Introduction to IPv6

Introducción a las Redes de Computadoras

Ariel Sabiguero

asabigue@fing.edu.uy

Agenda

- IPv6 History & backgroud
- IPv6 header format (vs IPv4 header)
- IPv6 addresses
- ICMPv6
- Neighbor Discovery
- Transition mechanisms
- IPv6 Ready Logo Programme

IPv6 history & background

IPv6 history

Los problemas de IPv4 son conocidos:

- En 1991 el IETF organizó un grupo de trabajo para analizar el crecimiento de Internet y discutir diferentes alternativas
- Para el siguiente año, el IETF determinó que una nueva generación de Protocolos de Internet (IP) era requerida: IPng (next generation)
- En 1994, entre las diferentes posibles soluciones (CATNIP, SIPP, TUBA), SIPP (Simple Internet Protocol Plus) evolucionó a IPv6
- En 1998 se publicó el primer juego de estándares maduros (RFC 2460, 2461, etc.).

IPv6 history (cont)

Los problemas atacados fueron principalmente:

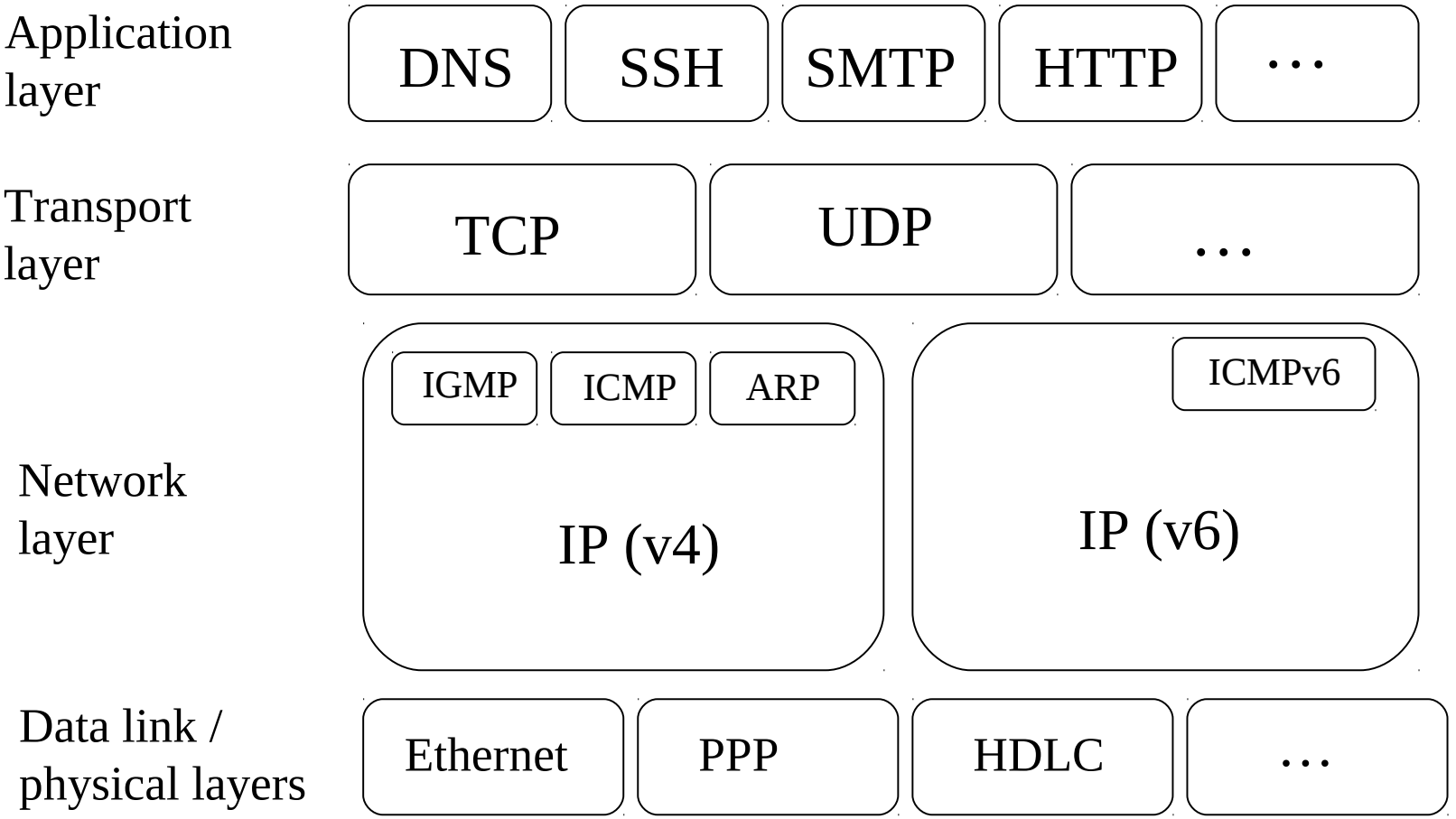
- *Escala*
  - Espacio de direcciones mayor
  - Soporte de ruteo jerárquico
- *Funcionalidad*
  - Seguridad
  - Autoconfiguration (plug-n-play)
  - Quality of service
  - Mobility

IPv6 history (cont)

Tamaño del campo de dirección...

- ***Algunos sugirieron usar 64 bits para las direcciones***
  - Cumple los requisitos impuestos a IPng
  - Minimiza el overhead
  - Procesamiento eficiente por software
- ***Otros sugirieron direcciones de 160 bits, de longitud variable***
  - Compatible con OSI NSAP
  - Autoconfiguración basada en IEEE 802
  - Permitía el crecimiento gradual de las direcciones
- ***IPv6 se diseñó con direcciones de 128 bits***

Stacks de referencia de IPv4 e IPv6



IP(v6) terminology

Node: dispositivo IPv6

Router: Node nodo que *forwardea* paquetes IPv6

Host: Un nodo que no es un router

Neighbors(vecinos): nodos conectados al mismo link

Interface: conexión del nodo al link

Address: valor asignado a una interfaz IPv6 de un nodo

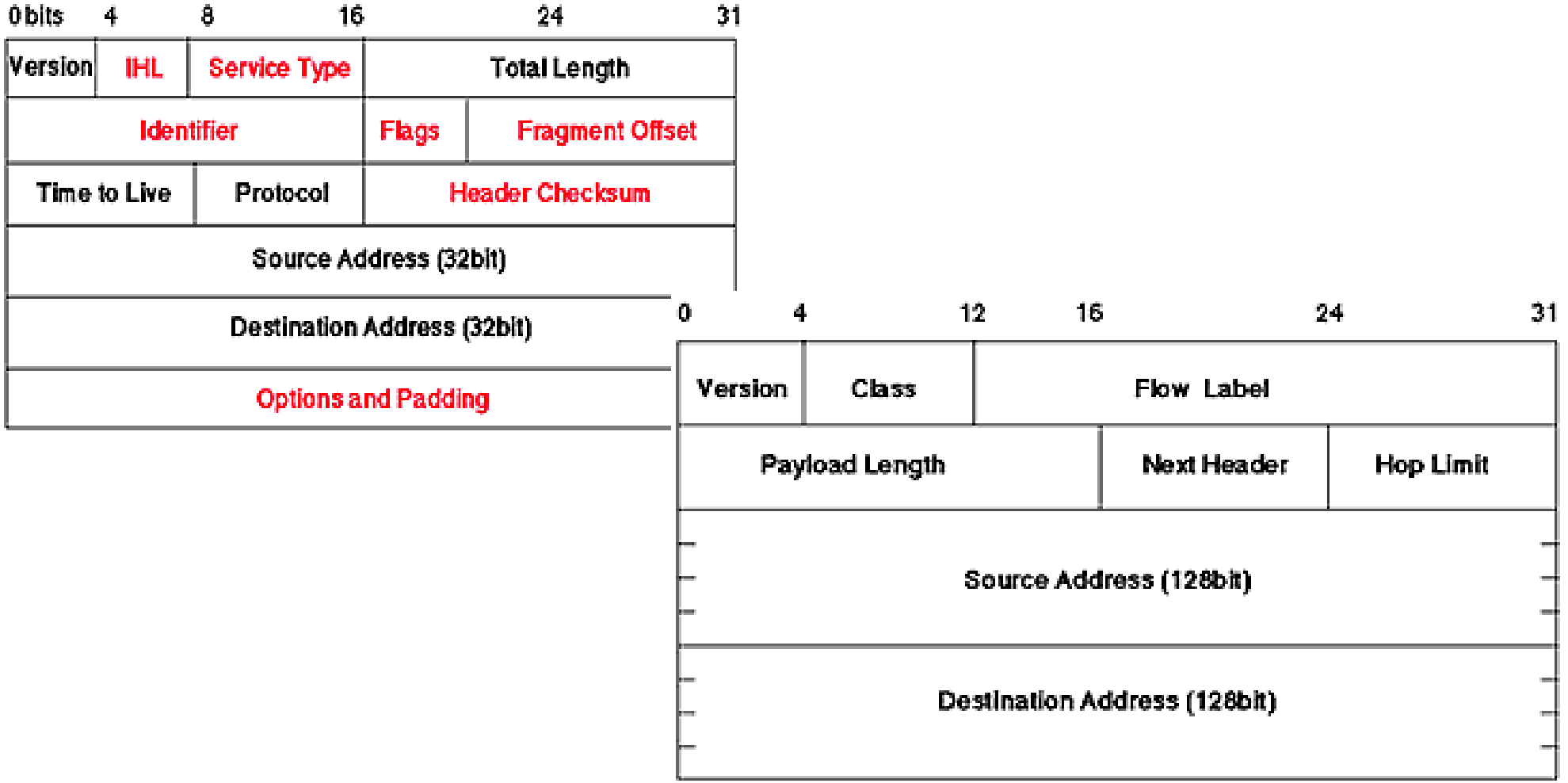
Packet: mensaje IPv6 (cabezal IPv6 + datos)

