



**Corso di Laurea in Ingegneria Informatica**

**Corso di Reti di Calcolatori**

**Antonio Pescapè ([pescape@unina.it](mailto:pescape@unina.it))**

---

**Il protocollo IPv6**



# Nota di Copyright

Quest'insieme di trasparenze è stato realizzato dai ricercatori del Gruppo di Ricerca COMICS del Dipartimento di Informatica e Sistemistica dell'Università di Napoli. Esse possono essere impiegate liberamente per fini didattici esclusivamente senza fini di lucro, a meno di un esplicito consenso scritto degli Autori. Nell'uso dovrà essere esplicitamente riportata la fonte e gli Autori. Gli Autori non sono responsabili per eventuali imprecisioni contenute in tali trasparenze né per eventuali problemi, danni o malfunzionamenti derivanti dal loro uso o applicazione.



# IP Next Generation (IPng o IPv6)

- E' la nuova versione del protocollo di Internet
- Mira a risolvere parte dei problemi che Internet sta incontrando a causa della sua crescita vertiginosa
- Principali questioni affrontate:
  - indirizzamento e routing
  - sicurezza
  - configurazione automatica
  - servizi di tipo real-time



# IPv6 : problemi affrontati in fase di progetto

- Supportare reti interconnesse di tipo globale
- Garantire una transizione chiara e diretta dell'immensa base di sistemi utilizzanti IPv4
- Sostenere l'elevato tasso di crescita delle reti
- Far fronte ai possibili scenari futuri nel mondo dell'internetworking:
  - mobile computing
  - networked entertainment
  - ecc...



# IPv6 : la fase di transizione

- La sfida per IPng è quella di completare la transizione prima che i problemi di IPv4 legati all'indirizzamento ed al routing emergano in tutta la loro tragicità, cioè prima che gli indirizzi di Internet perdano la loro unicità a livello globale.
- Ciò richiede:
  - una strategia di sviluppo flessibile ed incrementale
  - l'interoperabilità tra le due versioni di IP



# IPv6 : modifiche principali rispetto ad IPv4

- Espansione capacità di indirizzamento e di routing
  - la dimensione degli indirizzi passa da 32 (4 byte) a 128 bit (16 byte), per supportare una gerarchia su più livelli ed un numero di nodi molto più elevato
  - la scalabilità del routing multicast è migliorata grazie all'aggiunta di un campo *scope* agli indirizzi di classe D
  - viene definito un nuovo tipo di indirizzo (*anycast address*) che si riferisce ad un insieme di interfacce
    - un pacchetto inviato ad un indirizzo anycast, viene recapitato ad una delle interfacce che fanno parte dell'insieme da esso individuato (tipicamente da quella più “vicina”, secondo la misura di “distanza” utilizzata dal protocollo di routing)



- Semplificazione del formato dell'header:
  - alcuni campi dell'header (quelli che vengono sfruttati solo in casi particolari) sono stati eliminati o resi opzionali
    - ciò ha consentito di ottenere che, malgrado gli indirizzi di IPv6 siano 4 volte più lunghi di quelli di IPv4, l'header del primo è soltanto il doppio di quello del secondo



# IPv6 : caratteristiche generali

- Supporto per le opzioni migliorato:
  - alcuni cambiamenti nel modo di codificare le opzioni permettono uno smistamento più efficiente ed una maggiore flessibilità per introdurre, in futuro, nuove funzionalità
- Supporto della Quality of Service (QoS)
  - viene introdotta una nuova funzionalità per permettere di etichettare (*flow label*) i pacchetti appartenenti a flussi di dati particolari per i quali si richiede un trattamento di tipo non-default



- Autenticazione e salvaguardia della privacy:
  - definizione di estensioni che forniscono il supporto per:
    - l'autenticazione
    - l'integrità dei dati
    - la sicurezza, considerata elemento fondamentale del nuovo protocollo

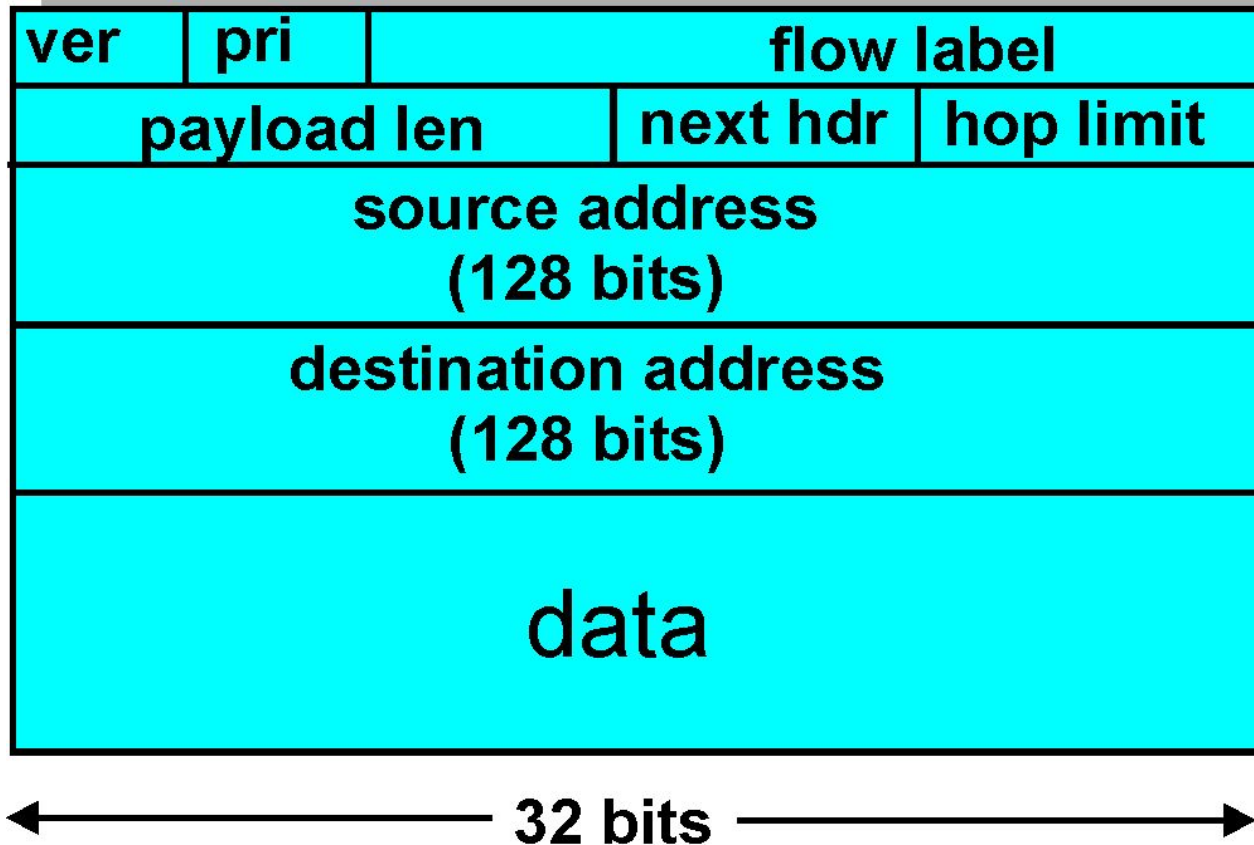


# Header principale ed extension headers

- L'header IPv6 consiste di due parti:
  - **header principale**
  - **extension headers**
    - introdotti per ospitare le eventuali opzioni
    - situati, all'interno del pacchetto, in una posizione intermedia tra l'header principale e l'header del protocollo di trasporto
    - forniscono, tra l'altro, informazioni relative:
      - al routing
      - alla frammentazione
      - all'autenticazione
      - alla sicurezza



