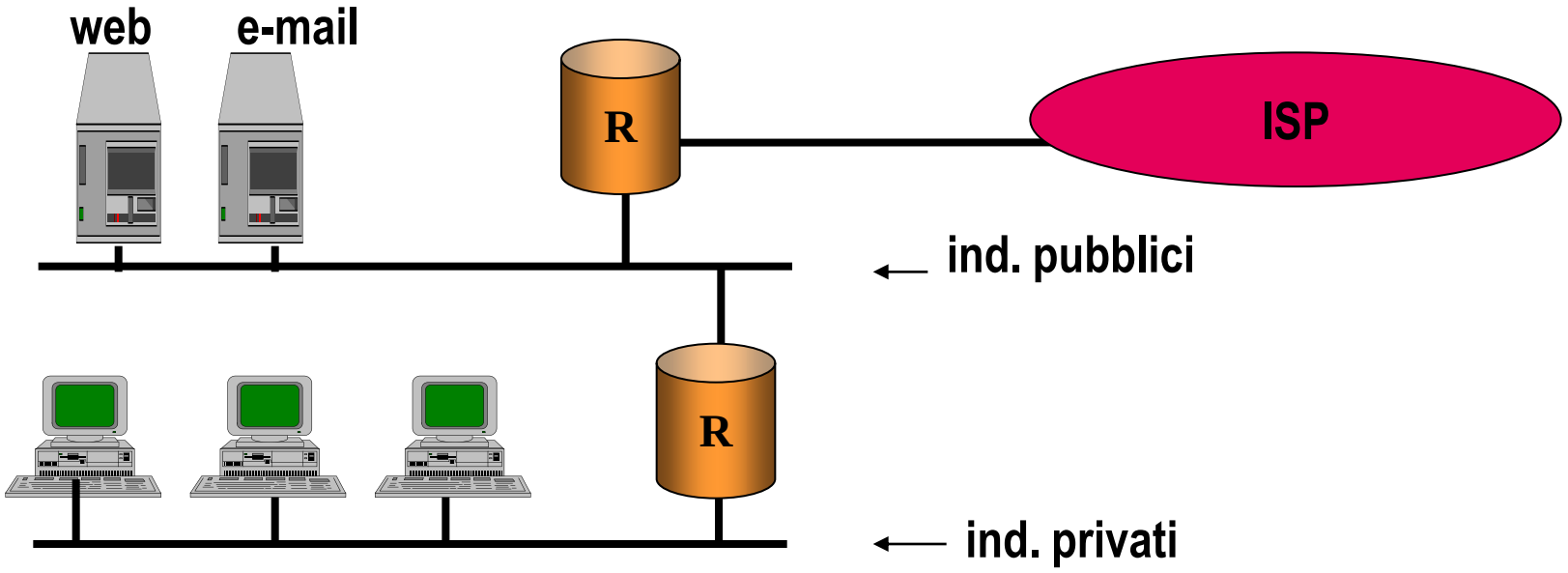
- L’aumento vertiginoso del numero di host collegati ad Internet ha reso il problema della disponibilità di indirizzi IPv4 pressante
- E’ questo problema che ha spinto alla standardizzazione di IPv6
- Nel frattempo però si è trovata un’altra soluzione basata su indirizzi privati
- Se una rete IP non è collegata con INTERNET può usare gli indirizzi che gli pare …

Indirizzamento privato

- La comunità Internet ha individuato gruppi di indirizzi IP che non vengono usati nella rete pubblica
- possono essere usati più volte purché all'interno di Intranet Private
- Non è ammesso che pacchetti con indirizzi privati (sorgente o destinazione) viaggino nella rete pubblica
  - classe A: rete 10.xx.xx.xx (16 milioni di indirizzi)
  - classe B: da 172.16.0.0 a 172.31.255.255(16 reti contigue da 65536 indirizzi)
  - classe C: reti 192.168.xx.xx (256 reti)

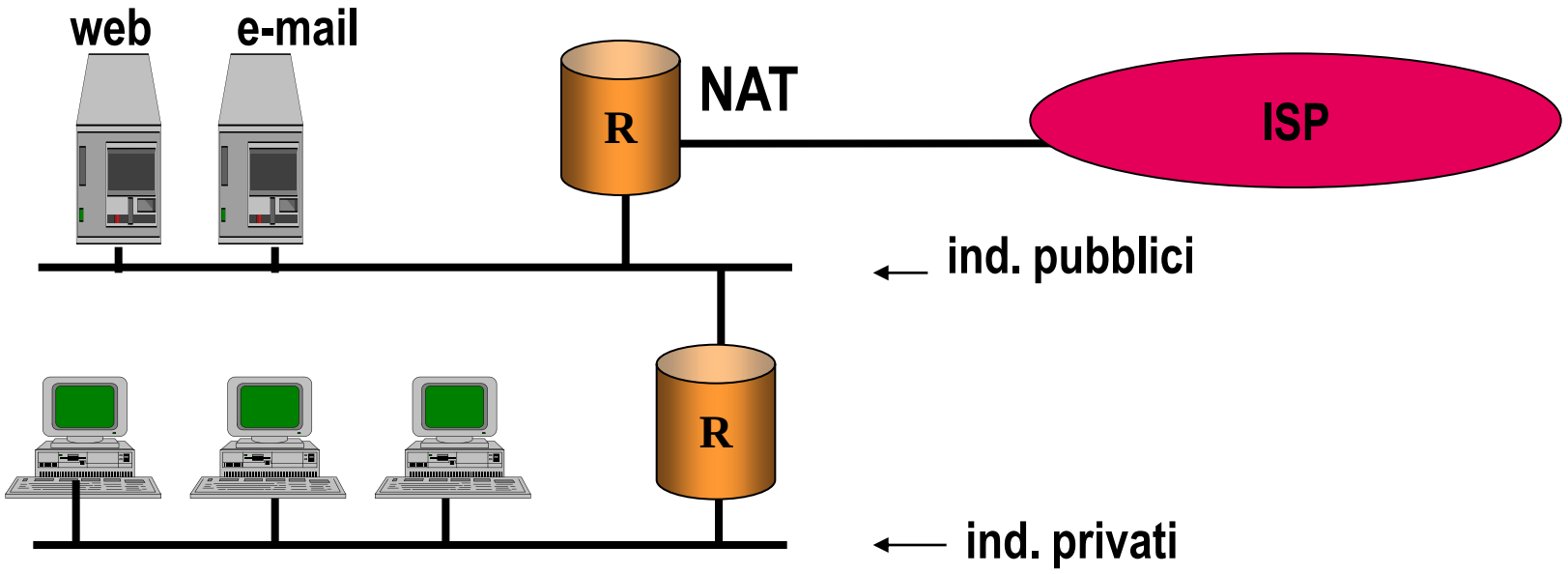
Utilizzo di numeri privati IETF

- Una rete privata ha normalmente una serie di servizi che sono accessibili dalla rete pubblica
- I server per questi servizi devono avere un indirizzo pubblico mentre gli host interni alla rete possono avere un indirizzo privato



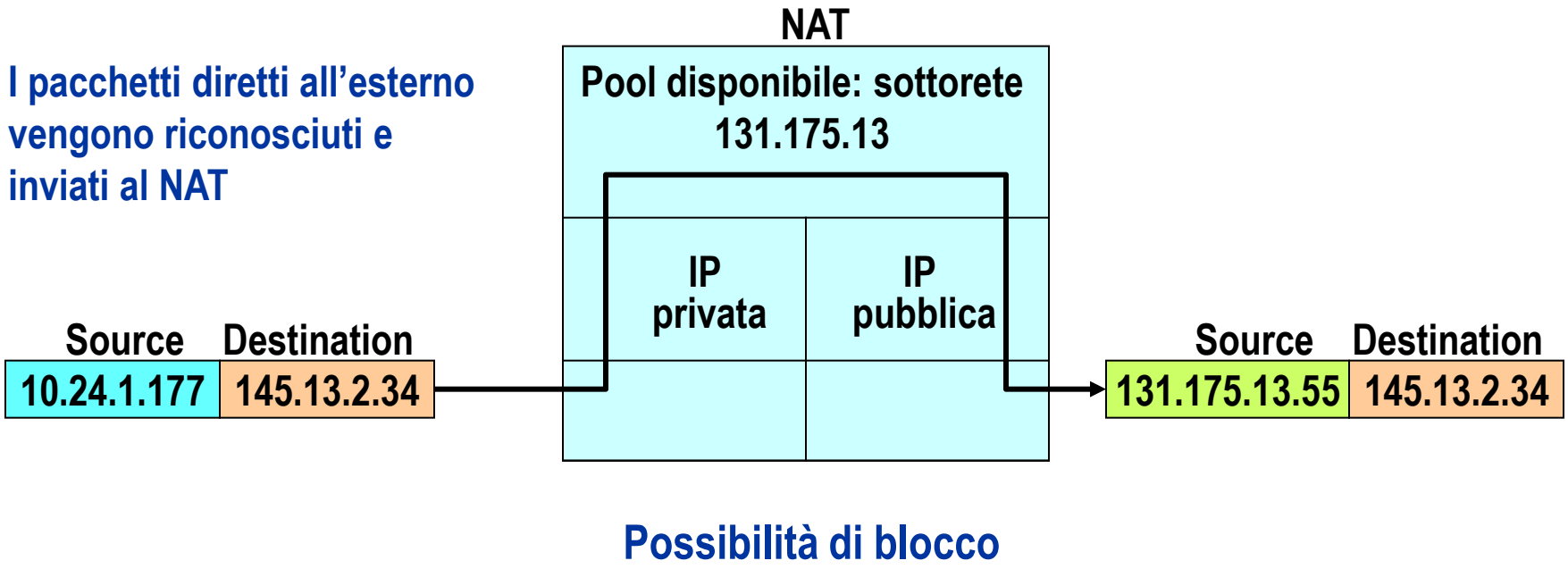
Utilizzo di numeri privati IETF

- E’ chiaro comunque che in questo modo si impedisce agli host della rete privata di aver accesso a tutti servizi di Internet
- Prima o poi sorge l’esigenza di consentire lo scambio di pacchetti tra host con indirizzo pubblico e host con indirizzo privato
- I metodi più comunemente usati per consentire il colloqui sono il **NAT** e i **Proxy**



