



*Corso di Laurea Triennale in Informatica
Università degli Studi della Basilicata*

Reti di Calcolatori

Docente: Ugo Erra

ugo.erra+reti@unibas.it

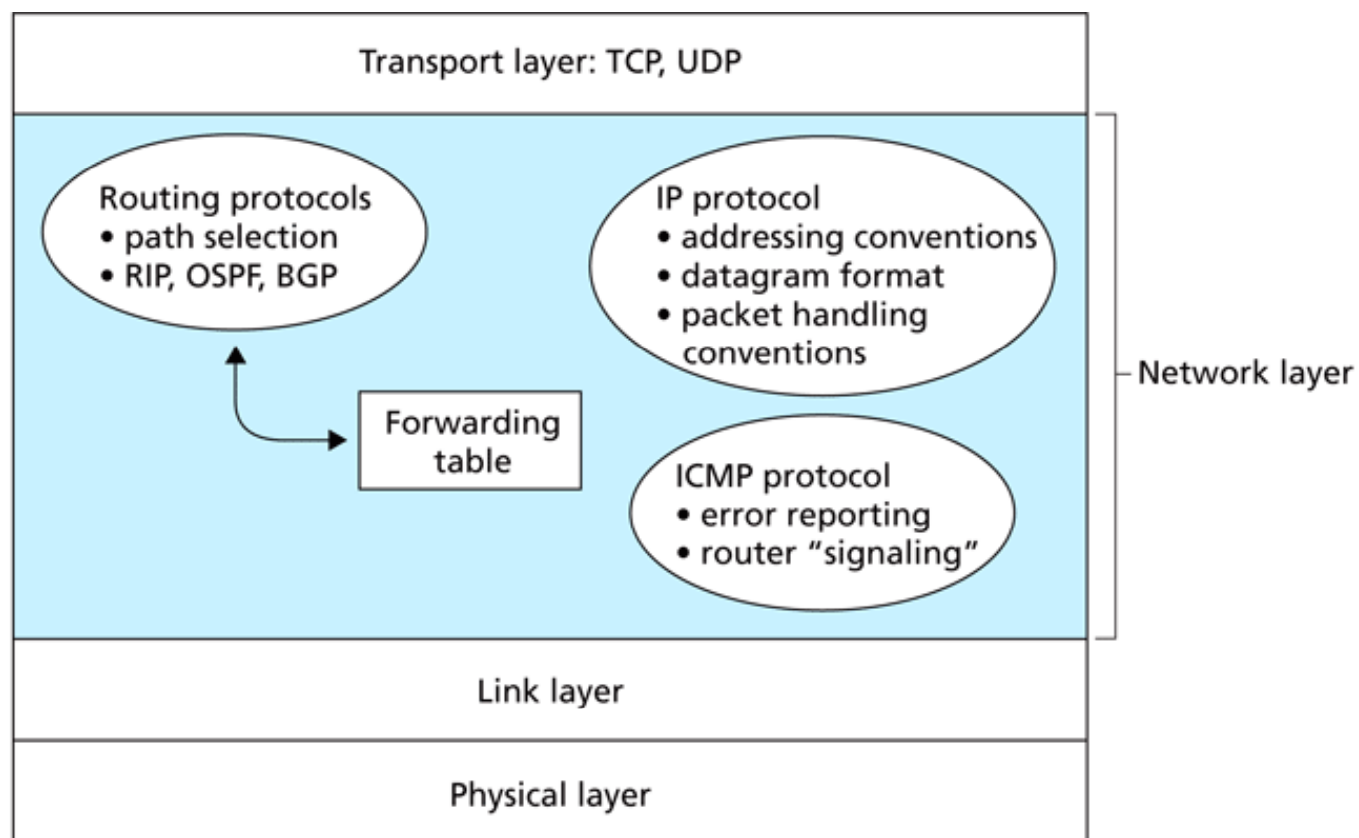
10° Lezione – Livello di rete– II° parte

Sommario



- **Protocollo Internet (IP)**
- Formato dei datagrammi
- Indirizzamento IPv4
- DHCP, NAT, ICMP
- IPv6

Dentro il protocollo IP

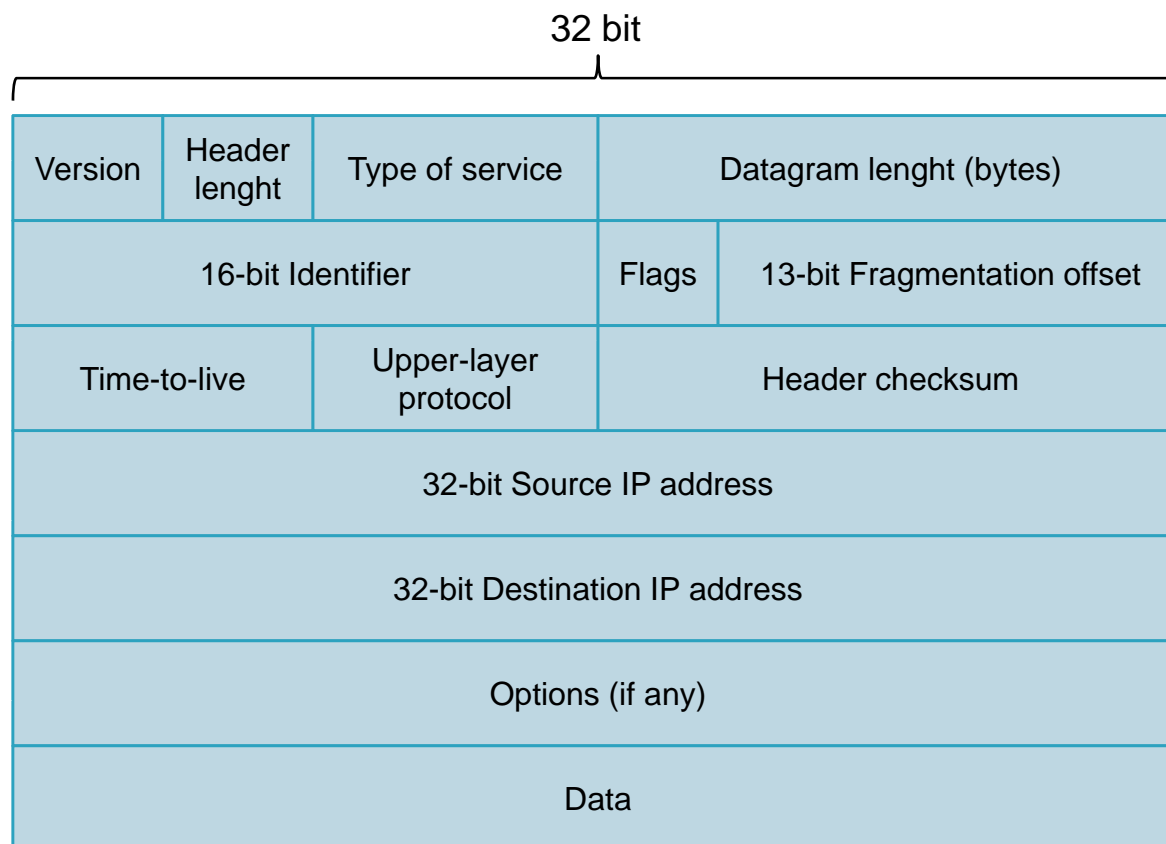


Sommario

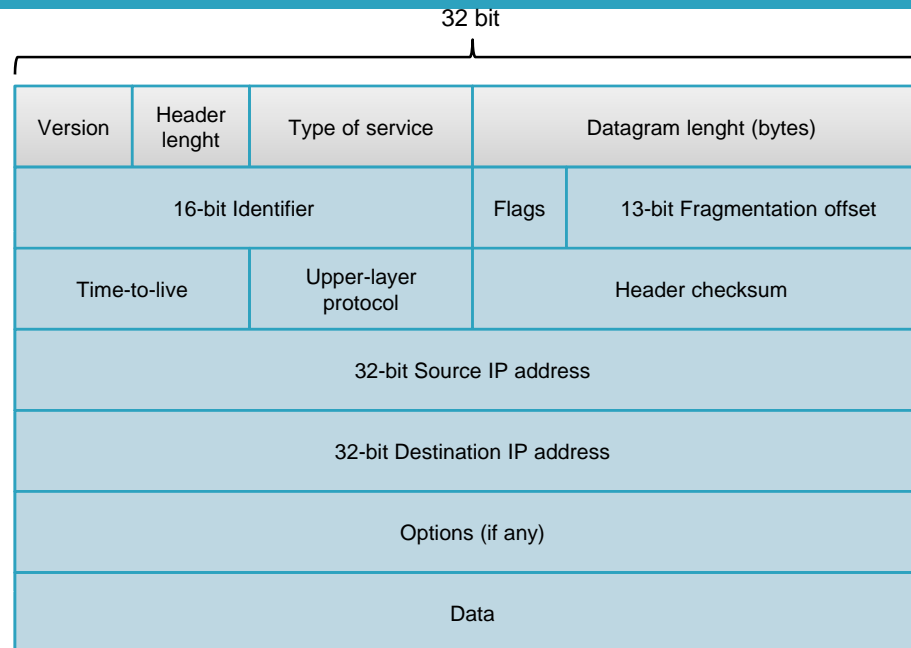


- Protocollo Internet (IP)
- **Formato dei datagrammi**
- Indirizzamento IPv4
- DHCP, NAT, ICMP
- IPv6