# L'header principale





# L'header principale

- **Vers** : numero della versione
- **Prio** : livello di priorità del datagramma
- **Flow Label** : associato alla QoS richiesta
- **Payload Length** : lunghezza del payload
- **Next Hdr** : tipo di header che segue quello IPv6
- **Hop Limit** : contatore del numero di hops
- **Source Address** : indirizzo del mittente
- **Destination Address** : indirizzo del destinatario



# Differenze con l'header IPv4

- **Checksum:** rimossa completamente per ridurre il tempo di processamento nei router ad ogni hop
- **Options:** sono previste, ma non nell'header. E' possibile prevederle fuori dall'header utilizzando il campo "Next Header"
- **ICMPv6:** nuova versione di ICMP
  - Messaggi addizionali, e.g. "Packet Too Big"
  - Funzioni per il management dei gruppi multicast



# La priorità dei pacchetti IPv6

<b>0</b>	<b>traffico non noto</b>
<b>1</b>	<b>traffico di riempimento (es. news)</b>
<b>2</b>	<b>traffico batch (es. e-mail)</b>
<b>3</b>	<b>riservato</b>
<b>4</b>	<b>traffico interattivo a bassa priorità (es. ftp, NFS)</b>
<b>5</b>	<b>riservato</b>
<b>6</b>	<b>traffico interattivo ad alta priorità (es. telnet, X)</b>
<b>7</b>	<b>traffico di controllo di internet (es. OSPF, SNMP)</b>

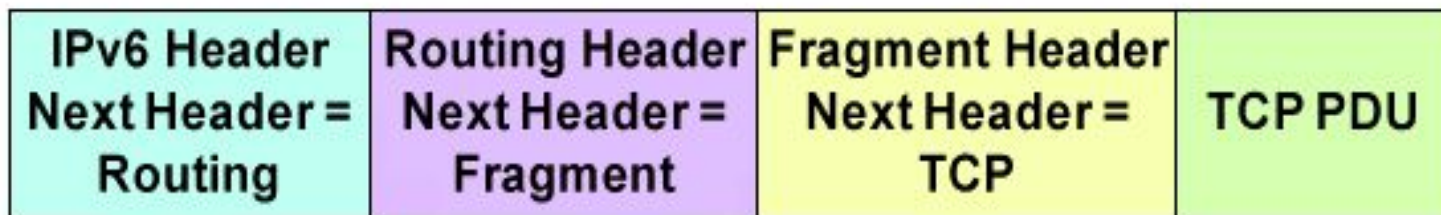
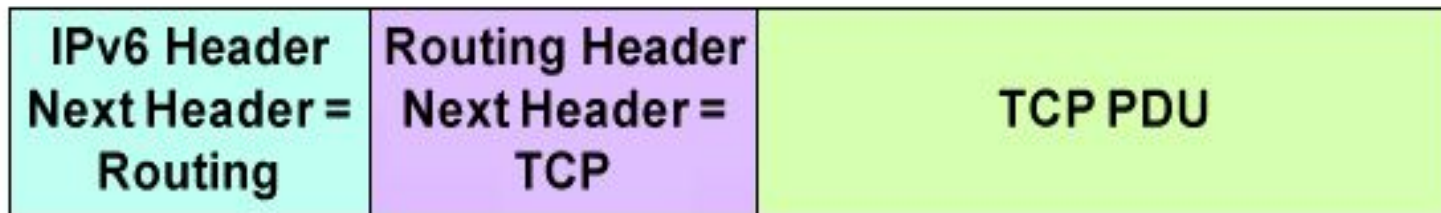


# Il campo Next Header

0		Reserved (IPv4)
0	HBH	Hop by Hop option (IPv6)
1	ICMP	Internet Control Message (IPv4)
2	IGMP	Internet Group Management (IPv4)
2	ICMP	Internet Control Message (IPv6)
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (IPv4 encapsulation)
5	ST	Stream
6	TCP	Transmission Control
17	UDP	User Datagram
29	TP4	ISO Transport class 4
43	RH	Routing Header (IPv6)
44	FH	Fragment Header (IPv6)
45	IDRP	Interdomain Routing
51	AH	Authentication Header
52	ESP	Encrypted Security Payload
59	Null	No next header (IPv6)
80	ISO-IP	ISO 8473 CLNP
88	IGRP	Interior Gateway Routing
89	OSPF	Open Shortest Path First



# Gli Extension Headers ed il Daisy Chaining





# Gli Extension Header

- **Hop by hop** option header
  - es: jumbograms
- **Routing** header:
  - *strict source routing*
  - *loose source routing*
- **Fragment** header:
  - gestisce la frammentazione
- **Authentication** header
- **Encrypted security payload** header
- **Destination option** header



# Extension headers

- Un pacchetto IPv6 può contenere zero, uno, o più *extension header* identificati dal campo “Next Header” dell’header precedente
- Gli **Extension headers** (eccetto l’header dell’opzione *Hop-by-Hop*) non sono elaborati, inseriti, o cancellati dai nodi lungo il percorso
- **L’header dell’opzione Hop-by-Hop** non è né inserito né cancellato, ma può essere esaminato ed elaborato dai nodi lungo il percorso



# Extension headers

- Quando nello stesso pacchetto è presente più di un extension header l'RFC raccomanda che gli header rispettino il seguente ordine:
  - IPv6 header
  - Hop-by-Hop Options header
  - *Destination Options header*
  - Routing header
  - Fragment header
  - Authentication header
  - Encapsulating Security Payload header
  - *Destination Options header*
  - Upper-Layer header
- Ciascun extension header dovrebbe (*should*) apparire al più una volta, fatta eccezione dell'header *Destination Options* che dovrebbe apparire al più due volte



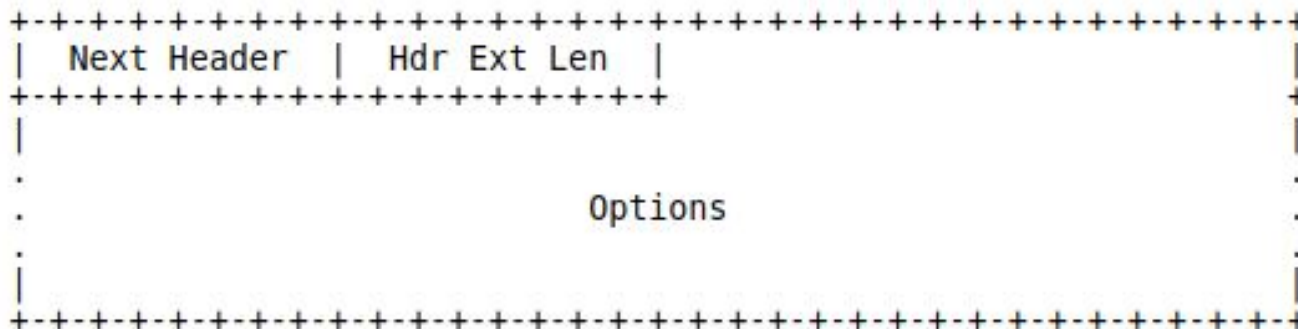
# Extension headers

- Il contenuto e la semantica di ciascun extension header determina se l'header successivo verrà analizzato
  - Gli extension header devono essere processati strettamente nell'ordine in cui appaiono nel pacchetto
- Se il valore del campo "next header" non è riconosciuto Il nodo dovrebbe (should) scartare il pacchetto ed inviare una messaggio ICMP parameter problem al mittente
  - ICMP Code value of "*unrecognized Next Header type encountered*"
  - Il campo pointer contiene l'offset del valore non riconosciuto nel pacchetto che ha generato l'errore