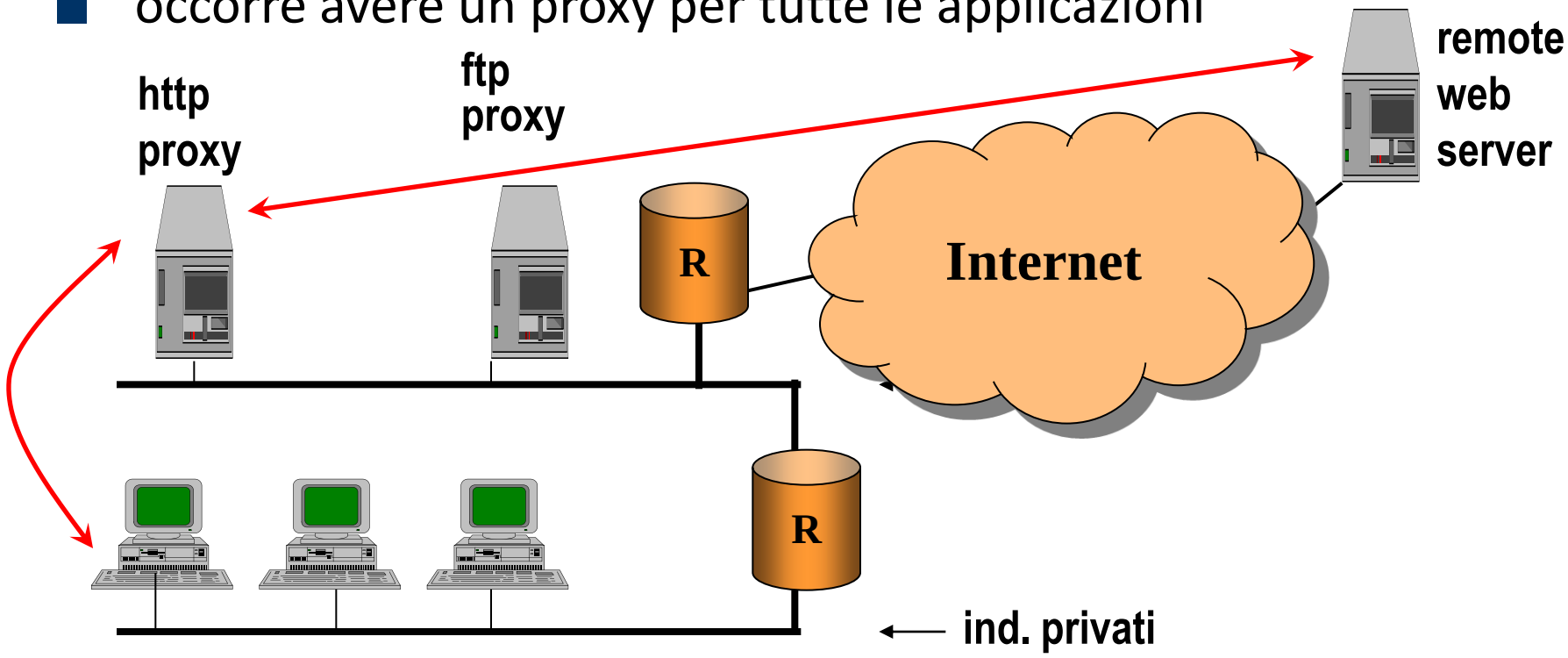
Network Address Translator (NAT)

- E’ un meccanismo reso disponibile su un router/gateway
- Consente di associare, anche temporaneamente, un ridotto numero di indirizzi pubblici, ai numeri della numerazione privata



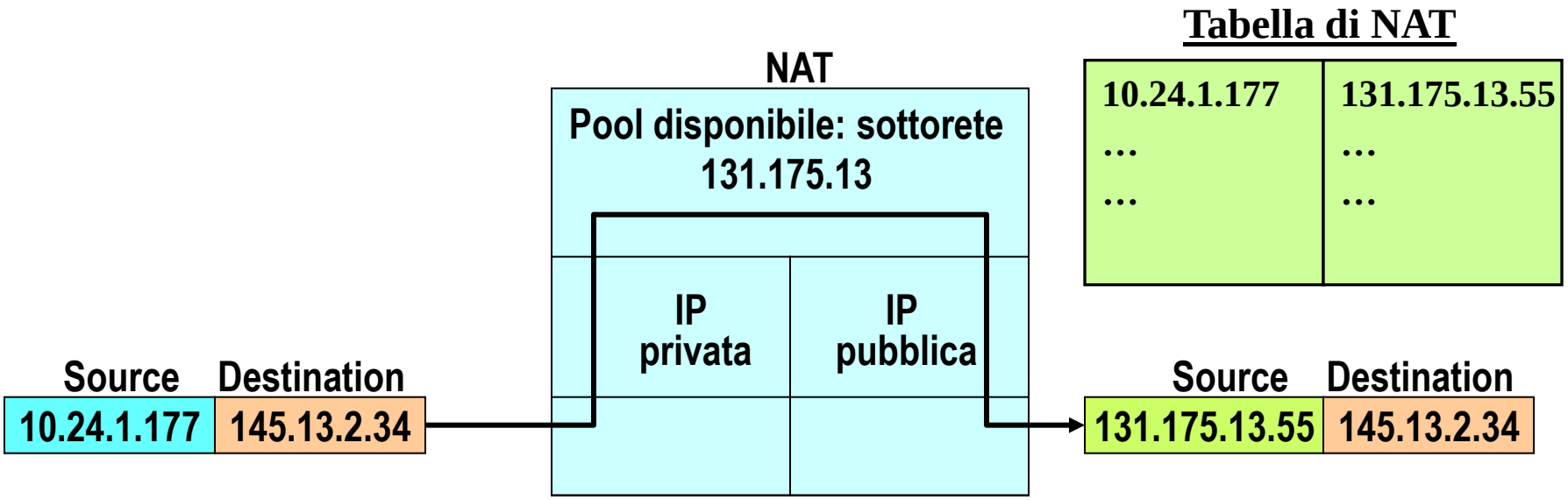
Application Proxy

- I proxy sono application gateway
- qualunque richiesta viene inviata al proxy che la inoltra con il proprio IP address pubblico
- occorre avere un proxy per tutte le applicazioni



NAT – Tabella di NAT

- Perché il colloquio sia bidirezionale occorre mantenere l'associazione tra indirizzo privato e pubblico un una tabella di NAT
  - Corrispondenza statica
  - Corrispondenza dinamica



NAT – assegnamento dinamico

- L'assegnamento dinamico si basa sul concetto di *sessione*
- Quando il NAT vede il primo pacchetto di una sessione crea l'associazione tra ind. privato e pubblico
- Al termine della sessione l'indirizzo viene rilasciato
- Cos'è una sessione?
  - Dipende dal protocollo utilizzato
  - Per TCP e UDP una sessione viene identificata dall'indirizzo di socket
  - Per ICMP dalla terna IP sorgente, IP destinazione e Identifier
  - Per direzione di una sessione si intende il verso di percorrenza del primo pacchetto

NAT – assegnamento dinamico

- Definita la sessione occorre capire quando inizia e quando finisce
- Inizio sessione:
  - TCP: pacchetto di SYN
  - UDP, ICMP: sono connection-less, non vi è un metodo unico
- Fine sessione:
  - TCP: pacchetti di FIN per entrambe i lati (però possono non arrivare mai …)
  - Altri prot.: non vi è un metodo univoco
  - Occorrono sempre dei time-out per recuperare situazioni d’errore o perdita di pacchetti

NAT – Application Level Gateway

- Alcune applicazioni trasportano nel Payload dei loro messaggi indirizzi IP (in formato ASCII o binario) e numeri di porta
- Gli Application Level Gateway (ALG) sono funzionalità aggiuntive che servono per un corretto funzionamento del NAT
- Sulla base del tipo di applicazione e del tipo di messaggio si preoccupano di modificare i messaggi applicativi in transito e, se del caso, adattare i segmenti TCP

Traditional NAT

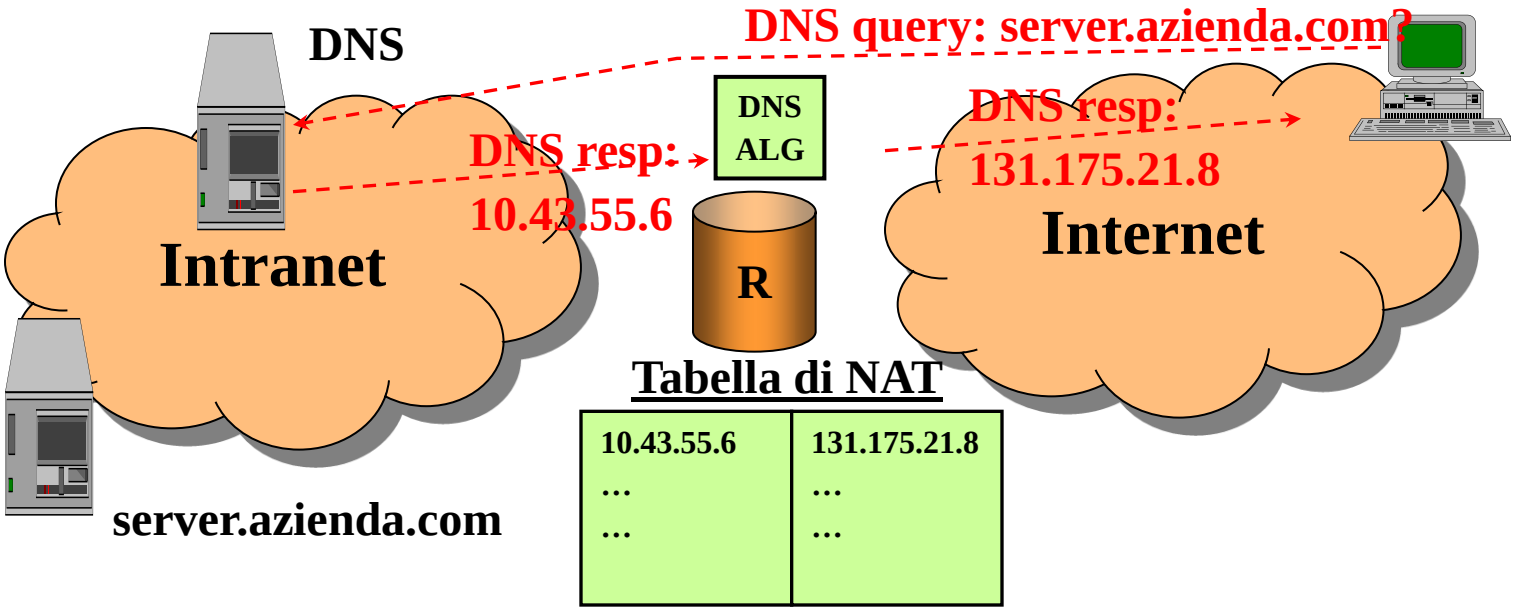
- Detto anche Outbound NAT
- Permette solo sessioni iniziate dall'interno (verso della sessione dall'interno verso l'esterno)
- Le informazioni di routing possono essere distribuite dall'esterno verso l'interno ma non viceversa
- 2 sotto-tipi
  - Basic NAT
  - NAPT (Network Address and Port Translator)

