

Servizi Applicativi su Internet

IPv6

Livello 3 per nuove applicazioni

Ing. Pierluigi Gallo

Introduzione

- IP é un protocollo di livello 3
- IPv6 successore di IPv4
- Perché' inserirlo in un corso sul livello applicativo?
 - IPv6 consente l'introduzione di nuovi servizi e nuove applicazioni
 - Sicurezza
 - Mobilità'
 - multicast
- Insufficienza di indirizzi IPv4
- 2^{32} indirizzi insufficienti ed allocati in modo non efficiente



Carenze di IPv4

- Numero di reti insufficienti
- CIDR cerca di risolvere il problema dell'allocazione e del routing ma é insufficiente
- Gli indirizzi IPv4 sono ufficialmente terminati
- l'Internet Assigned Numbers Authority (IANA), ha assegnato gli ultimi cinque blocchi rimasti a disposizione nel febbraio 2011 !!!

Differenze IPv6/IPv4

■ IPv4

- Indirizzi a 32 bit
- 2^{32} indirizzi
- ARP
- Incapsulamento in pacchetti ethernet con ethertype 0800

- Risorse DNS del tipo A
- Uso del NAT

■ IPv6

- Indirizzi a 128 bit
- 2^{128} indirizzi
- NDP (Neighbor Discovery Protocol) invece di ARP
- Incapsulamento in frame ethernet con ethertype 86DD
- Address autoconfiguration
- Risorse DNS tipo AAAA
- Non é necessario il NAT

Caratteristiche

- Autoconfigurazione
- Subnetting con 64 bit nella parte host e 64 nella parte rete
- Si possono avere anche subnet con netmask $> /64$
- IETF consiglia di avere subnet a 64 bit anch eper reti punto punto
- Supporta meccanismi di sicurezza
- IPv4 ed IPv6 sono tra di loro incompatibili
- Varie soluzioni per il periodo di transizione
 - Dual stack
 - Tunnelling

Caratteristiche IPv6

- header di lunghezza fissa (40 byte)
- I router non effettuano frammentazione (gli host si)
- eliminazione del campo checksum, già presente negli altri strati dello stack e perciò ridondante.
- Gli header sono piu' brevi (eventualmente ci sono degli header opzionali)
 - Il carico sui router é minore rispetto ad IPv4
- La configurazione degli apparati é piu' semplice ed avviene automaticamente
 - In genere non c'è necessita' di DHCP server

IPv4

Bits	0	3	4	7	9	15	16	31
	Version	Header length		Type of service		Total length		
	Identification				Flags	Fragment offset		
	Time to live		Protocol		Header checksum			
	32-bit source address							
	32-bit destination address							
	Options						Padding	

Entrambi hanno notazione big endian

IPv6

Bits	0	3	4	7	8	15	16	23	24	31
	Version	Priority		Flow label						
	Payload length				Next header		Hop limit			
	128-bit source address									
	128-bit destination address									



Header IPv4

- Version The IP version number, 4.
- Length The length of the datagram header in 32-bit words.
- type of service Contains five subfields that specify the precedence, delay, throughput, reliability, and cost desired for a packet. (The Internet does not guarantee this request.) This field is not widely used on the Internet.
- total length The length of the datagram in bytes including the header, options, and the appended transport protocol segment or packet.
- Identification An integer that identifies the datagram.
- flags Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.
- fragment offset The relative position of this fragment measured from the beginning of the original datagram in units of 8 bytes.
- time to live How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.
- Protocol The high-level protocol type.
- header checksum A number that is computed to ensure the integrity of the header values.
- source address The 32-bit IPv4 address of the sending host.
- destination address The 32-bit IPv4 address of the receiving host.
- Options A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.
- Padding Null bytes which are added to make the header length an integral multiple of 32 bytes as required by the header length field.