# Hop-by-hop header

- Utilizzato per trasportare informazioni aggiuntive che possono essere esaminate da ciascun nodo lungo il percorso
- Identificato dal valore 0 del campo “next header” dell’extension header precedente



- **Hdr Ext Len:** lunghezza del campo Options in byte, esclusi i primi 8 byte
- **Options:** campo di lunghezza variabile (l’intero header dell’opzione Hop-by-hop è un multiplo di 8 byte)
  - Contiene una o più opzioni *TLV-encoded*







# Fragment header

Il pacchetto iniziale è concettualmente scomposto in 3 parti:

- **L'header per-frammento** (*per-fragment*) è composto dall'header IPv6 più tutti gli extension header che devono essere esaminati dai nodi sul percorso
  - fino al routing header, incluso, se presente
  - Altrimenti, Hop-by-hop header, se presente
- **Gli extension header restanti e l'header del protocollo di livello superiore** (TCP, UDP, IPv4, IPv6, ICMPv6) vengono copiati solo nel primo frammento
- **La parte frammentabile**, composta dalla parte restante del pacchetto
  - è divisa in frammenti di lunghezza tale che la lunghezza dei pacchetti ottenuti coincida con l'MTU del percorso.

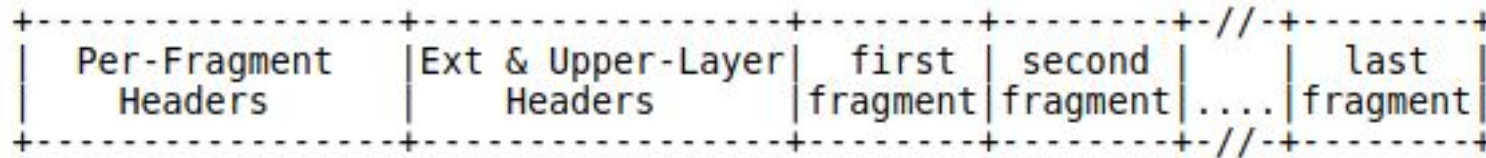
Ciascun frammento completo (ad eccezione di quello più a destra) è di dimensione multipla di 8 byte.



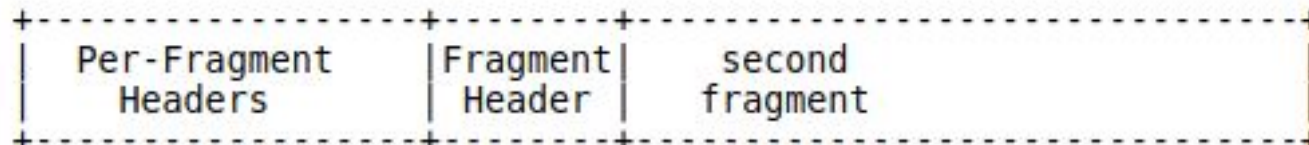
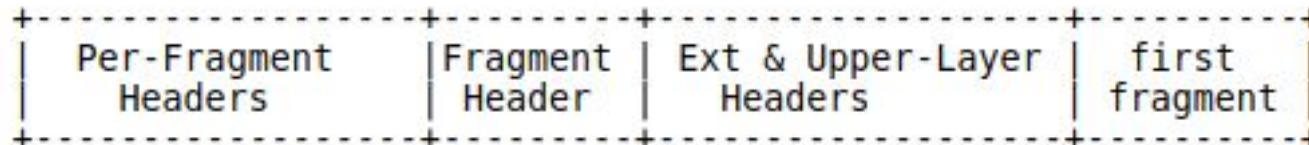
# Fragment header

The fragments are transmitted in separate "fragment packets" as illustrated:

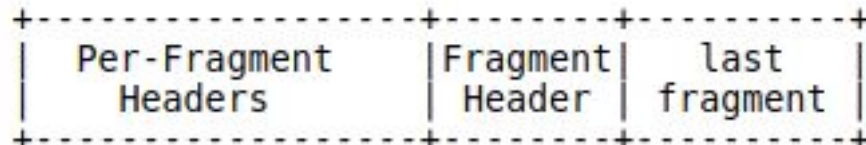
original packet:



fragment packets:



0  
0  
0





# Modalità di scrittura degli indirizzi in IPv6

- Si scrivono in esadecimale come 8 numeri naturali separati da “:”
  - FEDC:BA98:0876:45FA:0562:CDAF:3DAF:BB01
  - 1080:0000:0000:0007:0200:A00C:3423
- Esistono delle semplificazioni:
  - si possono omettere gli zero iniziali
    - 1080:0:0:7:200:A00C:3423
  - Si possono sostituire gruppi di zero con “::”
    - 1080::7:200:A00C:3423



# Tipi di indirizzo in IPv6

Allocation	Prefix	Fraction of Address Space
Reserved (IPv4)	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Geographic- Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256



# Address Type Identification

The type of an IPv6 address is identified by the high-order bits of the address, as follows:

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Global Unicast	(everything else)	



# Examples

- 2001:DB8:0:0:8:800:200C:417A *a unicast address*
- FF01:0:0:0:0:0:0:101 *a multicast address*
- 0:0:0:0:0:0:0:1 *the loopback address*
- 0:0:0:0:0:0:0:0 *the unspecified address*



# Examples

- 2001:DB8:0:0:8:800:200C:417A    *a unicast address*  
2001:DB8::8:800:200C:417A
- FF01:0:0:0:0:0:0:101    *a multicast address*  
FF01::101
- 0:0:0:0:0:0:0:1    *the loopback address*  
::1
- 0:0:0:0:0:0:0:0    *the unspecified address*  
::



# Unspecified address

- The address 0:0:0:0:0:0:0:0 is called the **unspecified address**
- It must never be assigned to any node
- The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing headers
- An IPv6 packet with a source address of unspecified must never be forwarded by an IPv6 router
- One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address



# Loopback Address

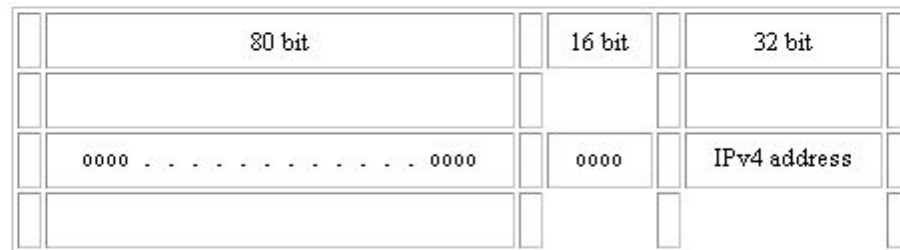
- The unicast address 0:0:0:0:0:0:0:1 is called the **loopback address**
- It may be used by a node to send an IPv6 packet to itself
- It must not be assigned to any physical interface
- The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node
- An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router
- A packet received on an interface with a destination address of loopback must be dropped



# Indirizzi di Compatibilità

## • Indirizzo compatibile con IPv4

- L'indirizzo compatibile con IPv4,  $0:0:0:0:0:w.x.y.z$  oppure  $::w.x.y.z$ , dove  $w.x.y.z$  è la rappresentazione decimale separata da punti di un indirizzo IPv4 pubblico.



- Viene utilizzato dai nodi a doppio stack che comunicano con IPv6 su un'infrastruttura IPv4.
- I nodi a doppio stack utilizzano entrambi i protocolli IPv4 e IPv6.
- Quando un indirizzo compatibile con IPv4 viene utilizzato come destinazione IPv6, il traffico IPv6 viene incapsulato automaticamente con un'intestazione IPv4 e inviato alla destinazione utilizzando l'infrastruttura IPv4.
- Usati nella transizione da IPv4 a IPv6, quando un nodo che supporta sia IPv6 che IPv4 non ha un router IPv6 a cui inviare i pacchetti.



