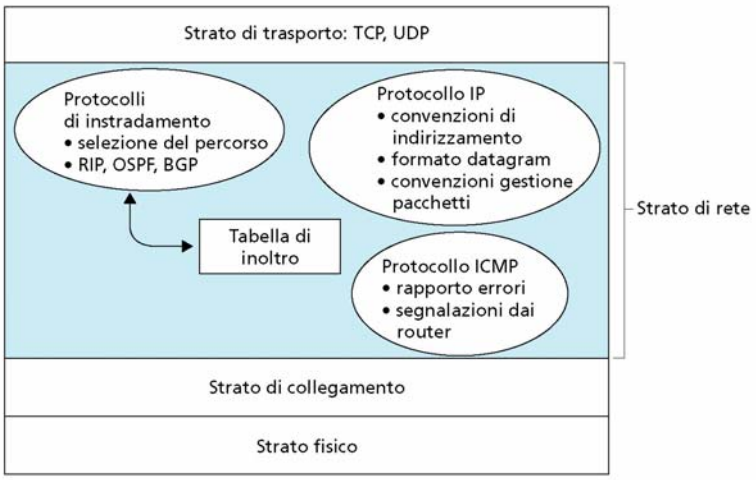
Reti di Calcolatori

Il livello Rete in Internet

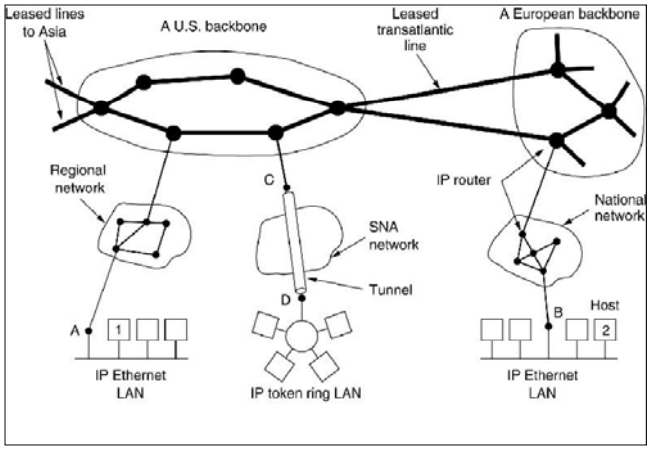
Funzioni del livello di rete in Internet



Il Protocollo IP

- IPv4
- Formato dei datagrammi IP
- Formato degli indirizzi IP
- Protocolli di controllo e di bootstrap
- IPv6

Internet



Internet è una collezione di reti basata su IP

Internet Protocol (IP)

- Lo standard **IPv4**, specificato dalla IETF (Internet Engineer Task Force) come RFC 791, è diventato il più diffuso protocollo del livello di rete.
- E' la base dell'attuale Internet.
- IP è un protocollo con organizzazione **a datagrammi**:
  - I pacchetti (o datagrammi) contengono l'indirizzo completo della destinazione.
  - Ogni datagramma viene spedito/gestito indipendentemente.

4-5

Datagramma IP

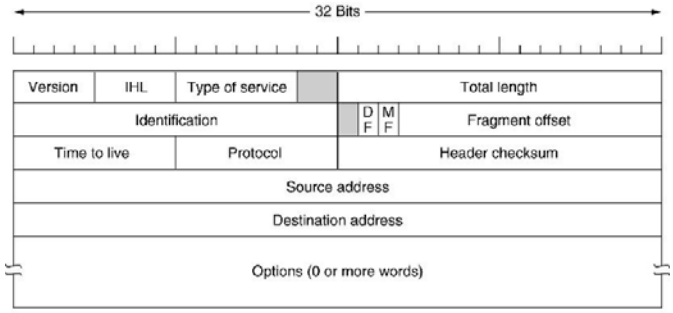
- Il datagramma IP è formato da blocchi di 32 bit.
- Ogni datagramma IP consiste di:
  - un **header** (o **preambolo**) di 20 byte fissi più un massimo di 40 byte opzionali e
  - una **parte dati** (o **payload**) che ovviamente contiene anche gli header dei protocolli di livello superiore
- I datagrammi IP possono contenere al massimo 64 Kbyte, ma in genere contengono tra 1000 e 1500 byte.