Link MTU: Maximum Transmission Unit del link

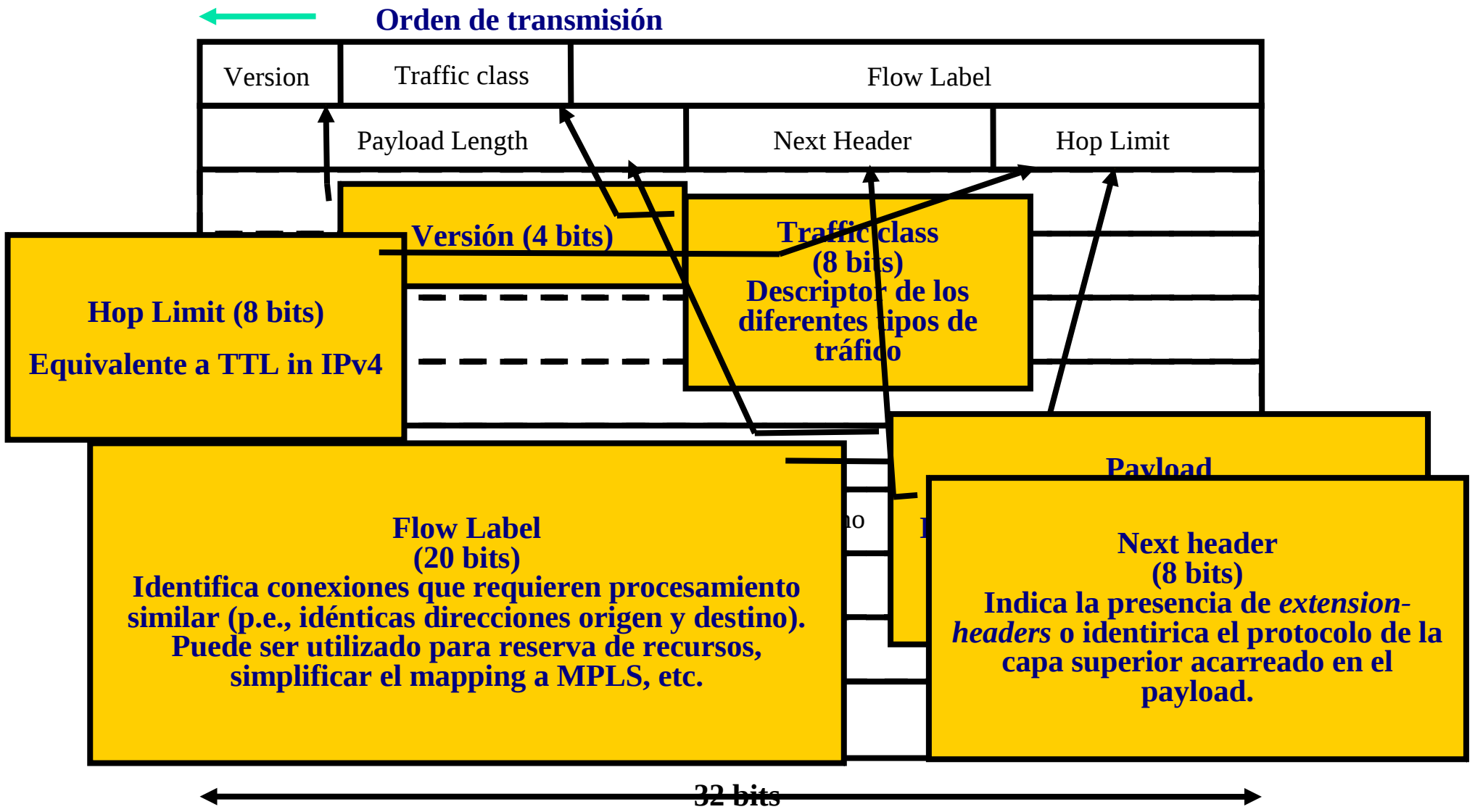
Path MTU: mínimo Link MTU a lo largo del camino entre dos nodos

Formato del cabezal IPv6

Cabezales de IPv4 e IPv6



IPv6 header


Orden de transmisión
Version
Traffic class
Flow Label
Payload Length
Next Header
Hop Limit
Versión (4 bits)
Traffic class
(8 bits)
Descriptor de los diferentes tipos de tráfico
Hop Limit (8 bits)
Equivalente a TTL in IPv4
Payload
Flow Label
(20 bits)
Identifica conexiones que requieren procesamiento similar (p.e., idénticas direcciones origen y destino).
Puede ser utilizado para reserva de recursos, simplificar el mapping a MPLS, etc.
Next header
(8 bits)
Indica la presencia de *extension-headers* o identirica el protocolo de la capa superior acarreado en el payload.
32 bits

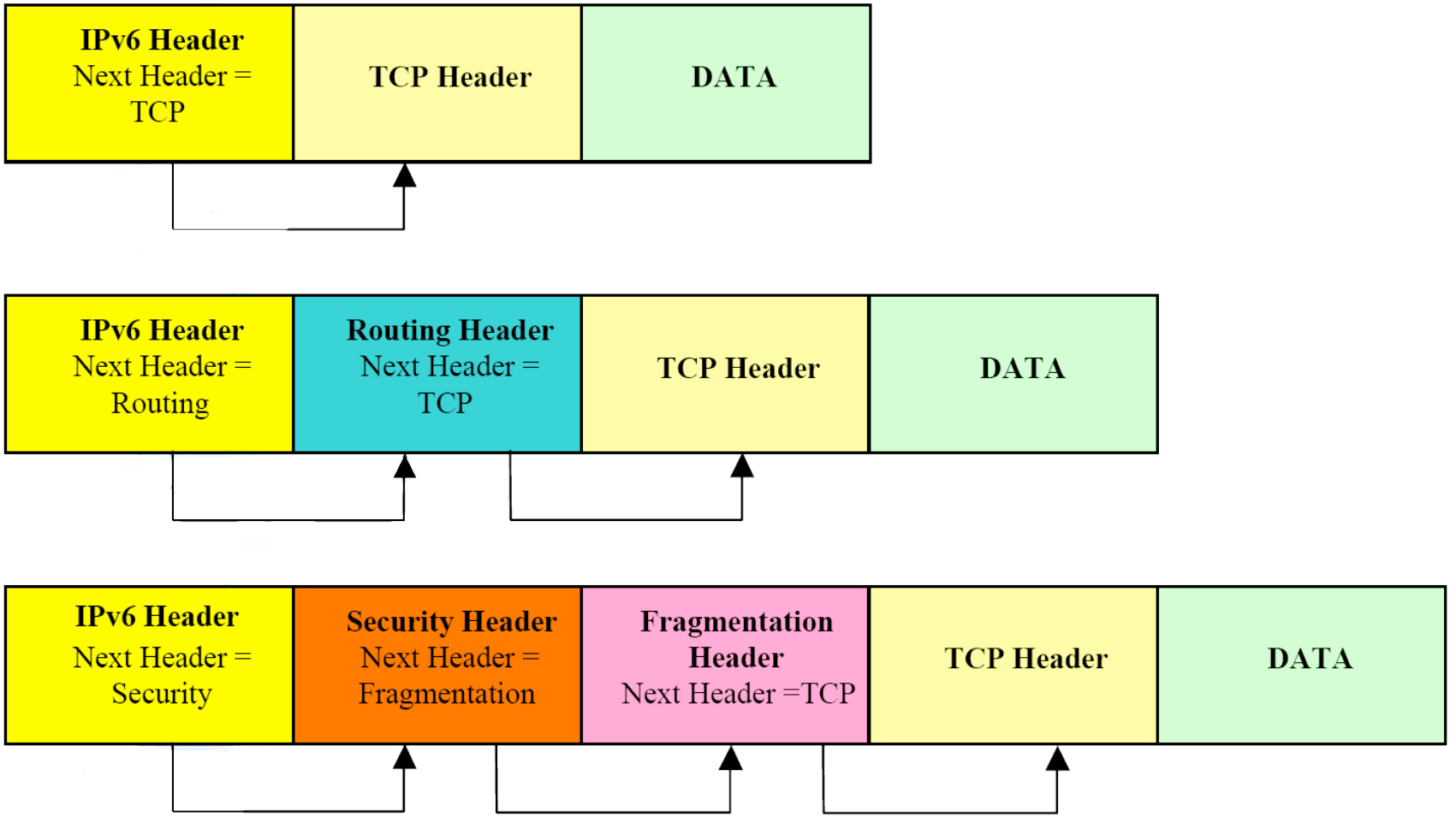
Cambios principales en el cabezal IPv6

- Largo fijo: 40 bytes
- Direcciones de 128 bits
- Se elimina la fragmentación y las opciones
- El largo solamente indica el payload efectivo
- Nuevo campo: flow label
- TOS -> Traffic Class
- Protocol -> Next Header
- Time to live -> Hop Count

IPv6 extension headers

- Las “opciones” son manejadas a través de *extension headers*
- Los headers son “enganchados” utilizando el campo Next Header
- Los valores son interoperables con los valores utilizados por el protocolo IPv4 (i.e. TCP = 6, UDP = 17 , etc.)
- Extension headers:
  - Hop-by-hop header (NH=0)
  - Routing header (NH=43)
  - Fragment header (NH=44)
  - Authentication header (NH=51)
  - Encapsulated security payload (NH=50)
  - Destination option (NH=60)

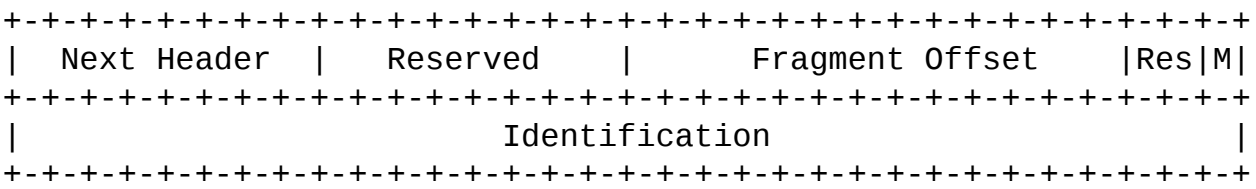
IPv6 extension headers



Fragmentation header

- Solamente se realiza fragmentación end-to-end (no se realiza en routers intermedios)
- Path MTU discovery algorithm
- IPv6 requiere un link MTU de al menos 1280 bytes para cualquier link, entonces, 1280 is también un posible valor para el path MTU
- El payload máximo es de 65536 bytes (MTU = Payload + header length)

Fragmentation header



Next Header	8-bit selector. Identifies the initial header type of the Fragmentable Part of the original packet (defined below). Uses the same values as the IPv4 Protocol field [RFC-1700 et seq.].
Reserved	8-bit reserved field. Initialized to zero for transmission; ignored on reception.
Fragment Offset	13-bit unsigned integer. The offset, in 8-octet units, of the data following this header, relative to the start of the Fragmentable Part of the original packet.
Res	2-bit reserved field. Initialized to zero for transmission; ignored on reception.
M flag	1 = more fragments; 0 = last fragment.
Identification	32 bits is used for facilitating each fragment is correctly reassembled at the receiver.

IPv6 addresses

Tipos de direcciones IPv6

- 128 bit addresses
- Tres tipos diferentes (además de rangos reservados):
  - ***Unicast***

    Identifican exactamente una interfaz
  - ***Multicast***

    Identifican a un grupo de interfaces. Un paquete enviado a una dirección de multicast es entregado a todos los miembros del grupo.
  - ***Anycast***

    Un paquete enviado a una dirección anycast es entregado al miembro *"más próximo"* del grupo.

Direcciones unicast IPv6

- ***Unicast*** **- (actualmente RFC 4291)**
  - global
  - link-local
  - site-local (deprecated)
  - Unique Local (ULA)
  - IPv4 compatible (deprecated)
  - IPv4 mapped

Númerso sobre las direccioens IPv6

- 340:282.366:920.938:463.463:374.607:431.768:211.456 direcciones diferentes
- 2^{96} veces más direcciones que en IPv4
- Nuestro planeta tiene aprox. 511:263.971:197.990 m^2

  ergo, disponemos de 655.570:793.384:866.943:898.599 direcciones por m^2
- Una esquema pesimista de asignación de direcciones realizada de forma jerárquica nos daría 1.564 addr / m^2
- Una esquema optimista nos daría 3:911.873:538.269:508.102 addr / m^2

Representando direcciones IPv6

Los 128 bits de una dirección IPv6 se notan como ocho enteros de 16 bits, en notación hexadecimal, separados por dos puntos (:).