Traditional NAT

- Basic NAT
  - Viene traslato il solo indirizzo IP
  - C'è una corrispondenza uno-a-uno nell'assegnamento degli indirizzi durante una sessione e due host non possono usare lo stesso indirizzo contemporaneamente
  - Ci può essere blocco a causa del numero scarso di indirizzi pubblici quando il traffico (numero di sessioni attive) è elevato
- NAPT
  - Viene traslata la coppia (indirizzo,porta)
  - Molti indirizzi interni possono usare lo stesso indirizzo esterno
  - Ci sono problemi con flussi diversi da UDP e TCP (per ICMP si può usare il campo Identifier)
  - Nel caso di frammenti tutto si complica ulteriormente

Bi-directional NAT

- Si può iniziare una sessione in entrambe i versi
- Problema:
  - Come fa un host pubblico ad iniziare un sessione con un host privato senza avere un indirizzo pubblico a cui raggiungerlo?
  - Occorre usare dei nomi simbolici e il servizio DNS che deve usare un unico spazio dei nomi



NAT – alcune considerazioni

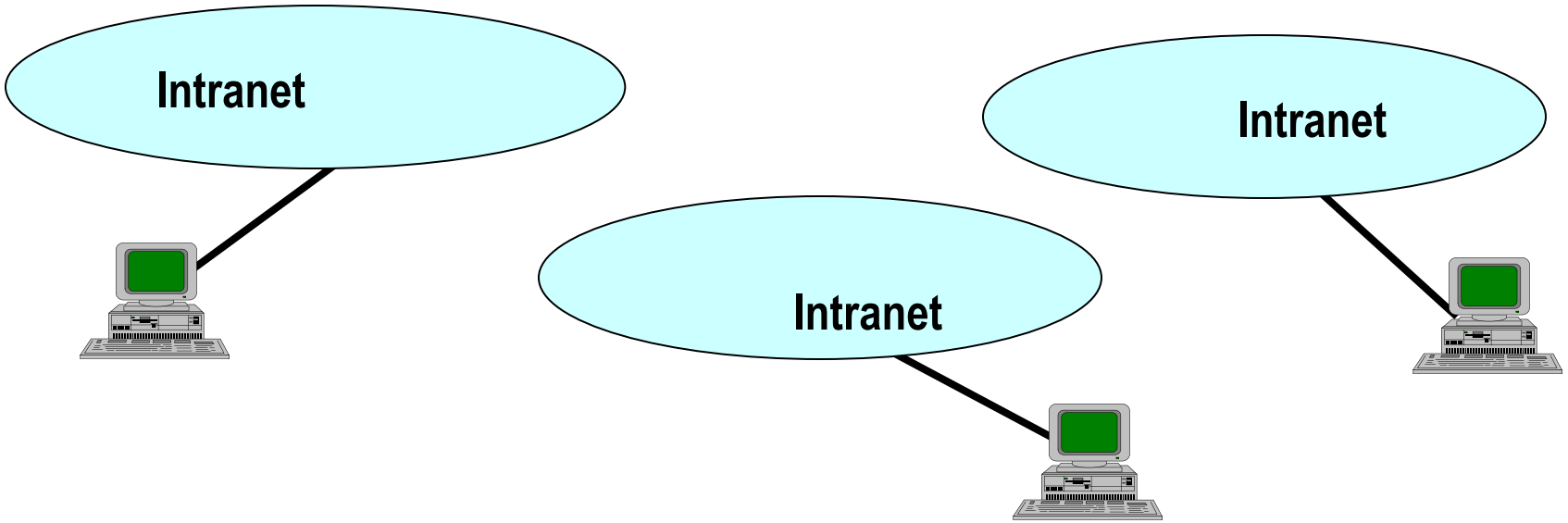
- Il cambio di indirizzo non è un'operazione indolore
- Esso impone:
  - Il ricalcolo del Header Checksum
  - Sostituzione degli indirizzi dei messaggi ICMP e ricalcolo header checksum
  - Il ricalcolo dei checksum di TCP o UDP con il nuovo pseudo-header
- Sorgono poi dei problemi con alcuni ALG per via del trasporto degli indirizzi e porte nei messaggi di livello applicativo

NAT – alcune considerazioni

- Il caso del FTP
  - Si usa il comando di PORT
  - PORT n1,n2,n3,n4,n5,n6 dove:
    - n1.n2.n3.n4 è l'indirizzo IP del client
    - N5x256+n6 = numero di porta del client per la connessione dati
  - Occorre traslare il comando di PORT ma la cosa non è così banale:
    - Da 10.43.55.6 (privato) in 131.175.21.1(pubblico)
    - Ma FTP è ACSI e nel mapping si allunga di due caratteri e quindi si sballano il conteggio dei byte per i SN e AN del TCP
    - ALG per FTP deve dunque costruirsi una tabella di mapping al volo anche per i numeri di sequenza e di ACK del TCP!!!

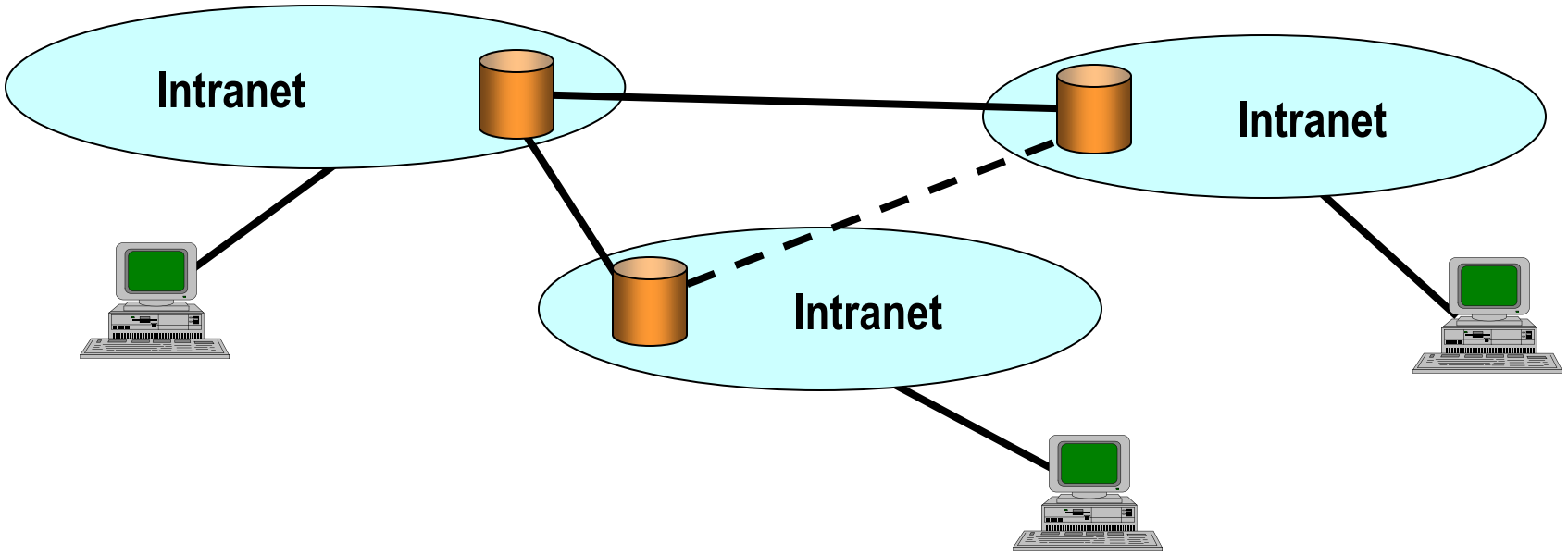
Connessione WAN di intranet remote

- Una volta create le Intranet può sorgere il problema di collegarle tra loro (ad es. sedi diverse di una stessa azienda)
- Problemi:
  - costo
  - uso di indirizzi privati
  - sicurezza



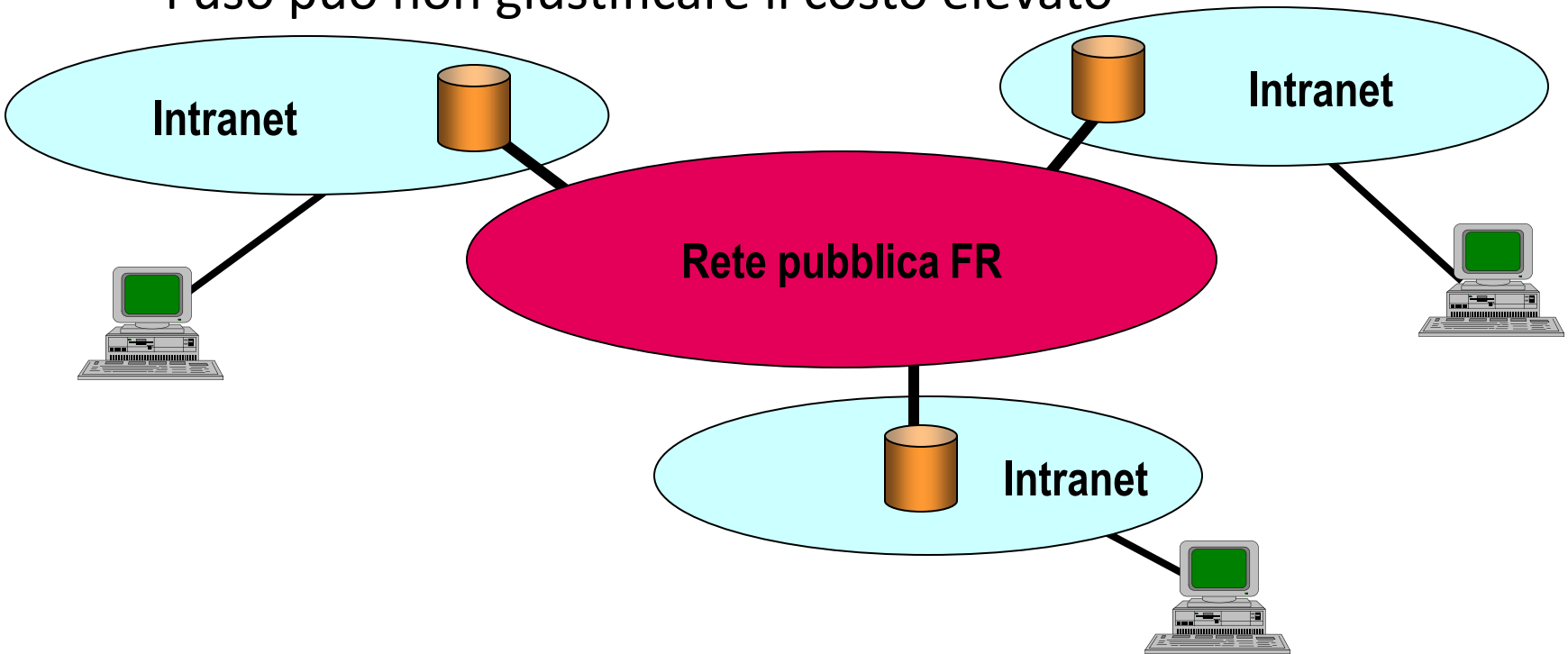
Connessione WAN di intranet remote

- Uso di canali dedicati
- Problemi:
  - l'uso può non giustificare il costo elevato