Header IPv6

- Campi eliminati rispetto ad IPv4
 - header length (la lunghezza é costante)
 - identification
 - flags
 - fragment offset (É diventato un extension headers)
 - header checksum (trattati dai livelli superiori o dal security extension header)
- Version [4 bit] per IPv6, ha valore 6 (da qui il nome IPv6).
- Traffic Class [8 bit] - permette di gestire le code by priority assegnando ad ogni pacchetto una classe di priorità.
- Flow Label [20 bit] - Usata dal mittente per etichettare una sequenza di pacchetti come se fossero nello stesso flusso. Supporta la gestione del QoS.
- Length [16 bit] - È la dimensione del payload, ovvero il numero di byte di tutto ciò che viene dopo l'header. Eventuali estensioni dell'header (utili ad esempio per l'instradamento o per la frammentazione) sono considerate payload, e quindi conteggiate in tale lunghezza. Se il suo valore è 65.535 byte, significa che ho un pacchetto di dimensione massima, anche detto Jumbogram.
- Next Header [8 bit] - Indica quale tipo di intestazione segue l'header di base IPv6. Molto simile al campo protocol dell'header IPv4, del quale usa gli stessi valori.
- Hop Limit [8 bit] – equivalente al Time to live.
- Source Address [128 bit] - l'indirizzo IP del mittente.
- Destination Address [128 bit] - Indica l'indirizzo IP del destinatario.

Indirizzamento

- Indirizzamento gerarchico
 - Indirizzi rilasciati dai LIR
 - Indirizzi a 128 bit
 - Raggruppamento
- 2EDC:BA98:0332:0000:CF8A:000C:2154:7313
 - 3762:0:0:0:0:B03:1:AF18 (semplificazioni:
leading zeros,
continuous zeros)
 - 3762::B03:1:AF18
 - 0:0:0:0:0:0:0:1 diventa ::1
0:0:0:0:0:0:0:0 diventa ::
 - IPv4-mapped IPv6 addresses
::FFFF:x1.x2.x3.x4 questo é un indirizzo del
tipo ::/96 - è utilizzato per interconnettere le
due tecnologie IPv4/IPv6 nelle reti ibride.

Tipologie di indirizzi

- Unicast
- Multicast
- Anycast
- Attenzione: non c'è il broadcast (si usa il multicast)

- link-local
- site-local
- Global

Indirizzi unicast e link-local

- Indirizzi unicast ed anycast hanno due parti:
- 64-bit network prefix (routing).
- 64-bit interface

General unicast address format

bits	48	16	64
field	<i>routing prefix</i>	<i>subnet id</i>	<i>interface identifier</i>

Link-local address format

bits	10	54	64
field	<i>prefix</i>	<i>zeroes</i>	<i>interface identifier</i>

- gli indirizzi link-local sono costruiti a partire dal MAC della scheda
- I 54 zeri li rendono non instradabili

node-scope multicast addresses

- FF01:0:0:0:0:0:0:1 All Nodes Address
- FF01:0:0:0:0:0:0:2 All Routers Address
- FF01:0:0:0:0:0:0:FB mDNSv6



Entita' coinvolte

- Both IPv4 and IPv6 addresses are generally assigned in a hierarchical manner.
- Gli Internet service providers (ISPs) assegnano gli indirizzi agli utenti.
- Gli ISPs ottengono gli indirizzi IP da:
 - Local Internet registry (LIR)
 - National Internet Registry (NIR),
 - Regional Internet Registry (RIR):

- <http://www.iana.org/numbers/rir-map-small.png>



Extension Header

- Le opzioni IPv6 rispetto a quelle nell'header IPv4 sono poste in estensioni separate. Esse si trovano tra l'header IPv6 e l'header di livello di trasporto.
- La maggior parte delle extension headers vengono ignorate dai router sul percorso. Con il meccanismo delle estensioni i router non sono costretti ad elaborare tutte le opzioni, come avveniva in IPv4 ma solo quelle di interesse.
- Extension headers possono avere lunghezza arbitraria (in IPv4 erano al massimo 40 B)
- Possibilità' di integrare nuove estensioni
- Possibilità' di aggiungere opzioni ignorate dai router ma utili al destinatario