Formato dei datagrammi - 1

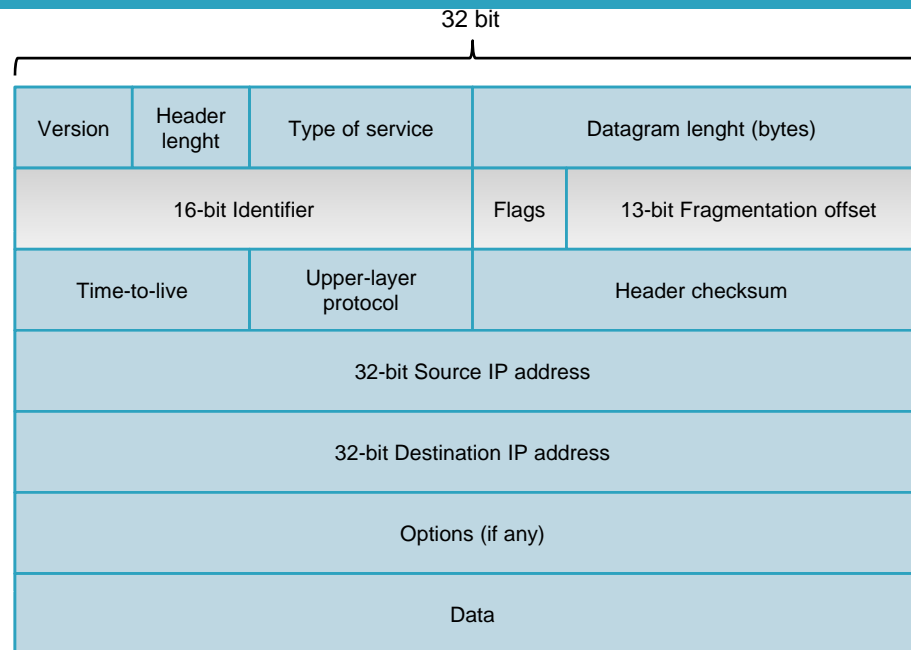


Formato dei datagrammi - 2



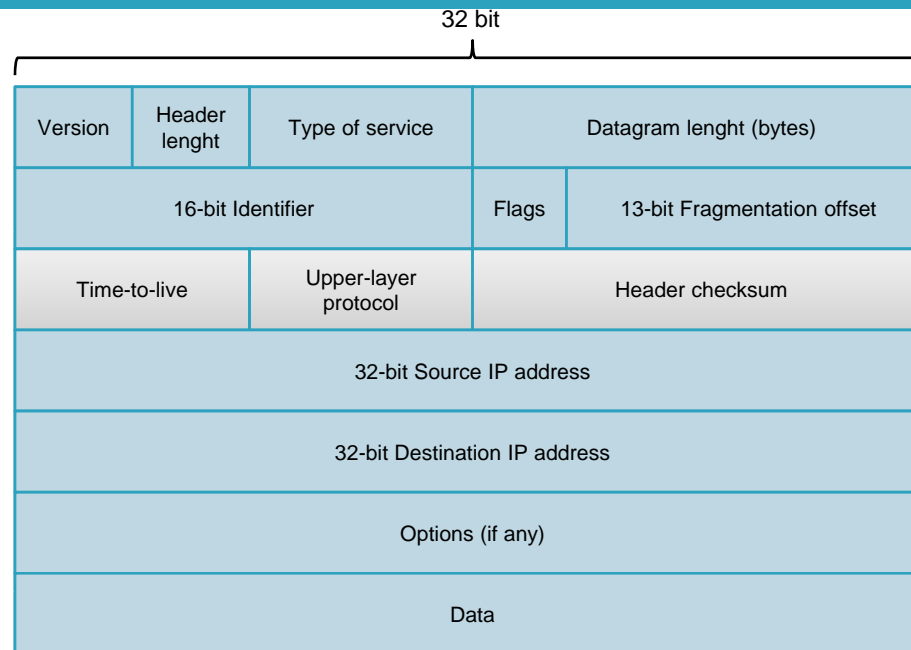
- Version (4 bit)
 - ▣ Numero di versione del protocollo IP (IPv4, IPv5, IPv6)
- Header length (4 bit)
 - ▣ Lunghezza dell'header del pacchetto in parole da 32 bit (minimo=20 byte, massimo=60 byte)
- Type of service (8 bit, non tutti necessariamente utilizzati)
 - ▣ Codifica la qualità del servizio richiesto dall'host alla communication subnet(in pratica è ignorato)
- Total length (16 bit)
 - ▣ Lunghezza totale del pacchetto, compreso l'header (massimo=65535 byte)

Formato dei datagrammi - 3



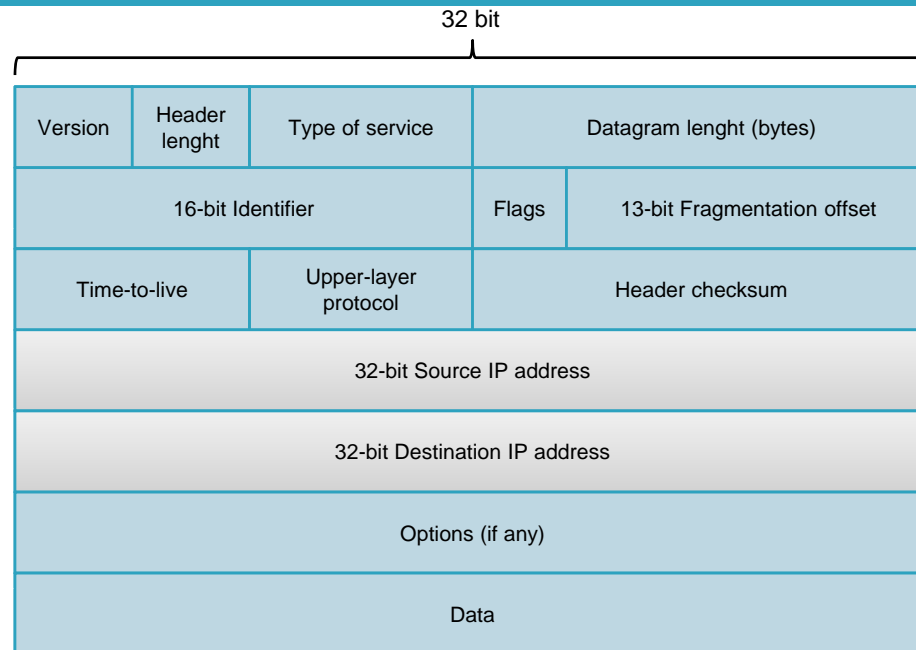
- Identification (16 bit)
 - ▣ Identificatore del datagram utilizzato in caso di frammentazione
- DF (1 bit, Don't Fragment)
 - ▣ Indica che il datagram non può essere frammentato (il ricevente non è in grado di riassemblare il pacchetto)
- MF (1 bit, More Fragments)
 - ▣ Indica che il frammento non è l'ultimo del datagram (se è l'ultimo deve riassemblarli)
- Fragment offset (13 bit)
 - ▣ Posizione relativa del frammento all'interno del datagram in multipli di 8 byte (non è il numero d'ordine del frammento!)

Formato dei datagrammi - 4



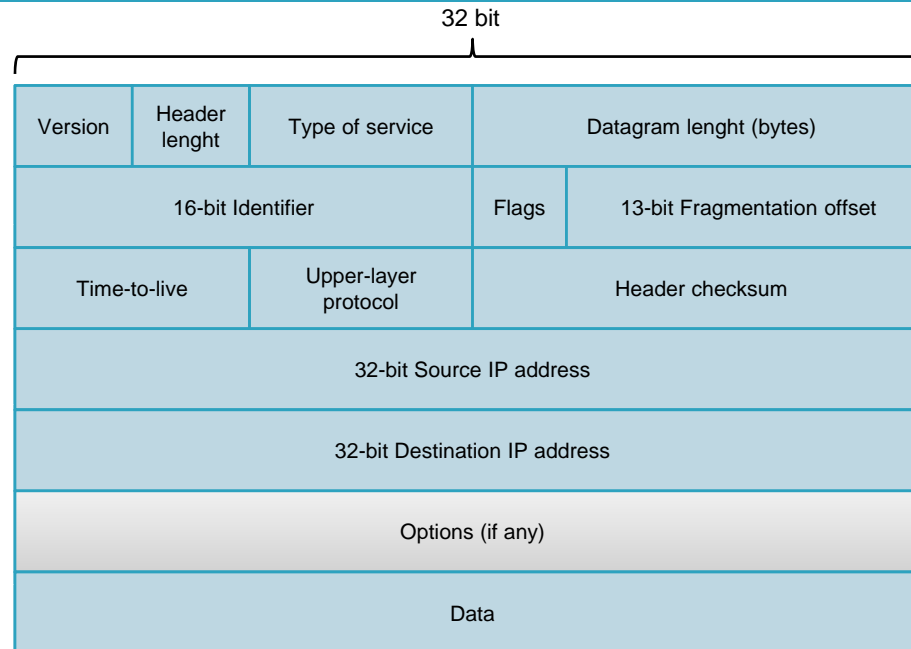
- Time-to-live o TTL (8 bit)
 - ▣ Contatore per limitare la vita del pacchetto; in teoria è decrementato una volta al secondo, in pratica ad ogni hop; quando raggiunge zero il pacchetto viene scartato ed un avvertimento inviato all'host sorgente
- Upper-layer protocol (8 bit)
 - ▣ Indica quale protocollo deve ricevere i dati nel pacchetto (generalmente un protocollo di livello Transport come TCP o UDP)
- Header checksum (16 bit)
 - ▣ Bit di controllo per il solo header
 - ▣ Deve essere ricalcolato da ogni router a causa della variazione del campo TTL