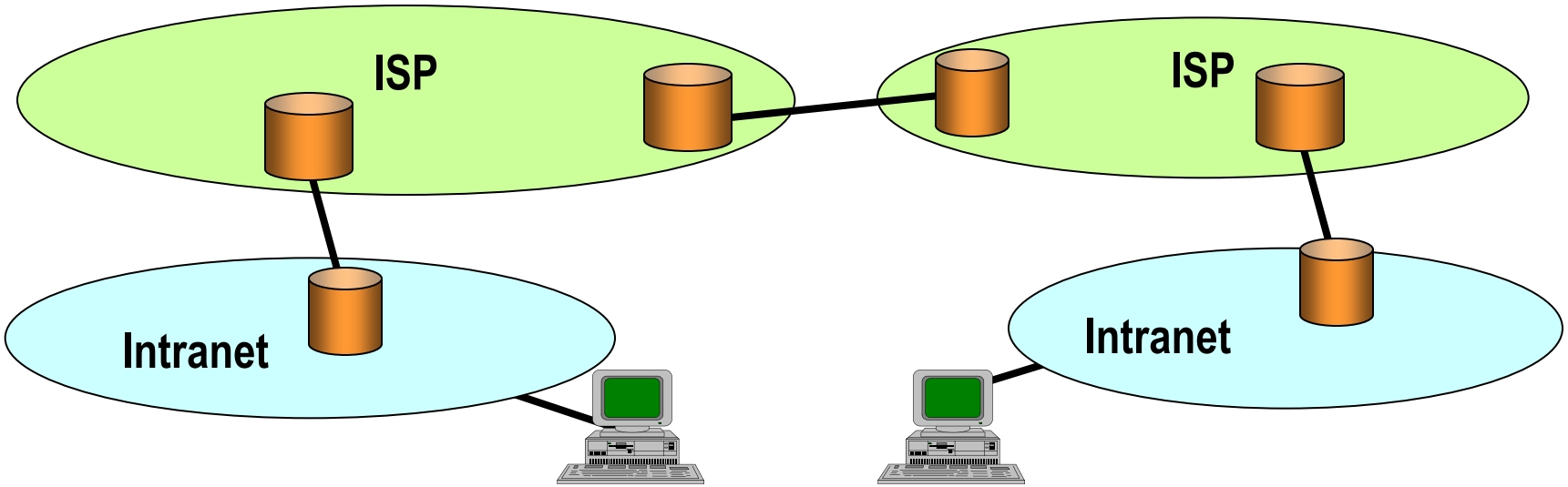
Connessione WAN di intranet remote

- Uso di reti a pacchetto pubbliche (ad es. Frame Relay)
- Problemi:
  - l'uso può non giustificare il costo elevato



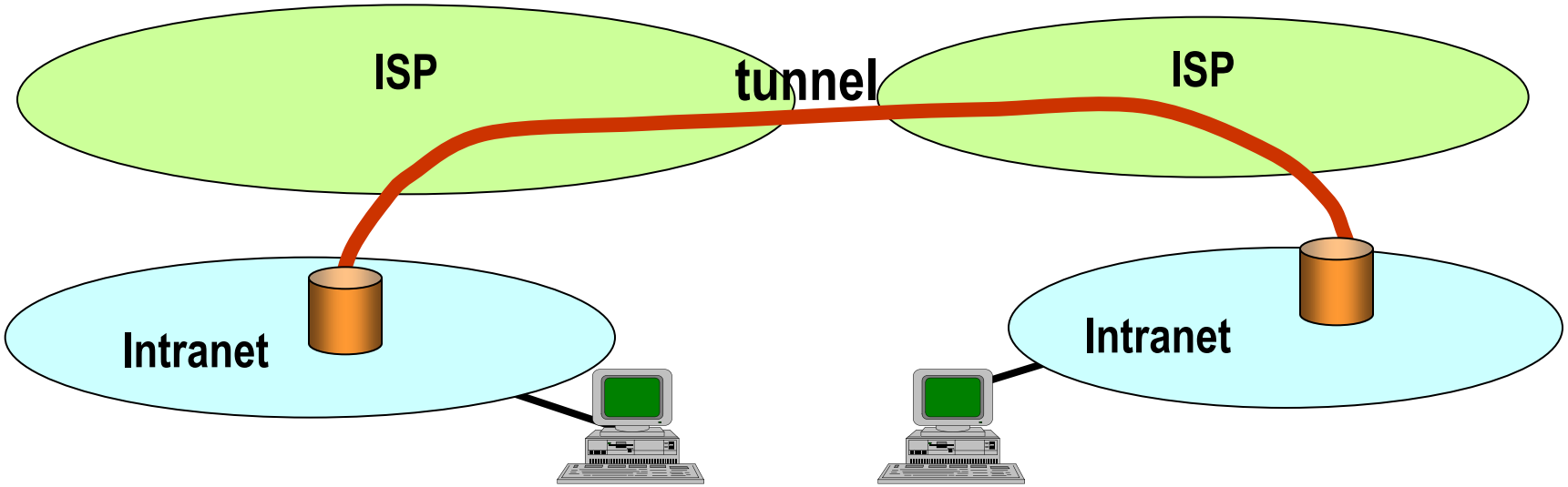
Connessione WAN di intranet remote

- Uso di INTERNET (Virtual Private Network - VPN)
- Problemi:
  - uso di indirizzi privati
  - sicurezza
  - prestazioni