# IPv4-Mapped IPv6 Address

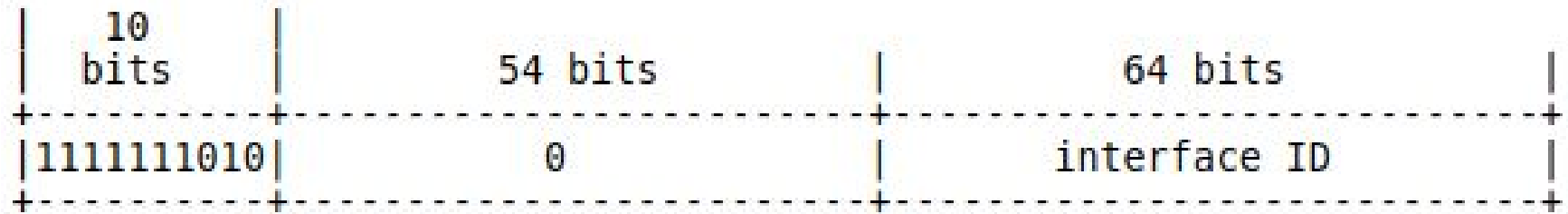
This address type is used to represent the addresses of IPv4 nodes as IPv6 addresses





# Link-Local IPv6 Unicast Addresses

- Link-Local addresses are for use on a single link



- Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present
- Routers must not forward any packets with Link-Local source or destination addresses to other links



# Anycast Addresses

- An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the "nearest" interface having that address, according to the routing protocols' measure of distance
- Anycast addresses are allocated from the unicast address space
- Anycast addresses are syntactically indistinguishable from unicast addresses



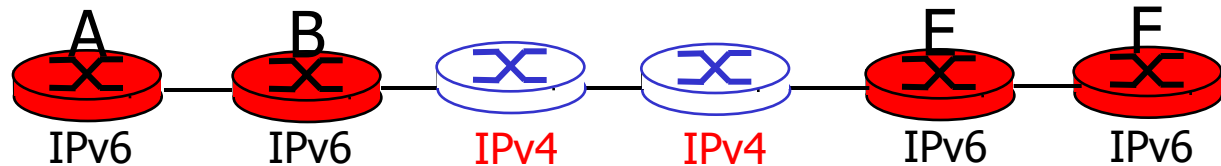
# Transizione da IPv4 a IPv6: Tunneling

**Tunneling:** I pacchetti IPv6 vengono trasportati come payload all'interno di datagrammi IPv4 tra router IPv4

Logical  
view:

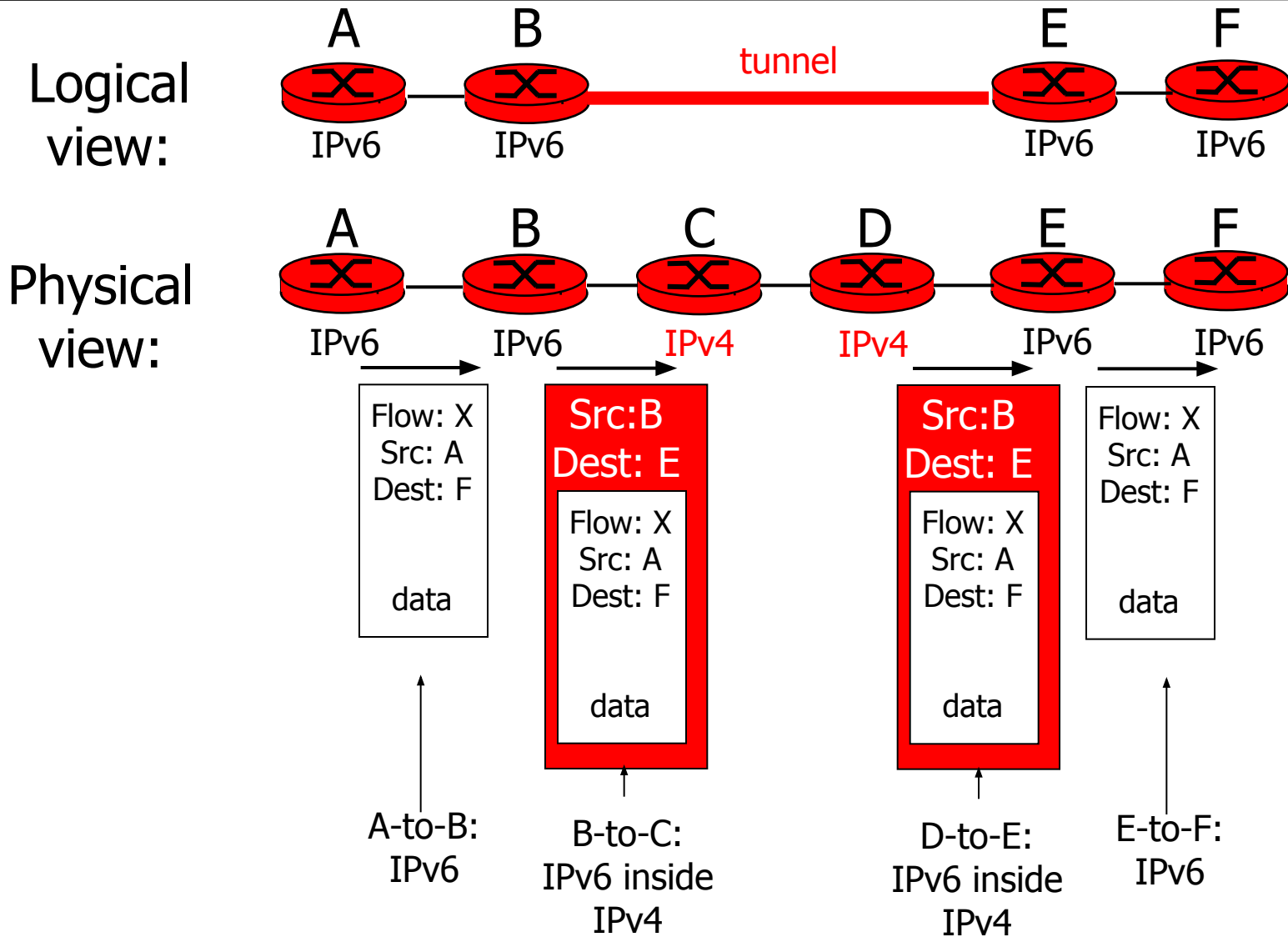


Physical  
view:





# Transizione da IPv4 a IPv6: Tunneling





# IPv6 deployment timeline

August 1990

Frank Solensky advised IETF that IPv4 allocation rates meant IPv4 address space would run out in less than five years

1998

IPv6 in its current specification was proposed jointly by Bob Hinden and Steve Deering

2006

ICANN ratified a policy for IPv6 prefix allocation

2007

JPNIC report called for action to deploy IPv6

2009

Over 300 ARIN members had been allocated IPv6 prefixes for testing and early deployment

January 2011

The Internet Assigned Number Authority (IANA) ran out of IPv4 addresses

April 2011

RIR for the Asia Pacific region, APNIC, ran out of IPv4 addresses

September 2012

RIR for Europe and Middle East, RIPE NCC ran out of IPv4 addresses

June 2014

RIR for Latin America and Caribbean, LACNIC, ran out of IPv4 addresses

September 2015

RIR for North America, ARIN, ran out of IPv4 addresses

April 2017

RIR for Africa, AfriNIC, ran out of IPv4 addresses



# Address assignment process

Both IPv4 and IPv6 addresses are generally assigned in a hierarchical manner.