Formato dei datagrammi - 5



- Source address (32 bit)
 - ▣ Network number e host number dell'host sorgente
- Destination address (32 bit)
 - ▣ Network number e host number dell'host destinazione

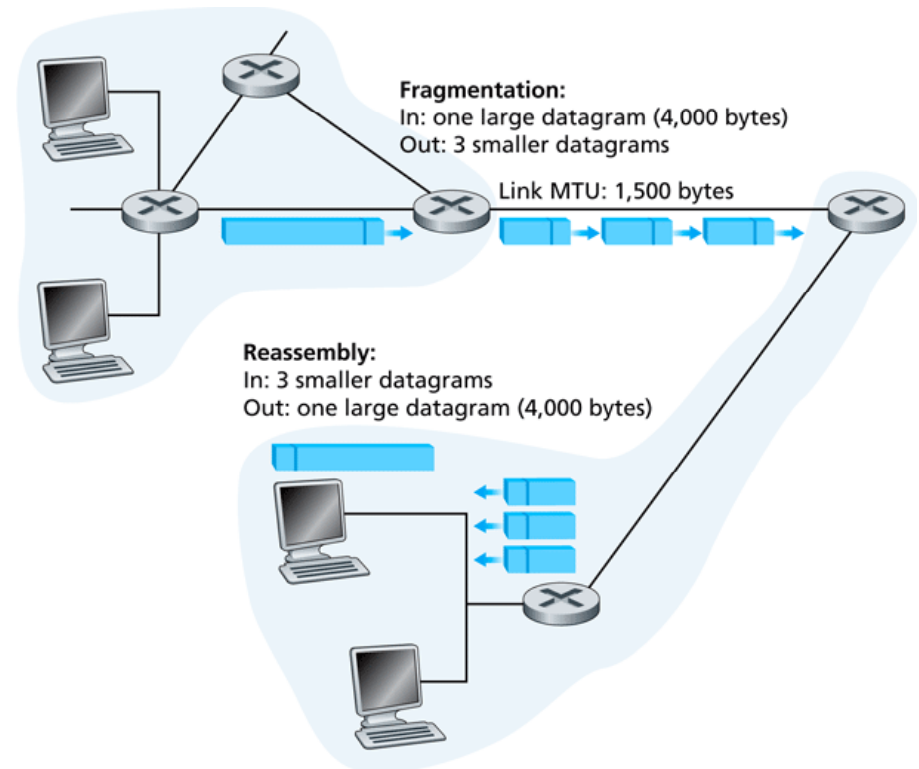
Formato dei datagrammi - 6



- Options (da 0 a 10 parole da 32 bit)
 - ▣ Security: indica la “segretezza” del datagram
 - ▣ Strict source routing: indica il percorso che il datagram deve seguire
 - ▣ Loose source routing: indica alcuni router da includere nel percorso
 - ▣ Record route: forza ogni router ad appendere il proprio indirizzo IP
 - ▣ Timestamp: come sopra, ma i router appendono anche un timestamp
- In totale sono state definite una ventina di opzioni ma non sono molto utilizzate, e non tutti i router sono in grado di gestirle

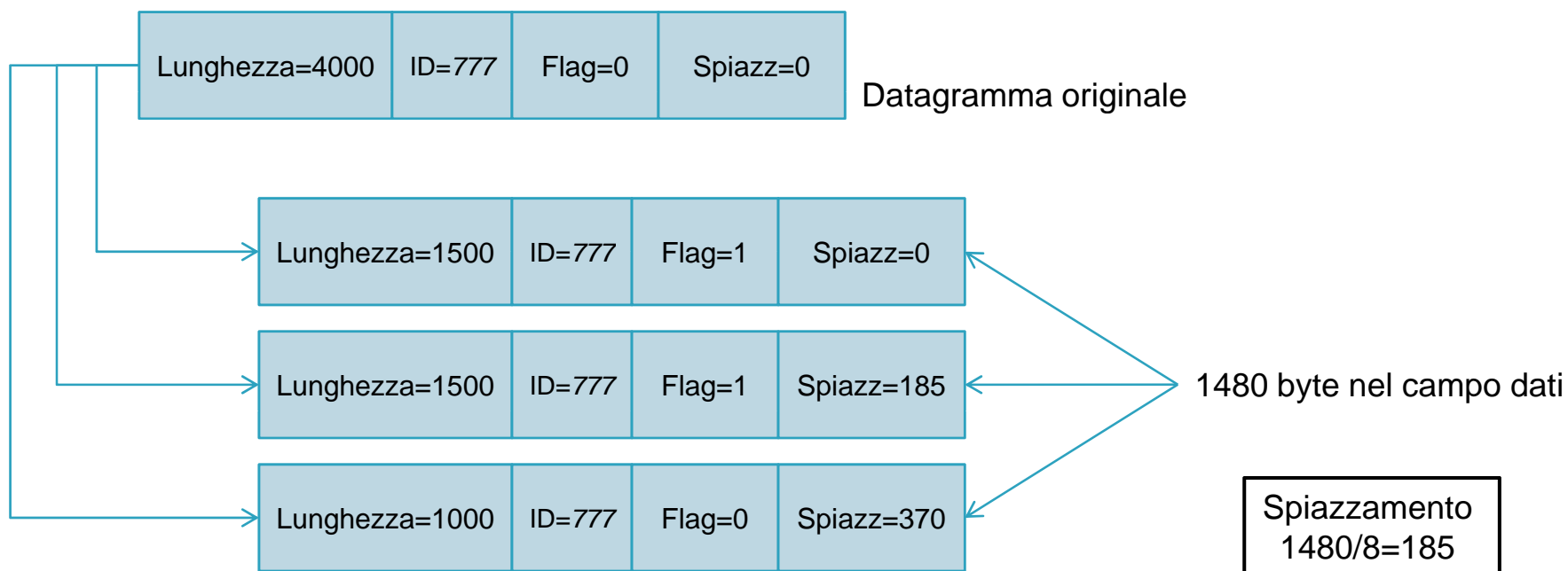
Frammentazione dei datagrammi

- L'**unità massima di trasmissione** (MTU) è la massima quantità di dati che un frame a livello di collegamento può trasportare
 - Differenti tipi di link implicano differenti MTU
- Datagrammi IP grandi vengono frammentati in datagrammi IP più piccoli
- Se un datagramma viene frammentato
 - I **frammenti** saranno riassemblati solo una volta raggiunta la destinazione
 - I bit dell'intestazione IP sono usati per identificare e ordinare i frammenti



Esempio frammentazione e riassettaggio

- Supponiamo di dover trasmettere:
 - ▣ Un datagramma di 4000 byte
 - ▣ L'intestazione è di 20 byte (per un datagramma privo di opzioni)
 - ▣ Utilizziamo un collegamento fisico con MTU=1500 byte



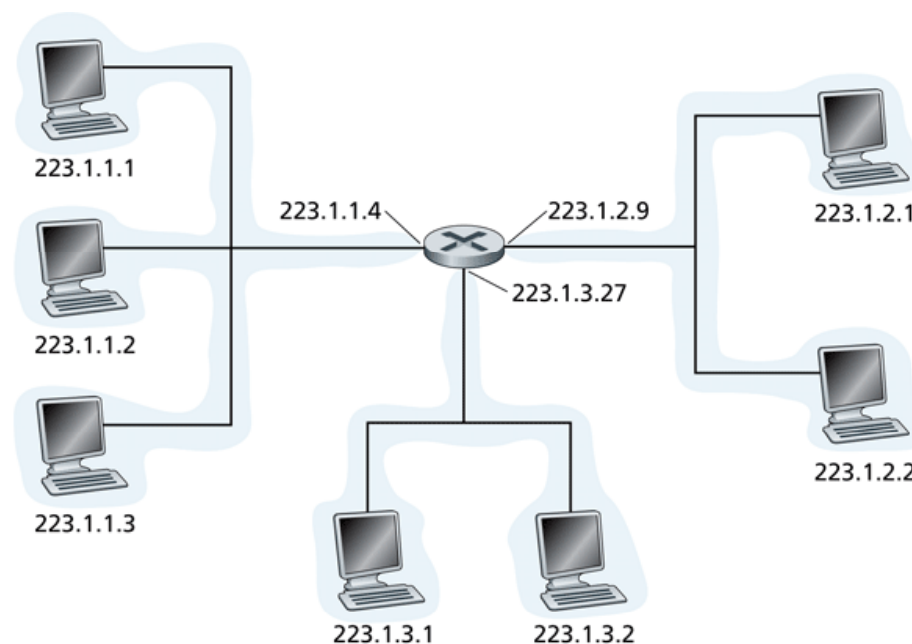
Sommario



- Protocollo Internet (IP)
- Formato dei datagrammi
- **Indirizzamento IPv4**
- DHCP, NAT, ICMP
- IPv6