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

IPv6 address: notación comprimida

El RFC 4291 define diferentes convenciones que permiten acortar la escritura de las direcciones:

- Los ceros a la izquierda (de cada entero) pueden ser omitidos

000F:000E:000D:000C:0003:0002:0001:0000

F:E:D:C:3:2:1:0

IPv6 address: notación comprimida

Un único juego de enteros con el valor cero puede ser abreviado mediante dos dos puntos

FEDC:BA98:0:0:0:0:1234:5678

FEDC:BA98::1234:5678

Se puede ver también la falta de unicidad de esta regla:

2001:0:0:0:2:0:0:3

2001:0:0:0:2::3

2001::2:0:0:3

IPv6 address: notación comprimida

Cuando las direcciones Ipv4 se convierten a IPv6 agregando un prefijo de 96 ceros, pueden (por simplicidad) ser escritas utilizando la notación decimal con puntos standard de IPv4

::164.73.32.2

instead of

::A449:2002

Este método es llamado “IPv4 compatible” y ha sido deprecado desde el RFC4291.

IPv6 address: notación comprimida

Cuando las direcciones IPv4 se convierten en direcciones IPv6 agregando un prefijo compuesto por 80 ceros y 16 unos, pueden ser escritas utilizando la notación decimal con puntos, como en IPv4

::FFFF:164.73.32.2

en vez de

::FFFF:A449:2002

Este método es llamado “IPv4 mapped” y es propuesto como reemplazo de las direcciones “IPv4 compatible”

Direcciones IPv6 dentro de URLs

Si debiésemos escribir direcciones IPv6 dentro de una URL, deben escribirse dentro de paréntesis rectos

http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]/index.html

Hay que configurar bien los servidores de DNS ;-)

IPv6 address: notación comprimida

Los prefijos son escritos utilizando la misma notación con barra que en IPv4 *(slashed notation)*:

FEDC:BA98:7600::/40 es una dirección de red con un prefijo de 40 bits

Direcciones IPv6 especiales (RFC 5156)

Unspecified address: pueded ser utilizada únicamente por un nodo que aún no tiene una dirección, y su valor es "0:0:0:0:0:0:0:0", pudiendo ser abreviada -aún más- como "::" o "::/128"

Loopback address: utilizada -como en IPv4- para enviar datagramas IPv6 al propio host. El valor de la dirección es el "0:0:0:0:0:0:0:1" se abrevia como "::1" o "::1/128"

Direcciones IPv6 especiales (RFC 5156)

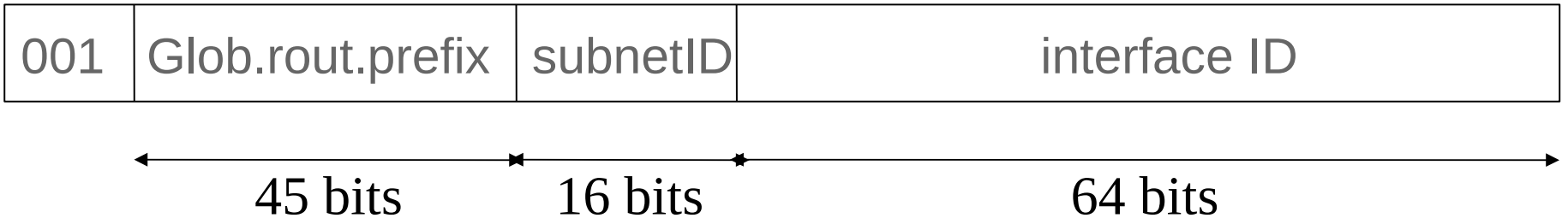
Default route: requerida para especificar el ruteo por defecto en las tablas de ruteo. Se representa por “0:0:0:0:0:0:0:0/0” y se abrevia como “::/0”

IPv6 address space

http://www.iana.org/assignments/ipv6-address-space

IPv6 Prefix	Allocation	Reference	
0000::/8	Reserved by IETF	[RFC4291]	
0100::/8	Reserved by IETF	[RFC4291]	
0200::/7	Reserved by IETF	[RFC4048]	
0400::/6	Reserved by IETF	[RFC4291]	
0800::/5	Reserved by IETF	[RFC4291]	
1000::/4	Reserved by IETF	[RFC4291]	
2000::/3	**Global Unicast**	**[RFC4291]**	
4000::/3	Reserved by IETF	[RFC4291]	
6000::/3	Reserved by IETF	[RFC4291]	
8000::/3	Reserved by IETF	[RFC4291]	
A000::/3	Reserved by IETF	[RFC4291]	
C000::/3	Reserved by IETF	[RFC4291]	
E000::/4	Reserved by IETF	[RFC4291]	
F000::/5	Reserved by IETF	[RFC4291]	
F800::/6	Reserved by IETF	[RFC4291]	
FC00::/7	**Unique Local Unicast**	**[RFC4193]**	
FE00::/9	Reserved by IETF	[RFC4291]	
FE80::/10	**Link Local Unicast**	**[RFC4291]**	
FEC0::/10	Reserved by IETF	[RFC3879]	site local
FF00::/8	**Multicast**	**[RFC4291]**	

Global Unicast Address (RFC 3587)



Global routing prefix: es el valor asignado a un sitio. Jerárquicamente, RIRs (Retional Internet Registry) e ISPs (Internet Service Providers)

Sub-net ID: Identificaror de red dentro de un site, utilizado por los RIRs e ISPs para administrar y asignar el espacio de direcciones

Interface ID: usualmente construida utilizando EUI-64

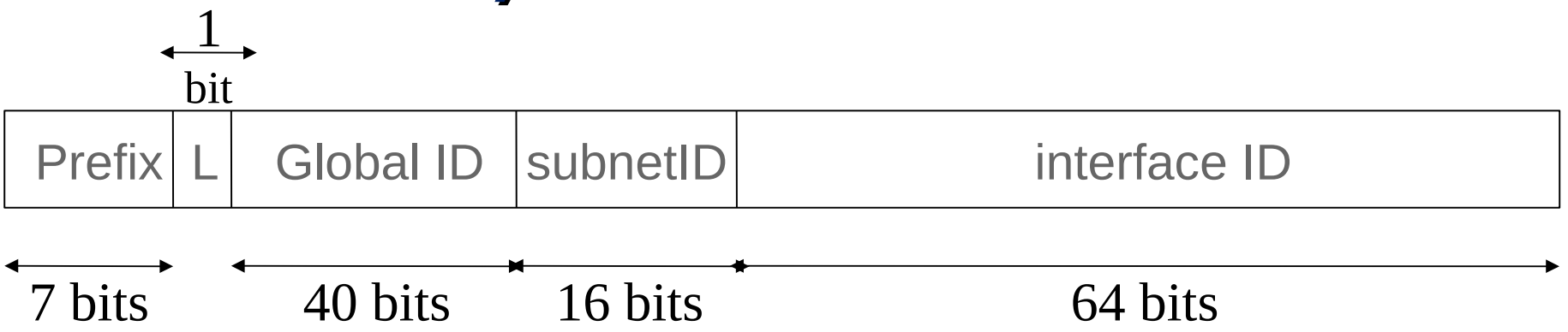
Unique Local IPv6 Unicast Addresses – IPv6 ULA (RFC 4193)

- Prefijo local (FC00::/7), sin garantías de unicidad, pero alta probabilidad (altísima segun Murphy)
- Reservadas para comunicaciones locales, normalmente dentro del site.
- Non reuteables a través de Internet.
- Pueden ser ruteables en un entorno más restringido (dentro de un sitio o una compañía)
- Prefijos bien conocidos (*Well-known* prefixes) que pueden ser filtrados fácilmente en el borde.

IPv6 ULA (RFC 4193) - (cont)

- ISP independientes pueden usarlos dentro de sitios con o sin acceso a Internet.
- Tráfico no filtrado que se “escape”, no causa daño (o al menos es menor)
- Las aplicaciones pueden usar estas direcciones como globales.

Formato IPv6 ULA format (RFC 4193)



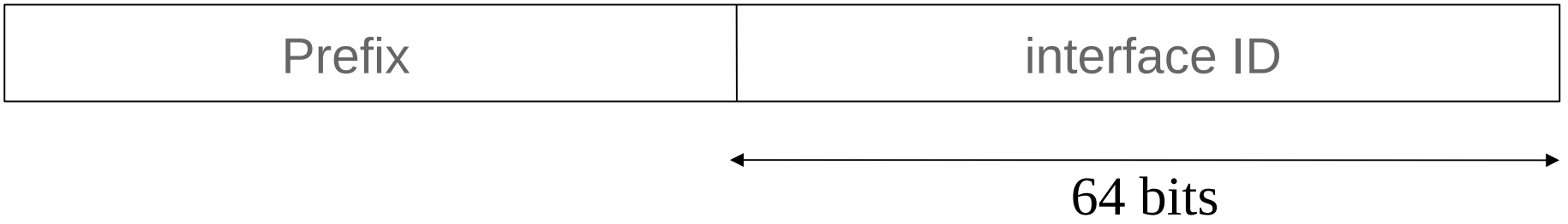
FC00::/7 prefix

L = 1 significa asignación local

L = 0 reservado para uso futuro, de acuerdo al RFC, habilitando la asignación central de direcciones.

Global ID debería ser creado de forma aleatoria para minimizar la probabilidad de colisiones

