

MODULO II:

Protocolos de

Capa Internet: IPv6

Objetivos



- Generalidades del Protocolo
 - Comparativas con IPv4
- Direcciones IPv6
 - Representación
 - Tipos de Direcciones
 - Direcciones Unicast
 - Direcciones Multicast
 - Direcciones Anycast
- ICMPv6
 - MTU Path Discovery
 - NDP
 - Proceso DAD
 - Proceso NUD
 - Proceso SLAAC
- Coexistencia IPv4 – IPv6

IPv6



- IP v1-3 definidos y reemplazados
- IP v4 – Versión Actual
- IP v5 – Protocolo de Stream
 - Procolo orientado a conexión.
 - Documentado en RFC 1819
 - Idea principal: ofrecer tráfico de tiempo real con calidad de servicio.
- IP v6 – reemplazo de IP v4
 - **RFC 2460 (1998)**

Porque cambiar IPv4



- Espacio de Direcciones Exhausto
 - Dos niveles de direccionamiento (network y host) desperdicia espacio
 - Crecimiento de Redes y la Internet
 - Uso Extendido de TCP/IP (no solo para redes de datos)
 - Dirección única asignada a cada host. Podrían necesitarse más de una dirección por host, lo cual aumentaría la necesidad de direcciones.
- Requerimientos de nuevos tipos de servicios.
 - IPv4 es un protocolo viejo que no considera aspectos como calidad de servicio, seguridad, etc.

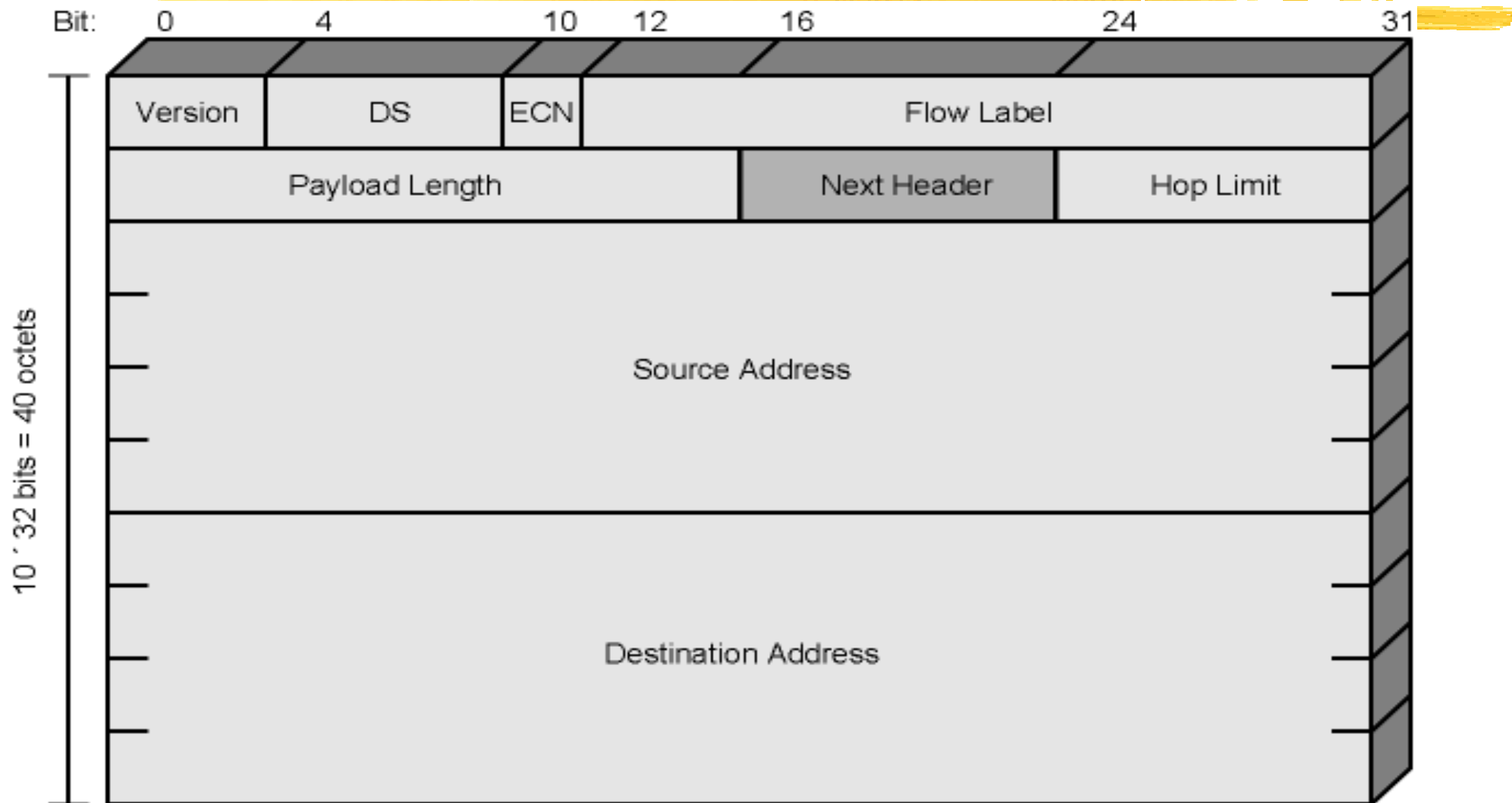
Mejoras de IPv6

- Espacio de Direcciones Expandido
 - 128 bits (aumento del espacio de direcciones en 2^{96})
 - 6×10^{23} direcciones x mts² de la tierra!!!
- Mecanismo de Opciones Mejorado
 - Encabezamiento opcional ubicado entre el header IP y header de capa de transporte.
 - Mejora velocidad y procesamiento simplificado de routers.
 - Simplicidad en la extensión de opciones.
- Autoconfiguración de Direcciones
 - Asignación dinámica de Direcciones.
 - Uso de autoconfiguración de direcciones "stateless" (routeables)
 - Autoconfiguración de Direcciones "Stateful" (con DHCPv6)
- Elimina el uso de NAT/PAT
 - Las direcciones IPv6 son públicas dentro y fuera de la organización.
 - Esto permite implementar aplicaciones problemáticas de resolver con NAT/PAT como Voz sobre IP, Peer-to-peer, video conferencia.
 - Uso de NAT64 para compatibilidad hacia atrás con IPv4.

Mejoras de IPv6

- Mayor Flexibilidad en el Direcccionamiento
 - Se eliminan los “broadcasts”.
 - IPv6 utiliza un mecanismo llamado **solicited node multicast addresses** para reemplazar ARP (usa Multicast).
 - Se introduce una dirección “**all-node multicast address** ” similar al Broadcast IPv4.
 - **Anycast** – Dirección a un nodo cualquiera dentro de un conjunto de nodos.
 - Mejora en escalabilidad de ruteo multicast
- Soporte de asignación de recursos
 - Reemplazo del campo Tipo de Servicio (IPv4)
 - Etiquetado de paquetes para un flujo determinado
 - Ejemplo de uso: Video, voz.
- Seguridad
 - Implementa autenticación, integridad y privacidad
- Herramientas de Transición
 - IPv6 posee varias herramientas que ayudan a la transición de IPv4 a IPv6 como Tunneling y NAT.

Cabecera IPv6

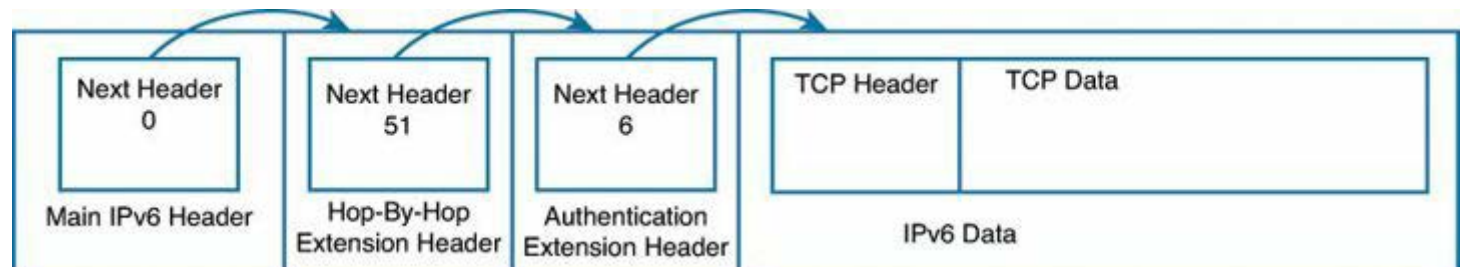


Campos de la cabecera IP v6

- Version (4 bits)
 - 6
- Clases de Tráfico (DS/ECN) (8 bits)
 - DS: Differentiated Service (6 bits)
 - ECN: Explicit Congestion Control (2 bits)
 - Clases o prioridades de paquetes.
 - Campo similar al "Type of Service" de IPv4
- Etiquetado de Flujo (20 bits)
 - Usado por hosts que requieren un trato especial en el tráfico.
 - Identifica un flujo continuo de paquetes de una dada aplicación.
 - Campo "experimental" por el momento.
- Longitud del "Payload" (16 bits)
 - Incluye todas las **extensiones** del encabezamiento mas el PDU de transporte.

Campos de la cabecera IP v6

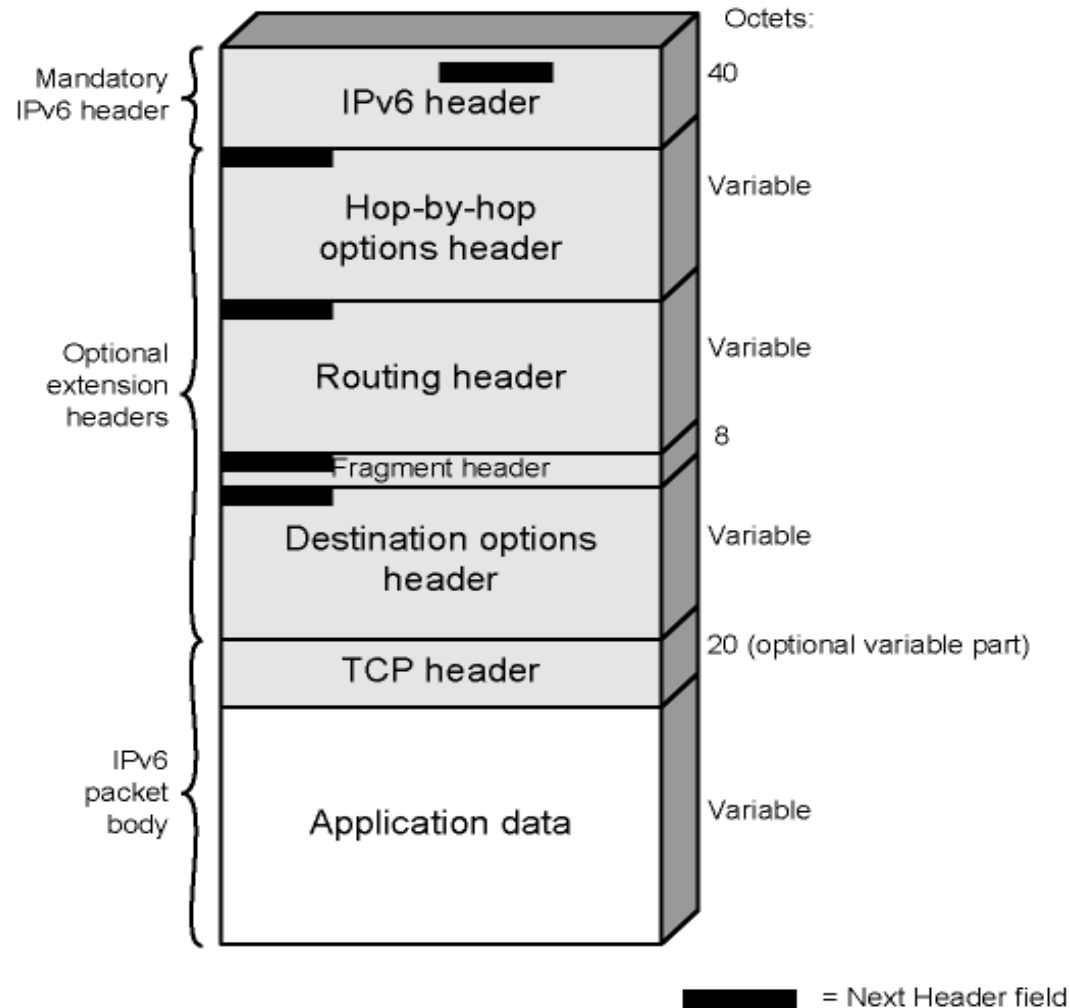
- Próximo Header (8 bits)
 - Identifica el tipo de Encabezado que sigue al Header de tamaño fijo:
 - Extensión del Header IPv6
 - Encabezado de la capa de transporte.
 - Lista completa en: www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
 - Encapsulación de:
 - **IPv4: 4**
 - **IPv6: 29**
 - Encabezado de Fragmentación: **2C**
- Límite de Saltos (8 bits) – Similar a TTL
- Dirección Origen (128 bits)
- Dirección Destino (128 bits)



Observaciones

- IPv6 no permite Fragmentación y Reensamblado en **routers intermedios** (solo en origen).
 - Si un router recibe un **paquete demasiado grande**, descarta el paquete y envía un mensaje ICMPv6.
 - Nodo deberá enviar un paquete de menor tamaño.
 - Se realiza esto para mejorar la performance global del protocolo IP
- No se computa Checksum del Header
 - Se considera que el checksum usado en capa de acceso a la red y protocolo de transporte es suficiente.
- Opciones: No existe un campo específico para opciones, sino que se pueden especificar cabeceras opcionales ("extension headers")
- Se define un nuevo ICMP para IPv6 (RFC 2463)
 - Incluye nuevos códigos
 - Implementa IGMP (Multicasting)

IPv6 con Cabecera de Extensión



Extensiones de cabecera



- Opciones Hop-by-Hop
 - Requieren procesamiento en cada router.
- Ruteo
 - Similar a IPv4 "source routing"
- Fragmentación
 - La fragmentación solo puede ser realizada por **host origen**
 - Este header contiene los campos necesarios para que el nodo destino ensamble.
- Autenticación
 - Provee integridad y autenticación de paquetes.
- Carga de Seguridad Encapsulada ("Encapsulating security payload")
 - Provee privacidad
- Opciones de Destino
 - Información opcional para ser examinada en el nodo destino.