Indirizzamento IPv4

- Gli indirizzi IP sono identificatori numerici a 32 bit associati in modo univoco ad una scheda di rete o NIC (Network Interface Card)
- L'**interfaccia** è il confine tra host e collegamento fisico
 - ▣ I router devono necessariamente essere connessi ad almeno due collegamenti
 - ▣ Un host, in genere, ha un'interfaccia
- A ciascuna interfaccia è associato un indirizzo IP
- Ogni interfaccia di host e router di Internet ha un indirizzo IP globalmente univoco



Notazione decimale puntata



- La **notazione decimale puntata** è una rappresentazione in formato più leggibile dei 32 bit che costituiscono un indirizzo IP
- Consiste dei quattro numeri decimali interi codificati nei quattro byte che compongono un indirizzo IP, separati da punti
- In genere in tutte le comunicazioni uomo macchina si usa questa notazione invece della stringa di 32 bit

Esempio

- Dato il seguente indirizzo IP come stringa binaria di 32 bit

11000001100111100001001100011000

lo possiamo immaginare diviso in 4 byte

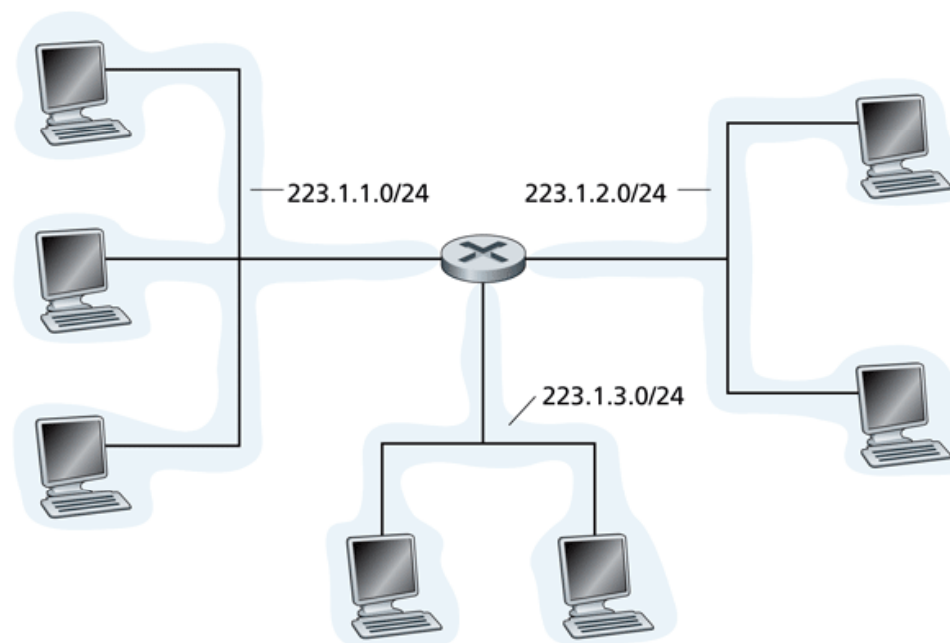
11000001 10011110 00010011 00011000

- Il suo valore in notazione decimale puntata diventa

193.158.19.24

Sottoreti

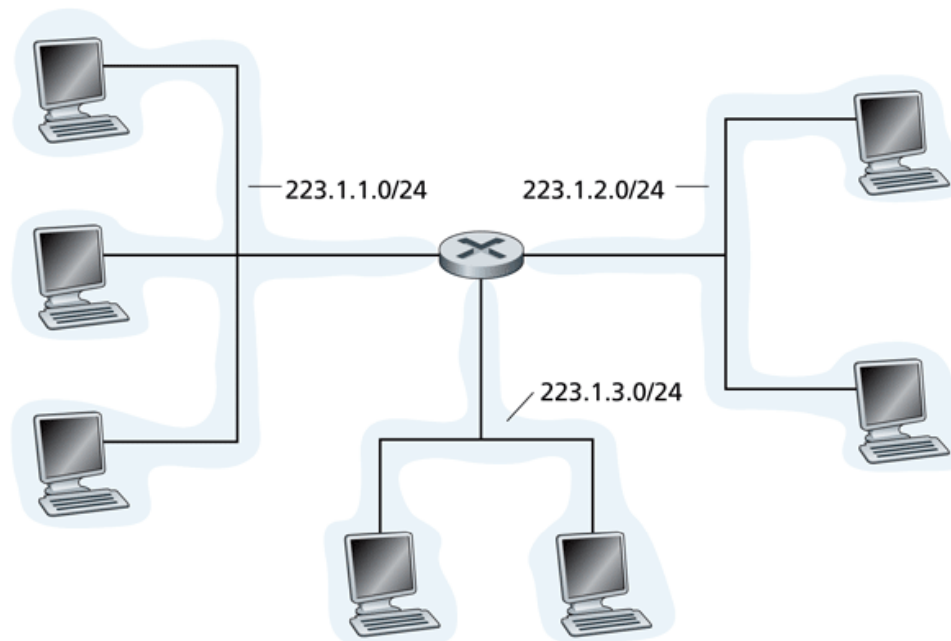
- Una **sottorete** per il protocollo IP è una rete che interconnette le interfacce degli host e l'interfaccia di un router
- ▣ Nella letteratura Internet le sottoreti sono anche chiamate **reti IP**



Rete composta da 3 sottoreti

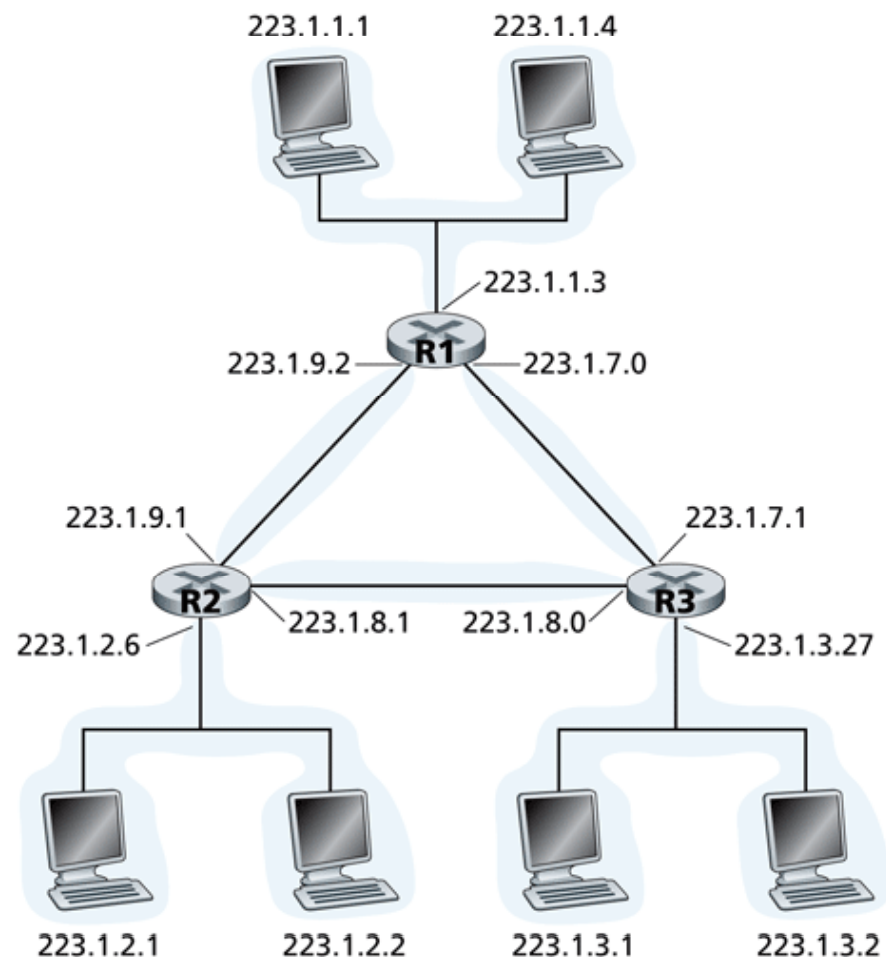
Definizione di sottorete

- Una **sottorete** è una rete isolata i cui punti terminali sono collegati all'interfaccia di un host o di un router



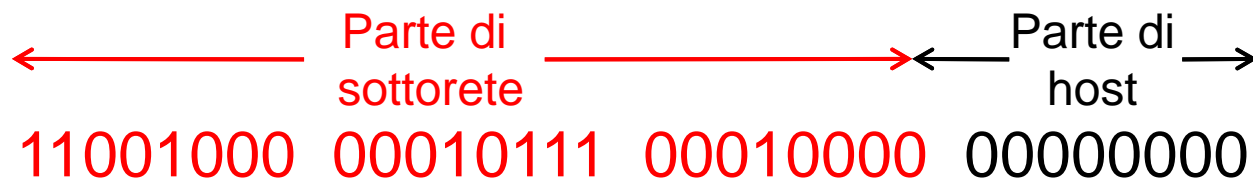
Maschera di sottorete /24

Esempio di sottoreti



Assegnazione indirizzi Internet CIDR

- **CIDR: Classless InterDomain Routing**
 - È la strategia di assegnazione degli indirizzi
 - Struttura dell'indirizzo: l'indirizzo IP viene diviso in due parti e mantiene la forma decimale puntata a.b.c.d/x, dove x indica il numero di bit nella prima parte dell'indirizzo