4-6

Frammentazione dei datagrammi IP

- Un datagramma IP attraversa un certo numero di router prima di giungere a destinazione.
- Un qualunque router può decidere di **frammentare** un datagramma se la rete da attraversare lo richiede (es. su una rete locale potrebbe esserci un limite alla lunghezza dei frame del livello di collegamento dati)
- Anche i frammenti sono datagrammi IP a tutti gli effetti.
- La deframmentazione avviene sull'host **destinatario**, e viene fatta prima di passare il datagramma al livello di trasporto.
- L'header del datagramma contiene alcuni campi utilizzati dai router per gestire la frammentazione e la deframmentazione: **identification**, **DF**, **MF**, **fragment offset**.

Formato dell'header IP



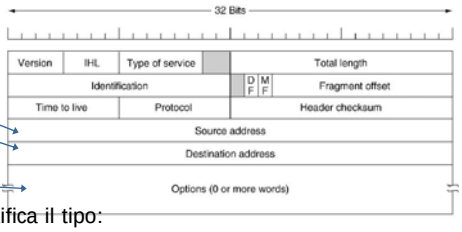
- **Version**: numero di versione del protocollo (4 bit)
- **IHL (IP Header Length)**: lunghezza dell'header in parole di 32 bit, da 5 a 15 (quindi da 20 a 60 byte).
- **Type of service**: affidabilità e velocità richiesta - ignorato dai router
- **Total length**: lunghezza del pacchetto (in byte), massimo 2^{16}-1 = 65.535 byte.

Formato dell'header IP

- **Identification**: identifica i frammenti di uno stesso pacchetto.
- **DF don't fragment** se=1, dice ai router di non frammentare questo pacchetto.
- **MF more fragments** se=1, indica che il pacchetto non è completo, ci sono frammenti successivi a questo, facenti parte dello stesso datagramma originario.
- **Fragment offset**: posizione del frammento nel pacchetto originario. La posizione del primo byte del frammento è ottenuta moltiplicando il valore di questo campo per 8. Poiché il campo ha 13 bit, possono esserci al massimo 2^{13}=8192 frammenti di uno stesso datagramma.
- **Time to live (TTL)**: contatore, inizialmente impostato a un numero <= 255; è decrementato ad ogni hop (o sec); se TTL = 0 il pacchetto viene scartato dal router.
- **Protocol**: codice del protocollo di livello trasporto cui consegnare i dati (es. codice di TCP o di UDP).
- **Header checksum**: verifica la correttezza dell'header (ma non della parte dati): si calcola ad ogni hop, perché almeno il *time to live* cambia valore dopo ogni hop.