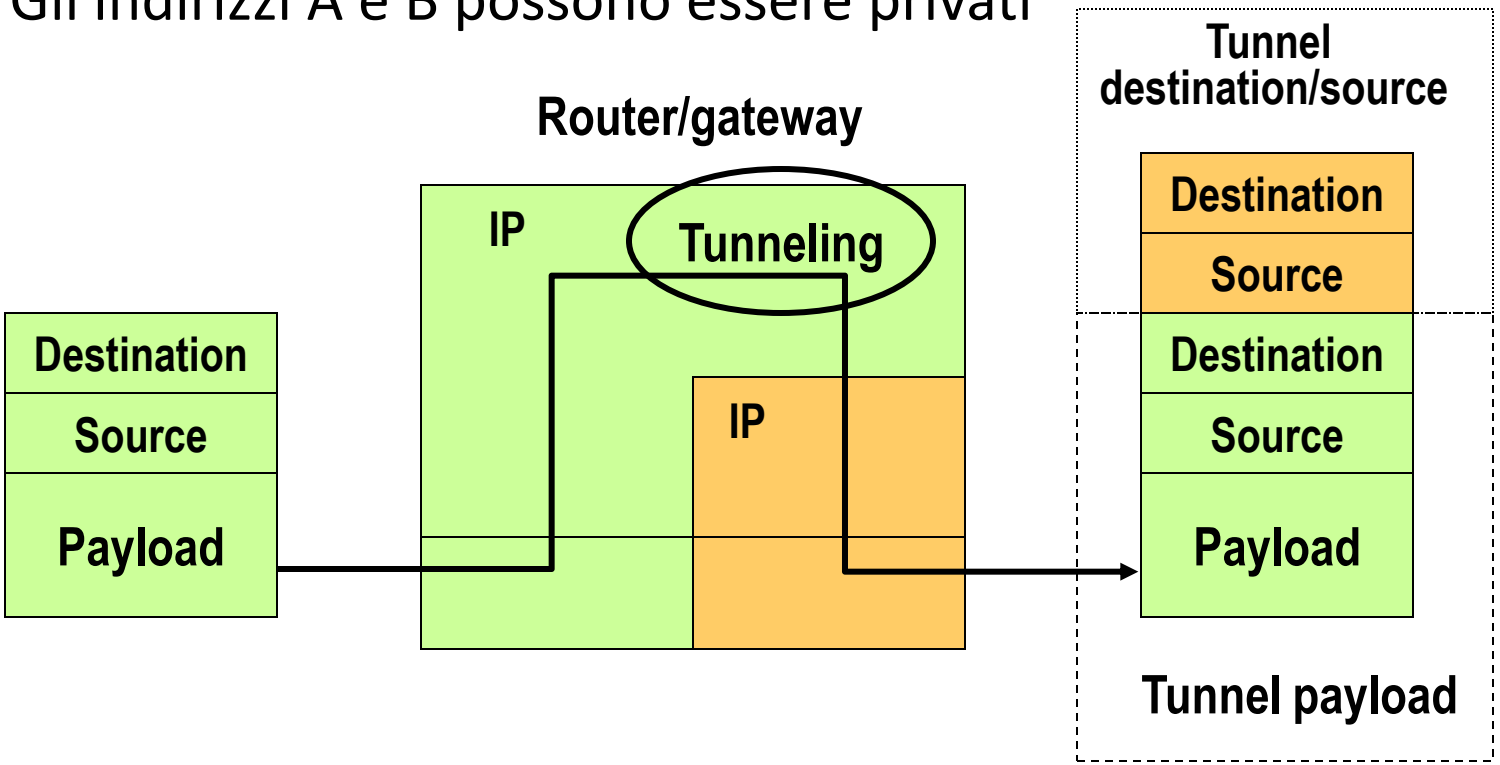
Virtual Private Networks

- Tunnel di collegamento

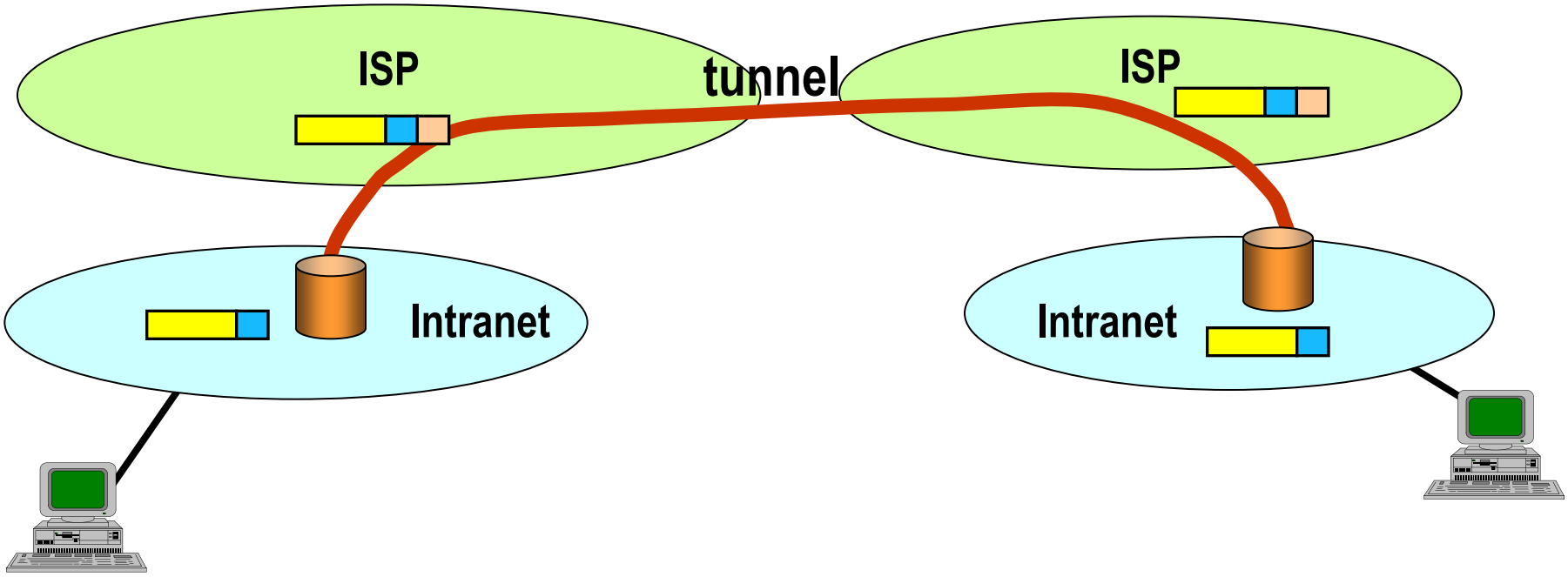


IP tunneling

- Il tunnel si costruisce incapsulando trame IP in altre trame IP
- Il payload che viaggia nel segmento pubblico può essere crittato
- Gli indirizzi A e B possono essere privati



IP tunneling



IPv6

Internet Prococol version 6

IPv6

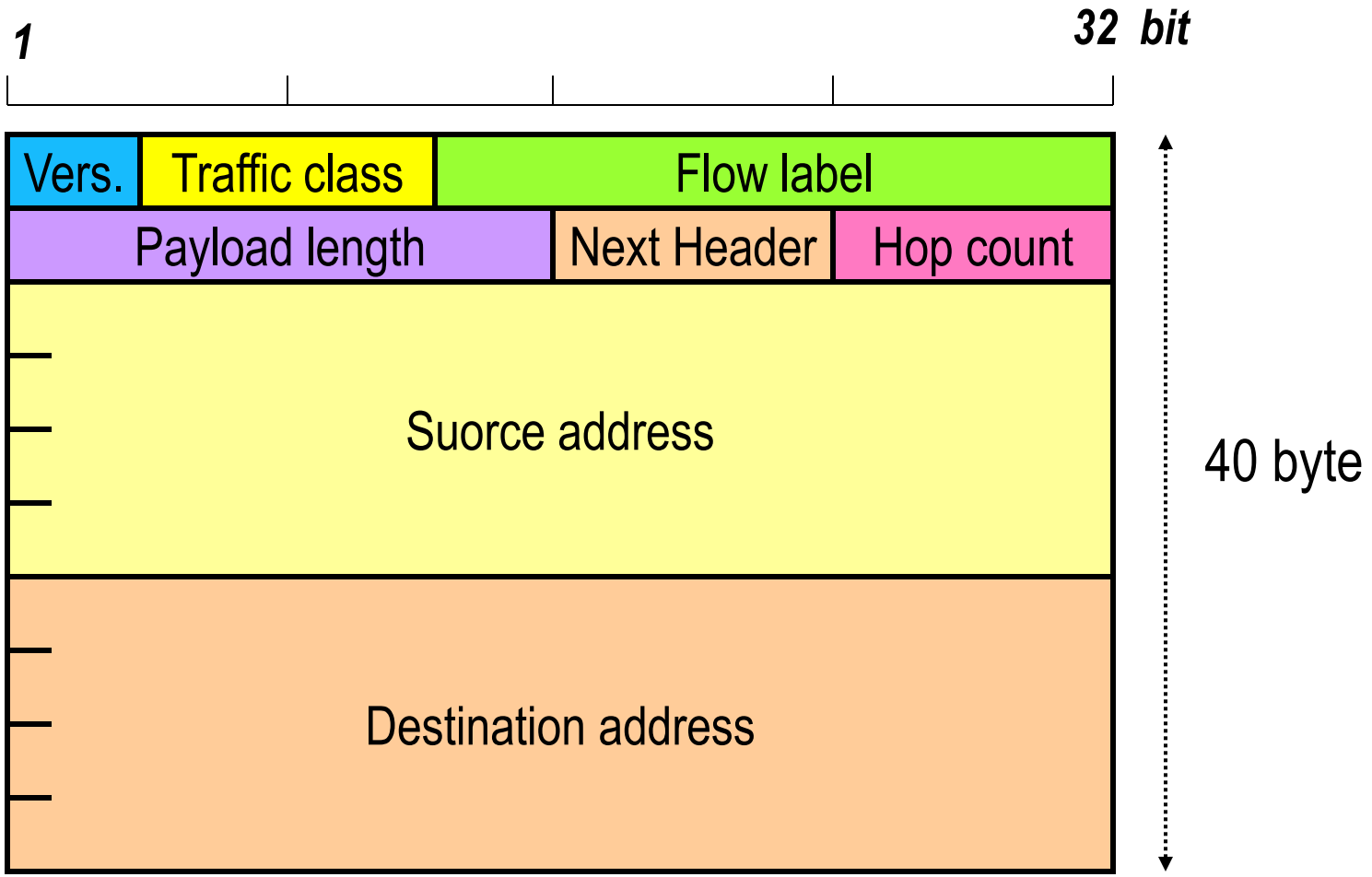
- IP versione 6 è la nuova versione dell'Internet Protocol il cui processo di standardizzazione è iniziato negli anni '90
- Mantiene l'impostazione fondamentale di IPv4 ma cambia molti aspetti
- … e soprattutto **aumenta la lunghezza** degli indirizzi da **32 a 128 bit**

IPv6: le novità principali

- IPv6
  - Indirizzi, gestione delle opzioni, gestione della frammentazione, identificazione flussi, classi di traffico, niente header checksum, ecc.
- ICMPv6:
  - Nuova versione di ICMP con funzionalità aggiuntive
- ARP:
  - Eliminato e sostituito da ICMPv6
- DHCPv6
  - Modificato per il nuovo protocollo (alcune funzioni sono svolte da ICMPv6)
- Routing
  - RIPng e OSPFv6