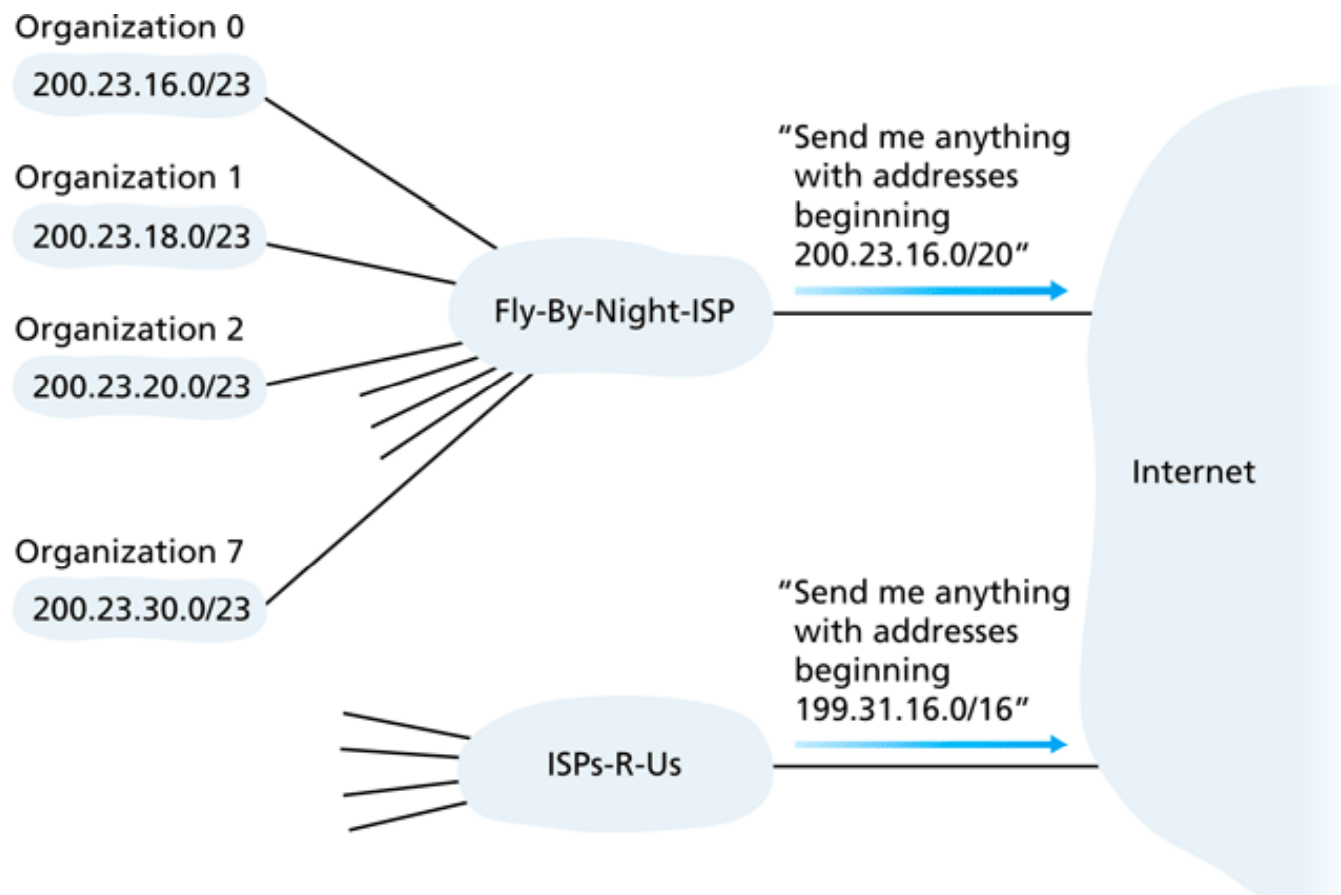


200.23.16.0/23

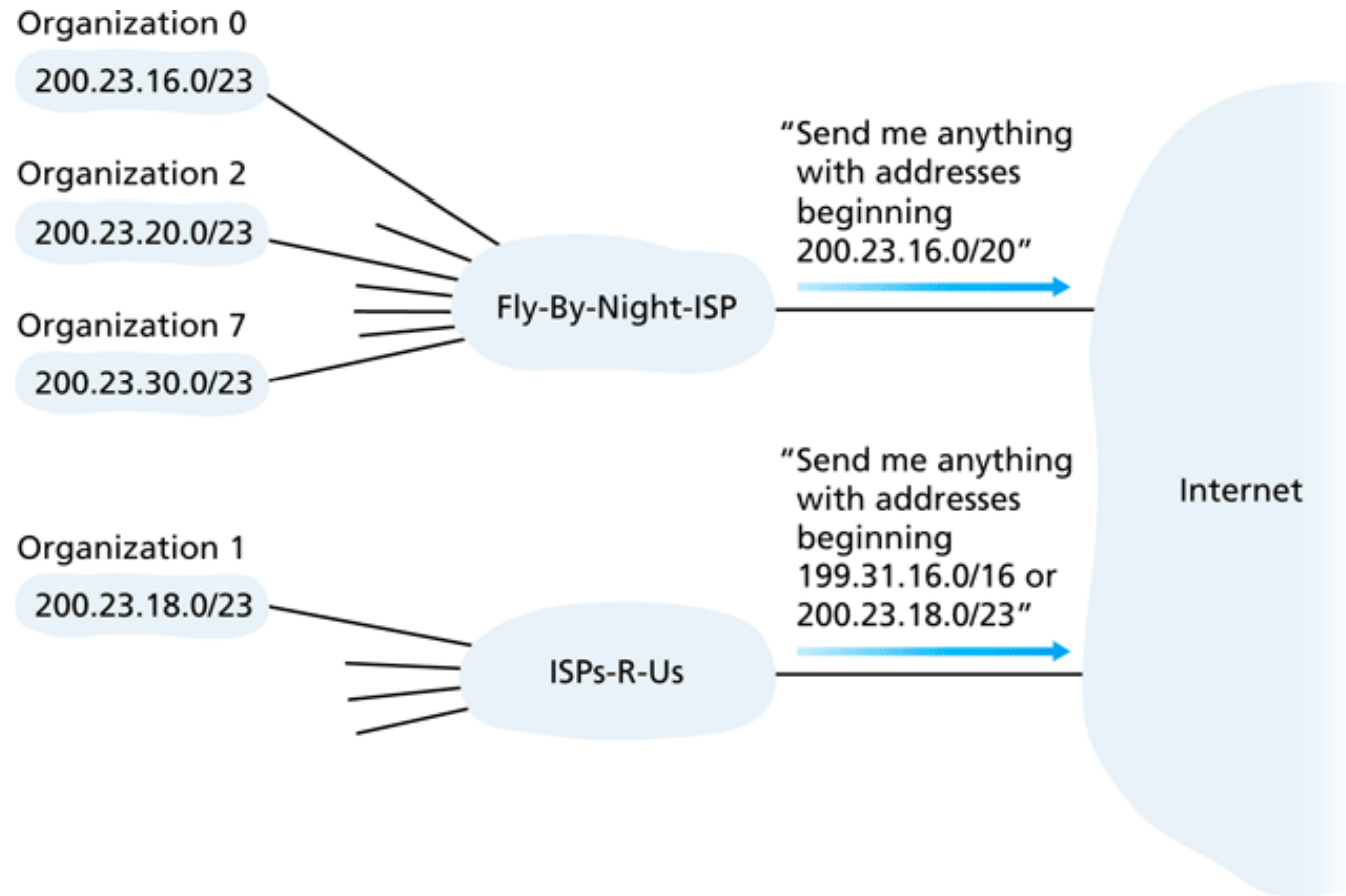
Possibili valori della maschera CIDR

Notazione CIDR	Notazione decimale	Numero di Host	Notazione CIDR	Notazione decimale	Numero di Host
/1	128.0.0.0	2147483648	/17	255.255.128.0	32768
/2	192.0.0.0	1073741824	/18	255.255.192.0	16384
/3	224.0.0.0	536870912	/19	255.255.224.0	8192
/4	240.0.0.0	268435456	/20	255.255.240.0	4096
/5	248.0.0.0	134217728	/21	255.255.248.0	2048
/6	252.0.0.0	67108864	/22	255.255.252.0	1024
/7	254.0.0.0	33554432	/23	255.255.254.0	512
/8	255.0.0.0	16777216	/24	255.255.255.0	256
/9	255.128.0.0	8388608	/25	255.255.255.128	128
/10	255.192.0.0	4194304	/26	255.255.255.192	64
/11	255.224.0.0	2097152	/27	255.255.255.224	32
/12	255.240.0.0	1048576	/28	255.255.255.240	16
/13	255.248.0.0	524288	/29	255.255.255.248	8
/14	255.252.0.0	262144	/30	255.255.255.252	4
/15	255.254.0.0	131072	/31	255.255.255.254	2
/16	255.255.0.0	65536	/32	255.255.255.255	1

Indirizzamento gerarchico



Indirizzamento gerarchico con prefisso più lungo



Come ottenere un blocco di indirizzi

- Un amministratore di rete per ottenere un blocco di indirizzi IP da usare in una sottorete deve contattare il proprio ISP e ottenere la divisione in otto blocchi uguali di indirizzi contigui