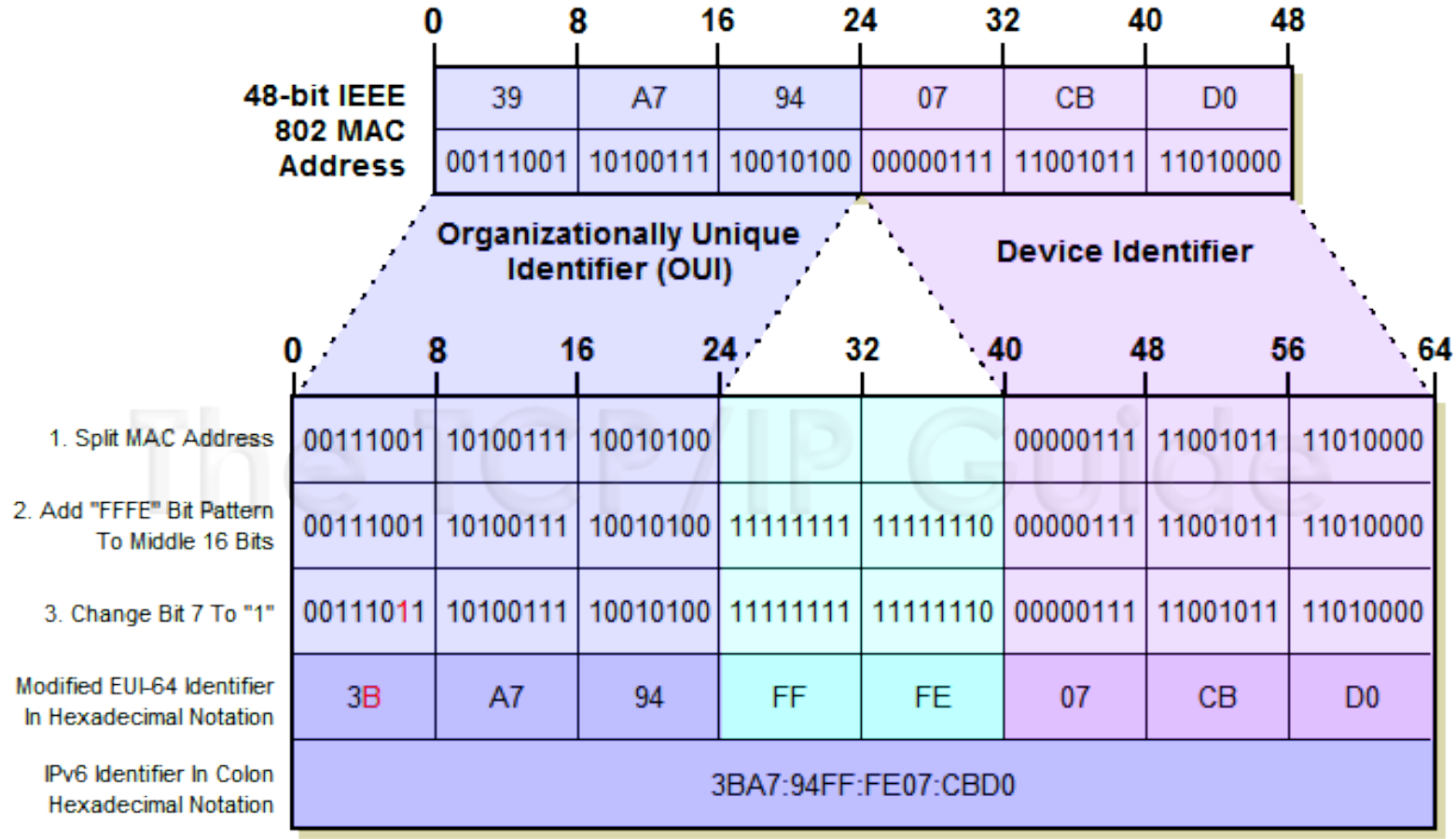
Interface ID



Los 64 bits de más a la derecha (“rightmost” 64 bits) de una dirección IPv6 unicast, que puede ser asignada a través de diferentes vias:

- autoconfiguration (modified EUI-64)
- DHCPv6
- configuración manual
- aleatoriamente
- futuros métodos

Interface ID – EUI 64 modificado



64-Bit IPv6 Modified EUI-64 Interface Identifier

http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm

Direcciones IPv6 obligatorias - Host

- Una dirección Link-local para cada interfaz (más toda otra dirección unicast o anycast manual o automáticamente configurada)
- Loopback address
- Direcciones de múlticast All-nodes (FF01::1 y FF02::1)
- Dirección de múlticast Solicited-Node para cada dirección unicast y anycast
- Direcciones de múlticast para todos los grupos a los que pertenezca el nodo

Direcciones IPv6 obligatorias - Router

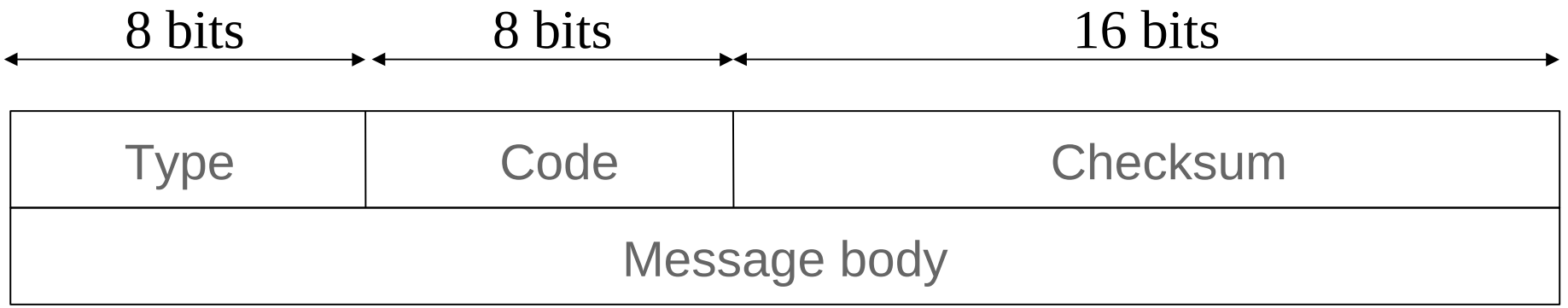
- Todas las direcciones de un host
- Dirección de anycast Subnet-router para todas las interfaces utilizadas para hacer forwarding de paquetes
- Toda otra dirección anycast configurada
- Direcciones de red múlticast All-routers (FF01::2 and FF02::2)

ICMPv6

ICMPv6 – (RFC4443)

- Obsoletes RFC2463, publicado en 1998, actualizado por el RFC4884
- Misma filosofía que en el ICMP para IPv4 (RFC 792), actualizado para IPv6
- Uses NextHeader value 58 (no se usa el valor 1 de ICMPv4)
- ICMPv6 es obligatorio (a MUST) en la suite de protocolos y debe ser completamente implementado por todo nodo
- ICMPv6 se utiliza para reportar errores a IPv6 y realizar pruebas (like ping6)

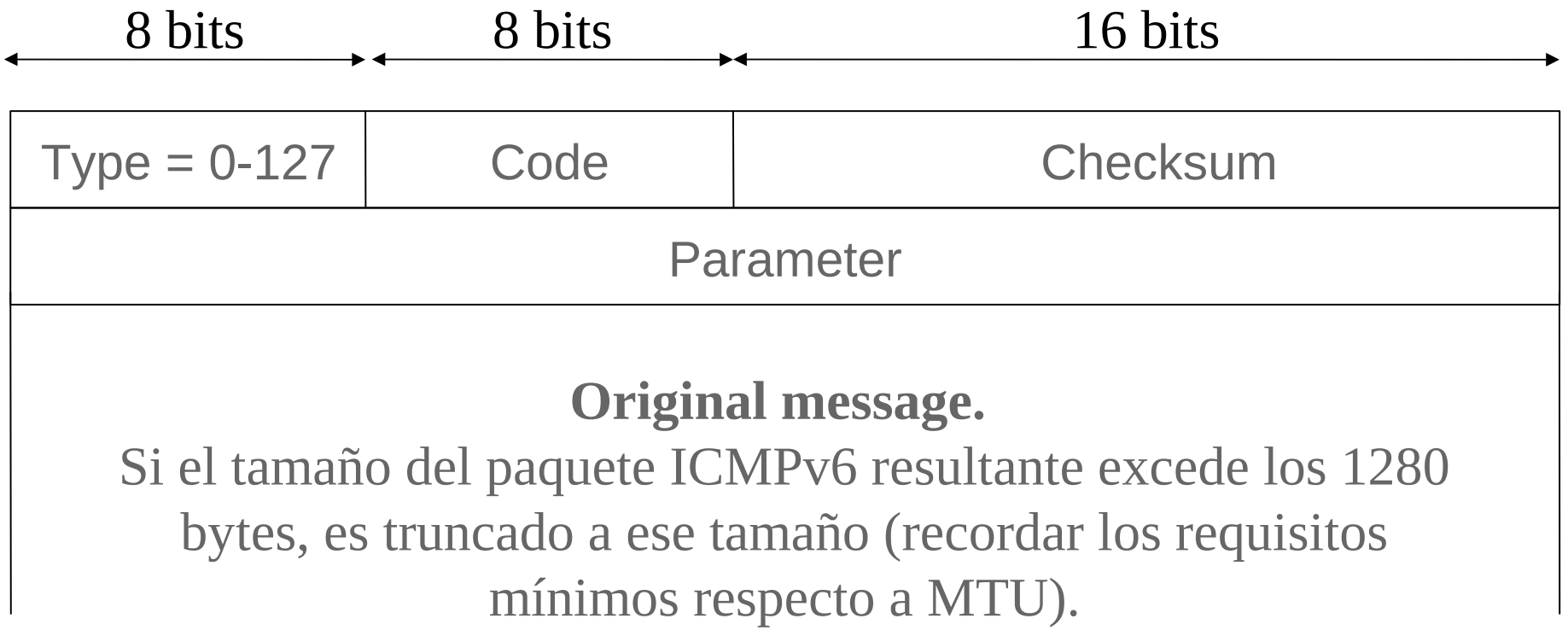
ICMPv6 Messages



Two classes:

- Error messages (types 0 to 127)
- Informative messages (types 128 to 255)

ICMPv6 error messages



Algunos mensajes de error ICMPv6

Destination unreachable message (type 1, parameter 0), code:

0 – No route to destination

1 – Communication with the destination administratively prohibited

2 – Beyond scope of source address

3 – Address unreachable

4 – Port unreachable

5 – Source address failed ingress/egress policy

6 – Reject route to destination

Algunos mensajes de error ICMPv6 (cont)

Packet too big message (type 2, code 0, parameter = next-hop MTU).

Time exceeded message (type 3, parameter = 0), code:

0 – Hop limit exdeeded in transit

1 – Fragment reassembly time exceeded

Parameter problem message (type 4), code:

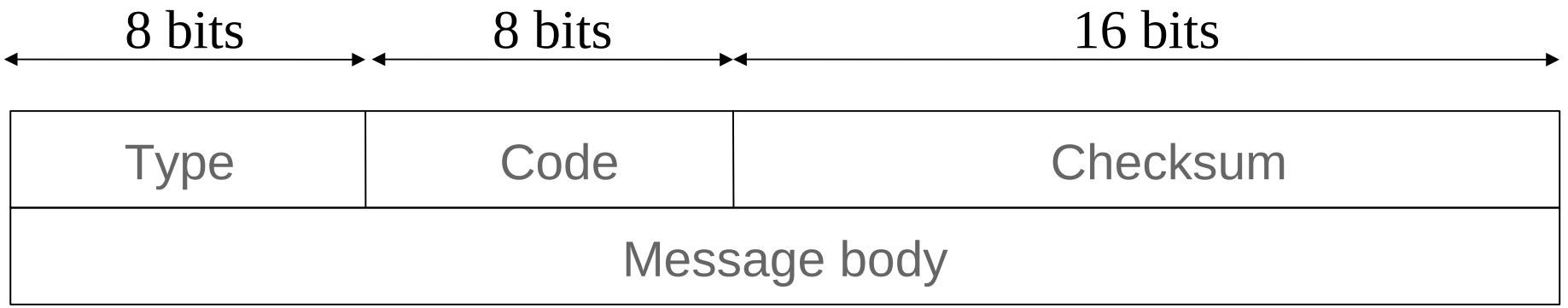
0 – Erroneous header field

1 – Unrecognized Next Header type

2 – Unrecognized IPv6 option

parameter field (called pointer) identifica el desplazamiento (offset) en bytes dentro del paquete original donde el error fue detectado