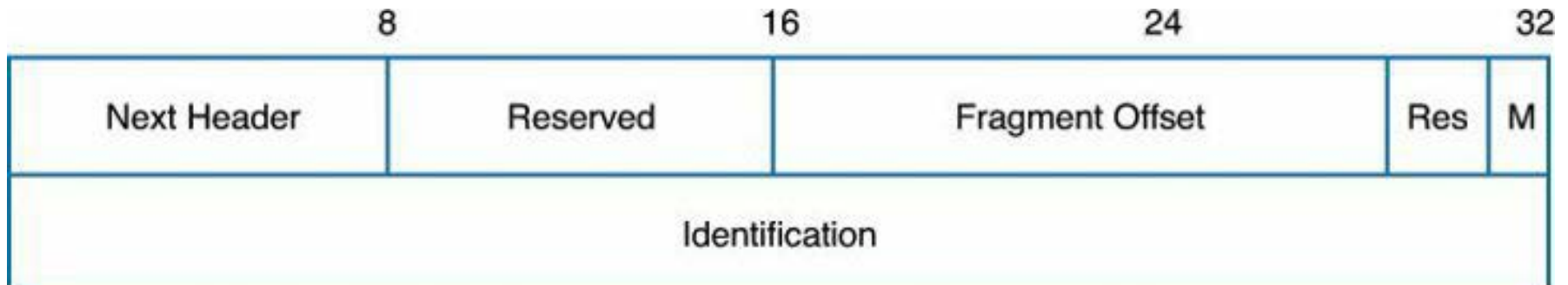
Orden



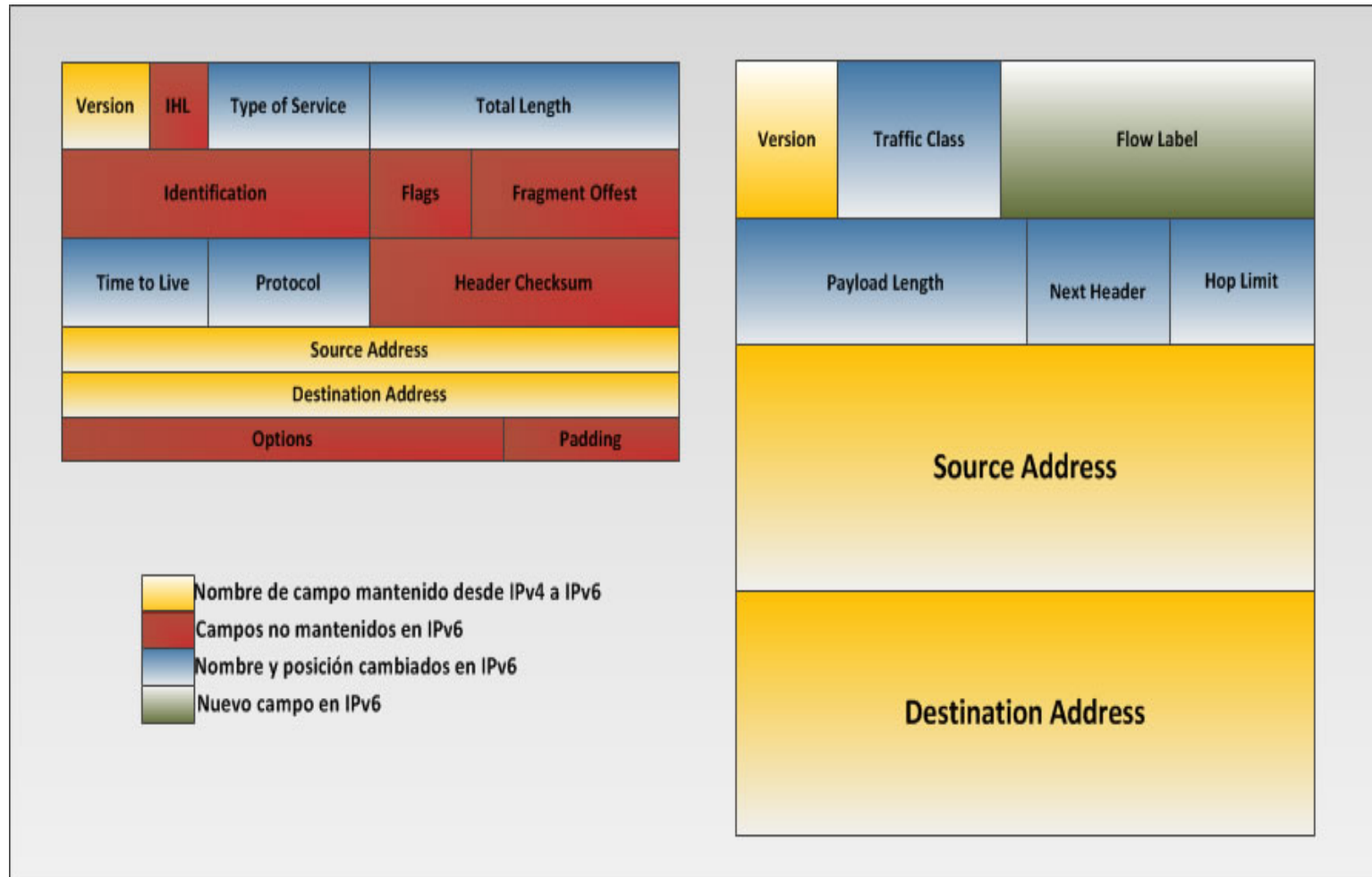
- RFC 2460 dice el orden en que deben usarse los headers de extensión cuando se usa mas de uno:
 1. Header IPv6 (Obligatorio)
 2. Opciones Hop-by-Hop
 3. Ruteo
 4. Fragmentación
 5. Autentication
 6. ESP: Encapsulating Security Payload
 7. Opciones de Destino
 8. Protocolos encapsulado (ICMP, TCP, UDP)

Ejemplo de Cabecera de Extensión: Fragmentación

- Este encabezamiento es usado cuando el nodo origen necesita fragmentar un paquete.
 - Los nodos intermedios **NO** realizan fragmentación
 - Si un router recibe un paquete IPv6 mas grande que el MTU de la interfaz de salida, descarta el packet y envía un mensaje ICMPv6 "Packet Too Big" al origen.
- Contenido similar al campo de fragmentación de IPv4 (sin el campo **DF**)



Comparación Header IPv4 vs IPv6



Observaciones: IPv4 vs IPv6 Header



- El encabezamiento IPv6 (sin extensiones) es más simple
 - Menor número de campos.
 - Menor procesamiento en router intermedios
- Tamaño mínimo de cabecera IPv6 es el doble que IPv4 (40 vs 20 bits)
- IPv6 reemplazó el campo opciones de IPv4 por las cabeceras de extensión.
- El campo **Payload Length** de IPv6 solo expresa la longitud de datos encapsulados (y headers de extension). En IPv4 **Total Length** abarca también la cabecera.

Otras diferencias con IPv4



- IPv6 con la cabecera de extensión “Hop-by-Hop” y la opción de “Jumbo Payload” aumenta el tamaño potencial de un paquete IP de 65,535 bytes (IPv4) a **4,294,967,295** bytes (IPv6)
- IPv4 requiere que un nodo pueda retransmitir un paquete de **68 bytes sin fragmentación** (MTU Mínimo).
- Cada nodo IPv4 destino debe estar capacitado de recibir un paquete de un tamaño mínimo de 576 bytes (un único paquete o fragmentos del original).
- IPv6 requiere que cada enlace maneje un MTU mínimo de **1280 bytes** (1500 bytes recomendado).
- En UDP el campo de checksum (opcional), se convierte en **obligatorio** con IPv6.

Direccionamiento IPv6

- Longitud: 128 bits
- Dirección IPv6 se la representa con **32 dígitos** Hexadecimales
- Cada 4 dígitos hexa (**hexteto**), se utiliza el carácter ":" como divisor.
- Por lo tanto se tienen **8** grupos de **4** dígitos hexadecimales para representar una IPv6
- Ejemplos:
 - 0000:0000:0000:0000:0000:0000:0000:0000
 - 0000:0000:0000:0000:0000:0000:0000:0001
 - FF02:0000:0000:0000:0000:0000:0000:0001
 - FC00:0001:A000:0B00:0000:0527:0127:00AB
- Existen formas de comprimir este formato

Formato Comprimido.

- Se introducen dos formas de comprimir una IPv6:
 - 1) Reducción de 0's más significativos de cada grupo de 4 dígitos
 - 2) Eliminación de grupos de 4 dígitos todos iguales a cero.
- Ejemplos:
 - 0000:0000:0000:0000:0000:0000:0000:0000
 - 1) 0:0:0:0:0:0:0:0
 - 2) ::
 - 0000:0000:0000:0000:0000:0000:0000:0001
 - 1) 0:0:0:0:0:0:0:1
 - 2) ::0001
 - 1 y 2) ::1
 - FF02:0000:0000:0000:0000:0000:0000:0001
 - 1) FF02:0:0:0:0:0:0:1
 - 2) FF02::0001
 - 1 y 2) FF02::1
 - FC00:0001:A000:0B00:0000:0527:0127:00AB
 - 1 y 2) FC00:1:A000:b00::527:127:AB

Formato Comprimido

- Nunca abreviar dos grupos de 0's separados por un grupo de dígitos que no sean todos ceros.

- Ejemplo:

- 2001::ABCD::1234 **INCORRECTO**

- Esto podría traducirse a más de una dirección IPv6:

- 2001:0000:0000:0000:0000:ABCD:0000:1234
 - 2001:0000:0000:0000:ABCD:0000:0000:1234
 - ...

- Se aconseja abreviar la mayor cantidad de 0's posibles.