Blocco dell'ISP	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/20
Organizzazione 0	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/23
Organizzazione 1	<u>11001000</u>	<u>00010111</u>	<u>00010010</u>	00000000	200.23.18.0/23
Organizzazione 2	<u>11001000</u>	<u>00010111</u>	<u>00010100</u>	00000000	200.23.20.0/23
...	
Organizzazione 7	<u>11001000</u>	<u>00010111</u>	<u>00011110</u>	00000000	200.23.30.0/23

Assegnare un indirizzo IP



- Per assegnare un indirizzo IP a un host ci sono diverse strategie
 - Configurazione manuale:
 - Wintel: control-panel->network->configuration->tcp/ip->properties
 - UNIX: /etc/rc.config
 - DHCP: Dynamic Host Configuration Protocol: permette a un host di ottenere un indirizzo IP in modo automatico
 - “plug-and-play”

ISP alla fonte



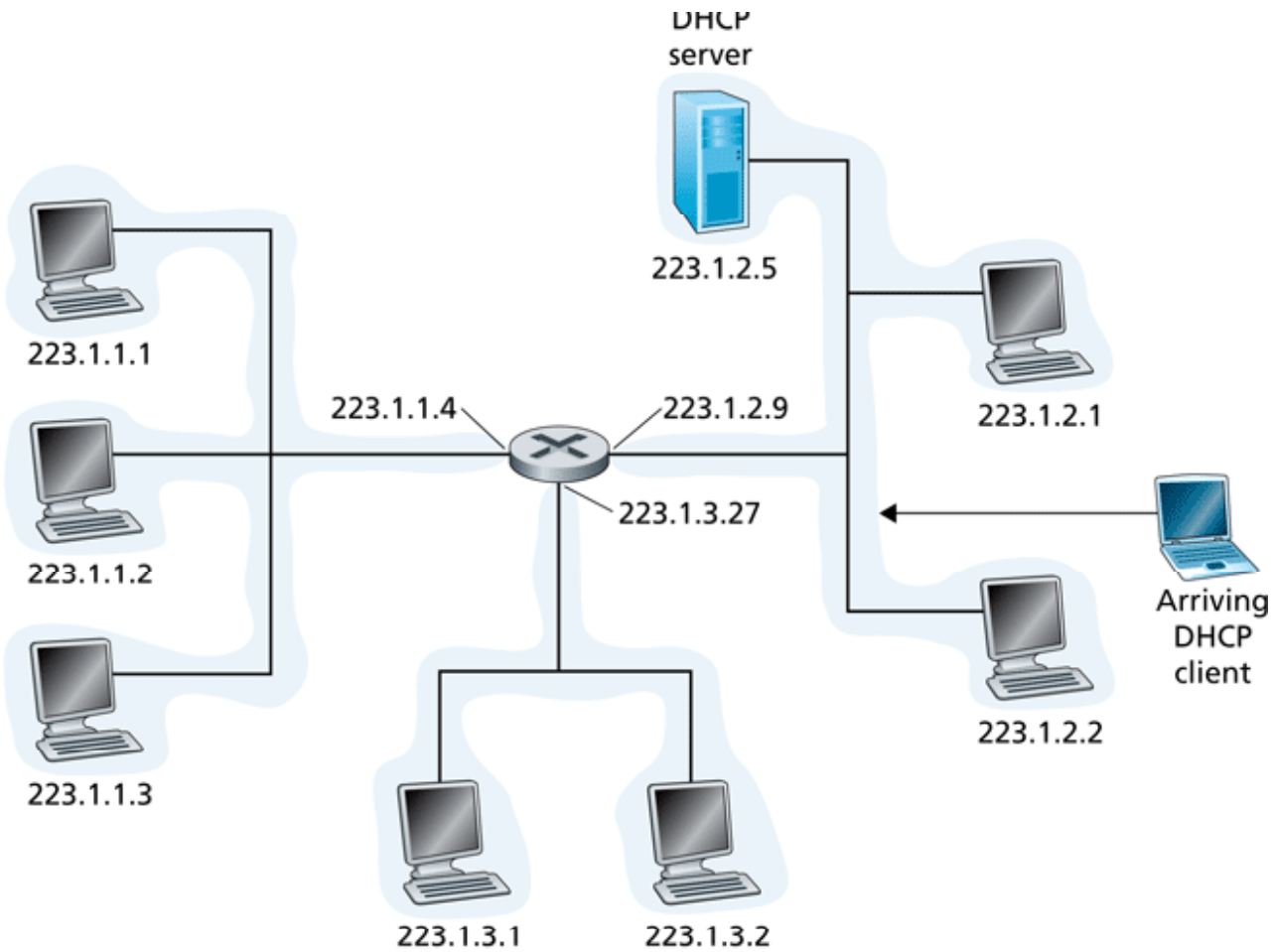
- Ma come fa un ISP, a sua volta, a ottenere un blocco di indirizzi?
 - ▣ ICANN: Internet Corporation for Assigned Names and Numbers
 - ▣ Ha la responsabilità di allocare i blocchi di indirizzi
 - ▣ Gestisce i server radice DNS
 - ▣ Assegna e risolve dispute sui nomi di dominio

Sommario

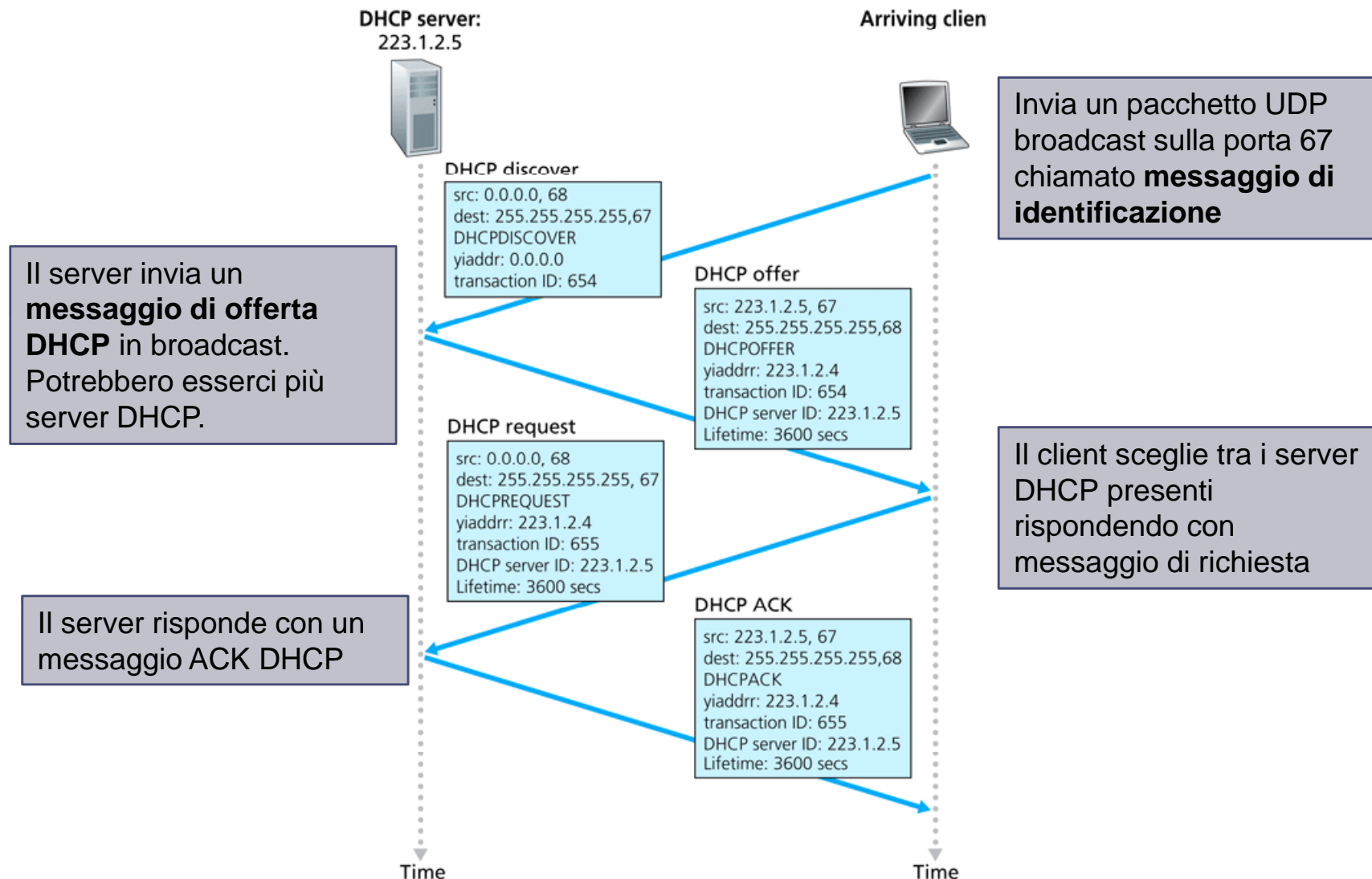


- Protocollo Internet (IP)
- Formato dei datagrammi
- Indirizzamento IPv4
- **DHCP, NAT, ICMP**
- IPv6