Header IPv6

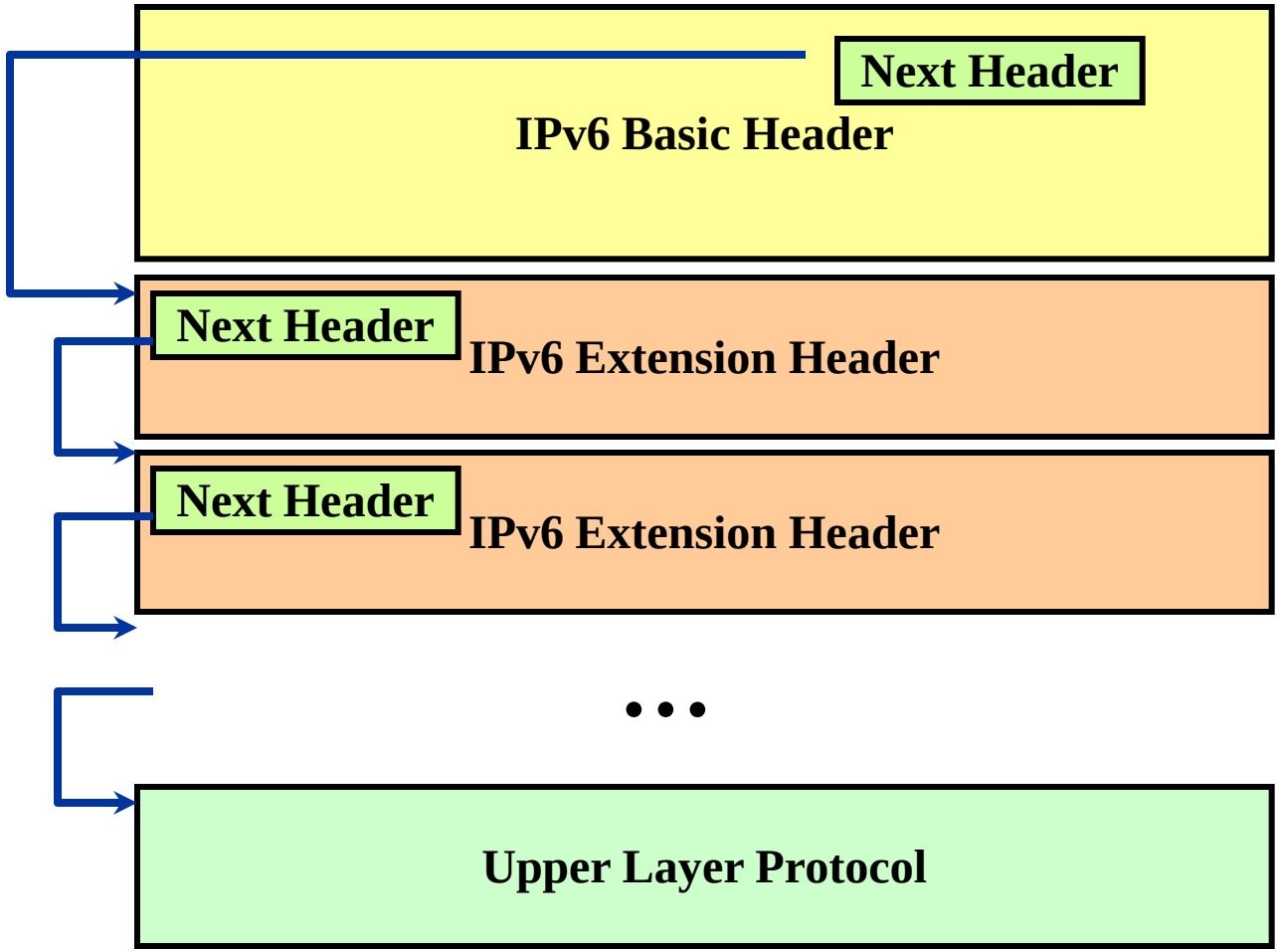
- Basic Header



Header IPv6

Campo	Lung. (bit)	Descrizione
Version	4	Versione del Protocollo (6)
Traffic Class	8	Campo utilizzabile per distinguere diversi tipi di traffico nelle reti Differentiated Services
Flow Label	20	Campo utilizzabile per identificare un flusso di pacchetti (stessa lunghezza di MPLS)
Payload Length	16	Lunghezza del pacchetto (eccetto basic header)
Next Header	8	Identifica il tipo di header che segue il basic header (può essere di livello superiore come TCP o un extension header)
Hop Limit	8	Stessa funzione del TTL di IPv4
Source Address	128	Indirizzo di sorgente
Destination Address	128	Indirizzo di destinazione

Next Header


Next Header
IPv6 Basic Header
Next Header
IPv6 Extension Header
Next Header
IPv6 Extension Header
• • •
Upper Layer Protocol

IPv6 Extension Headers

- Hop-by-hop option:
  - Deve essere interpretato dai router
  - Ha varie opzioni per pacchetti lunghi e gestione di allineamenti a 32 bit
- Source Routing:
  - Serve a obbligare i router a seguire un particolare percorso per il pacchetto
- Fragmentation:
  - Implementa la frammentazione, ma questa può essere eseguita solo dal mittente che deve conoscere la massima MTU del path (la ottiene mediante i messaggi di MTU Path discovery di ICMPv6)
- Autenticazione
  - Serve per l'autenticazione del mittente
- Encrypted security payload
  - Serve per crittare il payload (altro pacchetto IP o livelli superiori)

Indirizzi IPv6

- Notazioni sintetiche
- A gruppi di 2 byte in esadecimale:
  - 8000:0000:0000:0000:8965:0678:A45C:87D3
- Gli zeri possono essere omessi:
  - 8000::8965:678:A45C:87D3
- Notazione speciale per IPv4
  - ::131.175.21.173
- Numero di indirizzi per metro quadro di superficie terrestre: **$7x10^{23}$**
  - Maggiore del numero di Avogadro

Tipi di indirizzi IPv6

- IPv6 prevede un ricca varietà di indirizzi e assume che normalmente una interfaccia abbia più di un indirizzo associato
- Destinatario
  - Unicast (*uno*)
  - Anycast (*almeno uno di un gruppo*)
  - Multicast (*tutti quelli di un gruppo*)
- Uso
  - Globale
  - Locale (stesso link, stesso site)

Prefissi IPv6

- Così come IPv4 anche IPv6 assume i prefissi per una individuazione del campo che identifica l'interfaccia
- La notazione è la stessa (ad. Es. /60)
- I tipi diversi di indirizzi sono individuati dalla prima parte del prefisso (*format prefix - FP*)

Tipi di indirizzi IPv6

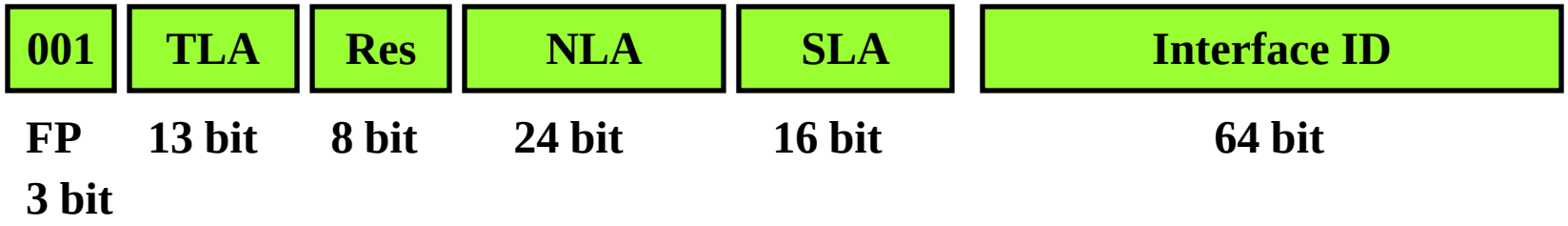
Prefix (binary)	Usage	Fraction
0000 0000	Reserved for IPv4 addresses	1/256
0000 0001	Unassigned	1/256
0000 001	OSI NSAP addresses	1/128
0000 010	Novell Netware IPX addresses	1/128
0000 011	Unassigned	1/128
0000 1	Unassigned	1/32
0001	Unassigned	1/16
001	Aggregatable Global Unicast add.	1/8
010	Unassigned	1/8
011	Unassigned	1/8
100	Unassigned	1/8
101	Unassigned	1/8
110	Unassigned	1/8
1110	Unassigned	1/16
1111 0	Unassigned	1/32
1111 10	Unassigned	1/64
1111 110	Unassigned	1/128
1111 1110 0	Unassigned	1/512
1111 1110 10	Link local use addresses	1/1024
1111 1110 11	Site local use addresses	1/1024
1111 1111	Multicast	1/256

Indirizzi speciali

- Unspecified address (0:0:0:0:0:0:0:0)
  - Usato come indirizzo di sorgente quando il nodo non conosce altri suoi indirizzi
  - Non può essere usato come indirizzo di destinazione
- Loopback address (0:0:0:0:0:0:0:1)
  - Indirizzo di loopback analogo al 127.x.y.z di IPv4
- IPv4-compatible IPv6 address (::IPv4_addr)
  - Utilizzato per far comunicare host IPv6 quando occorre attraversare una rete IPv4 (96 zero + 32 bit IPv4_addr)
- IPv4-mapper IPv6 address (::FFFF:IPv4_addr)
  - Utilizzati per far comunicare host IPv6 con host IPv4 (80 zero + 16 uno + IPv4_addr)

Aggregatable Global Unicast Address

- Formato unicast globale
- Struttura gerarchica per ridurre i problemi di scalabilità delle tabelle di routing
- 3 macrolivelli: Public Topology, Site Topology, Interface_ID



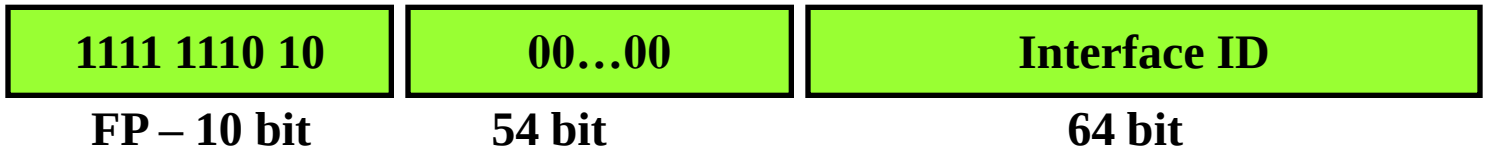
Aggregatable Global Unicast Address

- **TLA** (Top Level Aggregation)
  - Livello gerarchico più elevato normalmente assegnato su base geografica o agli ISP di backbone
- **Res** (Reserved) – future espansioni
- **NLA** (Next Level Aggregation)
  - Ogni ISP con un TLA può strutturare gerarchicamente le sue reti con diversi NLA
- **SLA** (Site Level Aggregation)
  - Livello legato al singolo site (sottorete)
- **Interface ID**
  - 64 bit con formato derivato da IEEE EUI-64

I livelli NLA e SLA possono essere ulteriormente divisi gerarchicamente

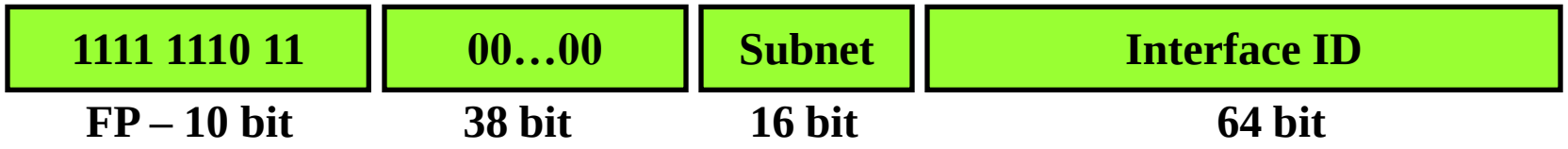
Link-Local Unicast Address

- FP = 1111 1110 10
- Sono indirizzi utilizzabili sono per l'indirizzamento su un singolo link (sottorete)
- IPv6 prevede che ogni interfaccia disponga di almeno un link-local unicast address
  - normalmente assegnato per autoconfigurazione a partire dall'indirizzo fisico di interfaccia (IEEE EUI-64)
- Questi indirizzi sono fondamentali nel processo di **Neighbor Discovery**



Site-Local Unicast Address

- FP = 1111 1110 11
- Anche questi destinati ad uso locale
- Definiscono una spazio di indirizzamento privato



Multicast Address

- FP = 1111 1111
- Diversi sotto-tipi
  - Multicast global
  - Multicast link-local
  - Multicast site-local
- All'interno esistono indirizzi per usi speciali