4-9

Formato del datagramma IP

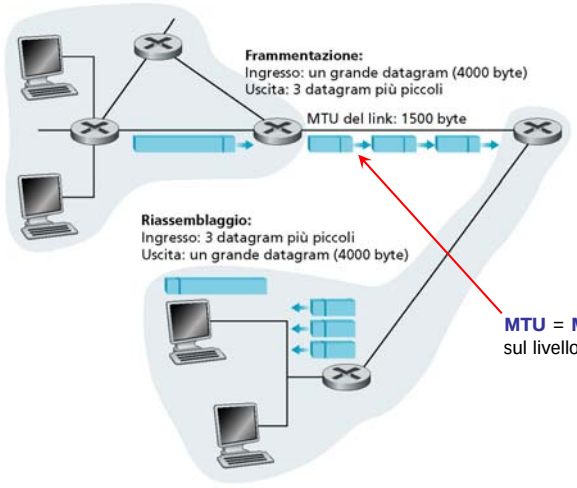


- **Source IP address**
- **Destination IP address**
- **Options**

  cinque tipi definiti, il primo byte identifica il tipo:
  - **security**: livello di segretezza del pacchetto (poiché i router spesso lo ignorano, è addirittura dannoso perché può servire alle spie per capire quali dati cercare);
  - **strict source routing:** lista di router che costituiscono il percorso obbligato e completo dei datagrammi;
  - **loose source routing:** lista di router da non mancare (ma ce ne possono essere altri in mezzo);
  - **record route:** ogni router che riceve il pacchetto deve inserire il proprio indirizzo: però i 40 bytes della parte opzionale non sono in genere sufficienti!
  - **timestamp:** oltre all'indirizzo il router deve registrare un timestamp.

4-10

Esempio di frammentazione



MTU = **Maximum Transfer Unit**
sul livello di collegamento dati

4-11

Frammentazione e riassemblaggio

Esempio

- Datagramma di 4000 byte
- MTU = 1500 byte

Lunghez.	ID	Flag	Offset
=4000	=x	=0	=0

Un datagramma IP grande viene frammentato in datagrammi IP più piccoli.

1480 byte nel campo dati

Offset= 1480/8

Lunghez.	ID	Flag	Offset
=1500	=x	=1	=0
=1500	=x	=1	=185
=1040	=x	=0	=370

Servizio best effort

IP fornisce un servizio senza connessione, **best effort**

I datagrammi possono seguire percorsi diversi pur facendo parte della stessa comunicazione e possono essere:

- ritardati
- duplicati
- distribuiti fuori ordine
- persi

Questi problemi sono eventualmente affrontati e risolti dal protocollo di trasporto (es. TCP); il protocollo di trasporto UDP invece **non** si preoccupa di risolverli e si affida semplicemente ad IP.

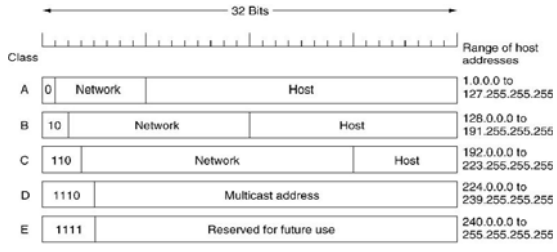
Indirizzi IP

- Un indirizzo IP **non** identifica un computer, ma una connessione (interfaccia) di un computer, o di un router, ad una sottorete.
- Un computer con connessioni multiple di rete ha assegnato un indirizzo IP per ogni connessione. Esempi:
  - un host con una interfaccia ad una rete LAN ha un unico indirizzo IP.
  - un router con N interfacce di rete (es. un router connesso a 2 LAN e ad una rete geografica) ha N indirizzi IP.

Indirizzi IP: formato

- L'indirizzo IP è lungo 32 bit, ed è diviso in due parti
  - network (o prefisso): identifica la sottorete
  - host (o suffisso): identifica l'host
- L'assegnamento di indirizzi univoci è effettuato da autorità nazionali (NIC, Network Information Center) coordinate a livello mondiale
- Un indirizzo di rete può essere assegnato ad un'azienda/istituzione: in seguito l'amministratore di rete dell'azienda assegna gli indirizzi ai vari host. Tali indirizzi hanno il prefisso comune ed il suffisso differenziato per ogni host.

Classi di Indirizzi IP



4 Classi di Formato
I 4 bit iniziali determinano la classe, che a sua volta determina il confine tra Network e Host.

Modo semplice per esprimere indirizzi IP: *rappresentare ogni byte in decimale (da 0 a 255) usando punti come separatori tra i byte*

Esempio: **196.145.63.1**

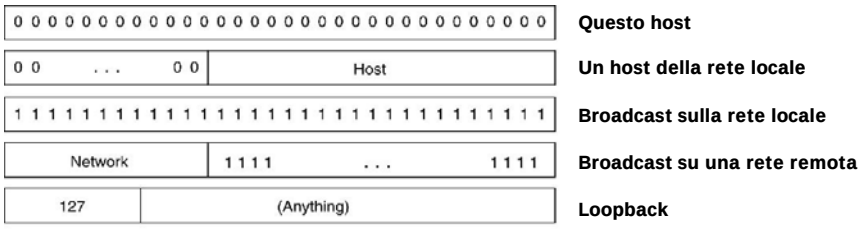
32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