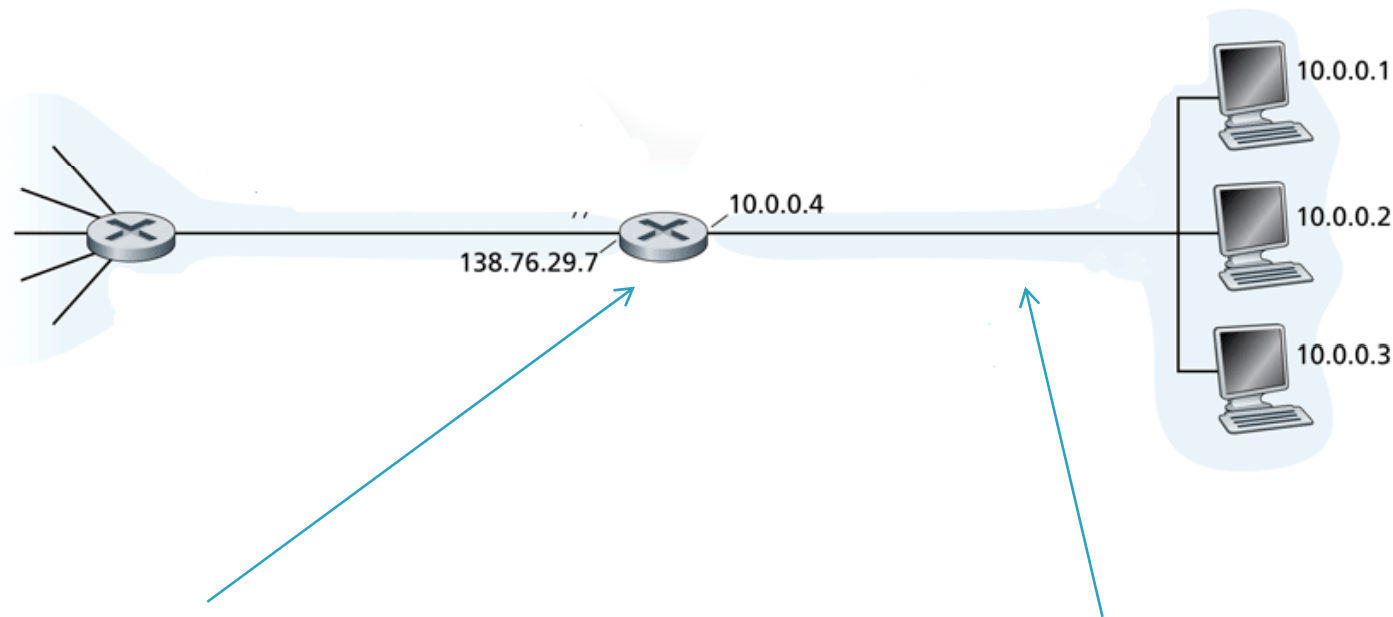
DHCP



Interazione client-server DHCP



Traduzione degli indirizzi di rete (NAT)



I router abilitati alla NAT non appaiono al mondo esterno come router ma come un *unico* dispositivo con un *unico* indirizzo IP.
Indirizzo IP origine: 138.76.29.7,
e tutto il traffico verso Internet deve riportare lo stesso indirizzo.

Spazio di indirizzi riservato alle reti private, molte delle quali usano un identico spazio, 10.0.0/24 per scambiare pacchetti tra i loro dispositivi

Traduzione degli indirizzi di rete (NAT)

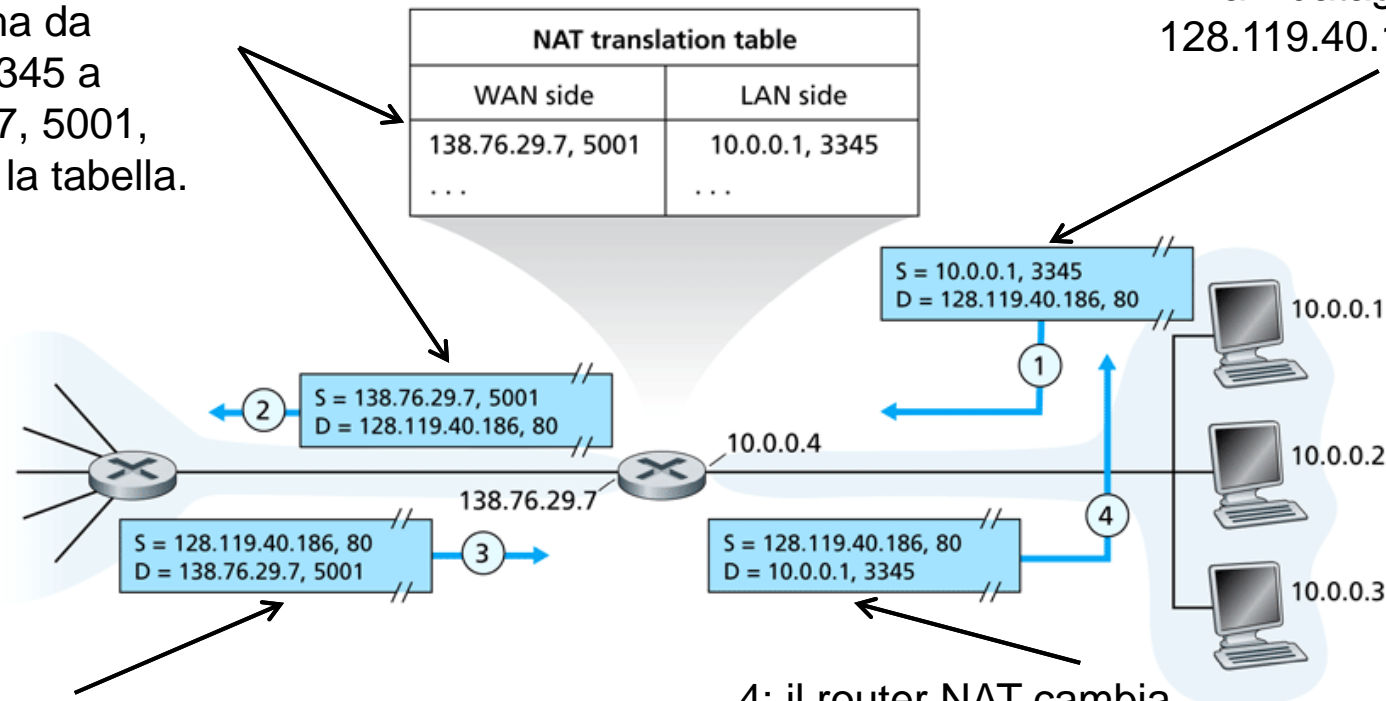


- Il router abilitato alla NAT nasconde i dettagli della rete domestica al mondo esterno
 - ▣ Non è necessario allocare un intervallo di indirizzi da un ISP: un unico indirizzo IP è sufficiente per tutte le macchine di una rete locale
 - ▣ È possibile cambiare gli indirizzi delle macchine di una rete privata senza doverlo comunicare all'Internet globale
 - ▣ È possibile cambiare ISP senza modificare gli indirizzi delle macchine della rete privata

Traduzione degli indirizzi di rete (NAT)

2: il router NAT cambia l'indirizzo d'origine del datagramma da 10.0.0.1, 3345 a 138.76.29.7, 5001, e aggiorna la tabella.

1: l'host 10.0.0.1 invia il datagramma a 128.119.40.186, 80



3: la risposta arriva all'indirizzo di destinazione: 138.76.29.7, 5001

4: il router NAT cambia l'indirizzo di destinazione del datagramma da 138.76.29.7, 5001 a 10.0.0.1, 3345

Traduzione degli indirizzi di rete (NAT)

- Il campo numero di porta è lungo 16 bit:
 - ▣ Il protocollo NAT può supportare più di 60.000 connessioni simultanee con un solo indirizzo IP sul lato WAN
- NAT è contestato perché:
 - ▣ I router dovrebbero elaborare i pacchetti solo fino al livello 3
 - ▣ Viola il cosiddetto argomento punto-punto
 - ▣ Interferenza con le applicazioni P2P, a meno che non sia specificamente configurato per quella specifica applicazione P2P
 - ▣ Per risolvere la scarsità di indirizzi IP si dovrebbe usare IPv6

UPnP

- Un host che possiede un indirizzo privato ed una porta privata non possono accettare connessioni dal mondo esterno
- UPnP (Universal Plug and Play) è un servizio di attraversamento del NAT
- Un host che si trovi dietro al NAT può richiedere la corrispondenza dell'indirizzo
(indirizzo IP privato, numero porta privata)
e
(indirizzo IP pubblico, numero porta pubblica)

Esempio UPnP

- Un client BitTorrent ha un indirizzo privato ed una porta
(10.0.0.1, 3345)
- L'indirizzo pubblico del NAT è
138.76.29.7
- L'applicazione BitTorrent può richiedere al NAT la creazione di una apertura da
(10.0.0.1, 3345) ↔ (138.76.29.7, 5001)
dove la porta 5001 è stata scelta dal server NAT
- Un server esterno può mandare un pacchetto TCP SYN verso (138.76.29.7, 5001) che lo inoltrerà al client BitTorrent

Internet Control Message Protocol(ICMP)

- Viene usato da host e router per scambiarsi informazioni a livello di rete
 - ▣ Report degli errori: host, rete, porta, protocollo irraggiungibili.
 - ▣ echo request/reply (usando il programma ping).
- Livello di rete “sopra” IP:
 - ▣ ICMP è considerato parte di IP
- Messaggi ICMP: hanno un campo tipo e un campo codice, e contengono l'intestazione e i primi 8 byte del datagramma IP

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Traceroute e ICMP

- Il programma invia una serie di datagrammi IP alla destinazione.
 - ▣ Il primo pari a TTL = 1
 - ▣ Il secondo pari a TTL=2, ecc.
 - ▣ Numero di porta improbabile
- Quando l'n-esimo datagramma arriva all'n-esimo router:
 - ▣ Il router scarta il datagramma
 - ▣ Invia all'origine un messaggio di allerta ICMP (tipo 11, codice 0)
 - ▣ Il messaggio include il nome del router e l'indirizzo IP
- Quando il messaggio ICMP arriva, l'origine può calcolare RTT
- Criteri di arresto dell'invio
 - ▣ Quando un segmento UDP arriva all'host di destinazione
 - ▣ L'host di destinazione restituisce un messaggio ICMP di porta non raggiungibile (tipo 3, codice 3)
 - ▣ Quando l'origine riceve questo messaggio ICMP, si blocca

Sommario



- Protocollo Internet (IP)
- Formato dei datagrammi
- Indirizzamento IPv4
- DHCP, NAT, ICMP
- **IPv6**

Quando termineranno gli indirizzi IP?