Algunos mensajes ICMPv6 informativos



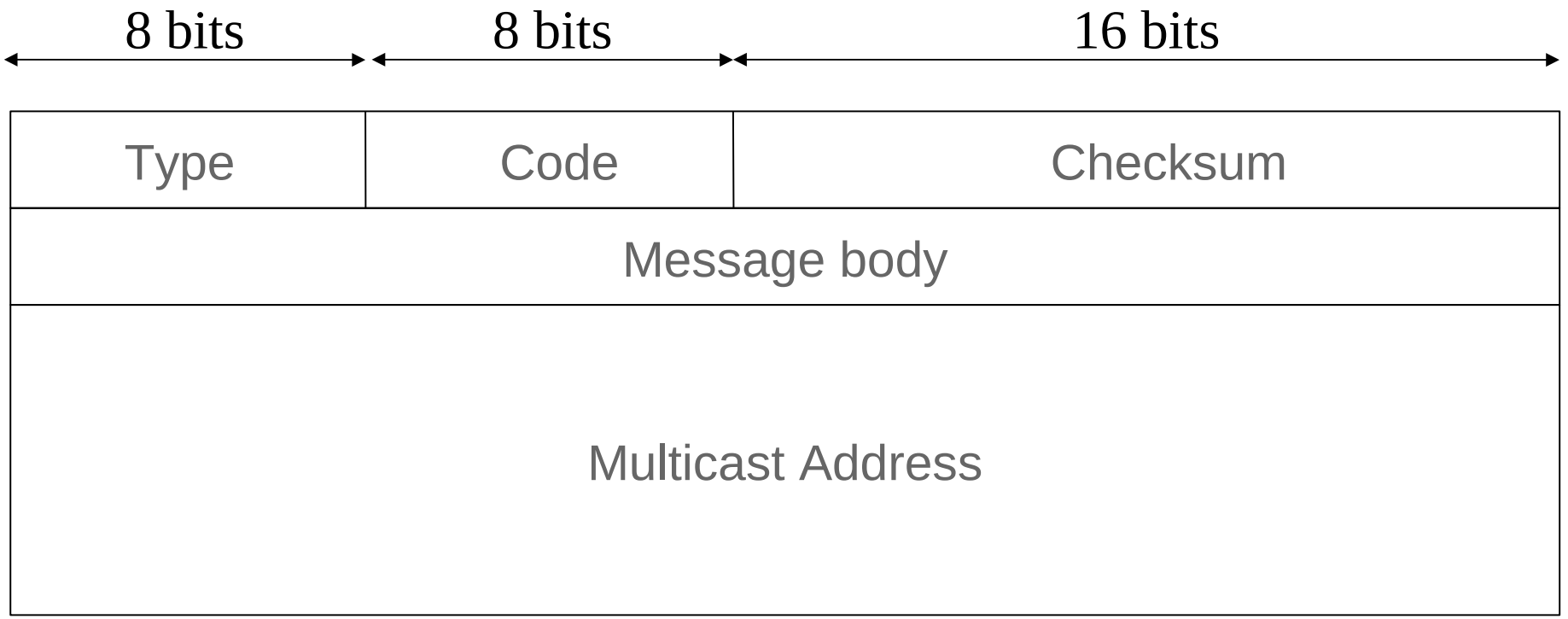
ping6

ICMPv6 Echo Request message (type 128, code 0)

ICMPv6 Echo Reply message (type 129, code 0)

Algunos mensajes ICMPv6 informativos

(cont)



Multicast Listener Discovery (MLD) Messages:

Query, report, done (as IGMP for IPv4)

Neighbor discovery

Neighbor Discovery ND

- Originalmente, RFC2461, publicado en 1998 definió el protocolo. Ahora ha sido actualizado por el RFC4861.
- Los nodos usan ND para determinar las direcciones de enlace (*data link layer address o* MAC address) de los nodos pertenecientes al mismo segmento de red.
- Los hosts utilizan también ND para encontrar los routers vecinos.
- ND es un elemento central de la autoconfiguración en IPv6.

Mensajes ND

ND define 5 tipos diferentes de paquetes:

- Router Solicitation (RS)
- Router Advertisement (RA)
- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- Redirect

ND – Router Advertisements

- En enlaces de acceso múltiple (i.e. IEEE 802 family), cada router periódicamente envía mensajes múlticast del tipo RA.
- Los hosts del link reciben los RA de todos los routers del link, construyendo sus propias tablas de ruteo (quizás con varias rutas por defecto “`::/0`”)
- Neighbor Unreachability Detection (NUD) es utlizando para detectar problemas de conectividad con los routers.

ND – Router Advertisements (cont)

- RA llevan la lista de prefijos asignados al link. La lista debe ser utilizada por los hosts en el link para autoconfigurar sus direcciones correspondientes, basadas en los prefijos recibidos.
- Hay diferentes flags presentes en los RA, asociadas a cada prefijo para permitir a cada router indicar como realizar la autoconfiguración (stateless o a través de DHCPv6)

ND – Neighbor Solicitation

- Los nodos envían mensajes NS para determinar dinámicamente el mapping IPv6 – MAC mapping.
- NS utiliza múlticast cuando el nodo necesita resolver una dirección y únicast para determinar alcance (reachability)
- NS reemplaza los mensajes “ARP request” de IPv4, brindando características mejoradas y teniendo mejor integración con la suite IPv6.

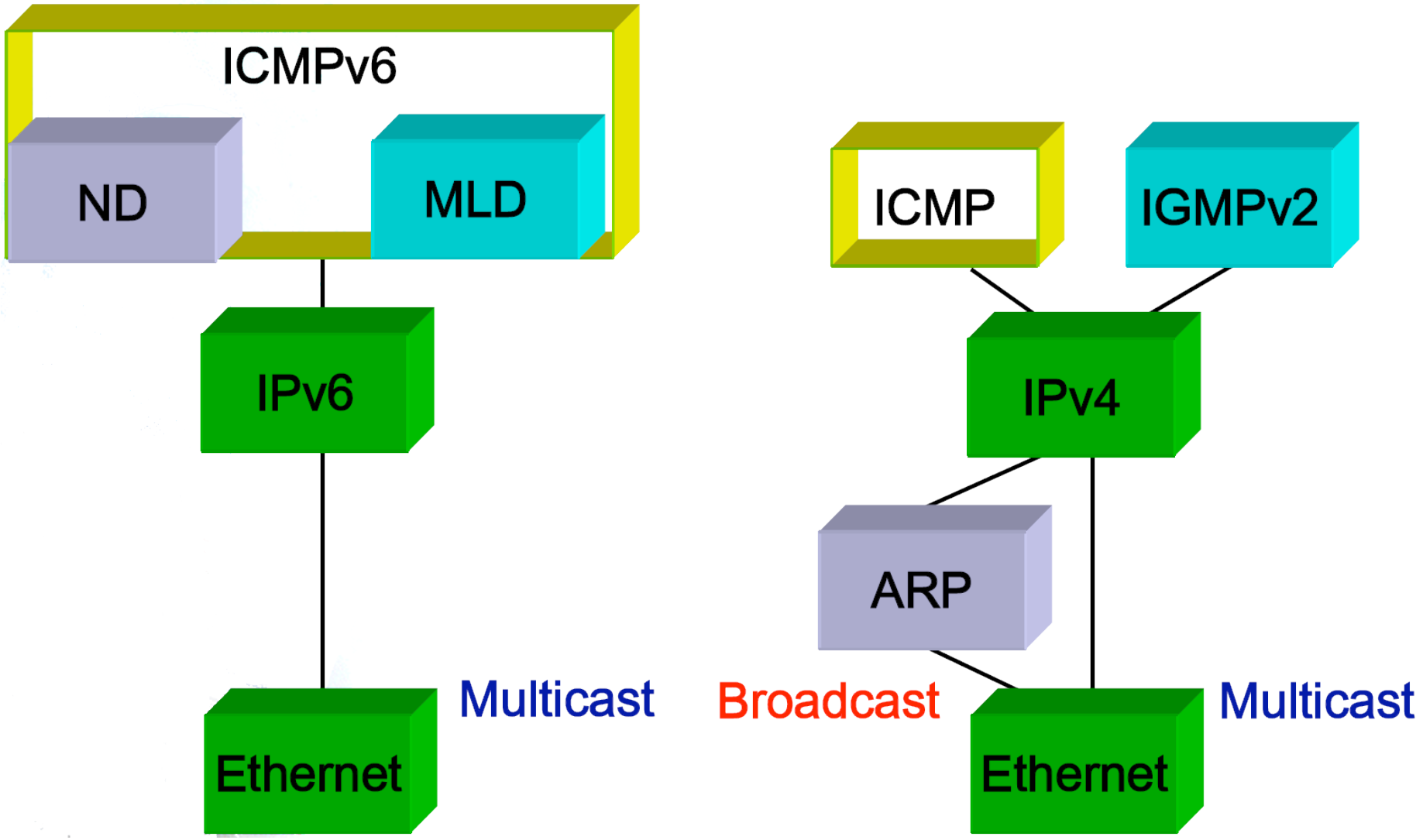
ND – Neighbor Advertisement

- Los nodos envían NA para responder a NS
- Los nodos también pueden enviar NS no solicitadas (unsolicited NS) a los efectos de propagar nueva información rápidamente.

ND – Redirect

- Los routers deben enviar paquetes de redirect para informar que existen *“mejores routers”* para destinos particulares.
- Los mensajes de redirect también pueden ser utilizados para informar a un host que el destino es un vecino.

IPv6 vs. IPv4 control planes



Mecanismos de transición

¿por y para qué?

- Internet existe, anda y corre en IPv4.
- No podemos cambiar la red en una noche (¿no podemos? - Ver campaña 1/1/11 [homework])
- Mientras hacemos los cambios requeridos, IPv4 e IPv6 deben coexistir
- No solamente los protocolos deben ser considerados, sino, toda la infraestructura construída sobre éstos

Esquemas de Transición

- Varias técnicas diferentes han sido diseñadas y pueden ser agrupadas en:
  - Dual-stack
  - Tunneling
  - Translation
- Estos mecanismos pueden ser utilizados simultáneamente.