Dimensioni delle Reti

- La massima dimensione di una rete dipende dalla classe
  - **Classe A: fino a più di 16 milioni di host (2^{24})**
  - **Classe B: fino a 65536 host (2^{16})**
  - **Classe C: al più 256 host (2^{8})**

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Indirizzi Speciali



Loopback: il datagramma non è trasmesso in rete ma è subito gestito come un pacchetto in arrivo; è usato per i test.

Indirizzi IP: formato CIDR

- L'utilizzo delle classi ha causato un enorme spreco di indirizzi IP.

  Es. se ad un'azienda con 1000 PC è assegnata una (sotto)rete di classe B, la maggior parte dei 65536 indirizzi verrà sprecata.

- La soluzione, in attesa di IPv6, è l'indirizzamento CIDR
  - CIDR: **Classless Inter Domain Routing**
  - È possibile assegnare blocchi di indirizzi di dimensione variabile, senza tener conto delle classi
  - A ogni rete è associato un indirizzo IP di base ed una **maschera** che indica quali bit identificano la sottorete e quali identificano l'host
  - I bit 1 della maschera corrispondono ai bit dell'indirizzo IP che identificano la sottorete. I bit 0 corrispondono all'indirizzo dell'host.

4-19

Indirizzi IP: formato CIDR

- Esempio di indirizzamento CIDR
  - ad una rete sono assegnati 1024 indirizzi, da 150.145.12.0 a 150.145.15.255
  - **indirizzo base** della rete in decimale:

    150.145.12.0 corrispondente, in binario, a

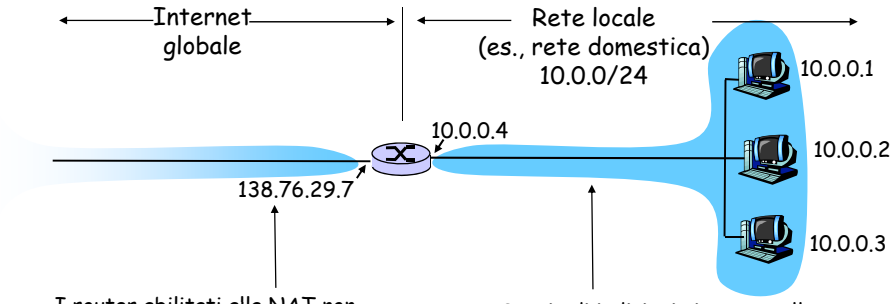
    10010110-10010001-00001100-00000000
  - **maschera** della sottorete in decimale:

    255.255.252.0 corrispondente, in binario, a
    11111111-11111111-11111100-00000000

    dalla maschera si deduce che la sottorete è identificata dai primi 22 bit, mentre l'indirizzo dell'host è identificato dagli ultimi 10 bit

4-20

Network Address Translation (NAT)

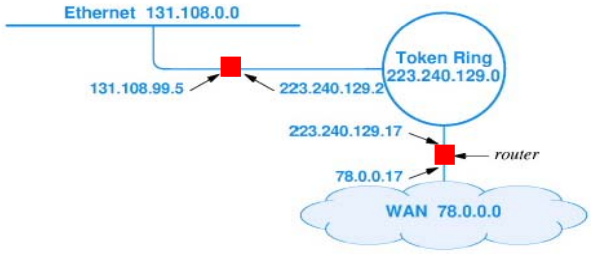


I router abilitati alla NAT non appaiono al mondo esterno come router ma come un *unico* dispositivo con un *unico* indirizzo IP.