Blocchi indirizzi IP

Allocated
Unavailable
Available

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Sono disponibili più di un miliardo e ogni anno ne vengono assegnati in media 180-190 milioni (*Global IPv6 Summit 2008*)

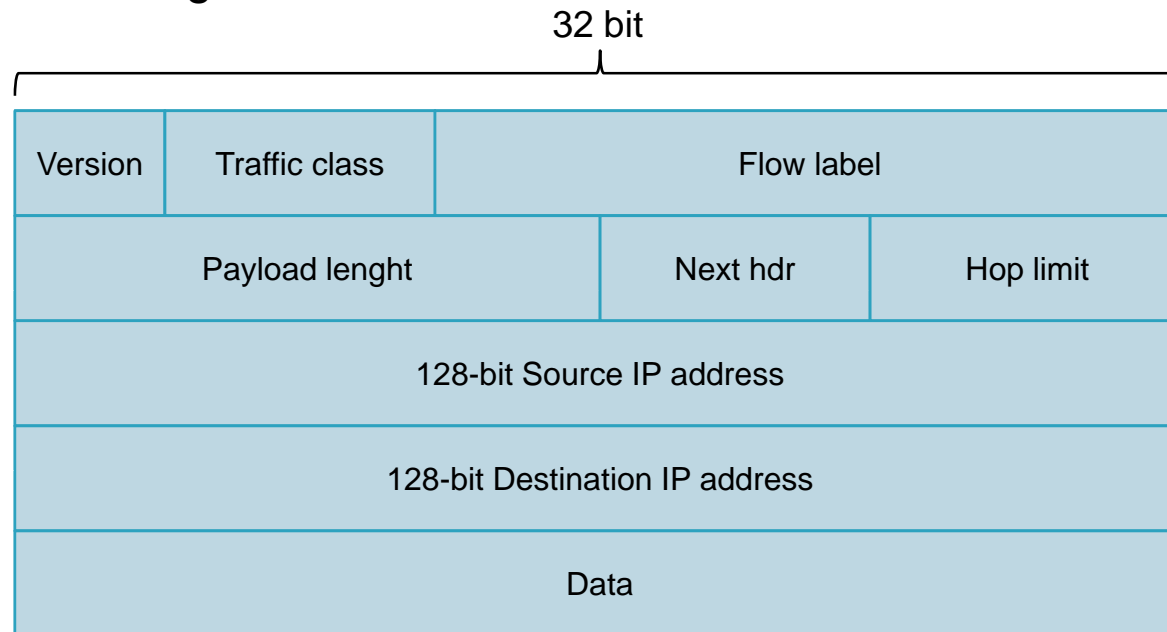
IPv6



- Esigenza principale: lo spazio di indirizzamento IP a 32 bit sta incominciando ad esaurirsi
- Altre motivazioni:
 - ▣ Il formato dell'intestazione aiuta a rendere più veloci i processi di elaborazione e inoltramento
 - ▣ Agevolare la QoS (Quality of Service)
- Alcune novità del formato dei datagrammi IPv6:
 - ▣ Intestazione a 40 byte e a lunghezza fissa
 - ▣ Non è consentita la frammentazione

Formato dei datagrammi IPv6

- **Priorità di flusso:** attribuisce priorità a determinati datagrammi di un flusso
- **Etichetta di flusso:** identifica i pacchetti che appartengono a flussi particolari (anche se il concetto di “flusso” è astratto)
- **Intestazione successiva:** identifica il protocollo cui verranno consegnati i contenuti del datagramma



Numero di host in IPv6



- Nei 16 byte dell'indirizzo IPv6 si possono codificare

$$2^{128} = 340282366920938463463374607431768211456$$

saranno sufficienti?

- Si presuppone che in un prossimo futuro i dispositivi collegati ad Internet saranno i più svariati

Notazione per indirizzi IPv6

- La rappresentazione degli indirizzi IPv6 è costituita da parole di 16 bit in esadecimale separate da “ : ”

47CD:0000:0000:0000:0022:1234:A456:0124

- Un indirizzo con un gran numero di zeri contigui può essere scritto in modo compatto omettendo i campi che valgono zero:

47CD::0022:1234:A456:0124

- Un indirizzo IPv6 avente i primi 96 bit nulli rappresenta un indirizzo IPv4

::A050:5001 equivale a 160.80.80.1

Altre novità di IPv6

- **Checksum:** i progettisti hanno deciso di rimuoverla dal livello di rete in quanto risultava ridondante
- **Opzioni:** non fa più parte dell'intestazione IP standard. Il campo non è del tutto scomparso ma è diventato una delle possibili "intestazioni successive" cui punta l'intestazione di IPv6
- **ICMPv6:** nuova versione di ICMP:
 - Assume le funzionalità dell'ICMP, e gestisce l'ingresso e l'uscita di host nei gruppi multicast

Frammentazione/riassemblaggio



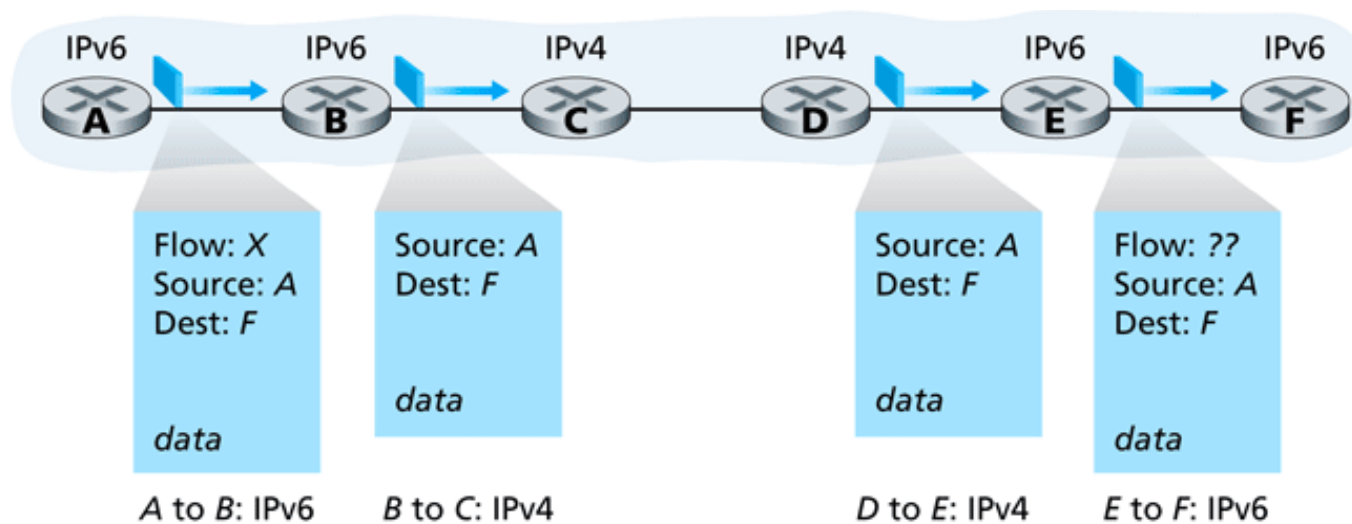
- Il protocollo IPv6 non consente più la frammentazione/riassemblaggio dei pacchetti
 - ▣ Si spreca troppo tempo presso i router
- Se un router riceve un pacchetto troppo grosso lo scarta e notifica la sorgente con un messaggio ICMPv6 “Pacchetto troppo grande”
- Il mittente deve quindi può rinviare i dati con la dimensione del datagramma inferiore

Passaggio da IPv4 a IPv6



- Non è possibile aggiornare simultaneamente tutti i router:
 - ▣ Impossibile dichiarare una “giornata campale” in cui tutte le macchine Internet verranno spente e aggiornate da IPv4 a IPv6
- Come riuscirà la rete a funzionare in presenza di router IPv4 e IPv6?
 - ▣ **Tunneling:** IPv6 viene trasportato come payload in datagrammi IPv4 quando attraversa router IPv4

Doppia pila



Tunneling

Logical view



Physical view