Indirizzi ed URI

- colon (:) characters in IPv6 addresses may conflict with the established syntax of resource identifiers, such as URIs and
- Il carattere ':' viene usato negli URI contenenti un indirizzo IPv4 per indicare il numero di porta
- l'uso con indirizzi IPv6 porterebbe a conflitti
- I conflitti vengono risolti mettendo l'indirizzo tra parentesi quadre es.
 - `http://[2a01::1234]:443`

Dimensioni pacchetti

- Con la jumbo payload extension header un pacchetto puo' raggiungere la dimensione di 2^{32} ottetti (4GB)!!!.
- Attenzione all'MTU quando si creano I tunnel

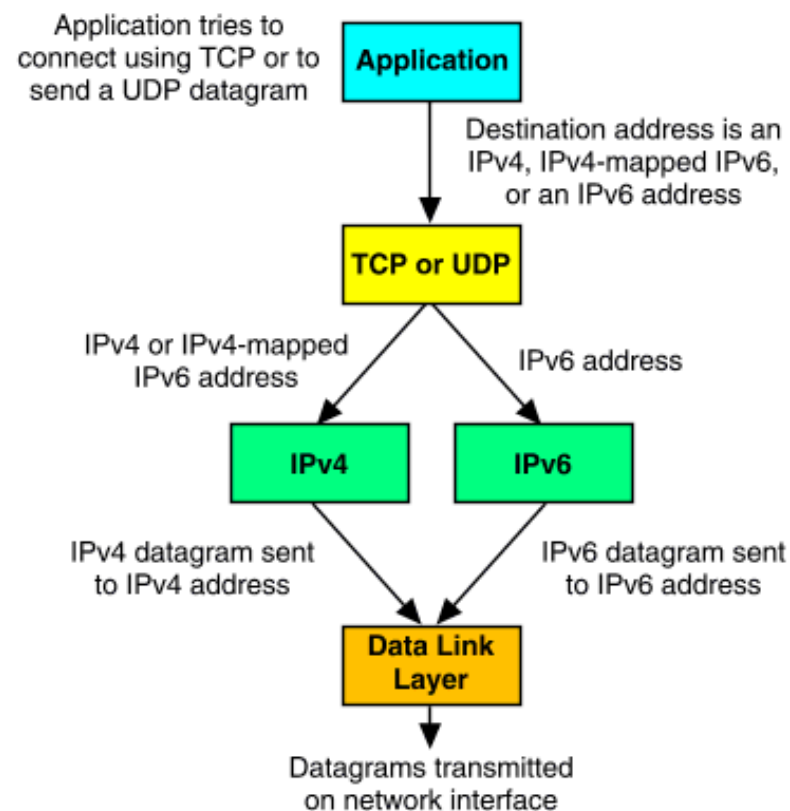
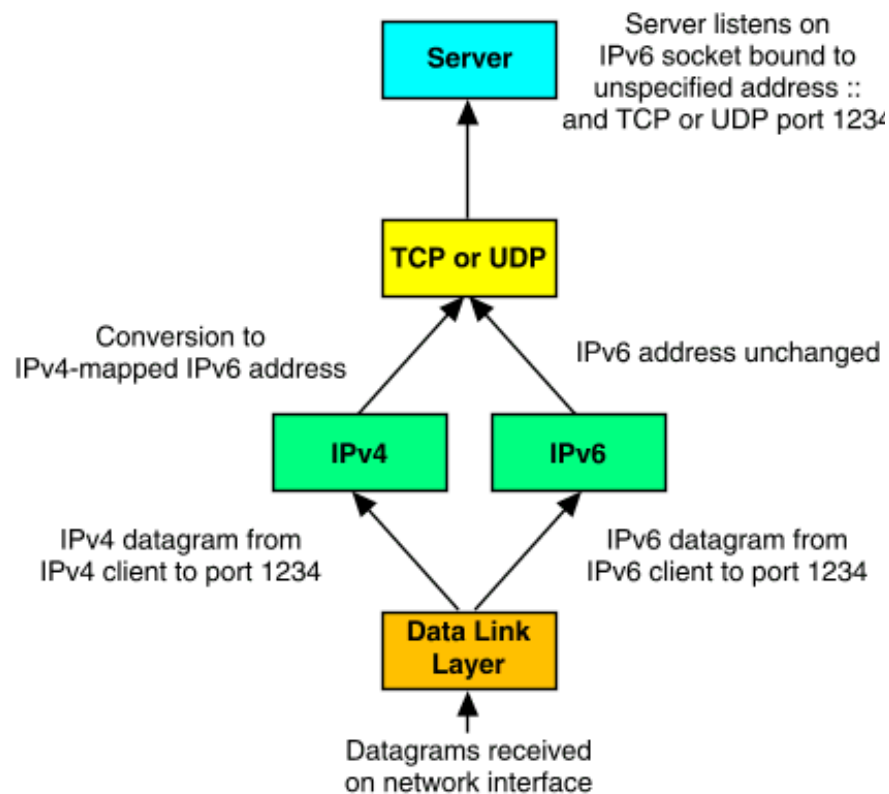