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

Routers e Indirizzamento



- Il router possiede informazioni di instradamento per ogni rete conosciuta, **non** per ogni host
- In questo esempio ogni router è connesso a due reti ed ha due indirizzi IP, appartenenti alle rispettive reti
- Il router dispone di una tabella che associa, per ogni **rete** di destinazione, il prossimo router cui inviare i dati

4-22

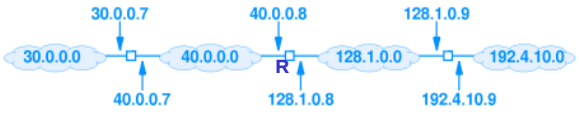
Tabella del router

- La tabella del router contiene tante righe quante sono le reti conosciute dal router.
- Per ogni rete la tabella riporta, su una stessa riga:
  - il campo **destination**: è l'indirizzo di base della rete conosciuta;
  - la **maschera di indirizzamento** della rete conosciuta;
  - il campo **next hop**: è l'indirizzo del router cui inoltrare il datagramma per farlo pervenire a questa rete destinazione. In pratica corrisponde ad una linea di uscita.
  - eventualmente il **numero di hop** per giungere a destinazione
- Il router effettua una operazione di **AND** bit a bit tra l'indirizzo dell'host destinazione (estratto dall'intestazione del pacchetto IP) ed ognuna delle maschere, riga dopo riga.
- Appena si verifica che il risultato dell'AND è uguale al campo *destination*, il datagramma è inoltrato al router individuato dal campo *next hop*. Se l'uguaglianza non si verifica mai, il datagramma è inviato ad un router di default.

Esempio: tabella di un router

Cosa succede se l'host destinazione è **128.1.10.12**?

e se è **192.4.10.255**?



(b)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

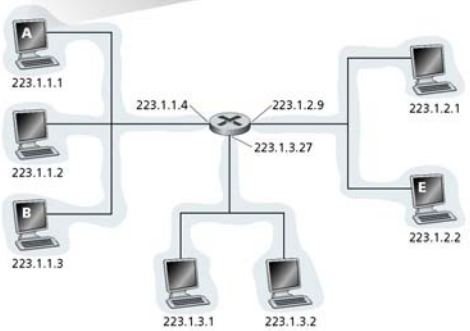
Tabella di instradamento di **R**

Esempio: tabella dell'host A

- Anche gli **host** hanno una tabella di routing.
- Devono conoscere il router di default della loro rete
- In questo esempio la maschera di indirizzamento è gestita con una notazione diversa. In **223.1.1.0/24**, il numero **24** indica il numero dei bit posti a 1 nella maschera. Corrisponde quindi alla maschera **255.255.255.0**

Tabella di rilancio in A

Rete di destinazione	Router successivo	Numero salti
223.1.1.0/24		1
223.1.2.0/24	223.1.1.4	2
223.1.3.0/24	223.1.1.4	2

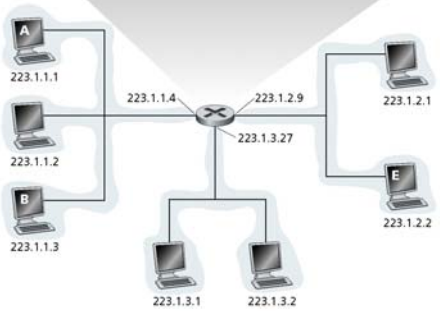


Esempio: tabella del router

- Cosa accade se un pacchetto viene inviato dall'host **A** all'host **E**?
- Basta considerare sia la tabella dell'host **A** (lucido precedente), sia quella del **router** (sotto)

Tabella di rilancio nel router

Rete di destinaz.	Router success.	N. hop	Interfaccia
223.1.1.0/24	—	1	223.1.1.4
223.1.2.0/24	—	1	223.1.2.9
223.1.3.0/24	—	1	223.1.3.27



In questo semplice caso non ci sono altri router: il pacchetto viene inviato su una linea di uscita (interfaccia) e quindi direttamente alla rete destinazione

Esercizio assegnato ad un appello

Un router IP ha la seguente tabella di routing:

Destination network	Next hop	Number of hops
150.145.66.0/24	Interfaccia 0	1
150.145.67.0/24	Interfaccia 1	1
150.145.64.0/23	Interfaccia 2	1
160.97.0.0/16	150.145.63.1	2
Default	150.145.63.1	> 2