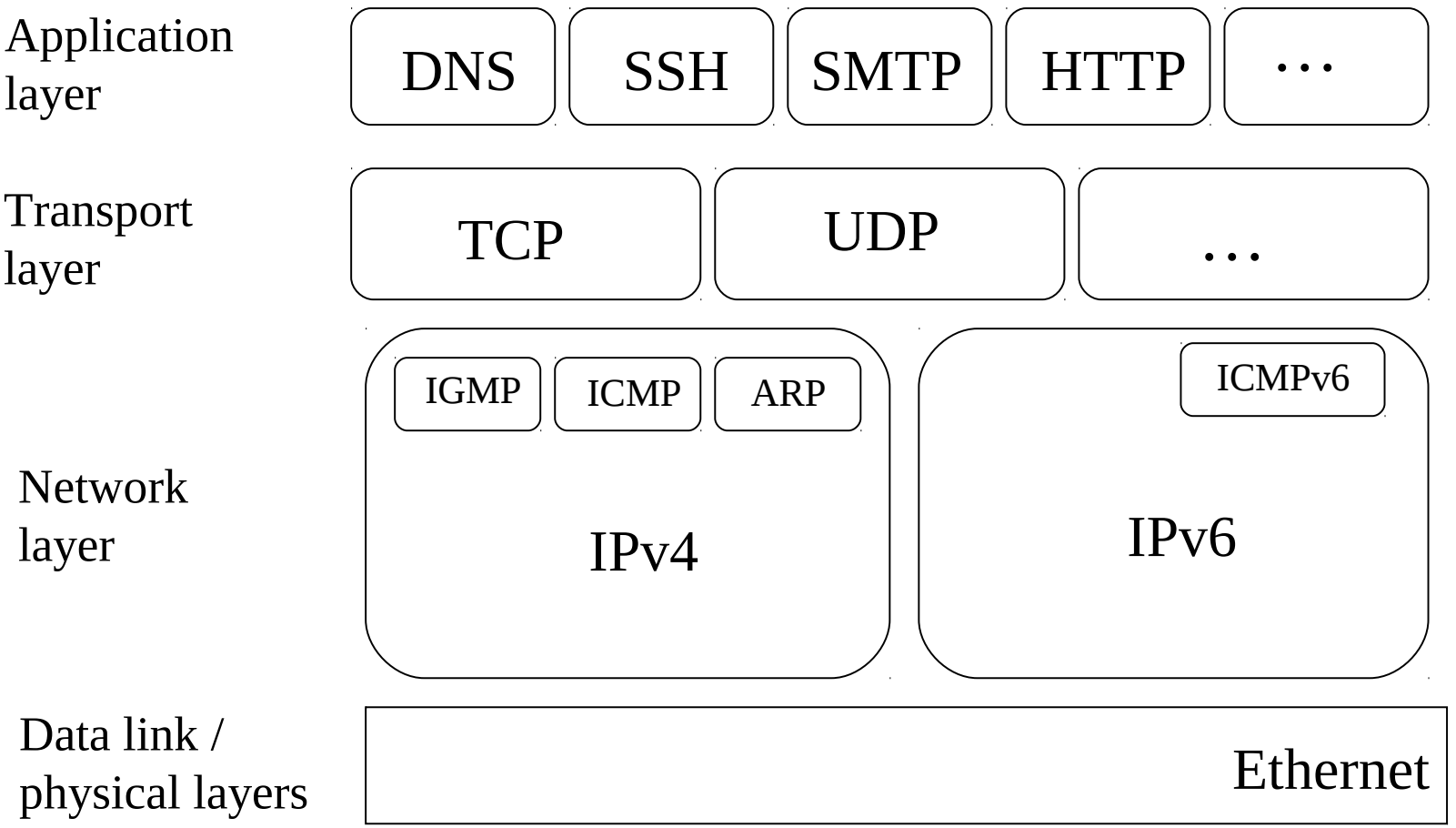
Dual Stack

- IPv6 puede ser agregado a cualquier dispositivo que hable IPv4.
- Los protocolos son multiplexados y de-multiplexados sobre los mismos enlaces (i.e. IEEE 802 family) utilizando diferentes números de protocolo en un una misma posición del frame
- Misma técnica a la utilizada para mezclar IPX, Appletalk, TCP, etc.

Dual Stack (cont)

- Es un problema de la aplicación elegir cual protocolo utilizar (i.e. si una respuesta a una consulta DNS contiene registros AAAA, entonces preferir TCP sobre IPv6 como transporte)
- Esto habilita una transición paulatina, permitiendo a los desarrolladores actualizar gradualmente sus aplicaciones
- Lenguajes como Java permiten la utilización de objetos de tipo InetAddress, generalizaciones de Inet4Address e Inet6Address, haciendo su manejo independiente del protocolo.

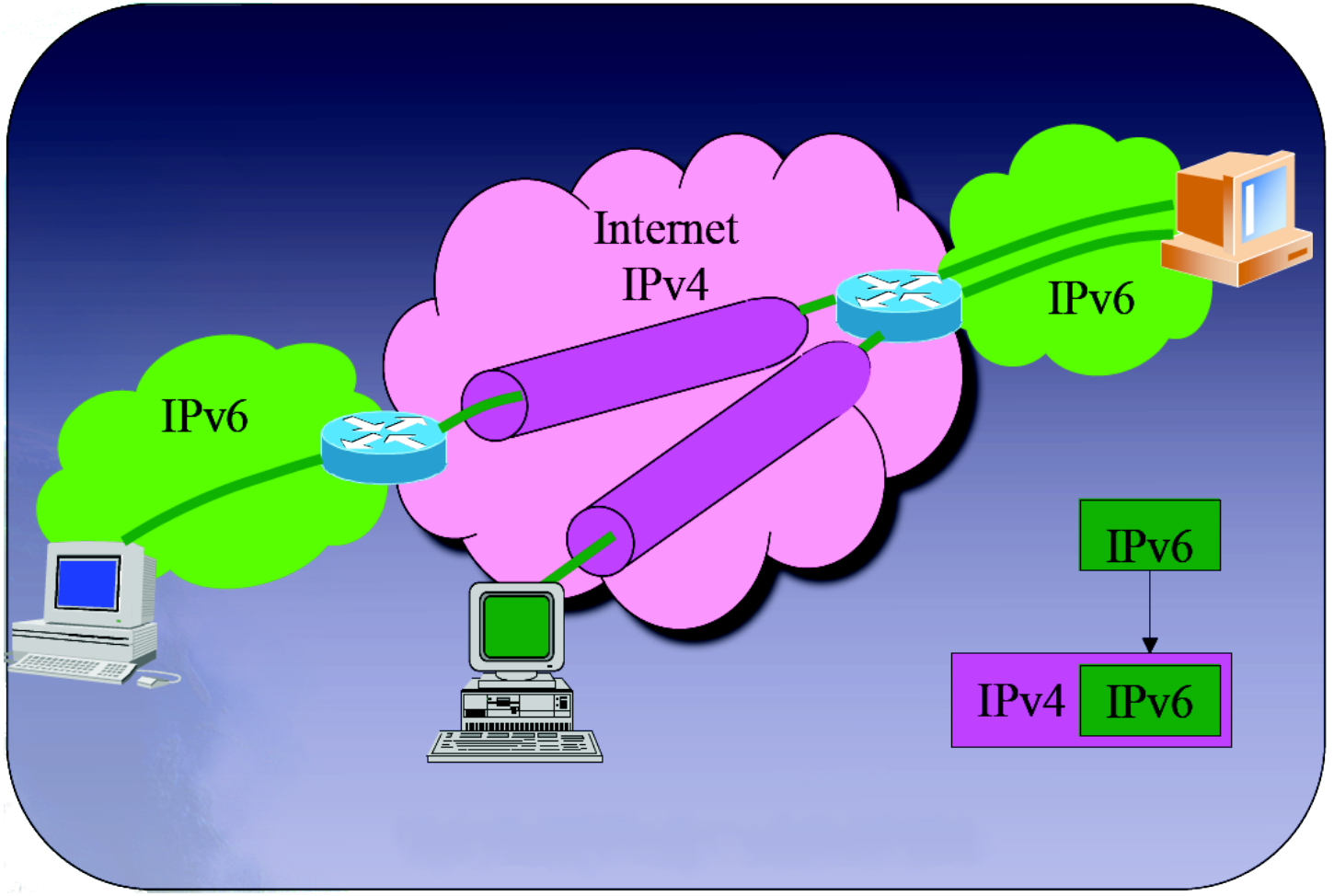
Dual stack schema



Tunneling

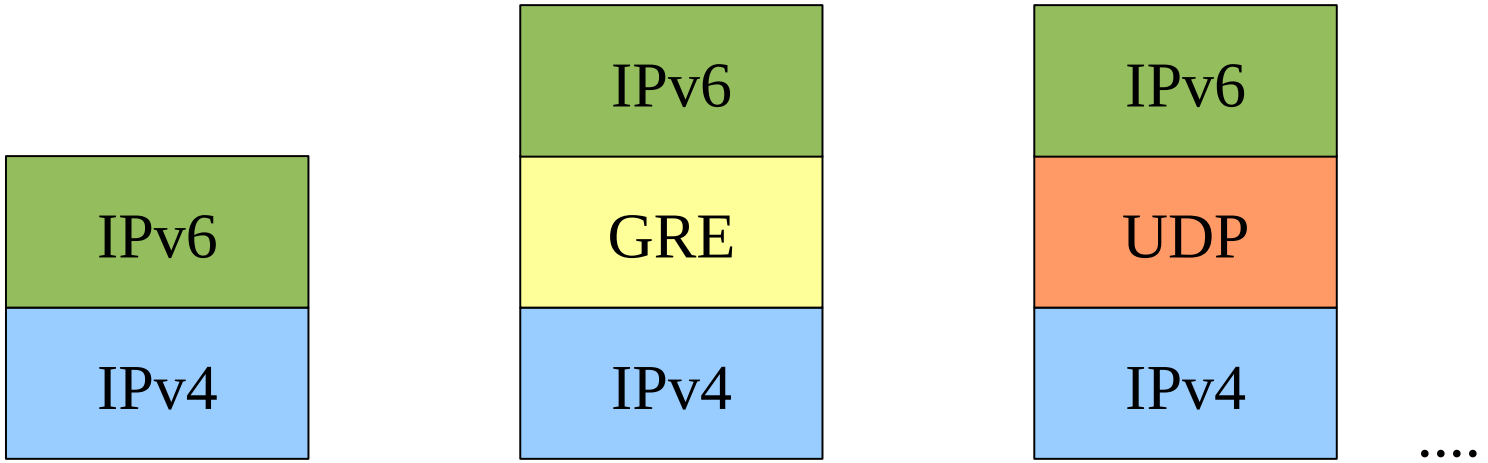
- Utilizamos el tunneling para “ocultar” tráfico IPv6 dentro de tráfico IPv4. De esta forma podemos cruzar secciones de Internet que nos son *IPv6 Ready* aún.
- Los paquetes IPv6 se encapsulan en paquetes IPv4, que pueden tratarse como tráfico IPv4 standard.
- Conceptualmente, puede pensarse como:
  - IPv6 utilizando IPv4 como una capa de enlace virtual
  - Una VPN IPv6 configurada sobre la Internet IPv4

Tunneling – Concepto gráfico



Conceptos de Tunneling

- Hay distintas formas de poner IPv6 en IPv4



Mecanismos de Tunneling

- Existe una amplia variedad de tecnologías, algunas de ellas son:
- 6in4
- TB
- TSP
- 6to4
- Teredo
- 6over4
- AYIYA
- DSTM
- .....