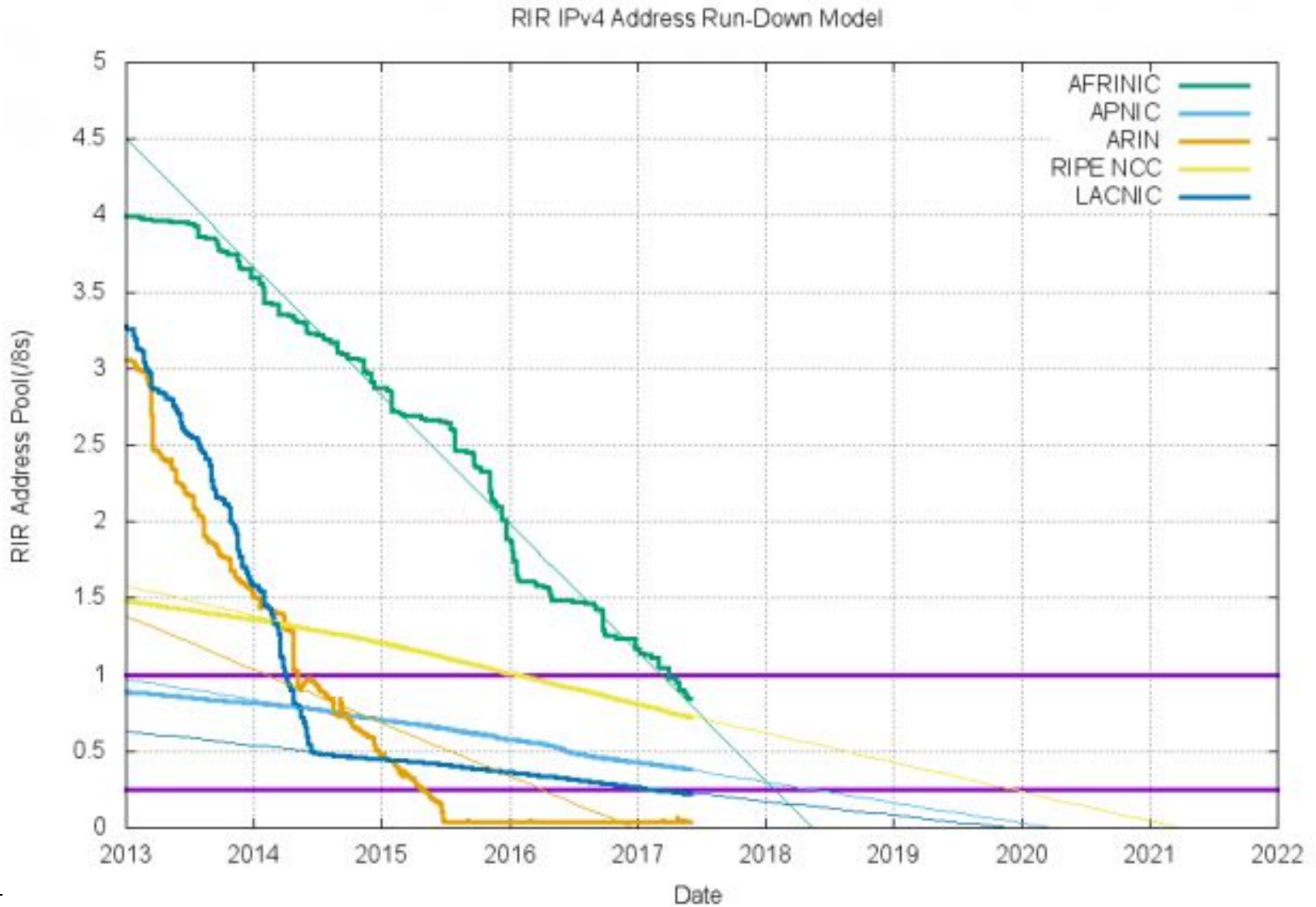
- Users are assigned IP addresses by Internet service providers (ISPs).
- ISPs obtain allocations of IP addresses from
  - a local Internet registry (LIR)
  - or National Internet Registry (NIR),
  - or from their appropriate Regional Internet Registry (RIR)



REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia



# IPv4 addresses exhaustion





# IPv6 deployment

- There is an abundance of data regarding the ongoing IPv6 deployment, but it is not all in one place
- **“Deployment”**: “to spread out, utilize, or arrange for a deliberate purpose.”
- Deploying a protocol means to change software in existing equipment, or install new equipment, that uses the protocol



# Measuring IPv6 deployment

- We measure deployment by the evidence it leaves
  - routing protocols, domain names, and applications that are accessible from the open Internet using IPv6
- We also measure it by connections users are able to make
- Note that if a user on a smartphone or computer can access a web site or send an email using IPv6, the action proves that all of the following worked using IPv6
  - The user's application,
  - The user's smartphone or computer,
  - The user's network,
  - The user network's upstream provider,
  - The server network's upstream provider,
  - The server network,
  - The server itself, and
  - The application running on the server,
  - Plus, anything else that the session might transit.



## IPv6 deployment is increasing around the world, with over 9 million domain names and 23% of all networks advertising IPv6 connectivity

- **Google** reports 37 countries exceeding 5% of traffic, with new countries being added weekly
  - in several cases, one third to one half
- **Akamai** reports 7 countries whose IPv6 traffic exceeds 15%
- In **Japan**, all three major mobile networks, NTT, KDDI, and Softbank, are deploying IPv6 this year
- In **India**, Reliance JIO's deployment has driven measures of IPv6 traffic in the country to exceed 20%

*The IPv4 Market Group comments that it expects IPv6 user count to exceed 50% world-wide in 2019, and with that, the start of the decline of the IPv4 address market*

Source: State of IPv6 Deployment 2017,

URL: <https://www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017/>



# Countermeasures to IPv4 addresses exhaustion

The IPv6 protocol came out of a recognition, reported on by Frank Solensky to the IETF in August 1990, that the allocation rate of IPv4 address space was such that the Internet would run out of address space in less than five years.