Multicast Address

- Flags:
  - T=1 indirizzo temporaneo
  - T=0 indirizzo permanente
- Scope:
  - 0: reserved
  - 1: node-local scope
  - 2: link-local scope
  - 5: site-local scope
  - 8: organization-local scope
  - E: global scope
  - Altri: unassigned

Multicast indirizzi speciali

- FF01::1 = all systems node-local scope
- FF02::1 = all systems link-local scope
- FF01::2 = all-routers node-local scope
- FF02::2 = all-routers link-local scope
- FF05::2 = all-routers site-local scope

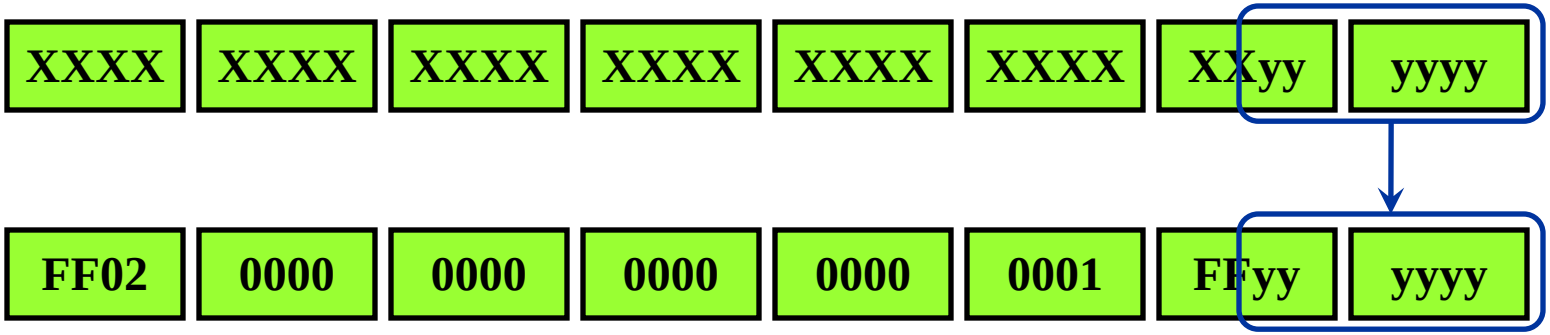
Indirizzi utilizzati in modo simile al broadcast locale suddividendo tra tutti i sistemi e tutti i router

Multicast indirizzi speciali

- Solicited-Node Multicast address
  - Ogni sistema IPv6 deve avere un “soliceted-node multicast address” per ogni indirizzo unicast o anycast configurato
  - Tale indirizzo viene costruito automaticamente concatenando il prefix

FF02::1:FF00:0/104

  - con gli ultimi 24 bit del corrispondente indirizzo unicast o anycast



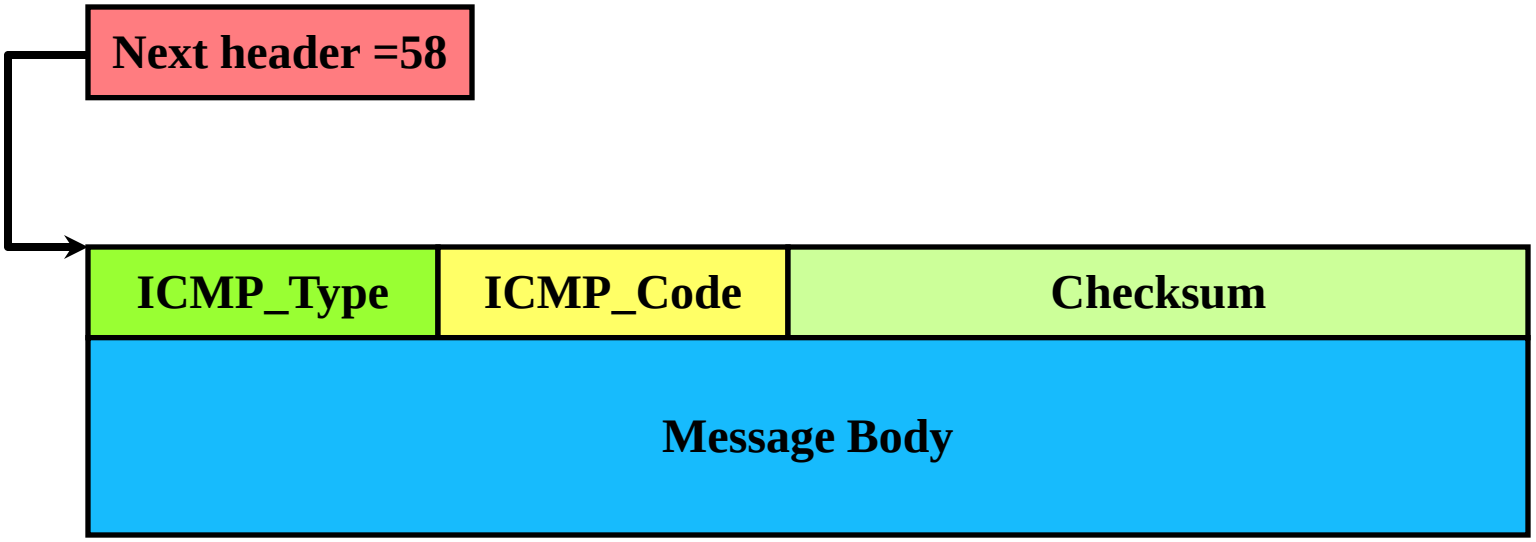
Molti indirizzi per diversi scopi

- IPv6 prevede l'uso di processi di autoconfigurazione
- Normalmente un nodo deve:
  - Autoconfigurarsi un link-local address a partire dall'indirizzo fisico di 64 bit
  - Autoconfigurarsi un solicited-node multicast address per ogni indirizzo
  - Può autoconfigurarsi altri indirizzi mediante diverse procedure (vedi ICMP e DHCP)

ICMP version 6

- ICMP ha un importanza molto maggiore con IPv6
- Vengono svolte molte funzioni:
  - Error reporting e diagnostica di rete
  - Risoluzione degli indirizzi di livello link
  - Individuazione del router corretto
  - Controllo degli indirizzi IPv6 assegnati
  - Autoconfigurazione degli indirizzi IPv6
  - Calcolo del PATH-MTU per la frammentazione

ICMPv6: struttura dei messaggi



Alcuni tipi comuni (ICMP_Type)

- Type=1 – destination unreachable
- Type=2 – Packet too big
- Type=3 – Time excedeed
- Type=4 – Parameter problem,
- Type=128 – Echo request
- Type=129 – Echo reply

ICMPv6 Neighbor Discovery

- Sono previste diverse procedure di *ND*
  - Address Resolution
    - Funzione analoga a quella di ARP per IPv4
  - Router Discovery
    - Segnalare e scoprire presenza di router sul link
  - Redirection
    - Simile all'opzione redirect di IPv4
  - Neighbor Unreachability Detection
    - Scopre irragiungilità di host noti

ICMPv6 Neighbor Discovery

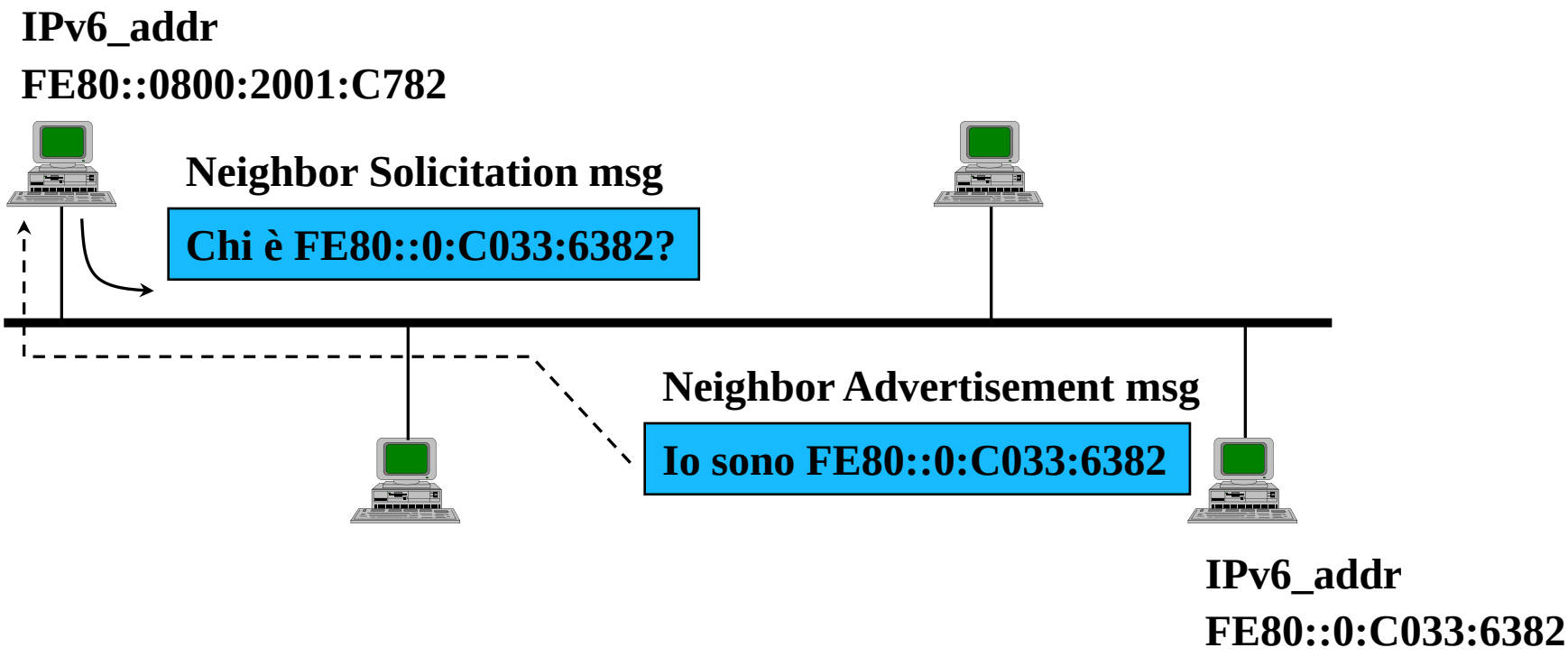
- Sono utilizzati molti indirizzi speciali (link-scope):
  - All-systems Multicast Address (FF02::1)
  - All-Routers Multicast Address (FF02::1)
  - Solicited-node Multicast Address
  - Unicast Link-Local Address
  - Unspecified Address (0::0)
- E sono introdotti 5 nuovi tipi di messaggio:
  - Router Solicitation message: type=133
  - Router Advertisement message: type=134
  - Neighbor Solicitation message: type=135
  - Neighbor Advertisement message: type=136
  - Redirect message: type=137