- Ejemplo:

- 2001:0000:0000:0000:0000:ABCD:0000:1234

- 2001::ABCD:0:1234

Tipos de Direcciones IPv6



- 3 tipos de direcciones:
 - Unicast
 - Anycast
 - Multicast
- Observar que no existen los **broadcasts**

Direcciones Unicast



- Una dirección IPv6 Unicast identifica a una interfaz en un host, mas que un host en si.
- Una interfaz puede tener múltiples direcciones IPv6 (e incluso una IPv4).
- Existen varios tipos de direcciones unicast:
 - Global unicast
 - Link-local unicast
 - Unique local unicast
 - Unspecified address
 - Loopback address

Direcciones Anycast



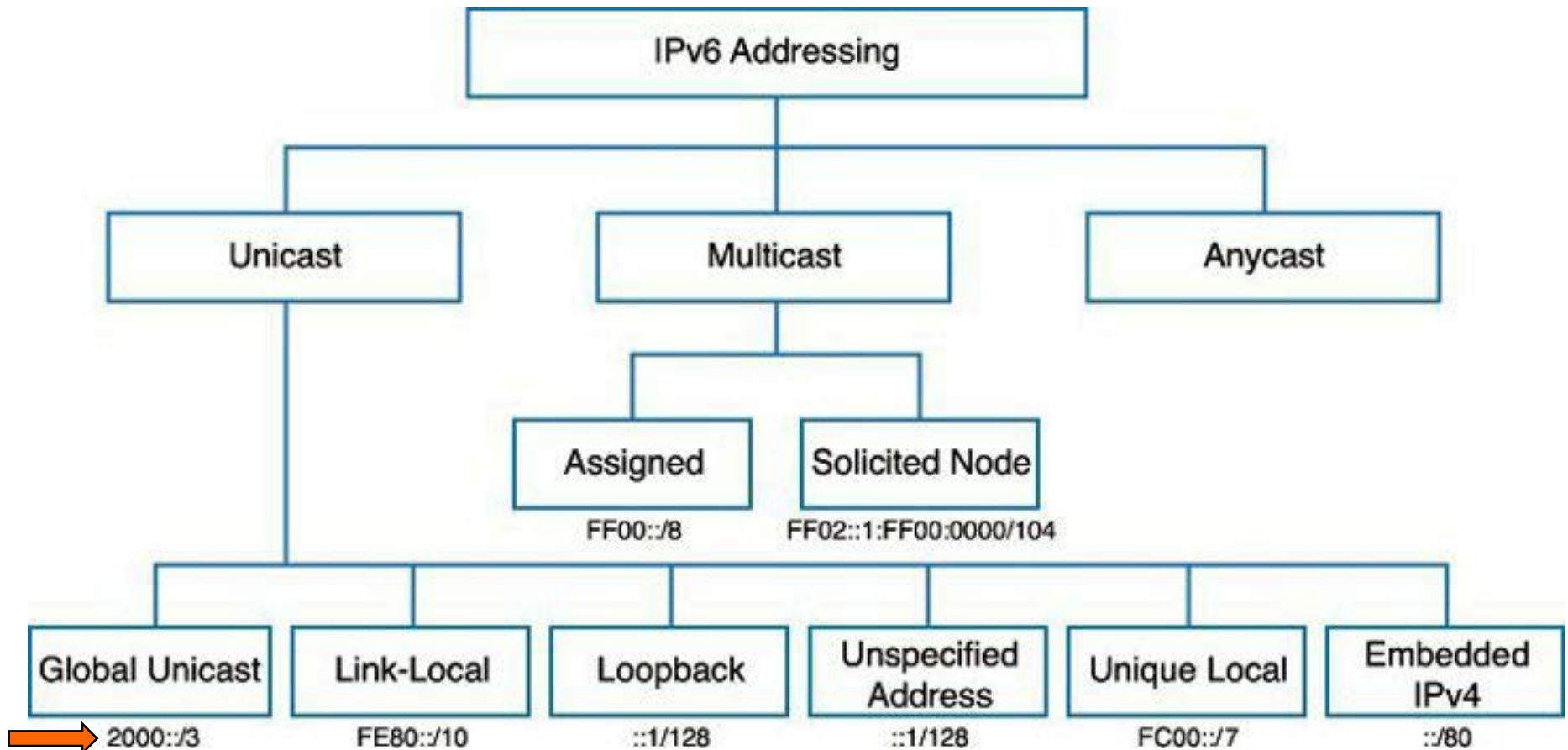
- Es una dirección **unicast** asignada a varios dispositivos.
- Un paquete enviado a una dirección anycast se entrega a solo **uno** de los dispositivos configurados con esa dirección.
- El paquete es entregado al dispositivo "mas cercano" (desde el punto de vista de ruteo).
- En IPv6 un dispositivo que se asignó una dirección anycast es explícitamente configurado para que reconozca que es una dirección de anycast.

Direcciones Multicast



- Identifica un grupo de interfaces que típicamente pertenecen a **diferentes** dispositivos.
- Un paquete enviado a una dirección de multicast es entregado a todos los dispositivos identificados por dicha dirección.
- En IPv6 no existe la dirección de broadcast.
 - Se utiliza la dirección multicast **all-nodes**

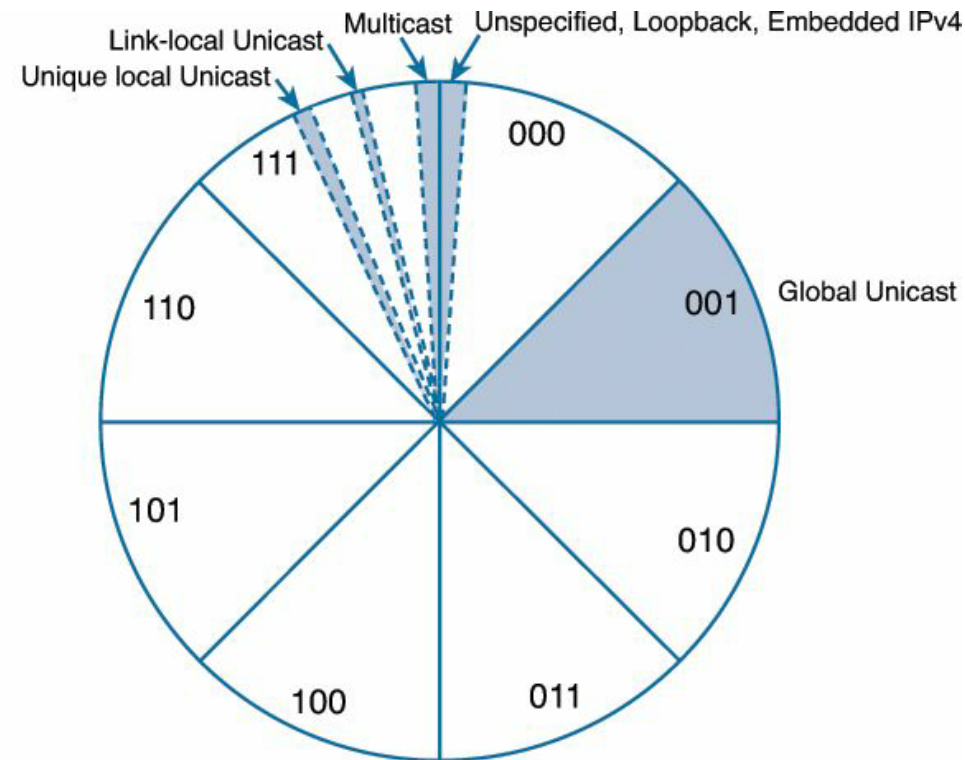
Resumen Direcciones IPv6



Asignación de Direcciones IPv6 (IANA) – Secciones de 1/8

➤ Observar:

- La mayoría del espacio de direcciones esta reservado para direcciones unicast (excepto una pequeña fracción para Multicast)
- Las direcciones Global Unicast actualmente asignadas, comienzan con 001 (2000:: ... 3FFF::) y corresponden a 1/8 del espacio total
- Asignación de direcciones Global Unicast:
<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml>
- La mayor porción de direcciones permanece NO-Asignada por ICANN



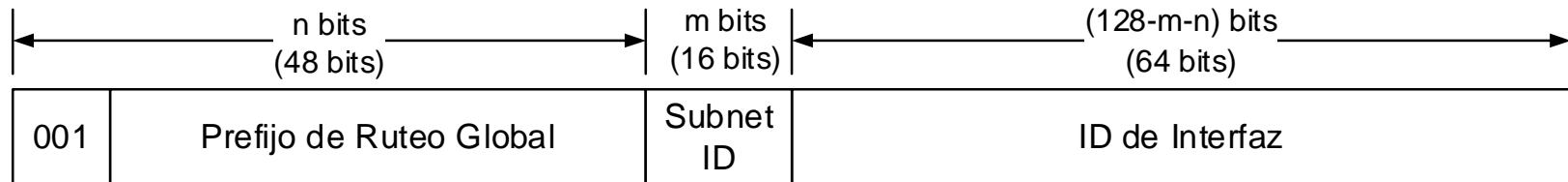
Observaciones



- La mayor parte del espacio de direcciones está reservado por IETF (casi un 7/8)
- Cada tipo de dirección tiene un rango del primer **hexteto** pre-establecido
 - Ejemplo: Global Unicast
 - Rango: 2000:: - 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
 - Solo predefinidos los tres primeros bits de la dirección.

Dirección Global Unicast

- Direcciones globalmente ruteables y alcanzables en la Internet IPv6 (equivalentes a IPv4 Públicas)
- Estructura:
 - Global Routing Prefix
 - Asignado por **ISP** al cliente final
 - Típicamente **/48**
 - Subnet ID
 - Diferencia IPv4 - IPv6: En IPv6 el Subnet ID es un campo separado y **no parte de la porción del Host ID**
 - Típicamente 16 bits
 - Se pueden usar todos 0's y 1's
 - Interface ID
 - Equivalente al HostID
 - Normalmente de 64 Bits
 - **Se pueden usar todos 0's y 1's**

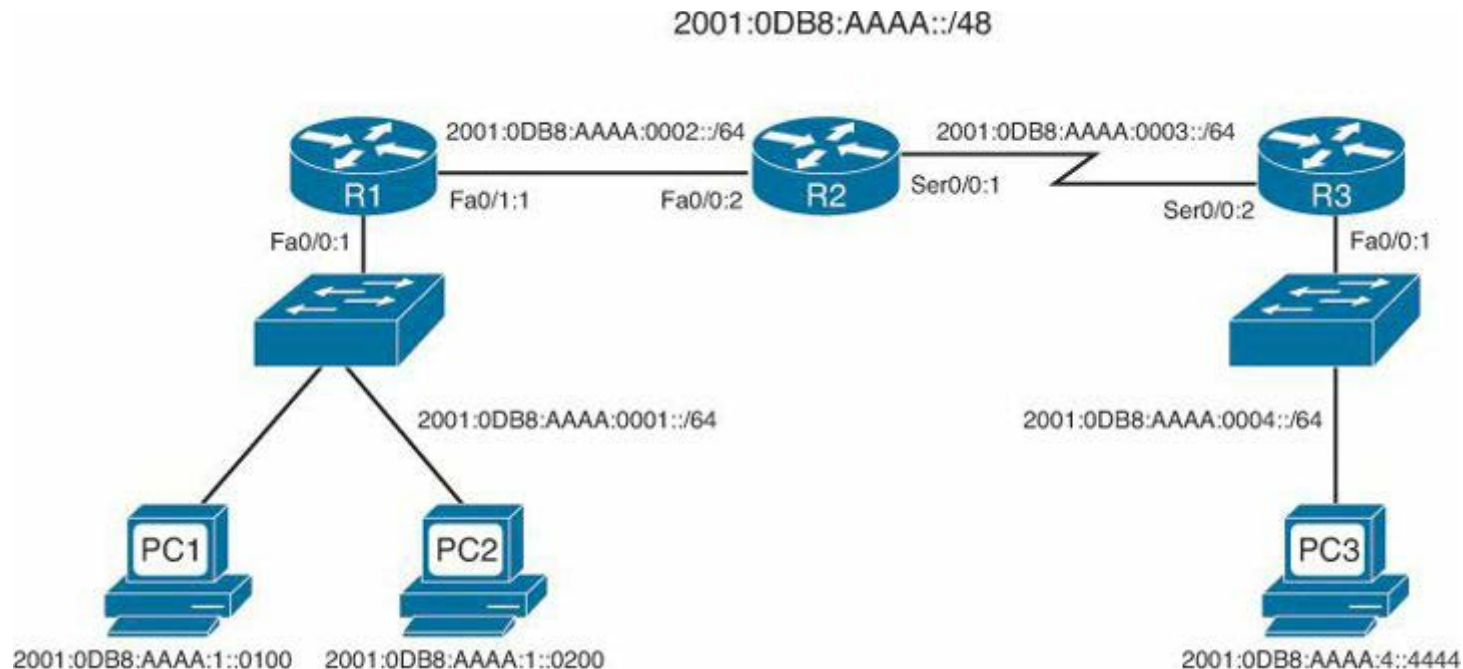


Dirección Global UNICAST

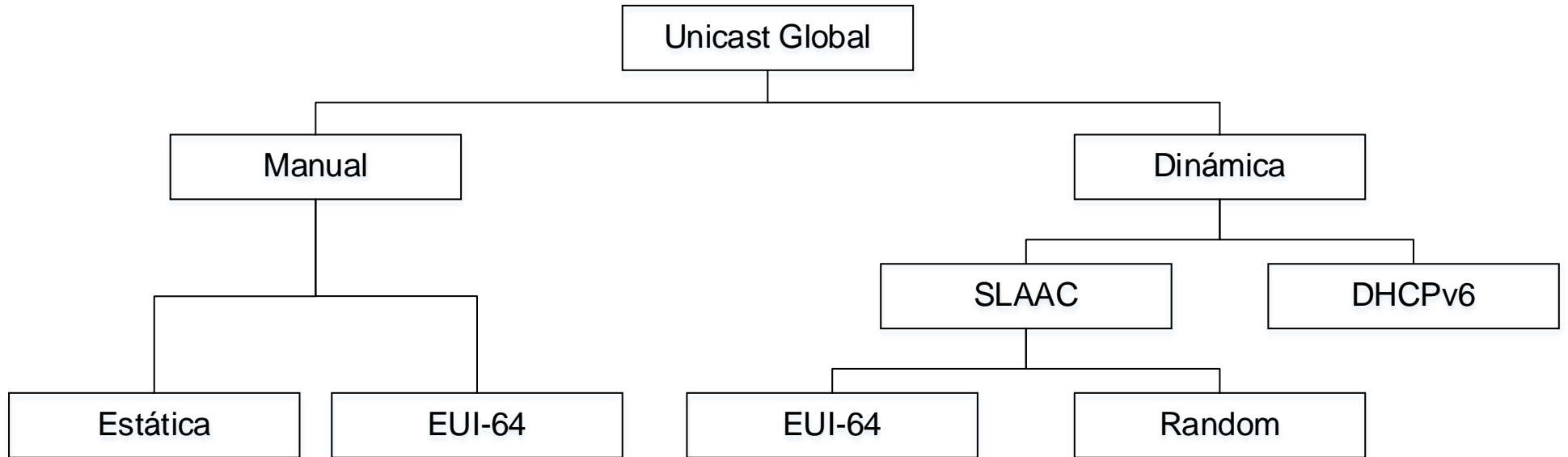
- Notación PI (Π): 314
 - 3 Hextetos Global Routing Prefix
 - 1 Hexteto para Subnet ID
 - 4 Hextetos para Interface ID
- Ejemplos:
 - 2001:0DB8:AAAA:1234:1111:2222:3333:4444
 - Global Routing Prefix: 2001:0DB8:AAAA
 - Subnet ID: 1234
 - Interface ID: 1111:2222:3333:4444
 - 2001:DB8:ABC::
 - Global Routing Prefix: 2001:0DB8:0ABC
 - Subnet ID: 0000
 - Interface ID: 0000:0000:0000:0000

Ejemplo de Topología.