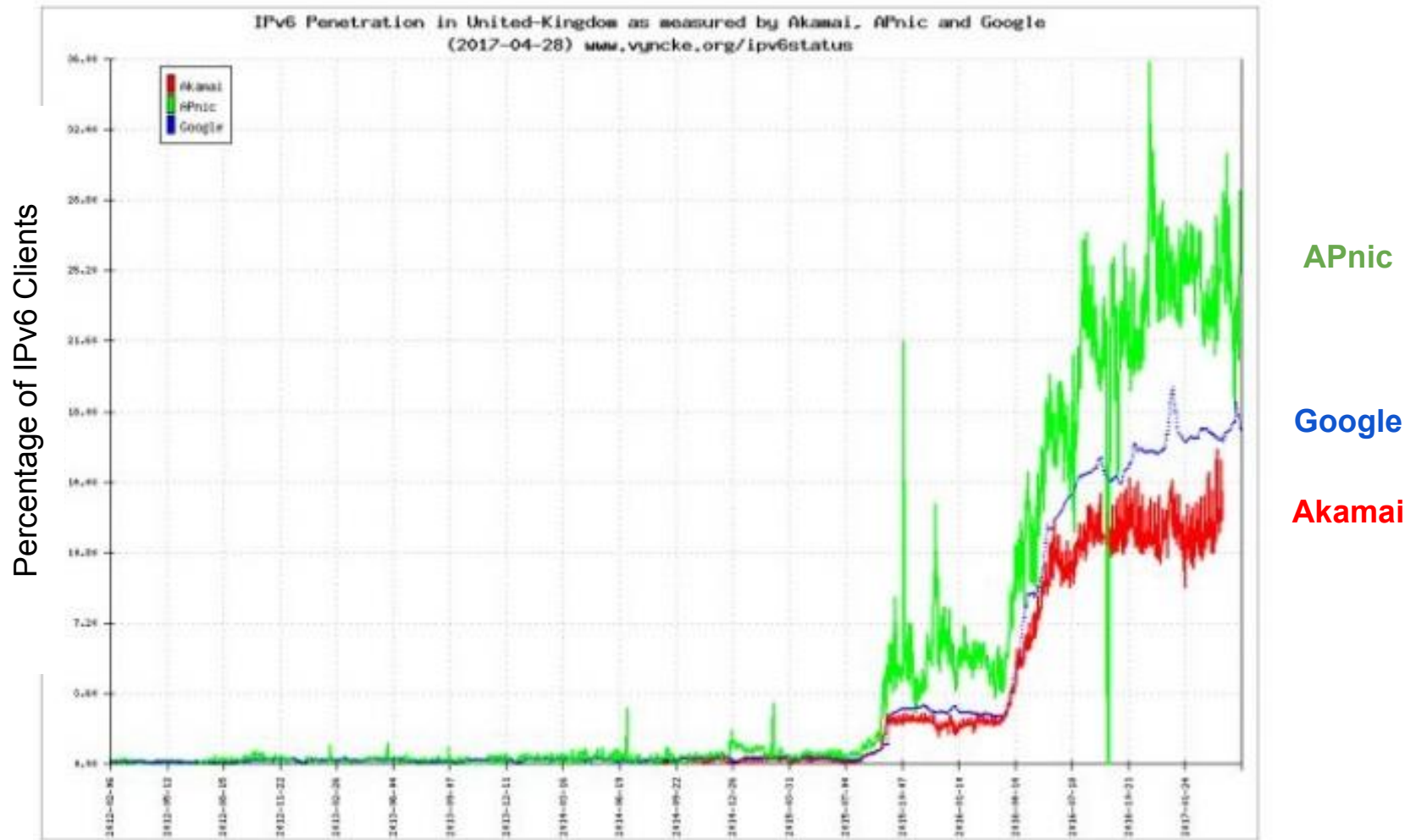
There were four immediate outcomes:

- The existing Regional Internet Registries (RIRs) and IETF changed from classful addressing to Classless Inter-Domain Routing (CIDR) addressing in allocation and in protocols
- There was a call to recover address space that was allocated but not in use, which is ongoing
- **The IETF invited proposals for a next generation protocol**
- The initial concepts behind Network Address Translation (NAT) were developed



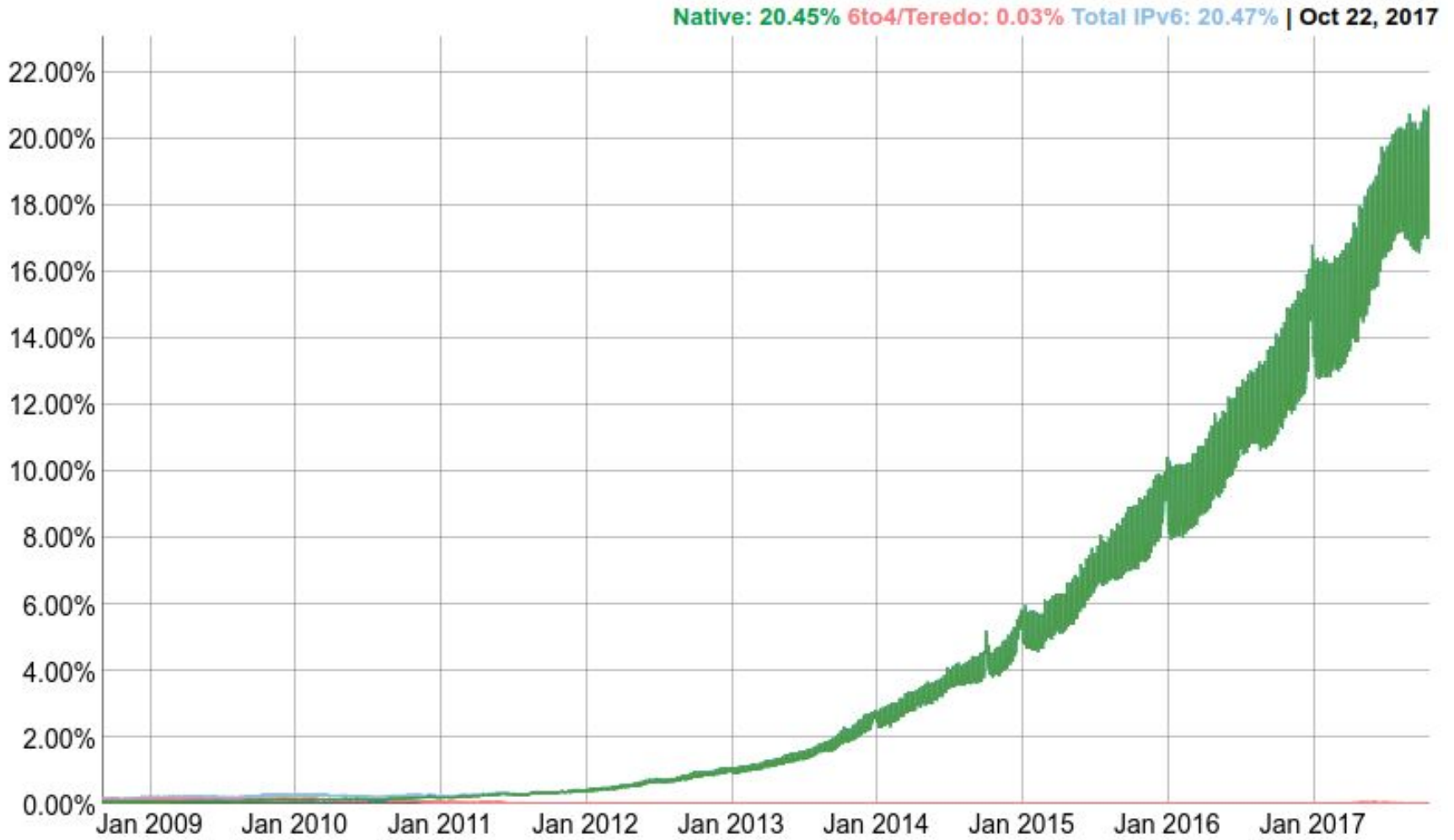
# IPv6 deployment: measurement procedure matters!