La transizione da IPv4 a IPv6

- Tunnelling
 - IPv6 viene trasportato in IPv4
- Host e router dual-stack
 - Supportano sia IPv4 che IPv6
 - Possono inviare pacchetti IPv6 attraverso reti IPv4 effettuando un incapsulamento in IPv4
 - Simple Internet Transition (SIT) – sit interface
 - Il punto di ingresso al tunnel (encapsulating node)
 - aggiunge l'header IPv4
 - trasmette il pacchetto incapsulato.
 - Il punto di uscita dal tunnel (decapsulating node) riceve il pacchetto incapsulato
 - rimuove l'header
 - Aggiorna l'header IPv6
 - Processa il pacchetto IPv6
 - Per ciascun tunnel vengono mantenute delle informazioni di stato (ad esempio l'MTU),



Funzionamento dual stack



- how the kernel handles incoming requests to a server process that is listening on an IPv6 listening socket

Interoperabilità IPv4/v6

- 6Bone
 - rete overlay implementata con tunnel IPv6 su IPv4

- 6to4 relays:
 - Non sono necessari tunnel
 - Vengono usati dei relays
 - Indirizzi 2002::/16
 - RFC 3056

Autoconfiguration

- NDP Neighbor Discovery Protocol
 - Neighbor solicitation (request)
 - Neighbor advertisement (response)
- Autoconfiguration
 - Router solicitation (inviato al link-local all-routers broadcast address)
 - Router advertisement (IPv6 address prefixes, inviati periodicamente)

ARP vs neighbor solicitation



- The NDP (neighbor discovery protocol) uses ff02::1 to send a packet in multicast. All-hosts on the local link receive it.
- What happens, in IPv4, when your box (10.0.0.2) wants to communicate with another box (10.0.0.1)?
 - ARP request to ethernet broadcast -> FF:FF:FF:FF:FF:FF who-has 10.0.0.1 tell 10.0.0.2 ?
 - All boxes receive, the one with 10.0.0.1 replies from its MAC: -> 10.0.0.1 is-at 00:20:12:34:56:AB
 - your box sends the frame to 00:20:12:34:56:AB from its MAC address.
- Now what happens with IPv6 when your box wants to talk to another ?
 - IPv6 neighbor solicitation is sent to IPv6 multicast address ff02::1 fe80::203:47ff:fe73:1f0f -> ff02::1 Neighbor Solicitation for 3ffe:8350:1:51:210:7bff:fe30:591
 - All boxes receive (this is mandatory!), the one with 3ffe:8350:1:51:210:7bff:fe30:591 replies from its link-local address: fe80::210:7bff:fe30:591 -> fe80::203:47ff:fe73:1f0f Neigh Adv for 3ffe:8350:1:51:210:7bff:fe30:591 (which it sends to the link-local the NS came from in the first place: your link-local)
 - Your box sees the MAC address where this advertisement came from and now knows the MAC address of 3ffe:8350:1:51:210:7bff:fe30:591