ICMPv6 Address Resolution

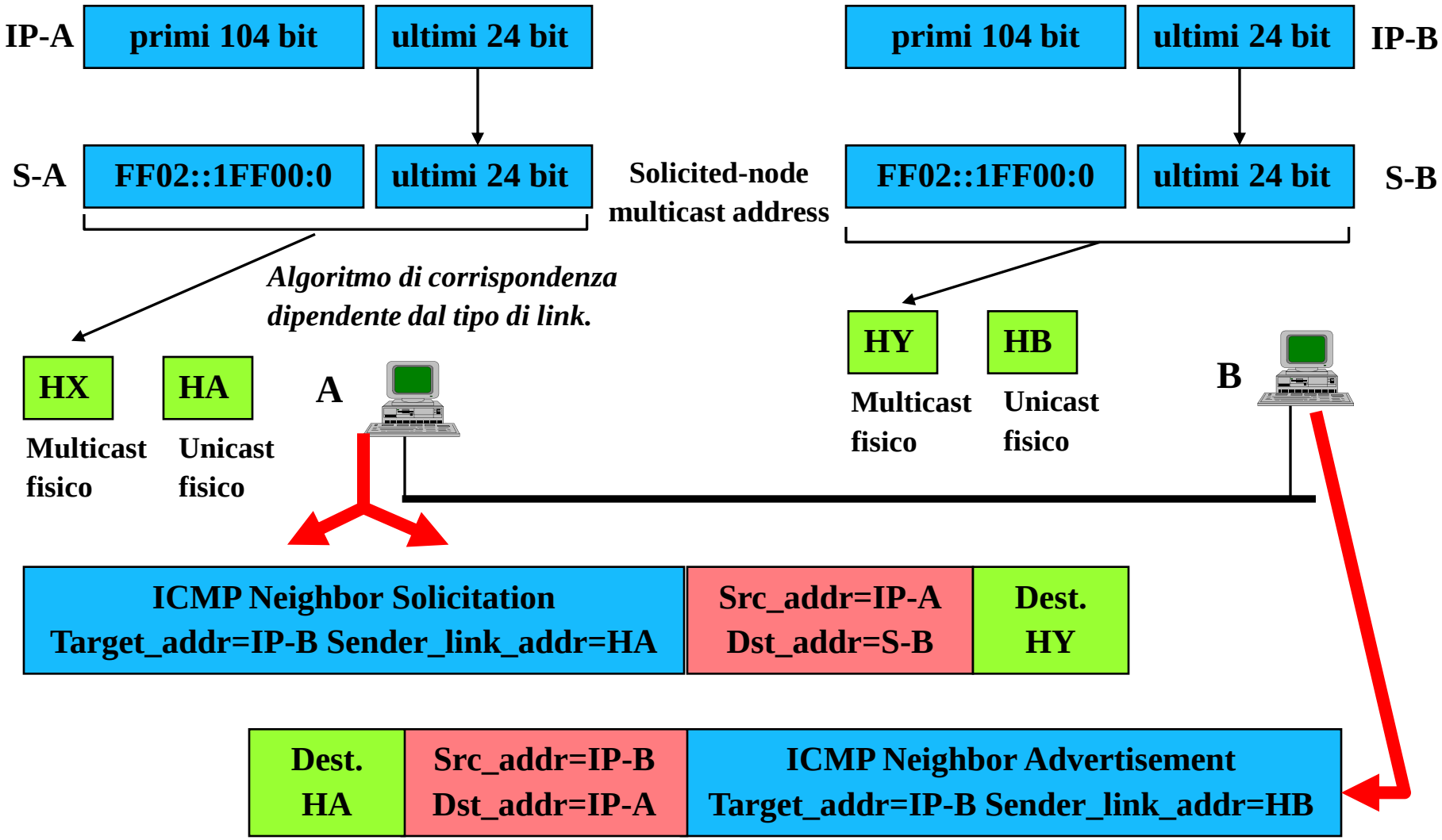
- Stessa funzione di ARP
- Servono indirizzi multicast/broadcast sul livello inferiore
  - Si suppone l'esistenza di un mappaggio tra indirizzi multicast IPv6 e multicast/broadcast a livello link
- Si fa uso dei messaggi di "Neighbor Solicitation" e "Neighbor Advertisement"

ICMPv6 Address Resolution

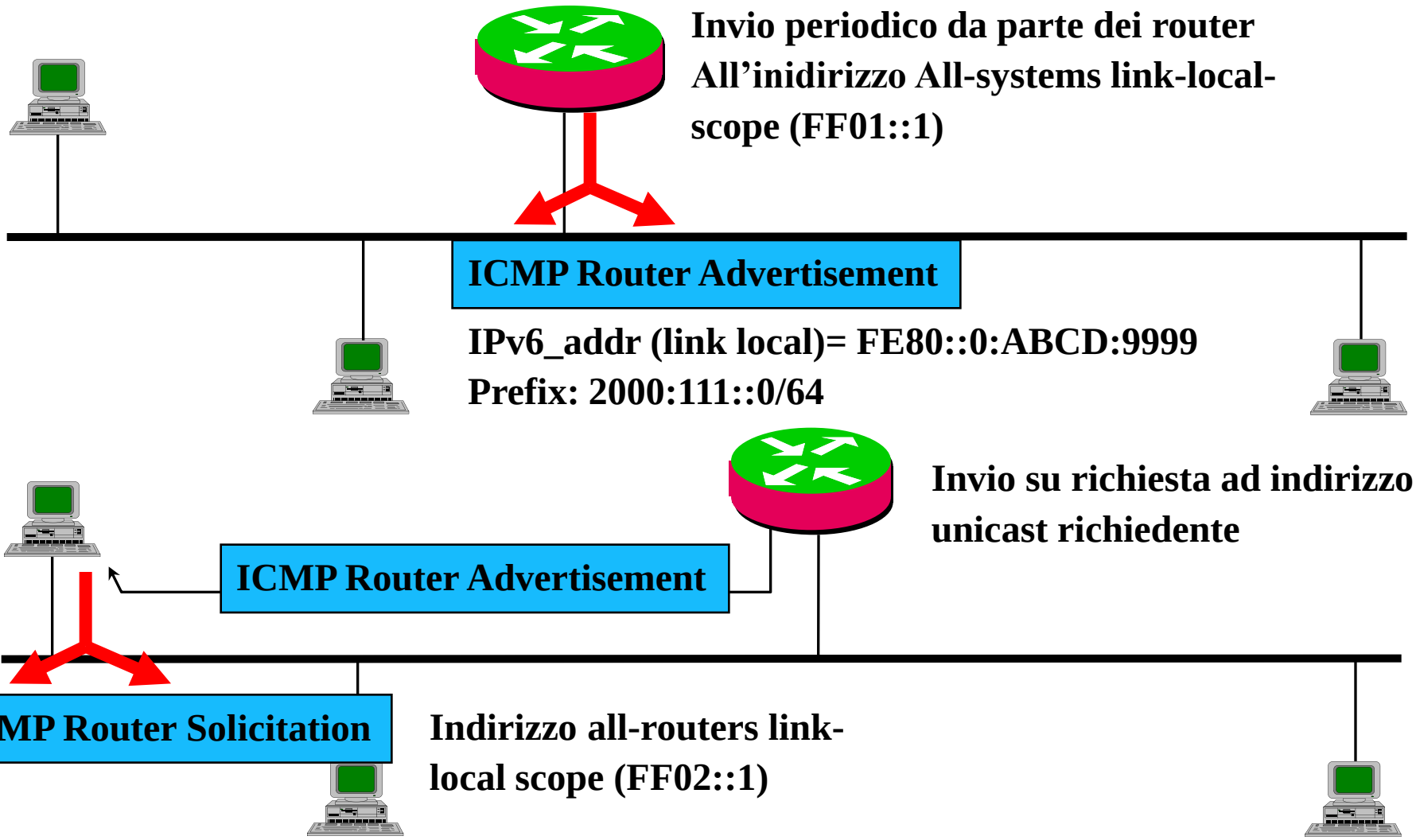
- Il messaggio di Neighbor Solicitation viene inviato all'indirizzo node-solicited multicast address che può essere ricavato anche dal richiedente
- Il messaggio di Neighbor Advertisement viene inviato all'indirizzo IPv6 di sorgente del pacchetto di richiesta



ICMPv6 Address Resolution



Router Discovery



Autoconfigurazione Indirizzi

- Oltre agli indirizzi Link-local si possono autoconfigurare indirizzi globali
  - Stateful configuration (tramite DHCPv6)
  - Stateless configuration (tramite ICMP)
    - Noto il prefisso annunciato dai router
    - Si può ricavare l'indirizzi a partire dall'indirizzo fisico a 64 bit

MTU Path Discovery

- **Obiettivo**: Il mittente deve sapere la MTU più piccola sul percorso
- Invia 1 pacchetto lungo quanto MTU primo link
- Se arriva messaggio ICMP errore “Packet too big” ridurre MTU
- Fino a che non arrivano più messaggi di errore

Migrazione IPv4 – IPv6

- Si basa sull'uso delle seguenti conponenti
- Dual stack
  - Sistemi con doppio stack IPv4 e IPv6
- Tunneling
  - Attraversamento di porzioni di rete IPv4 mediante tunneling
- Header translation
  - Traduzione degli header dei due formati

IPv6: Approfondimenti

- **Altro materiale didattico**:
  - Materiale del corso di Infrastrutture e Protocolli per Internet del Prof. Giuseppe Rossi (http://www.elet.polimi.it/upload/grossi)
- **Libri**:
  - C. Huitema, IPv6: The Next Generation Protocol, Prentice Hall, Englewood Cliffs, NJ, 1997.
- **Articoli** (disponibili sul sito web del corso):
  - W. Stallings, “IPv6: the new Internet protocol”, IEEE Communications Magazine , July 1996, pp. 96 –108.
  - D.C. Lee et alt., “The next generation of the Internet: aspects of the Internet protocol version 6”, IEEE Network , vol. 12, no 1, Jan.-Feb. 1998, pp. 28 –33.
- **Links**:
  - IP Next Generation (R. Hinden), http://playground.sun.com/pub/ipng/html/ipng-main.html