## IPv6 penetration in UK





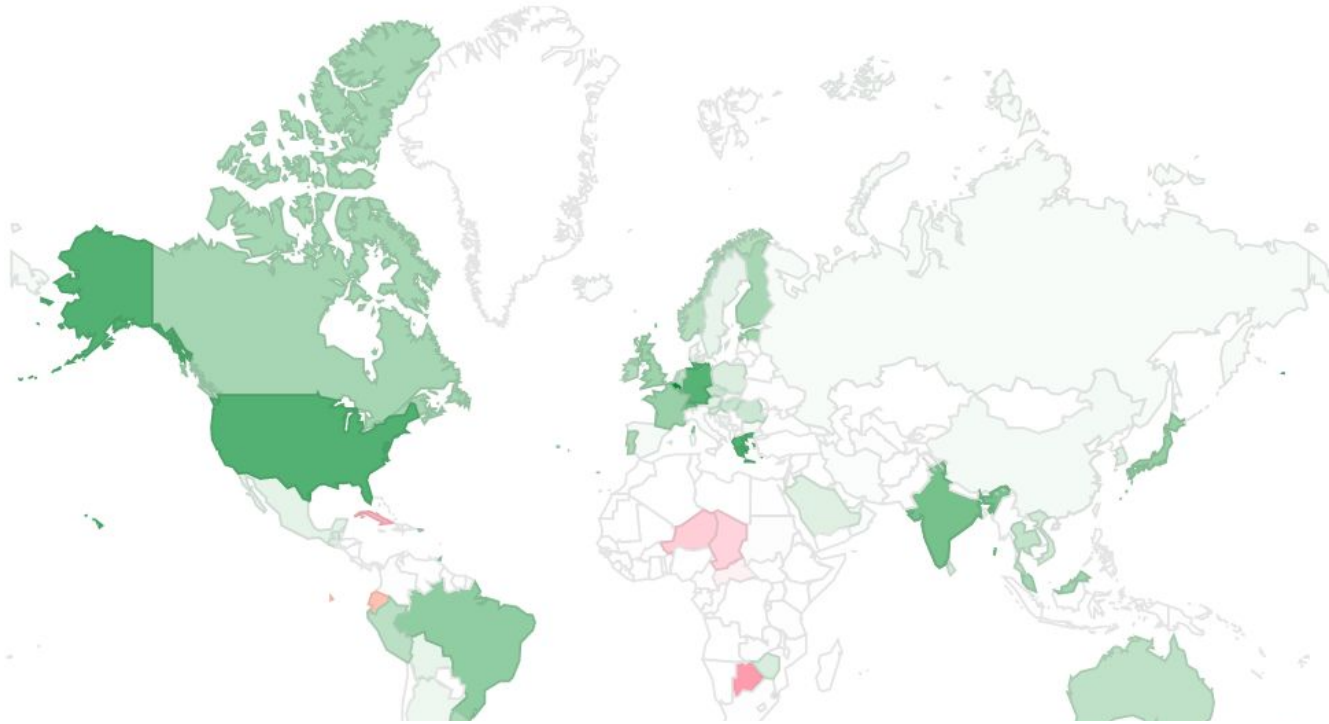
# IPv6 adoption (according to Google)






<https://www.google.com/intl/en/ipv6/statistics.html>



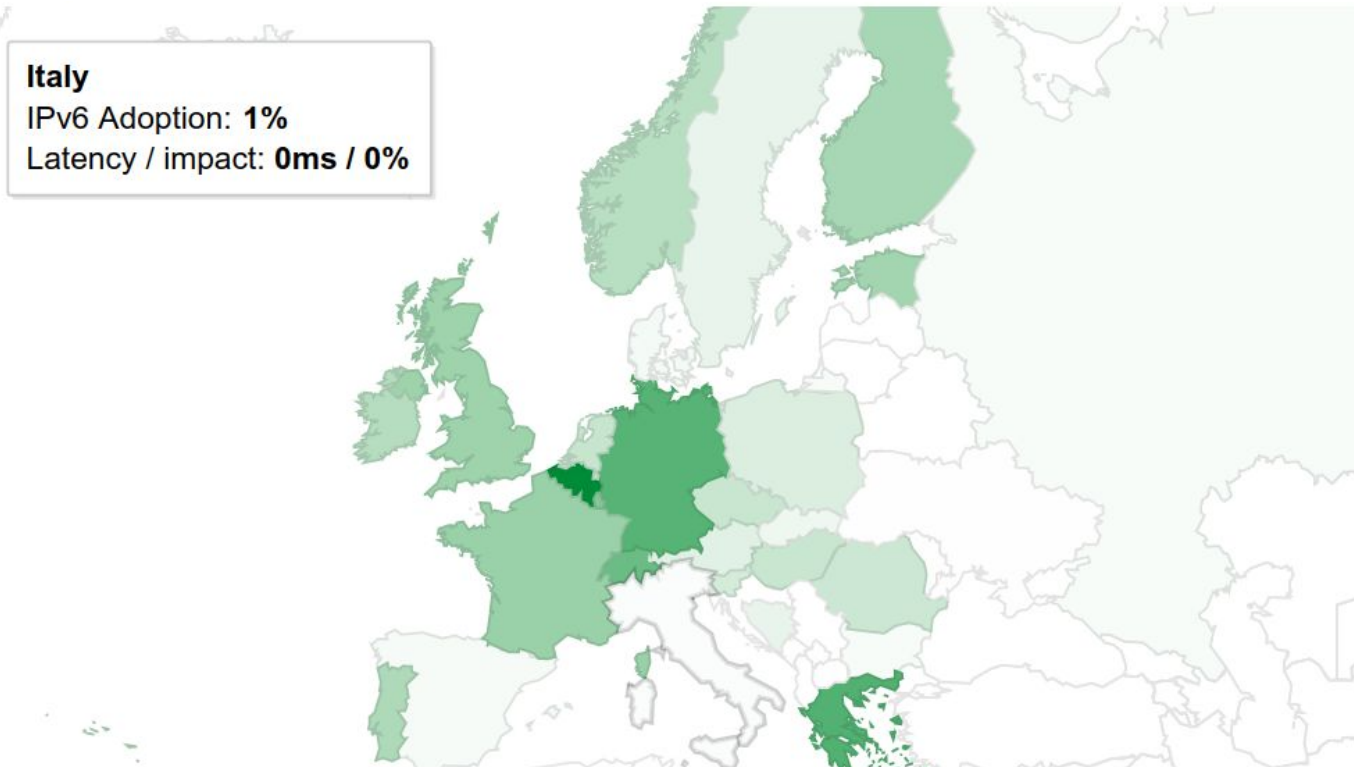
# Per-country IPv6 adoption






-  Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.



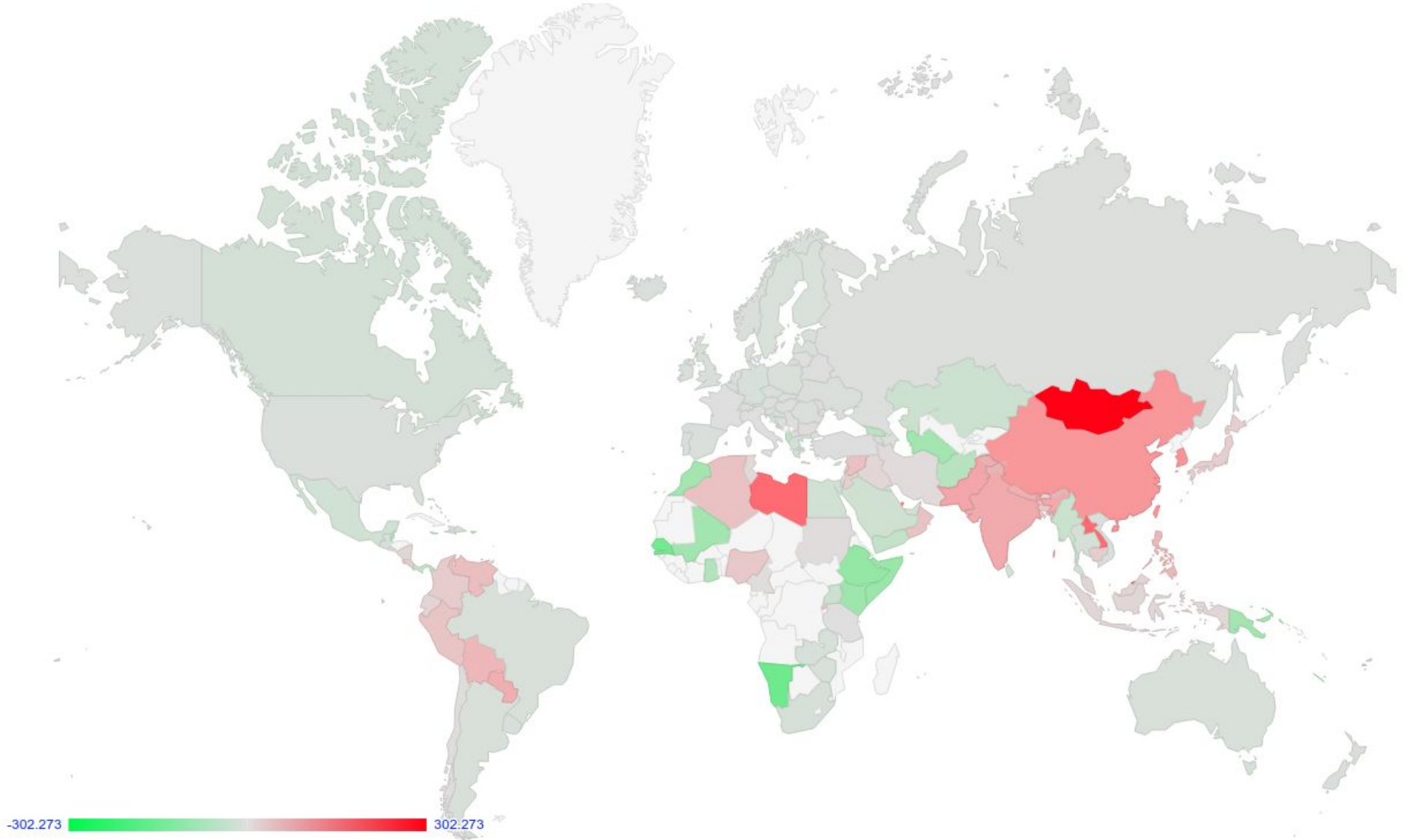
# Per-country IPv6 adoption (Europe)