- Global Routing Prefix: 2001:0DB8:AAAA (recibida del ISP)
- Se divide la red en 4 subredes (/64):
 - 2001:DB8:AAAA:0001/64, 2001:DB8:AAAA:0002/64
 - 2001:DB8:AAAA:0003/64, 2001:DB8:AAAA:0004/64

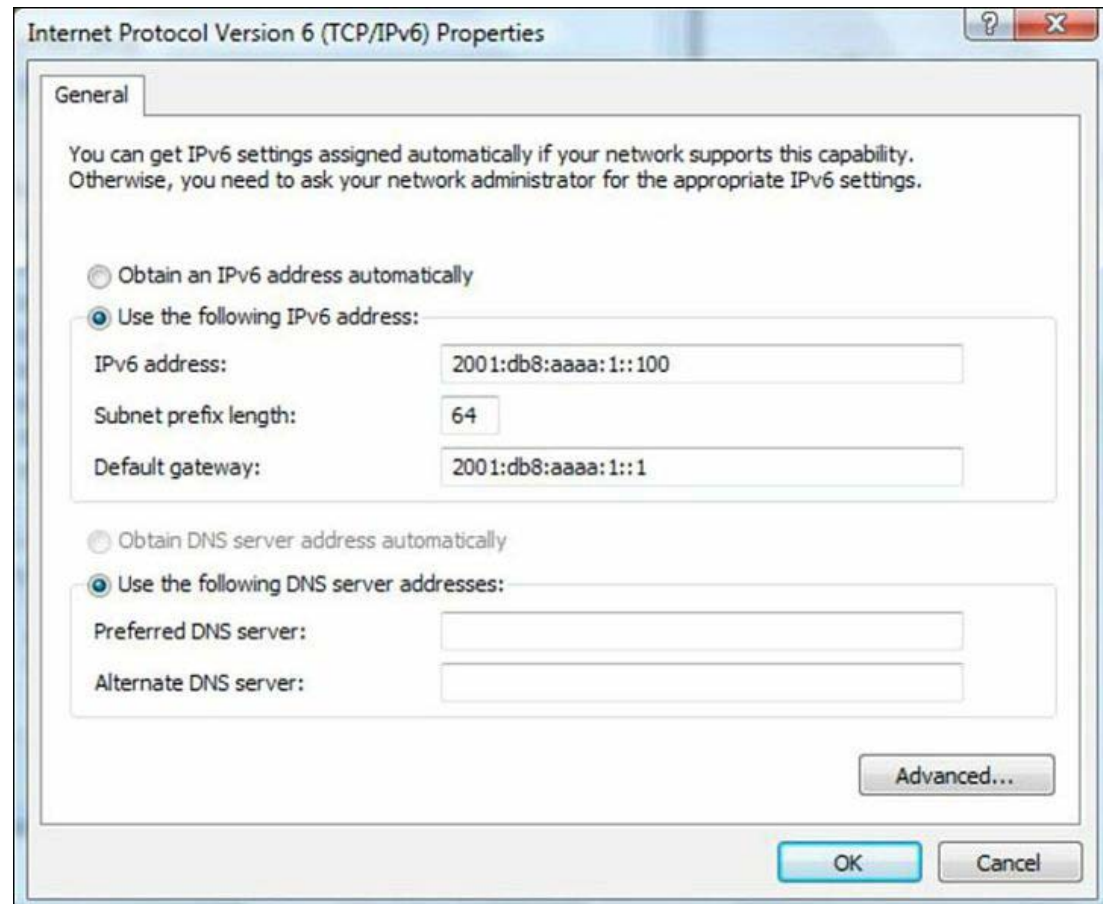


Configuración Manual o Dinámica de Global Unicast



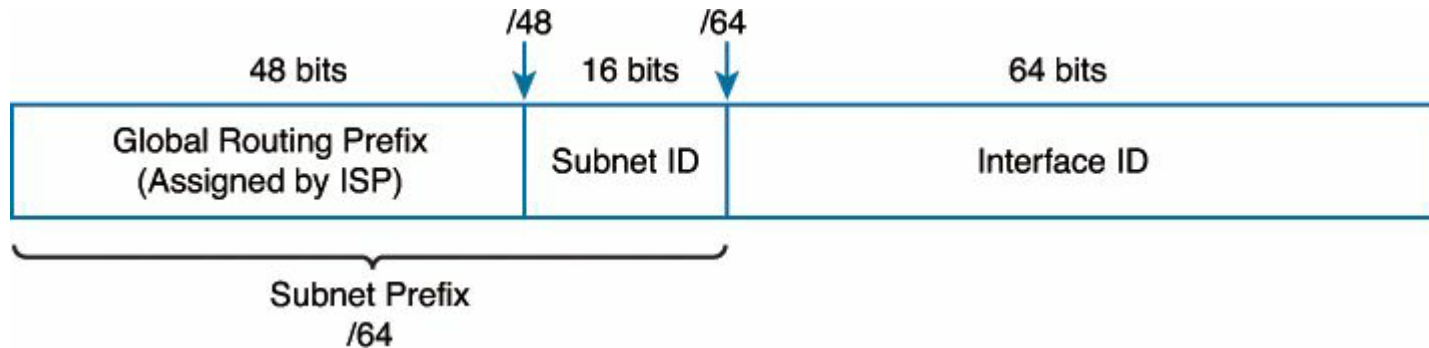
Configuración Manual: Estática

- Se configura igual que dirección IPv4
- Se debe especificar la longitud del prefijo
 - Notar: no incluye la longitud del prefijo de **subnet**.



Subnet ID vs. Prefix ID

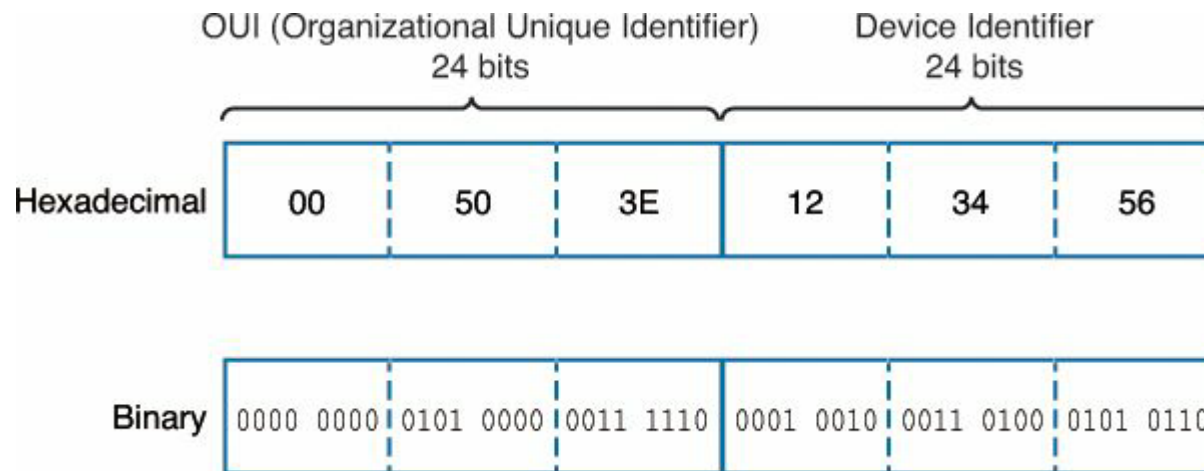
- Se distingue el Subnet ID y el Prefix ID



- El **subnet ID** es el **contenido** del campo usado para denotar subredes individuales.
- El **Prefijo de Subred** abarca al Global Routing Prefix y al Subnet ID
- Observación:
 - El prefijo puede extenderse por encima de /64 (por ejemplo /112) pero no es común su uso, salvo para casos específicos
 - Normalmente se usa prefijo /64 para permitir configuración automática de direcciones **stateless**

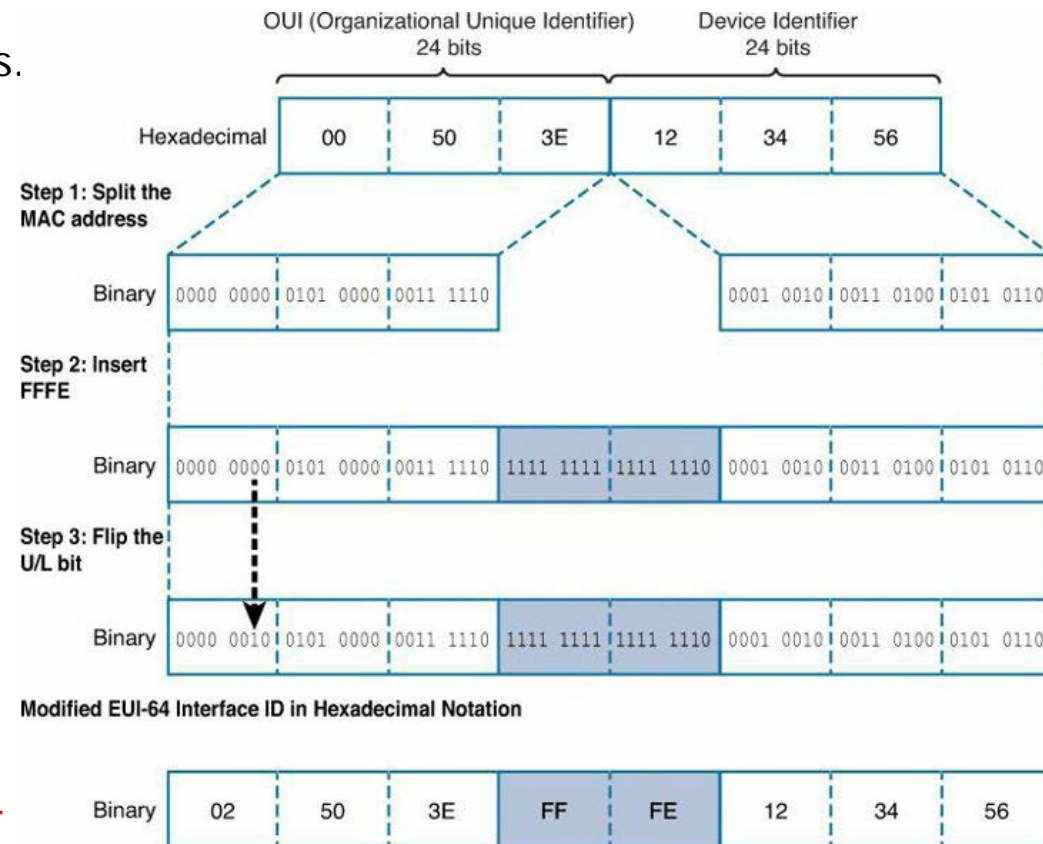
Configuración Manual: EUI-64

- Se configura la porción de Red en forma manual
- El proceso EUI-64 asigna automáticamente la porción de InterfaceID.
- Se parte de la MAC Add de la placa. Recordar:
 - 3 primeros Bytes: OUI (establecido por IEEE)
 - 3 últimos Bytes: Identificador de Dispositivo (establecido por el fabricante)



Algoritmo "Modified EUI-64"