IPv6 ed il DNS

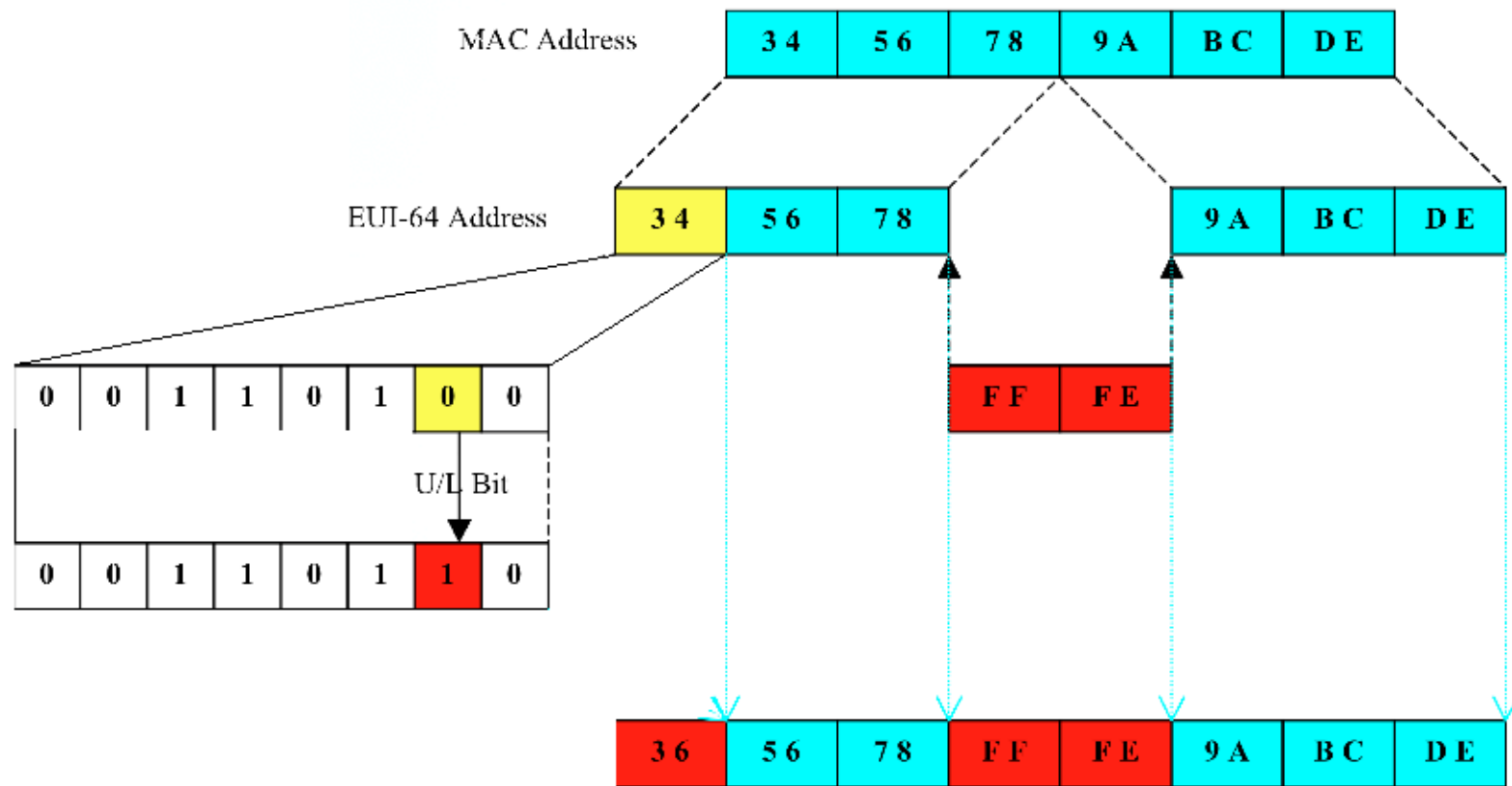
- BIND server
- nuovo tipo di resource record: AAAA (quad-a)
- (vedi esercitazione)

Approfondimento

- <http://bgp.he.net/ipv6-progress-report.cgi>
- <http://www.iana.org/numbers/>
- <http://www.ibiblio.org/pub/linux/docs/HOWTO/translations/it/pdf/Linux+IPv6-HOWTO.pdf>
- <http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml>