-  Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is more widely deployed but users still experience significant reliability or latency issues connecting to IPv6-enabled websites.
-  Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites.

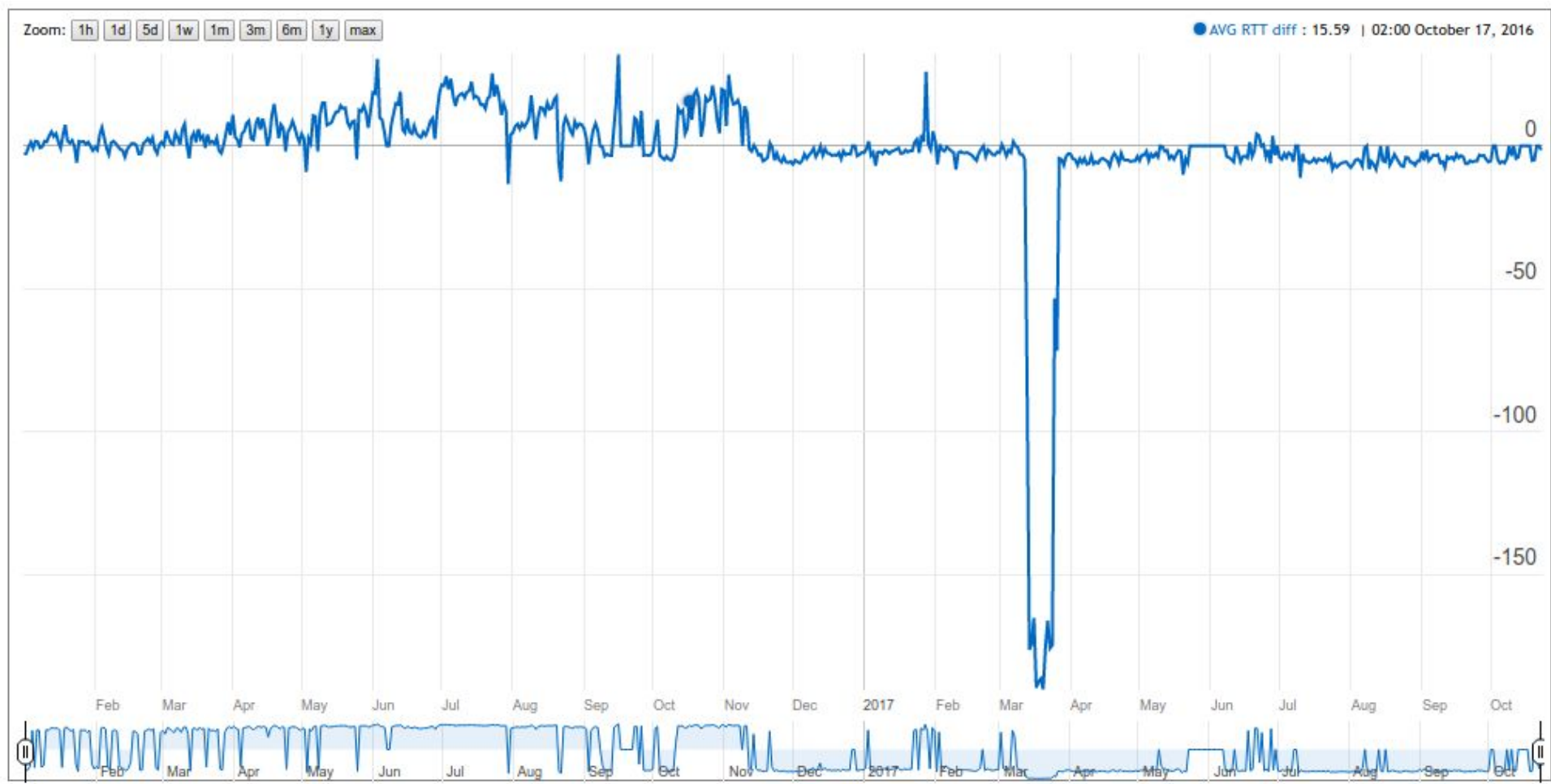


# IPv4 vs IPv6 performance comparison





# Average RTT difference (ms) IPv6-IPv4 for Europe



<https://stats.labs.apnic.net/v6perf/XE>



# Average RTT difference (ms) IPv6-IPv4 for Italy



<https://stats.labs.apnic.net/v6perf/IT>



# Industry deployment

Most **backbone ISPs** (those that offer transit service to corporate customers) advertise IPv6 prefixes in BGP today

- Considered by country, transit ISPs offering IPv6 services exist in every country, with the exception of parts of Africa, the Middle East, and China

**Google, LinkedIn, Akamai, Netflix, and Facebook** are actively deploying IPv6 within their networks, and connecting to IPv6 users outside

- An interesting point is that they report that delivering their services using IPv6 appears to improve user experience in terms of download times



# Industry deployment

**Mobile Wireless**, today, is rapidly becoming an IPv6-majority market

- *Reliance JIO* (that launched commercial service in September 2016) reports that about 90% of its traffic uses IPv6, driven by its major content providers.
- *Verizon Wireless* similarly reports that about 90% of its traffic uses IPv6
- *T-Mobile* is among the providers in the process of turning IPv4 off
- Other major cellular IPv6 providers include AT&T Wireless, Sprint, Telus, Tele2, EE, KDDI, Softbank, OTE, Rogers and many others

**Enterprise operations** tend to be the “elephant in the room” when it comes to IPv6 deployment

- if 23% of AS's advertise IPv6 prefixes, 77% do not, and those are likely to be enterprise networks



# Conclusioni

- Cambiare il protocollo di rete (*le fondamenta*) non è cosa semplice
  - IPv6, Multicast, RSVP
- Cambiare/Aggiungere protocolli di livello applicativo (*tinteggiare nuovamente le pareti*) è cosa più semplice
  - Streaming, p2p, gaming ...