1. Convertir MAC ADD a Binario. Dividirla en las dos porciones de 24 bits (OUI – Device ID).
 2. Insertar **FFFE** entre las dos porciones divididas.
 3. Invertir el Universal/Local bit (7mo bit del primer Byte)
- El resultado se conoce como Modified EUI-64 Interface ID
 - Ejemplo:
 - Mac: 00-50-3E-12-34-56
 - OUI: 00-50-3E
 - Device ID: 12-34-56
 - Inserción FF:FE
 - 00-50-3E-FF-EE-12-34-56
 - Invertir 7mo bit – 1er Byte
 - 02-50-3E—FF-FE-12-34-56
 - Ejemplo de Configuración (Cisco):
 - **ipv6 address 2001:0db8:aaaa:0001::/64 eui-64**
 - Los sistemas operativos de computadoras normalmente no permiten este tipo de configuración



Configuración Dinámica



➤ Dos métodos:

1. Stateless Address Autoconfiguration (SLAAC)
2. DHCPv6

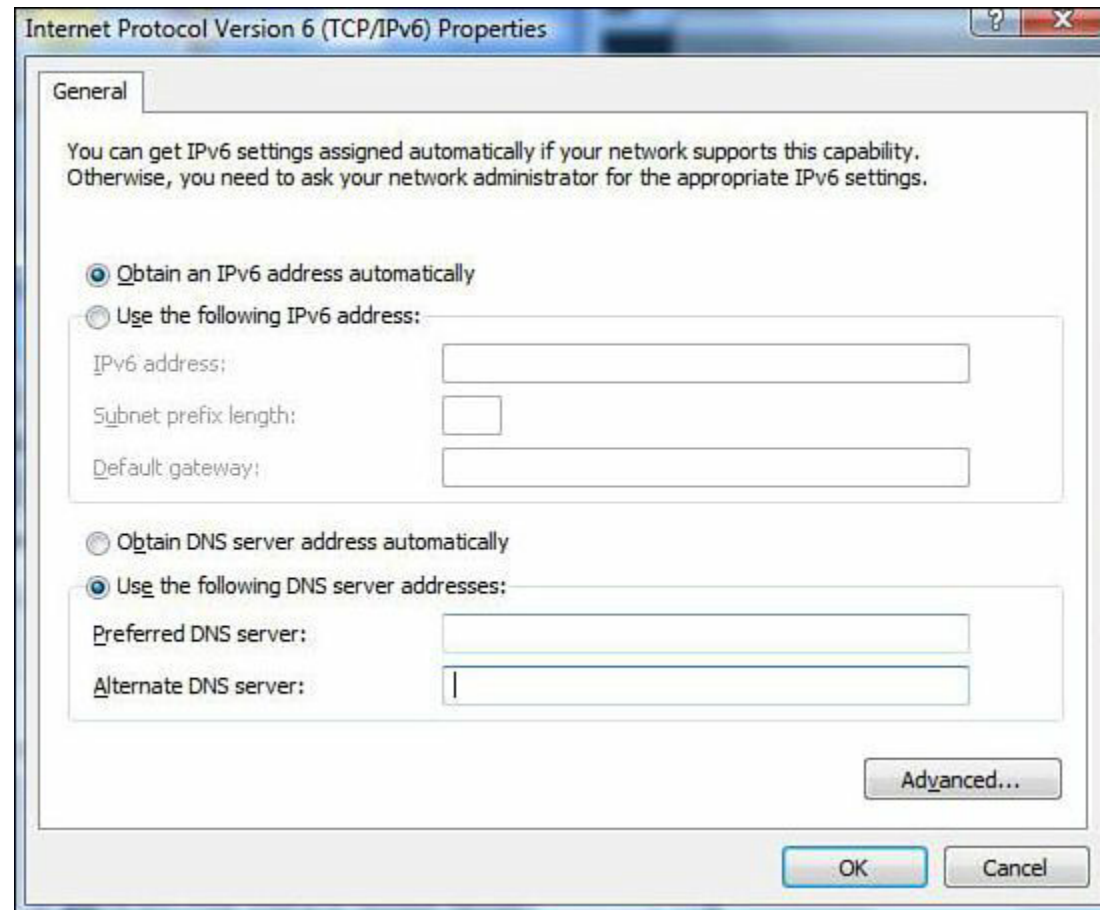
SLAAC (RFC 4862)



- Utiliza el IEEE-Modified EUI-64 o Random para la Interface ID.
- El **Prefijo de Subred** lo obtiene a través del **router** mediante el protocolo "**Neighbor Discovery**" (NDP o ND).
- NDP utiliza a su vez a ICMPv6 para su funcionamiento.
- Los dispositivos pueden recibir mensajes ND para determinar automáticamente:
 - Prefijo de red
 - Longitud del prefijo
 - Default gateway
 - Otra información.
- La dirección obtenida es "**Stateless**" (no recuerda datos del cliente de un request al próximo).
- Debe haber una verificación posterior de no-duplicidad.

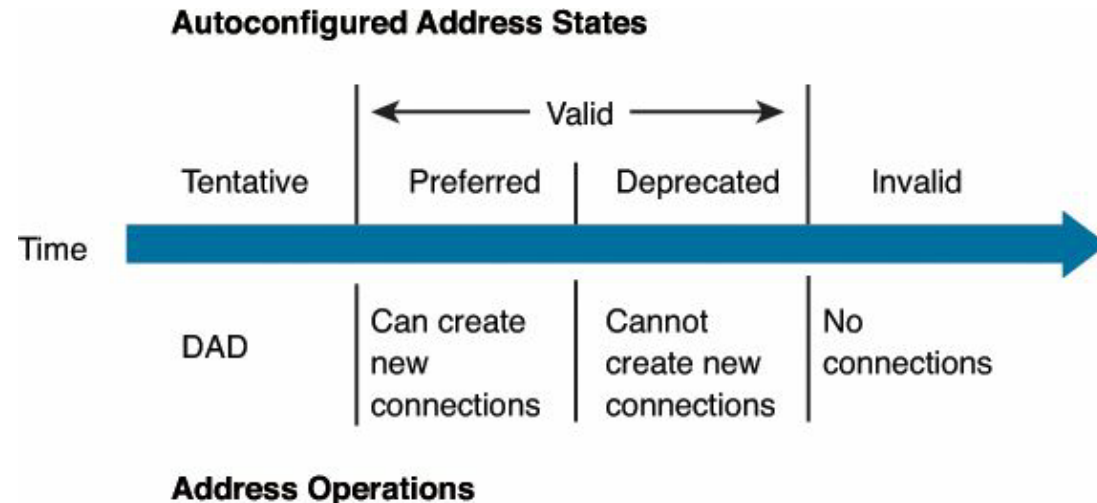
Asignación Dinámica en MS

- El host obtendrá una dirección SLAAC o vía DHCPv6 (si está presente)



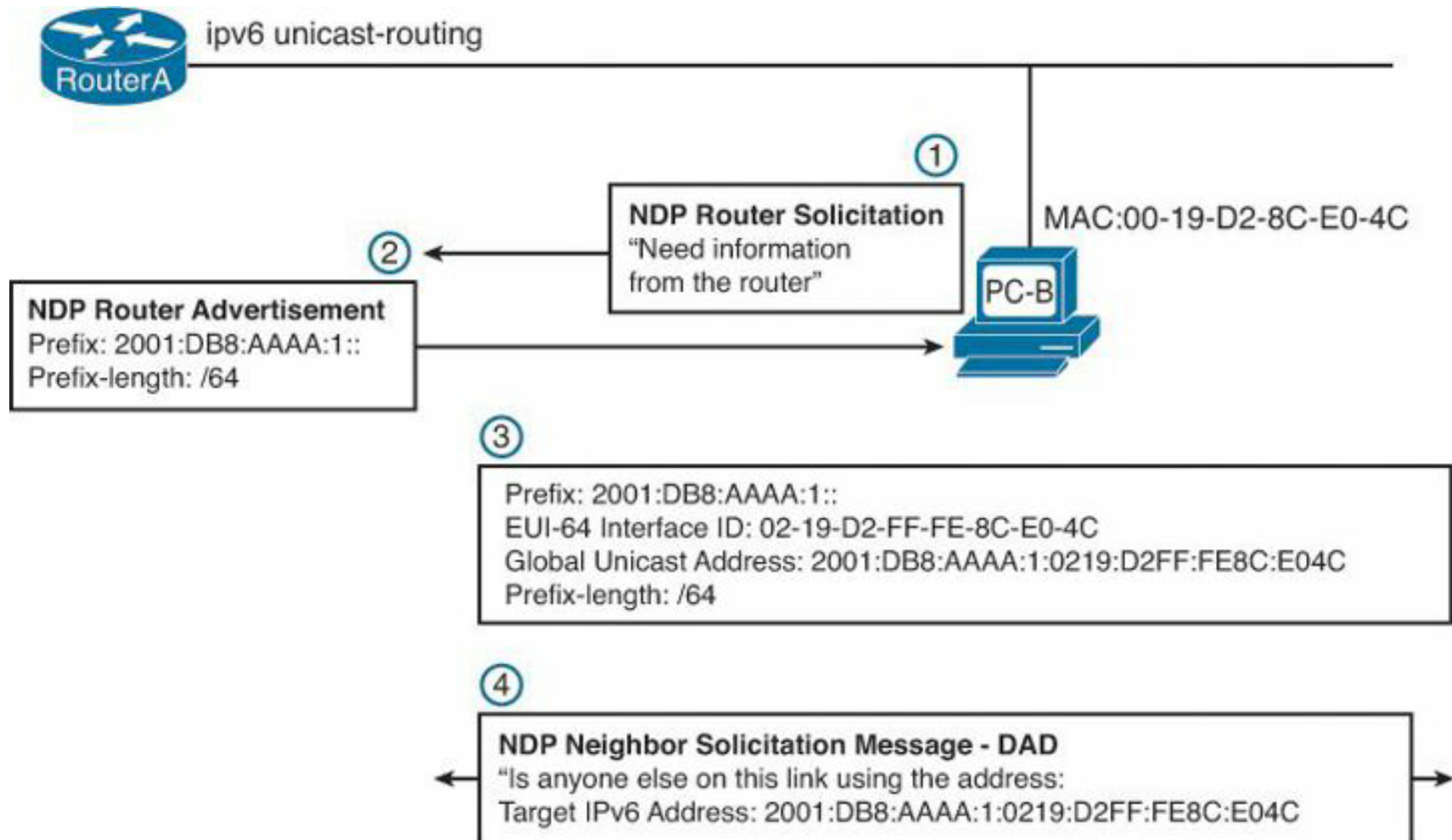
Estados de Direcciones SLAAC

- Una dirección IPv6 **Stateless** puede estar en uno o mas de los siguientes estados:
 - Tentativo: Siendo verificada si es única.
 - Preferida: Verificada que es única. **Tiempo de validez incluido en el mensaje del router (ND)**
 - Obsoleta ("Deprecated"): Válida pero se aconseja **no** usarla (se la puede seguir usando en conexiones existentes pero no para nuevas conexiones).
 - Válida: Preferida o en Desuso. **Tiempo de validez mayor o igual al tiempo de vida de estado preferido.**
 - Inválida: Tiempo de vida expirado. No pueden ser usado como dirección destino u origen.



NOTA: **DAD** Duplicate Address Detection

Proceso para obtención IPv6 SLAAC

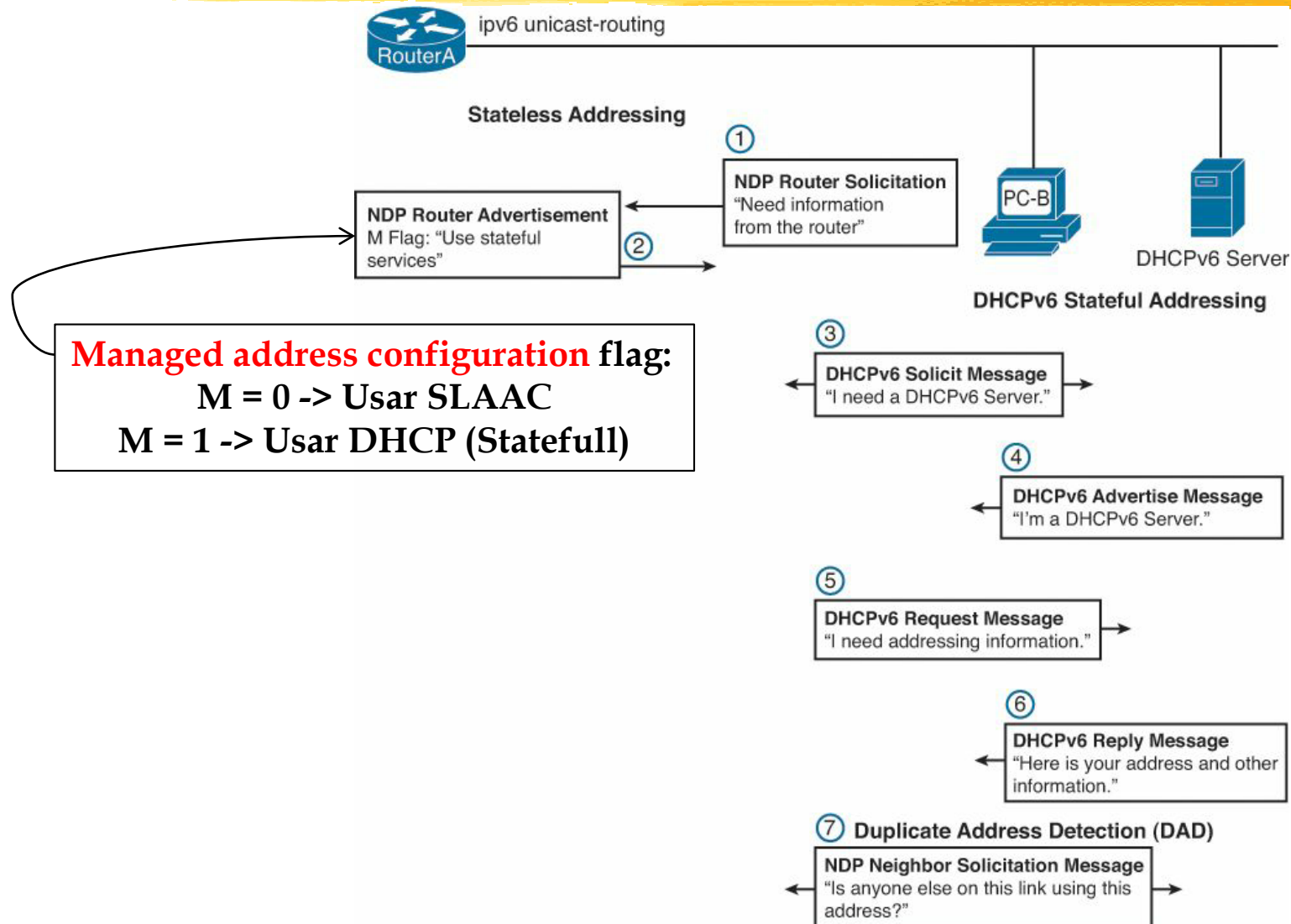


DHCPv6 (RFC 3315)