EUI64



Intestazioni di estensione

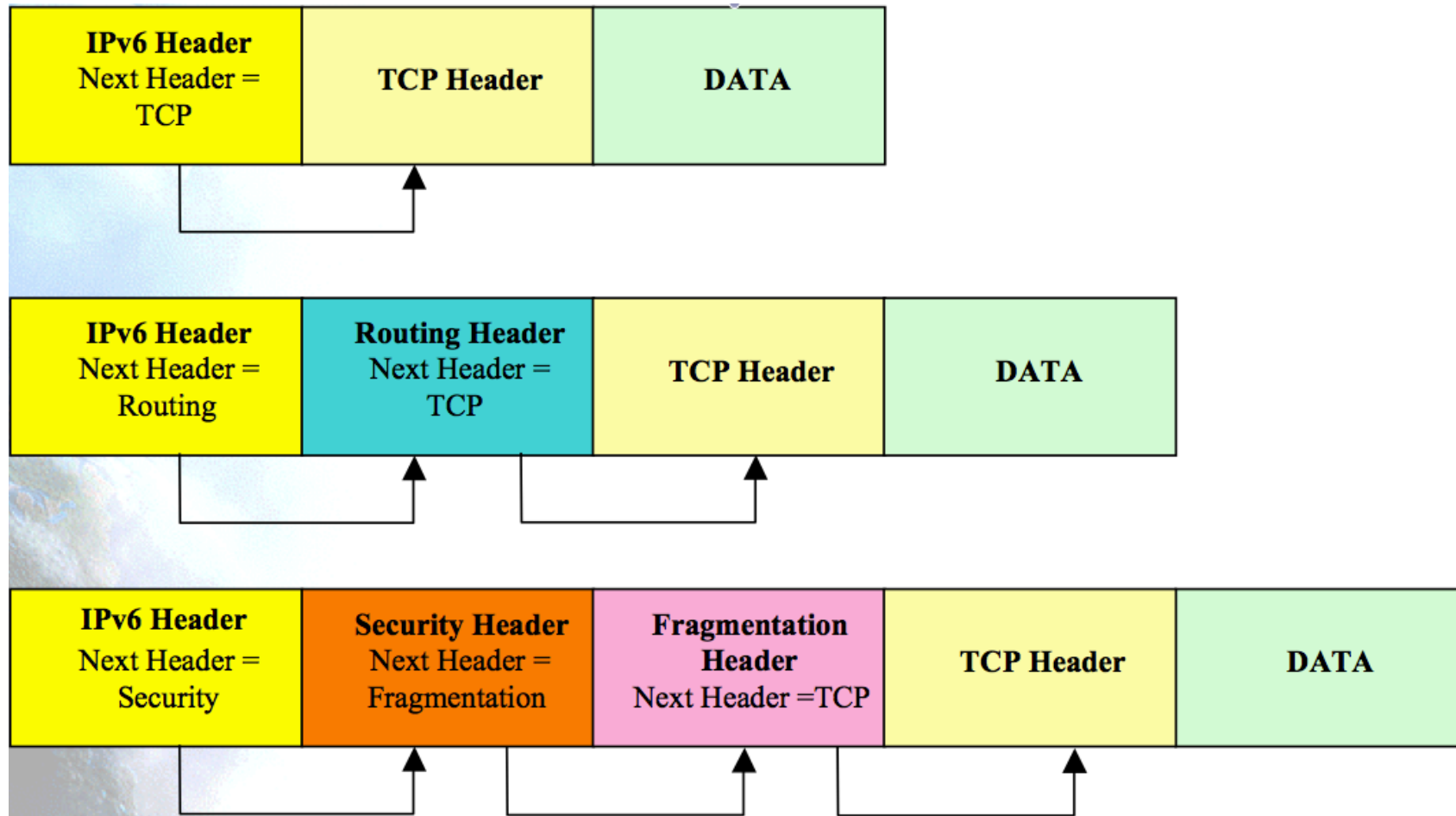
- Ciascuna serve a implementare un meccanismo diverso
- Esempi:
 - Autenticazione
 - Frammentazione/deframmentazione
 - Instradamento
 -
- Ogni datagramma contiene soltanto le intestazioni necessarie