Spiegare il significato della tabella, e tracciare uno schema della porzione della rete che circonda il router.
Inoltre specificare come vengono smistati (e perché) i pacchetti in arrivo sul router, se hanno i seguenti indirizzi IP di destinazione:

- 150.145.64.27
- 150.145.67.24
- 150.145.65.46
- 160.97.23.25
- 160.96.4.21

Protocolli di Controllo del livello di rete

- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- BOOTP (Bootstrap Protocol)
- DHCP (Dynamic Host Configuration Protocol)

ICMP (Internet Control Message Protocol)

- Controllo dell'operatività delle sottoreti – i router scambiano tra loro messaggi informativi o di errore
- IP utilizza ICMP per migliorare le performance. A loro volta i messaggi ICMP sono incapsulati in datagrammi IP
- Alcuni tipi di messaggi ICMP:
  - **source quench** (la coda è piena, rallenta la trasmissione!)
  - **destination unreachable** (avviso: il datagramma non arriverà!)
  - **time exceeded** (il TTL è arrivato a 0)
  - **redirect** (richiesta di cambiare cammino)
  - **echo request** (chiede se un host è attivo)
  - **timestamp request** (echo con richiesta di timestamp)
  - **echo reply**
  - **timestamp reply**
  - **parameter problem** (un parametro dell'header è errato)

Uso di ICMP

- Programma **ping** (sintassi: *ping <host>*, terminare con CTRL-C)
  - Utilizza il messaggio ICMP **echo request** per verificare la raggiungibilità di un host e calcolare i tempi di risposta
- Programma **traceroute**/**tracert** (sintassi: *traceroute <host>*)
  - Restituisce il percorso completo verso un host
  - Il programma invia datagrammi con TTL=1, 2 ecc.
  - Quando un router riceve un datagramma con TTL=0, invia al mittente un messaggio ICMP *time exceeded*
  - L'ultimo router invia un messaggio *destination unreachable*, dal momento che il datagramma è inviato ad una porta inesistente (*NB: la porta è specificata tramite il protocollo di trasporto UDP*)
  - Il programma intercetta i messaggi ICMP e ricostruisce il percorso, calcolando i tempi di risposta

Risoluzione degli indirizzi

- Ad ogni passo i router inoltrano i pacchetti ad altri router di cui conoscono **l'indirizzo IP**
- Per farlo devono conoscere **l'indirizzo fisico** (es. l'indirizzo di scheda Ethernet) del router successivo, che è l'unico tipo di indirizzo riconosciuto dai livelli più bassi.
- Devono cioè **risolvere** l'indirizzo IP nel corrispondente indirizzo fisico.

  *Provare il comando **ipconfig –all** su Windows per avere informazioni su indirizzo IP ed indirizzo di scheda Ethernet del vostro computer.*

4-31

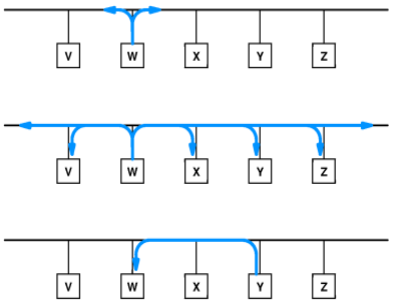
IP - Protocolli di Risoluzione degli indirizzi

- **ARP** (Address Resolution Protocol)
  deriva **dall'indirizzo IP** dell'host di destinazione **l'indirizzo di livello data link, o indirizzo fisico,** (es. Ethernet) necessario per inviare il frame su una rete locale
- **RARP** (Reverse Address Risolution Protocol)
  è usato da un host per richiedere il proprio indirizzo IP (a partire dall'indirizzo fisico) alla rete, in fase di avvio (bootstrap)
- **BOOTP**, **DHCP**
  sono protocolli utilizzati per l'avvio e la configurazione automatica degli host (es. dei portatili); tali protocolli richiedono ad un server informazioni quali l'indirizzo IP, il server DNS, il router di default ecc