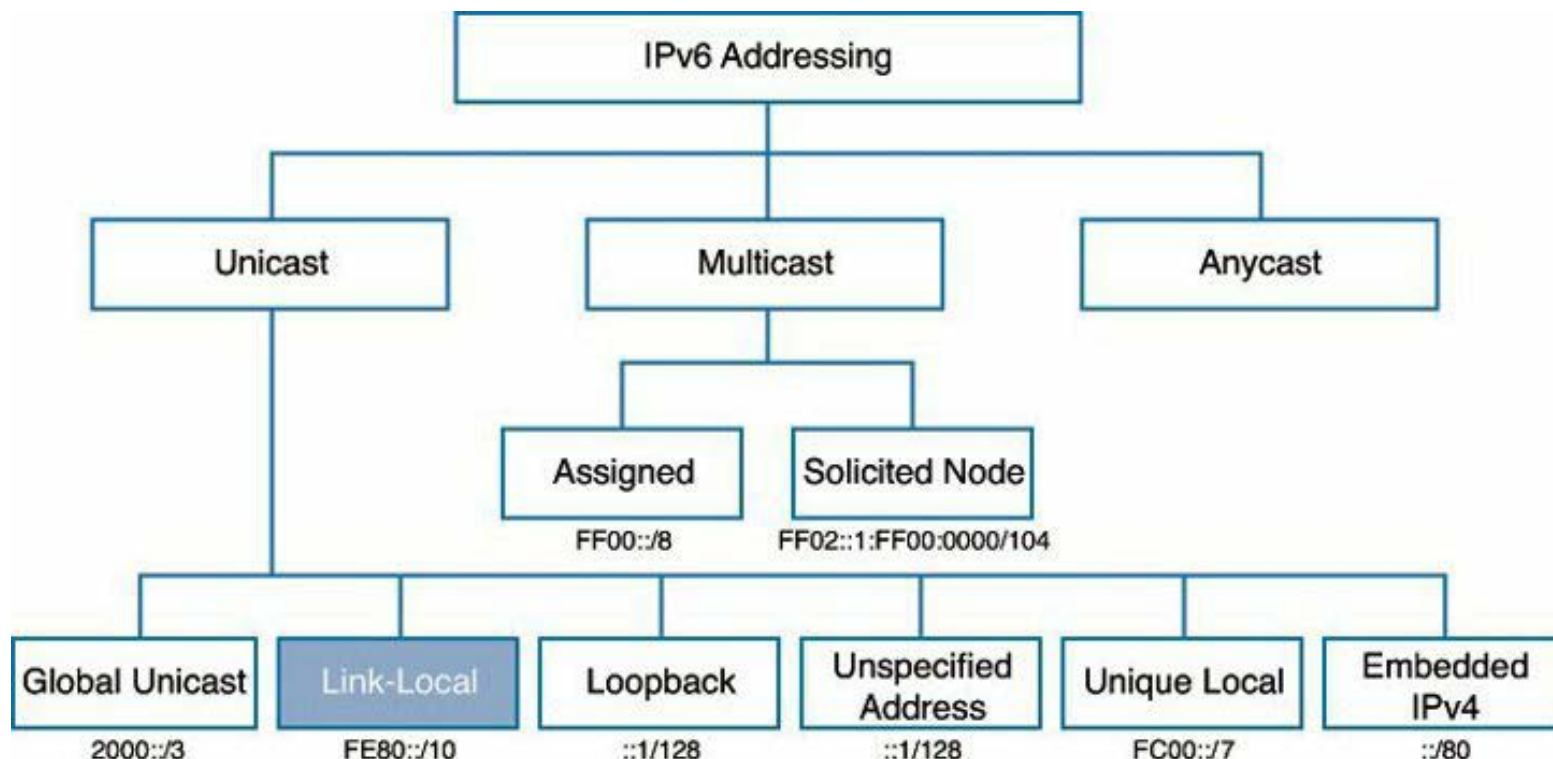
- Provee direccionamiento similar a DHCPv4
- Puede ofrecer autoconfiguración stateful o **stateless**
- El cliente selecciona uso de:
 1. Dirección stateless usando Router Advertisements
 2. Stateful con DHCPv6
- La próxima transparencia muestra:
 - Elección de dirección Stateless o Stateful
 - Obtención de dirección con DHCPv6

Obtención IPv6 Stateful (DHCPv6)



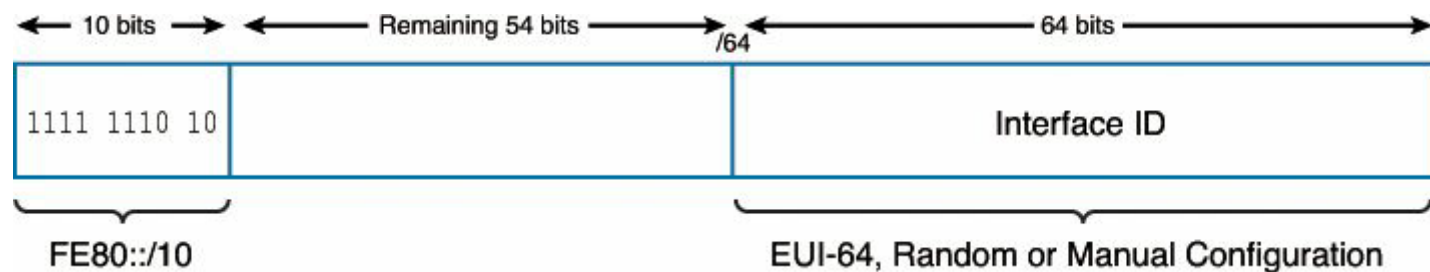
Direcciones Link Local (unicast)

- Confinadas a un único enlace
- **No-routeable** (un router nunca reenvía un paquete con esta dirección)
- Similares a las direcciones APIPA



Direcciones Link-Local

- Son creadas por un dispositivo sin la necesidad de un servidor DHCPv6 ni de mensajes de Router Advertisement.
- Formato:



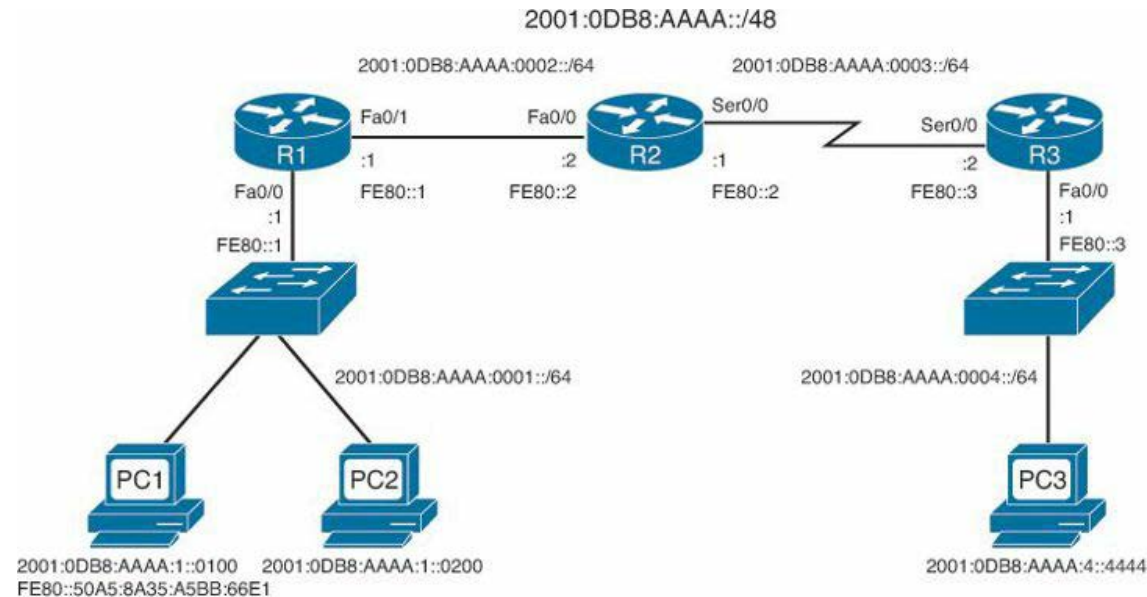
- **Prefijo: FE80::/10 (Rango del primer Hexteto: FE80 a FEBF)**
- 54 bits que siguen al prefijo son 0's
- La interfaz ID puede ser obtenida por 3 métodos:
 - Dinámicamente (EUI-64)
 - Interface ID generado aleatoriamente.
 - Estáticamente (ingreso manual)

Direcciones Link-local

- Las direcciones Link-local se crean automáticamente cuando se habilita IPv6 en una interfaz:
- En algunos dispositivos como routers se las puede configurar manualmente
- Usos de Direcciones Link-local
 - Son **usadas** (no como las APIPAS...)
 - Utilizada como **Default Gateway** por Routers en sus "Router Advertisements messages".
 - Utilizada por routers que corren protocolos de ruteo dinámico como EIGRP para IPv6 y OSPFv3 para establecer adyacencias.
 - Las rutas dinámicas en las tablas de ruteo IPv6 utilizan la dirección de link-local como su dirección next-hop.