Esempio

- Route serve per l'instradamento
- Auth serve per servizi di autenticazione
- TCP indica che la porzione che segue contiene un segmento TCP (i dati del datagram IPv6)
- Router esaminano solo alcune intestazioni di estensione

Intestazione Base Next = Route	Intestazione Route Next = Auth	Intestazione Auth Next = TCP	Segmento TCP (Dati)
--------------------------------------	--------------------------------------	------------------------------------	---------------------

Next Header



Alcuni header

- Routing (43)
 - Simile all'opzione IPv4 Loose Source Route
 - Indica una lista di router da attraversare
- Fragment (44)
 - Frammentazione (v. avanti)
- Authentication Header (51)
 - Serve a implementare meccanismi di autenticazione
- Encapsulating Security Payload (50)
 - Garantisce che solo il destinatario autorizzato sarà in grado di leggere il pacchetto

Opzioni IPv6

- IPv6 permette di definire intestazioni per ulteriori opzioni
- Permettono estensioni future del protocollo
- Estensioni hop-by-hop
 - Devono essere elaborate da ogni router intermedio
- Estensioni point-to-point
 - Elaborate soltanto a destinazione

Formato delle opzioni

- Next Header
 - Tipo prox header di intestazione
- Header length
 - Lunghezza complessiva header (nell'es. 11 byte)
- Type
 - Specifica il tipo di opzione
- Length
 - Lunghezza dell'opzione (nell'es. Opzione 2 ha lunghezza 2 byte)

0 8 16 24 31

Next Header	Header length	Type Opzione 1	Length Opzione 1
Valore Opz. 1			Type Opzione 2
Length Opzione 2	Valore Opz. 2		

Campo Type

- I router possono non comprendere alcune opzioni
- I 2 bit piu' alti del campo Type specificano cosa fare in tal caso
 - 00: saltare l'opzione
 - 01: scartare Dgram; non inviare mess. ICMP di notifica
 - 10: scartare Dgram; inviare mess. ICMP di notifica alla sorgente
 - 11: scartare Dgram; inviare mess. ICMP multicast di notifica



Il routing

- viene usato il prefisso piu' lungo che soddisfa il matching con la tabella di routing (come in IPv4 CIDR)
- pochi cambiamenti nei corrispondenti protocolli per IPv4
- routing unicast:
 - OSPF, RIP, IS-IS, BGP, ...
- routing multicast
 - MOSPF, PIM, ...



Esercitazioni

alcuni comandi per le esercitazioni di laboratorio



Esercitazione Indirizzi e DNS

- Configurazione IPv6
 - LINUX
 - Windows
- Ping6 su indirizzi link-local (attenzione!!!)
- Impostazione di un tunnel IPv6
 - traceroute6
- Impostare il radvd server
- Sniffing IPv6 pkts
- `http://[2a00:1450:8002::63]`

Indirizzi multicast

- `ping6 -I eth0 ff02::1` (all nodes) – puo' servire a trovare i neighbors
- `ping6 -I eth0 ff02::` (all routers)



MTU discovery

- Installare iputils-tracepath
 - e.g. apt-get install iputils-tracepath

Firewalling

- `ip6table -L`
- `ip6tables -n -v --line-numbers -L`
- `modprobe ip6_tables`
- `ip6tables --table filter --append INPUT -j LOG --log-prefix "INPUT:" --log-level 7`
- `ip6tables --table filter --append INPUT -j DROP`
- `ip6tables -A INPUT -i sit+ -p icmpv6 -j ACCEPT`

Il punto di vista della rete

- IPv6 port scan
- IPv6 looking glass

41



IPv6 Routing

- `route add -inet6 2001:230:3:: -prefixlen 64 2001:230:3::203:feff:4377:1890`
- `ip -6 addr add 2001:db8:beef::2/64 dev $INTERFACE`
- `ip -6 route add default via 2001:db8:beef::1`
- Quagga and zebra