4-32

Funzionamento di ARP

1. L'host **W** vuole conoscere l'indirizzo fisico dell'host **Y**
2. **W** trasmette in broadcast sulla rete locale una richiesta ARP contenente l'indirizzo IP di **Y**
3. La richiesta è incapsulata in un frame del livello Data Link (es. Ethernet)
4. Tutti gli host della rete locale ricevono la richiesta
5. L'host **Y** riconosce il proprio indirizzo IP e trasmette la risposta (cioè il proprio indirizzo fisico) **direttamente** a **W**



4-33

ARP: uso della cache

- Una volta che un indirizzo IP è stato risolto, ARP memorizza le associazioni <indirizzo IP, indirizzo fisico> in una tabella di cache.
- Prima di richiedere una risoluzione, ARP verifica se l'informazione è presente nella cache.
- Se la ricerca ha successo, la risoluzione è effettuata immediatamente, altrimenti si invia la richiesta in broadcast, come spiegato nel lucido precedente.

4-34

Dynamic Host Configuration Protocol (DHCP)

- Serve per assegnare in maniera dinamica gli indirizzi IP e gli altri parametri di configurazione (server DNS, router di default)
- Con DHCP è possibile evitare le configurazioni manuali
- All'avvio gli host chiedono il proprio indirizzo IP ai server DHCP, inviando le richieste in broadcast
- I server DHCP assegnano due tipi di indirizzi: permanenti (es. per altri server) e volatili
- Gli indirizzi IP volatili sono considerati validi per un periodo di predefinito (es. un giorno)

4-35

Problemi di IPv4

- Crescita di Internet e conseguente esaurimento degli indirizzi
- Header troppo complesso
- Non sono ben gestite le classi di servizio e le priorità
- Mancanza di tecniche per la sicurezza (anche se sono state aggiunte con IPsec)

4-36

Il futuro: una nuova versione di IP

IPv6: IP versione 6, successore di IP versione 4

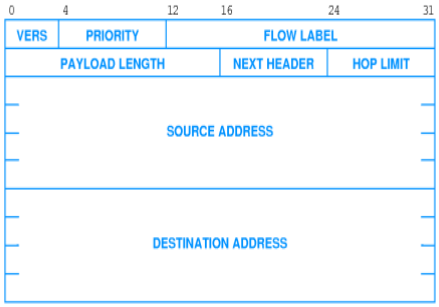
Principali differenze rispetto a IPv4:

- indirizzi di **16** byte -> 2^{128} indirizzi IP possibili!
- header semplificato: 8 campi contro 13 (risparmio nei tempi di computazione dei router), e lunghezza fissa (40 byte)
- funzioni di autenticazione e privacy, basate su crittografia
- supporto delle classi di servizio e della priorità
- supporto molto più flessibile delle opzioni (possibilità di header addizionali)

Ipv6 non è completamente compatibile con IPv4

Caratteristiche dell'header IPv6

L'header ha lunghezza fissa: 40 byte



Priority
Importanza relativa dei pacchetti

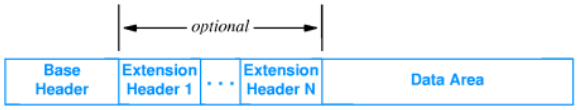
Flow label
id. di una pseudo-connessione (una specie di circuito virtuale)

Payload length
numero di byte dopo l'header

Next Header
tipo di header addizionale successivo (se esiste)

Hop Limit
equivale al TTL di IPv4

Header addizionali di IPv6



Esistono diversi tipi di header addizionali..

Tali header consentono l'uso di un gran numero di opzioni, ad esempio:

- Frammentazione
- Definizione totale o parziale dei cammini da seguire
- Autenticazione del mittente
- Crittografia dei dati
- Dimensione dei pacchetti: i normali pacchetti sono limitati a 64 KB, ma l'header addizionale di tipo *jumbogram* può avere dimensioni superiori