Tunneling: 6in4 (RFC 4213)

- Encapsulamiento directo de IPv6 sobre IPv4 utilizando el protocolo IP número 41
- Comunmente utilizado para conectar:
- End-node → router
- Router → router
- También es posible utilizarla para realizar conexiones del tipo end-node → end-node connections
- El tunel es considerado como un link point-to-point, contabilizado como un único hop

Tunneling: 6in4 (RFC 4213) (cont)

- Las direcciones IPv6 en ambos extremos del nodo tienen el mismo prefijo
- 6in4 requires configuración manual
- Todas las conexiones IPv6 del end-node son tunelizadas y ruteadas a través del router al final del tunel
- Se requiere tener el forwarding del protocolo 41 habilitado a lo largo de todo el camino entre los extremos del tunel
- Puede ser iniciado detrás de un NAT, dado que implemente protocol 41 forwarding

Tunneling: TB (RFC 3053)

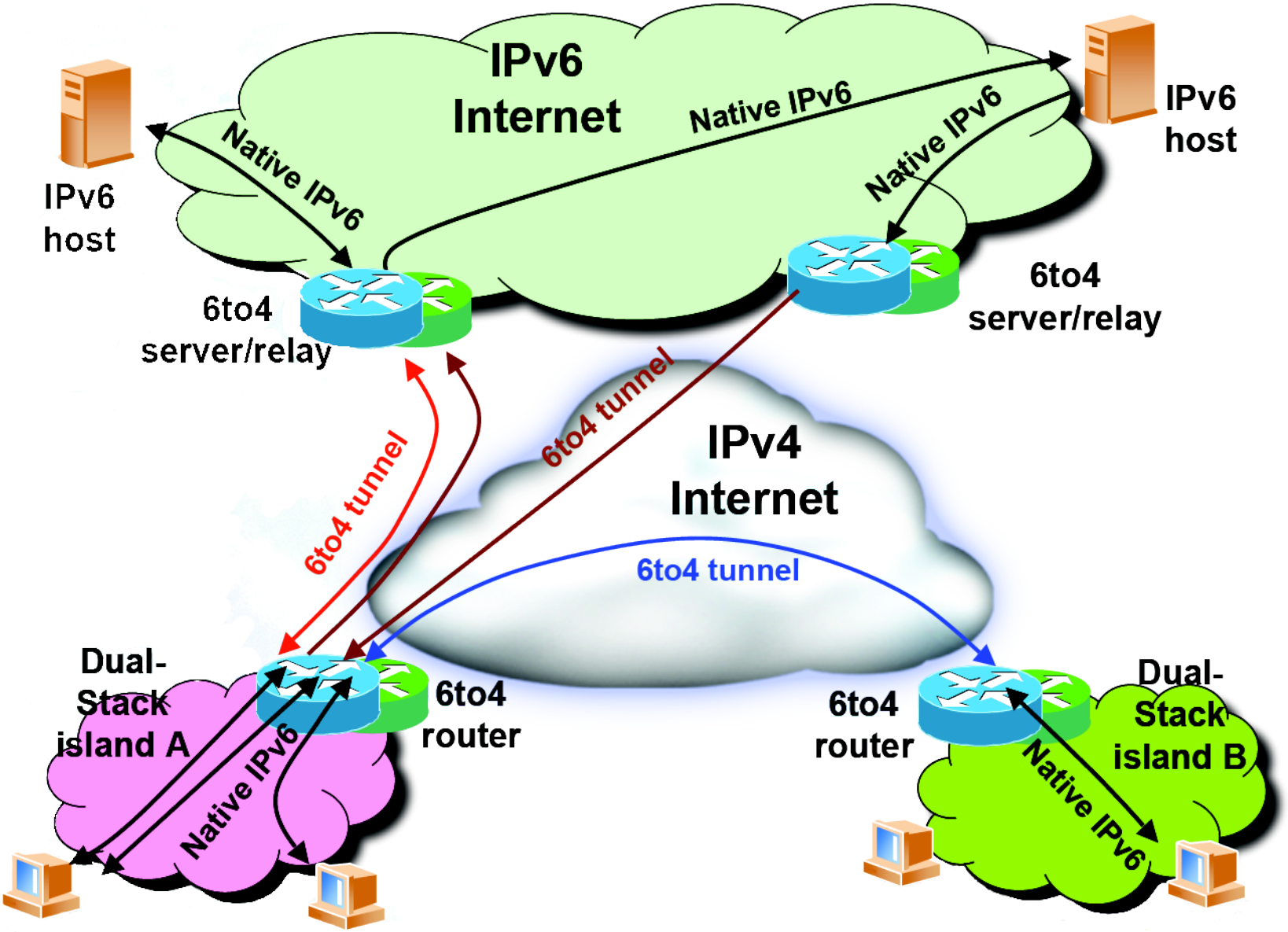
- La idea detrás del Tunnel Broker es simplificar la configuación end-node y la administración de direcciones
- Usualmente, el TB ofrece una interfaz web para interactuar con el sistema final
- Cuando el usuario requiere la creación de un tunel, el TB configura el router que proveerá acceso a IPv6, asignará una dirección IPv6 al cliente y proveerá las instrucciones para crear el tunel del lado cliente.
- Listas de TB en

http://www.ipv6tf.org/using/connectivity/test.php

Tunneling: 6to4 (RFC 3056)

- Encapsulado de IPv6 en IPv4 similar a 6in4
- Las principales diferencias son:
- Las direcciones IPv6 del lado cliente no dependen del router al cual está conectado, sino, de su dirección IPv4 publica
- El tráfico saliente es enrutado a través del mismo “6to4 relay”, pero el tráfico entrante puede venir desde otros “6to4 relays”.

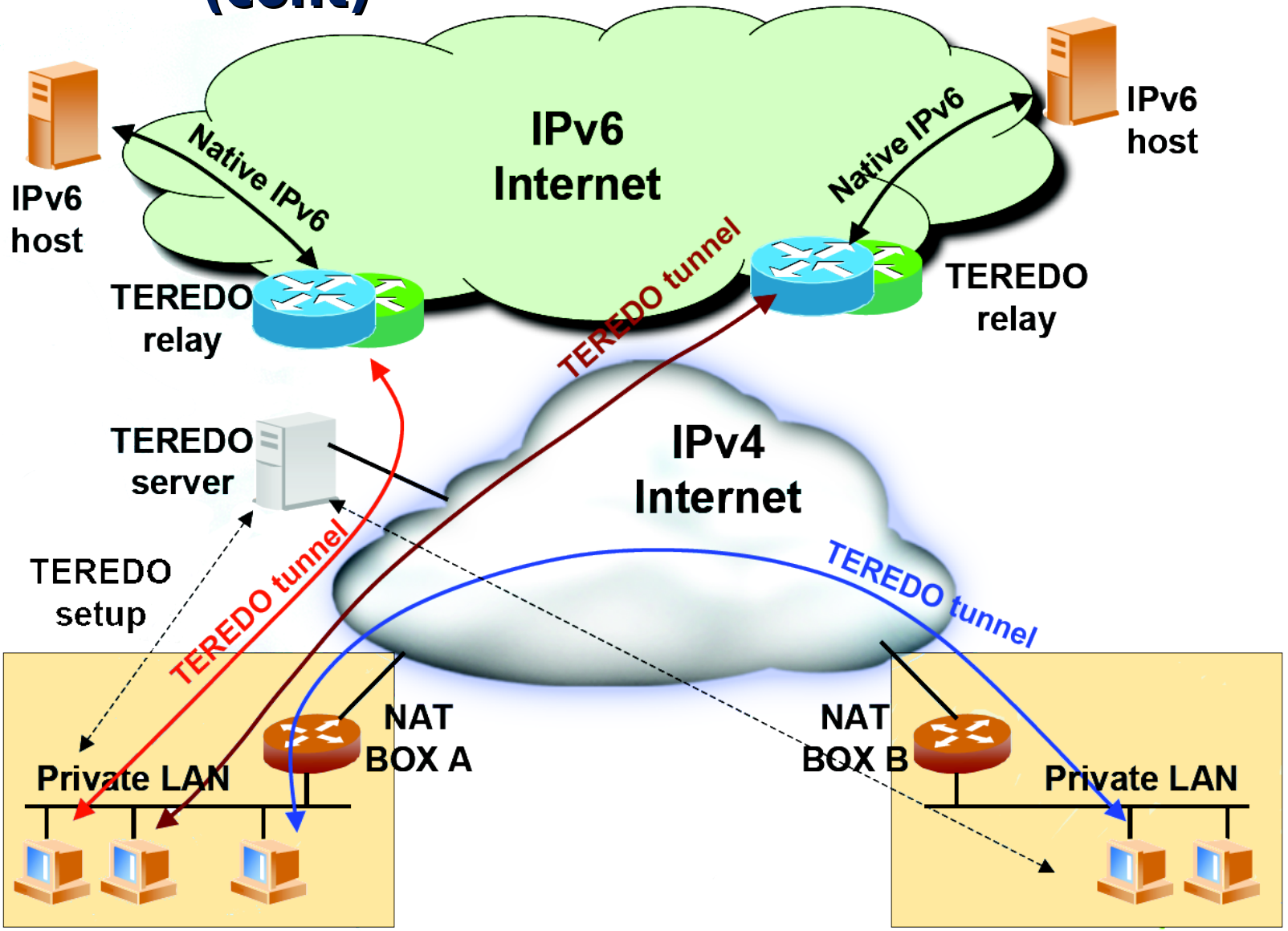
Tunneling: 6to4 (RFC 3056) (cont)



Tunneling: Teredo (RFC 4380)

- Encapsulado IPv6 sobre UDP, sobre IPv4
- Diseñado para proveer acceso a hosts detrás de dispositivos de NAT, sin requerir protocol 41 forwarding
- Diferentes agentes involucrados:
- Teredo Server
- Teredo Relay
- Teredo Client

Tunneling: Teredo (RFC 4380) (cont)



Tunneling: ...

- Hay -mucho- más que decir sobre tunneling de IPv6... (ahora no tenemos suficiente tiempo)
- La transición ocurrirá a medidad que la cobertura de las redes IPv6 nativas crezca.
- Las islas están y serán unidas por algún tipo de tunel (de otra forma, no tenemos conectividad global)
- La transición terminará cuando todas las islas se conviertan en una única -nueva- Internet
- ... igual, seguiremos utilizando túneles IPv6-IPv6 para diferentes propósitos. Son una gran herramienta, no solamente para transición.

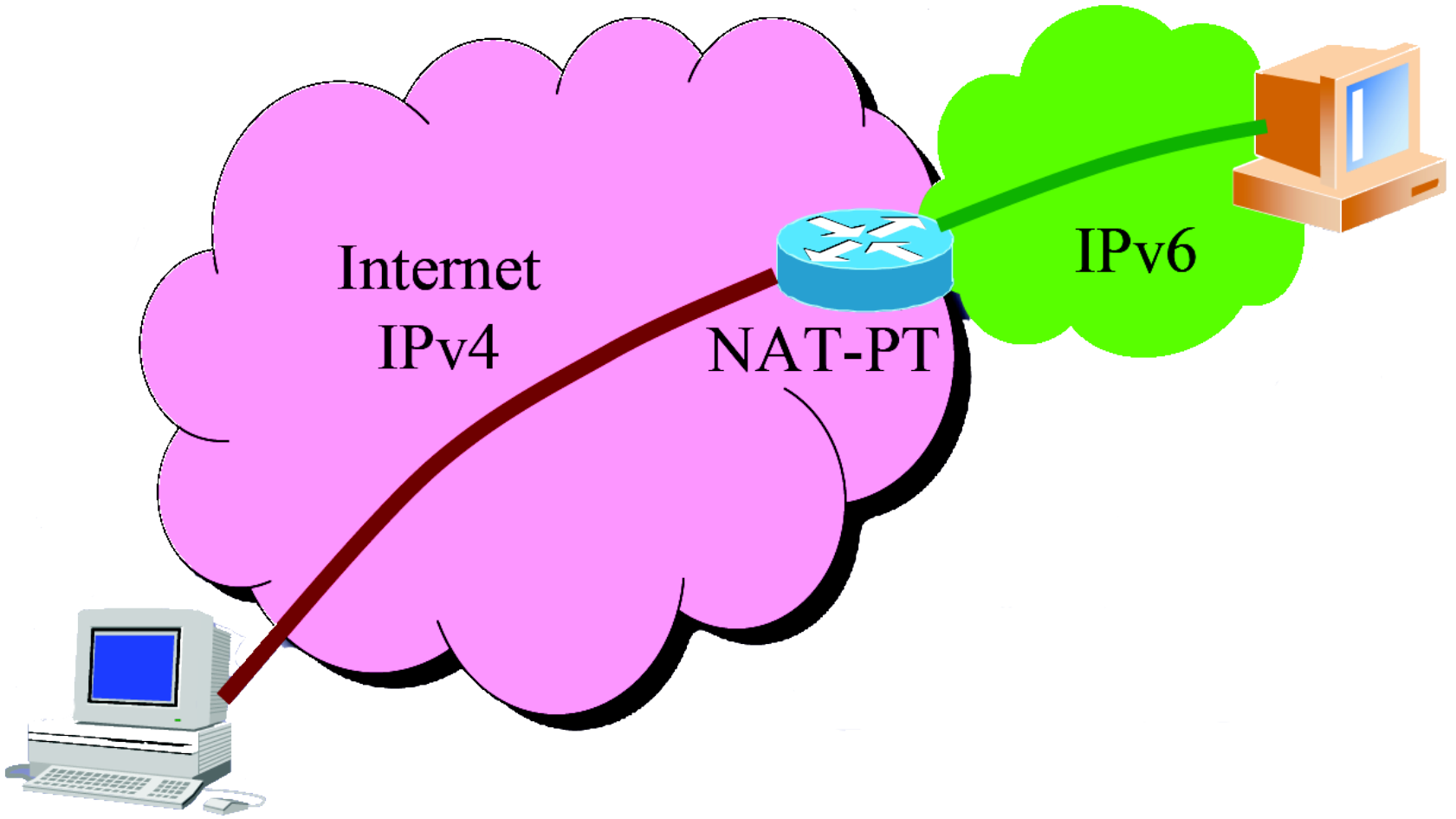
Translation - Traducción

- Los mecanismos de traducción estan en su totalidad deprecados al día de hoy (si bien, algunos se siguen utilizando)
- Se basan en la conversión de paquetes IPv4 en IPv6 y viceversa.
- Podría ser considerado como una extensión de las técnicas de NAT/PAT, afectando no solamente a direcciones y puertos, sino a toda la capa de red
- En la red “IPv6 native” tenemos servicios completos, pero en la red “IPv4 translated” tenemos algunos servicios restringidos

Traducción (cont)

- Dado que los protocolos de la capa de red no son funcionalmente equivalentes, la inspección de la capa superior debe ser realizada a los efectos de realizar la traducción de algunos protocolos (demasiados!)
- Desde el punto de vista de la complejidad, esta es la peor solución
- Puede tener sentido para sistemas legados, donde no hay upgrade posible

Traducción: NAT-PT (ejemplo)



IPv6 Ready Logo Programme
v6RL

v6RL - ¿por qué?

- Evitar confusión en la mente de los clientes, con un programa único globalmente
- Dar una señal fuerte al mercado que IPv6 está listo y disponible
- Proveer las garantías de interoperabilidad requeridas entre los distintos productos IPv6
- Aumentar la confianza de los usuarios que IPv6 está actualmente operativo

"The IPv6 Ready Logo program should contribute to the feeling that IPv6 is available and ready to be used."

v6RL committee (v6LC)

- Lanzado por el IPv6 Forum con el soporte de WIDE/TAHI (Japón), ETSI e IRISA (Europa) y el UNH-IOL (USA)
- Basado principalmente en resultados de testing de interoperabilidad y conformidad

ipv6ready-admin

- Define procedimientos y pasos para el Logo Program
- Otorga los derechos de uso de los logos IPv6 para productos

ipv6ready-tech

- Provisión de especificaciones y herramientas de testing
- Examen técnico de solicitudes de aprobación

v6RL – smooth and gradual approach

Diferentes fases:

- Phase I “Silver” / (bootstrap)
  - Desde setiembre de 2003
  - Basado en eventos y herramientas de interoperabilidad existentes
  - Requerimientos mínimos sobre los protocolos centrales (“MUST”)

- Phase II “Gold”
  - Lanzada en enero de 2005
  - Los productos tienen que satisfacer requerimientos más fuertes (“must” and “should”)
  - Core Protocols, Ipsec, MIPv6, NeMO, Transition mechanisms, Multicast (MLD)

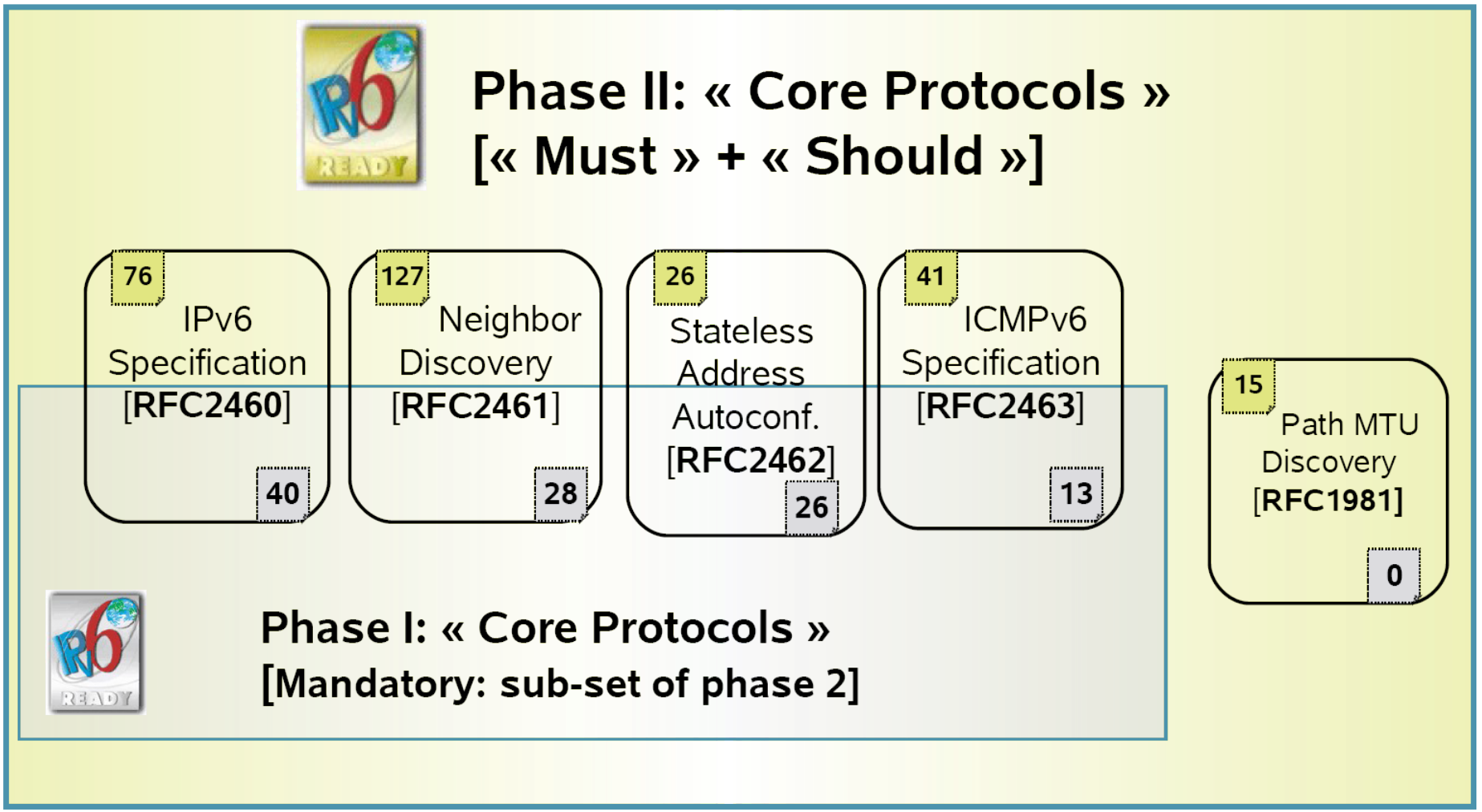
- Phase III to follow

Algunas cosas del RFC 2119

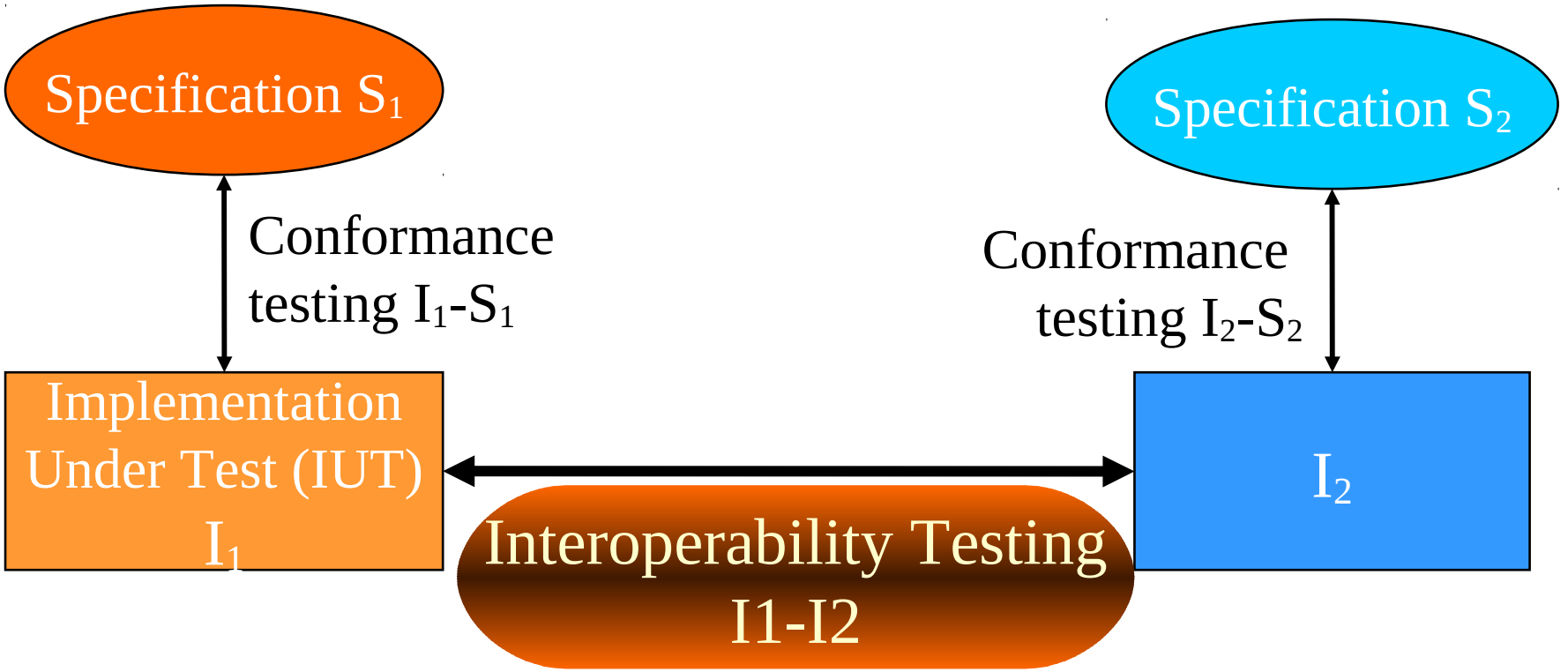
MUST This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification

SHOULD This word, or the adjective “RECOMMENDED”, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully wighted before choosing a different course.

Cobertura de los tests



Conformance vs Interoperability testing



Interoperability platform for IPv6 testing