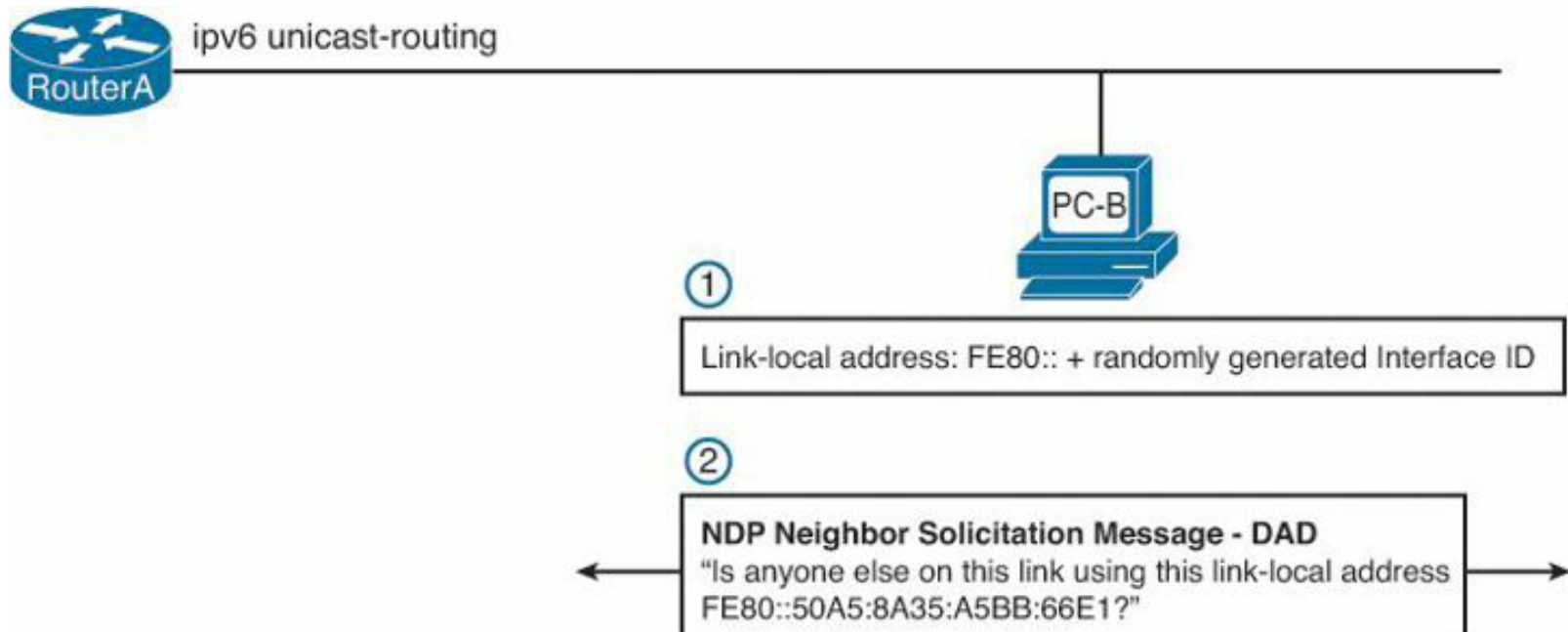
Direcciones Link-Local: Obtención

- Interfaz ID generada aleatoriamente
 - Se elimina la trazabilidad de una dirección IPv6 y la MAC Address (privacidad).
 - Su uso depende del dispositivo:
 - Routers CISCO normalmente usan EUI-64
 - MS superiores a XP usan Interfaz ID Aleatorio.
- Interfaz ID estática
 - Usualmente configurada en interfaces de **routers** para que sea más **legibles**
 - Se termina la dirección usando dígitos bajos



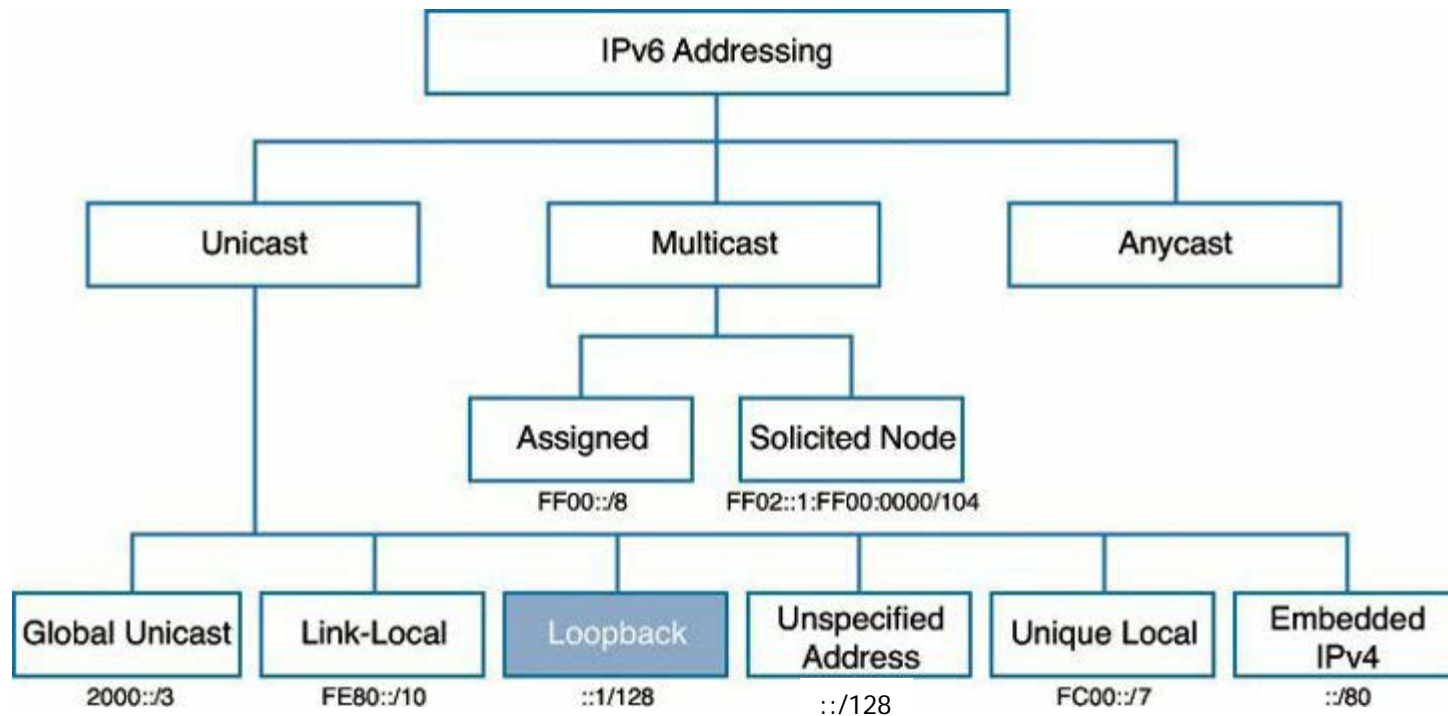
Link Local: DAD

- Las direcciones link local configuradas manual o automáticamente pueden ser duplicadas.
- Con DAD se detecta duplicidad de direcciones.
- Si hay duplicidad aparece un mensaje de warning
 - Ejemplo Cisco: ***%IPV6-4-DUPLICATE: Duplicate address FE80::3 on Serial0/0**



Dirección Loopback y Unspecified

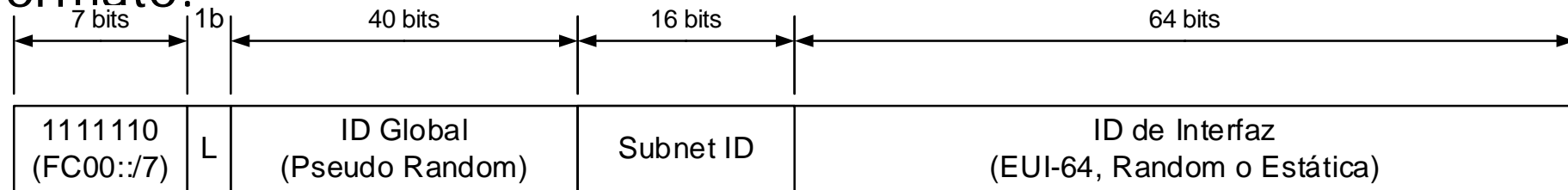
- Loopback
 - `::1/128`
- Unspecified (usado para denotar "este" host)
 - `::/128`



Unique Local Address ó ULA (unicast) – RFC 4193

- Equivalente a las direcciones IPv4 Privadas pero **globalmente únicas**.
- Usadas dentro de la red corporativa pero **NO** ruteables a **Internet** (si en la red privada)

➤ Formato:



➤ Características:

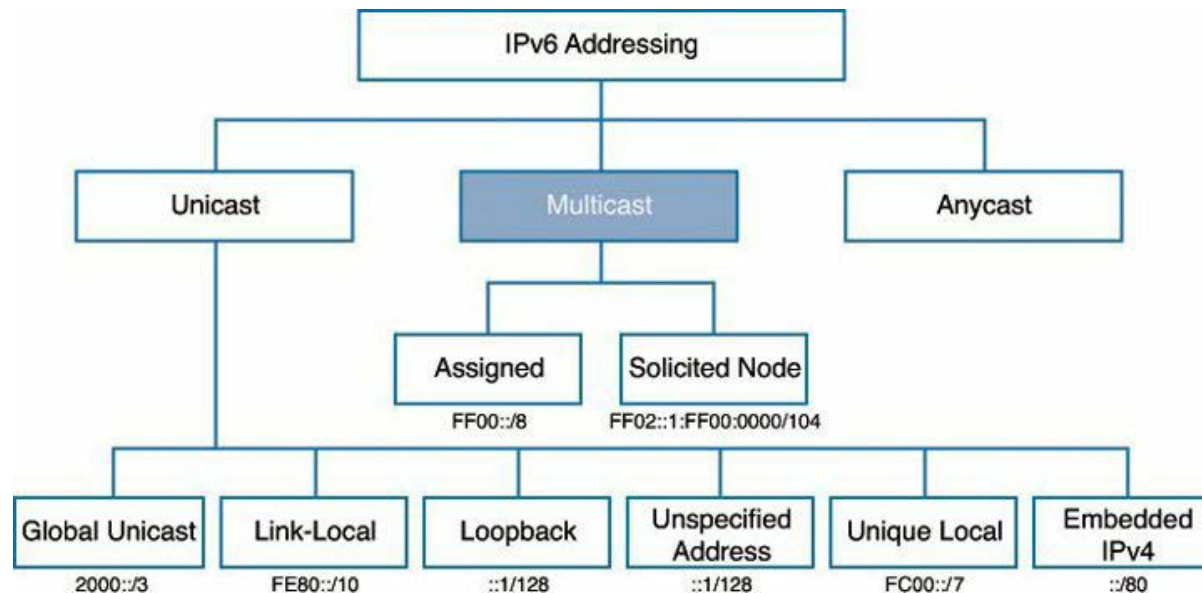
- Bit L siempre en 1.
- Posee un prefijo global único (alta probabilidad de ser único). (RFC 4193)
- Permite que sitios se conecten en forma privada sin conflicto de direcciones o reenumerado de direcciones.
- Independiente de cualquier ISP (direcciones privadas)
- Aunque son privadas son únicas globalmente

Direcciones IPv4 Embebidas

- Usadas para transición de IPv4 a IPv6
- Dos tipos:
 - IPv4-compatibles IPv6 (discontinuadas)
 - Formato: 0:0:0:0:0:0:0:ipv4
 - Ejemplo: 0:0:0:0:0:0:0:189.14.8.97
 - IPv4-mapeadas a IPv6 (en uso)
 - Idéntico al anterior excepto que precedido por FFFF antes de IPv4:
 - Formato: 0:0:0:0:0:0:FFFF:ipv4
 - Ejemplo: 0:0:0:0:0:0:FFFF:189.14.8.97

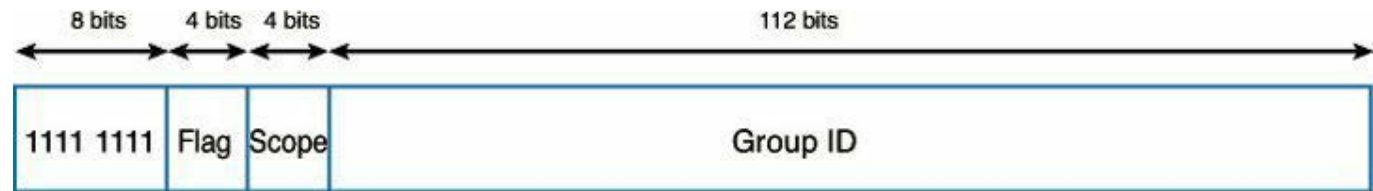
Direcciones Multicast

- Define a un grupo de dispositivos (grupo *multicast*)
- Equivalente a IPv4: 224.0.0.0/4.
- Un paquete enviado a un grupo multicast siempre tiene un dirección origen unicast.
- Una dirección multicast **nunca** puede ser usada como dirección **origen**.
- Posee el prefijo **FF00::/8**



Direcciones Multicast

➤ Estructura:



FF00::/8

Flag

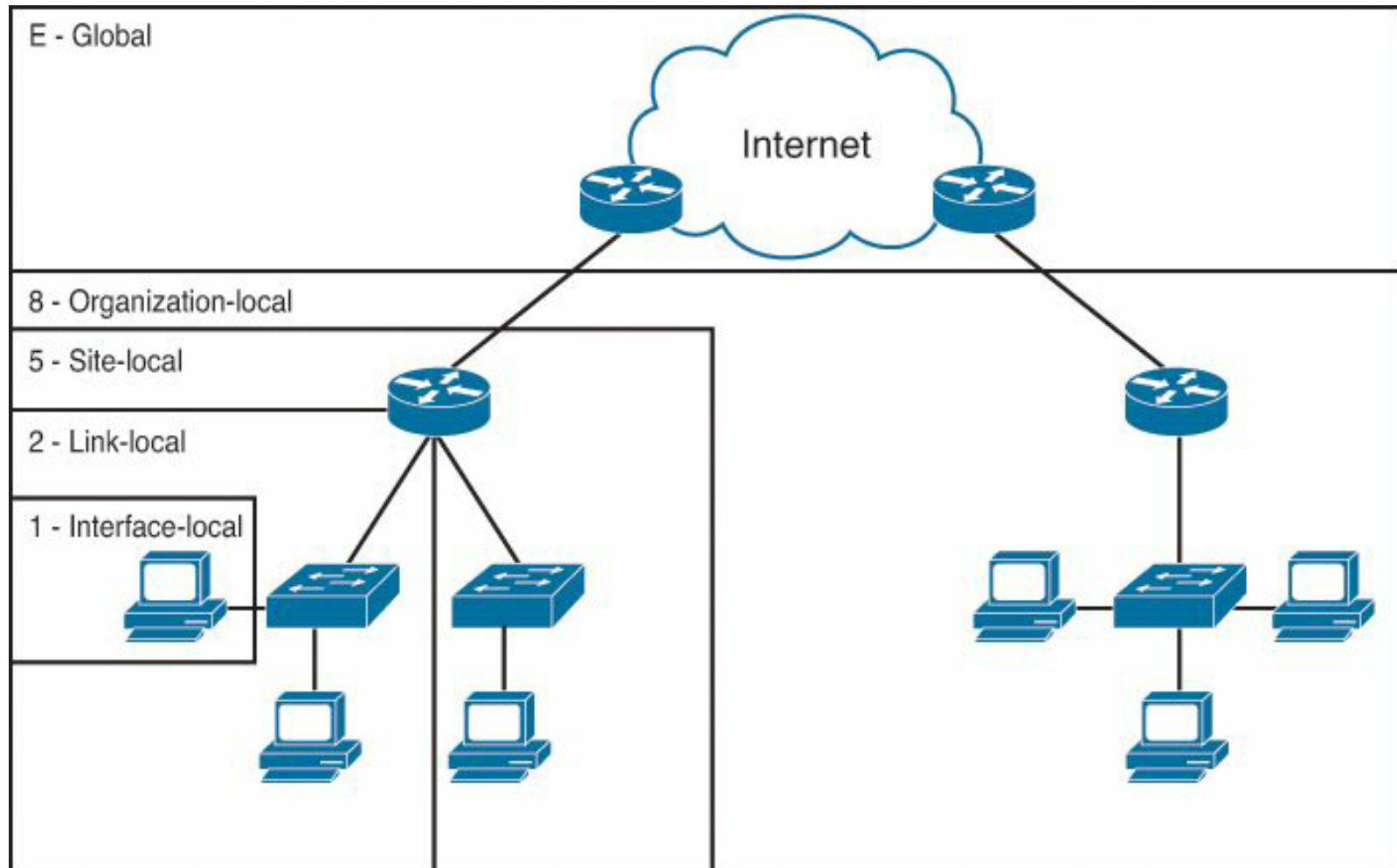
- 0 Permanent, well-known multicast address assigned by IANA
- 1 Non-permanently-assigned ("transient" or "dynamically" assigned) multicast address

Scope

- 0 Reserved
- 1 Interface-Local scope
- 2 Link-Local scope
- 3 Unicast-prefix-based address
- 4 Admin-Local scope
- 5 Site-Local scope
- 6 Unassigned
- 7 Rendezvous Point flag
- 8 Organization-Local scope
- 9 Thru D Unassigned
- E Global scope
- F Reserved

Multicast Scope

- Ejemplo de usos de algunos scopes:



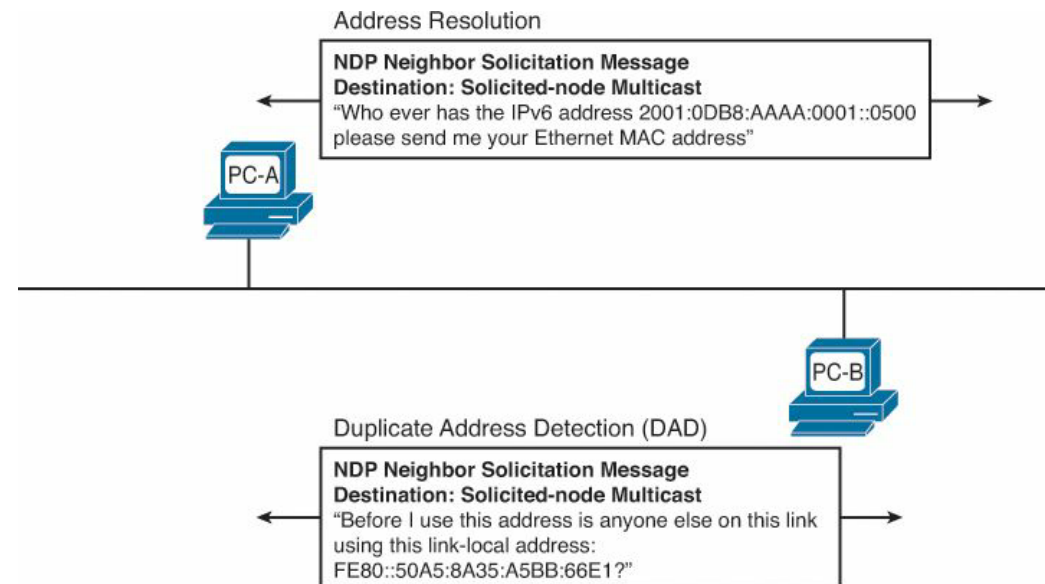
Algunas direcciones multicast globalmente asignadas

/8 Prefix	FF	Flag 0	Scope (0–F)	Predefined Group ID	Compressed Format	Description
<i>Interface-local Scope</i>						
FF		0	1	0:0:0:0:0:0:1	FF01::1	All-nodes
FF		0	1	0:0:0:0:0:0:2	FF01::2	All-routers
<i>Link-local Scope</i>						
FF		0	2	0:0:0:0:0:0:1	FF02::1	All-nodes
FF		0	2	0:0:0:0:0:0:2	FF02::2	All-routers
FF		0	2	0:0:0:0:0:0:5	FF02::5	OSPF routers
FF		0	2	0:0:0:0:0:0:6	FF02::6	OSPF designated routers
FF		0	2	0:0:0:0:0:0:9	FF02::9	RIP routers
FF		0	2	0:0:0:0:0:0:A	FF02::A	EIGRP routers
FF		0	2	0:0:0:0:0:1:2	FF02::1:2	All DHCP agents
<i>Site-local Scope</i>						
FF		0	5	0:0:0:0:0:0:2	FF05::2	All-routers
FF		0	5	0:0:0:0:0:1:3	FF05::1:3	All DHCP servers

- Observar que se puede enviar un paquete con el mismo GROUP ID a todo el Site o a un link dependiendo del Scope (o rango) (FF02::2 – FF05::2)

Dirección de Multicast: "Solicited-Node"

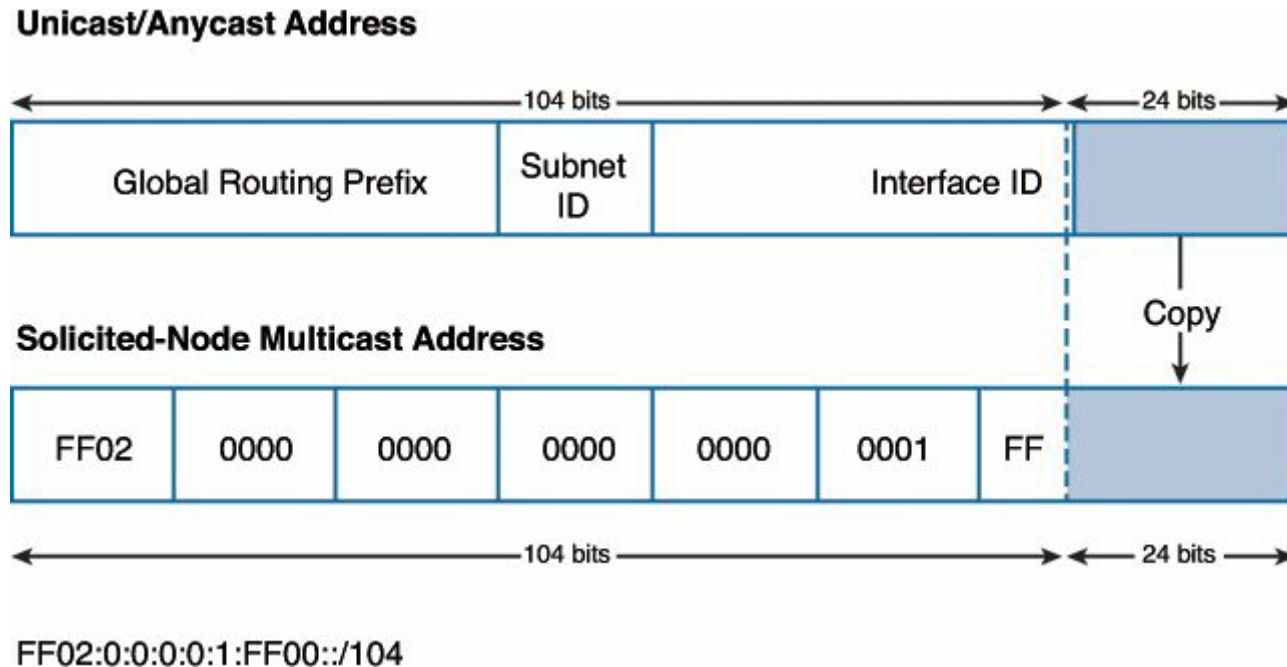
- Además de las direcciones unicast y multicast que se crean en un nodo/router, siempre se crea la dirección de **multicast Solicited-Node**:
 - **FF02:0:0:0:0:1:FF00::/104**
- Reemplaza al Broadcast de IPv4
- Estas direcciones pueden llegar a todos los dispositivos del link pero sin que todos procesen el paquete.
- Son usadas para dos mecanismos básicos de IPv6:
 - Resolución de Direcciones (reemplazo de ARP)
 - Permite obtener la MAC asociada a una IPv6
 - Duplication Address Detection (DAD)
 - Permite descubrir si la dirección IPv6 obtenida por SLAAC es única



Creación de Multicast Solicited-Node Address

- Se crean en forma automática para **cada** dirección **unicast** de un dispositivo agregando los 24 bits menos significativos al prefijo multicast.
- Estas direcciones IPv6 multicast obviamente son traducidas a direcciones multicast de la capa de acceso (Ethernet).
 - Para traducción IPv6 IEEE reservó el prefijo de 16 bits: 33:33
 - Los 32 bits restantes son copiados desde la dirección IPv6 Multicast.
- Ejemplo: PC1 con dirección Global Unicast y Link-Local
 - **Global**: 2001:DB8:AAAA:1::100
 - Se crea automáticamente: Solicited Node: FF02::1:FF**00:100**
 - Se une al grupo multicast (Ethernet): 33:33:FF:00:01:00
 - **Link Local**: FE80::50A5:8A35:A5BB:66E1 – Solicited Node: FF02::1:FF**BB:66E1**
 - Se crea automáticamente: Solicited Node: FF02::1:FF**BB:66E1**
 - Se une al grupo multicast (Ethernet): 33:33:FF:BB:66:E1

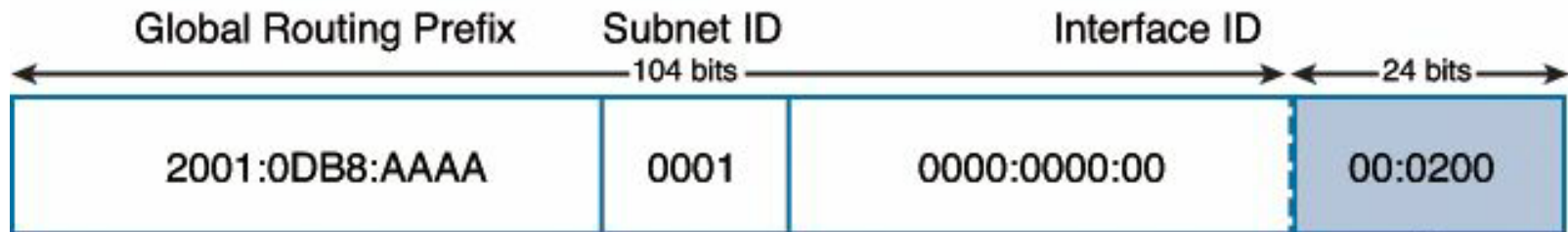
Multicast solicited node



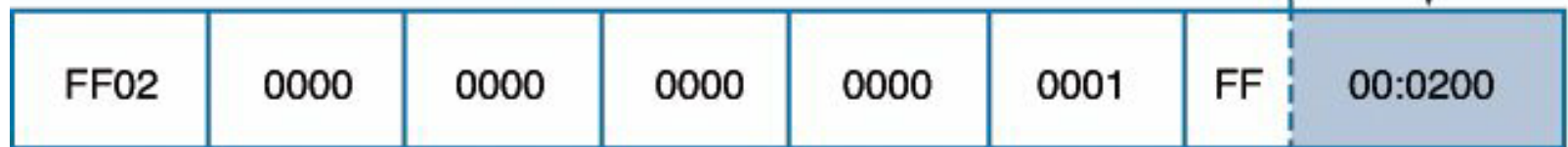
- MAC Multicast traducida asociada a cualquier dirección IPv6 Multicast se forma utilizando el prefijo MAC: 33:33 y luego insertando los 32 últimos bits de la dirección IPv6 multicast.

Solicited-Node Multicast Address: Ejemplo

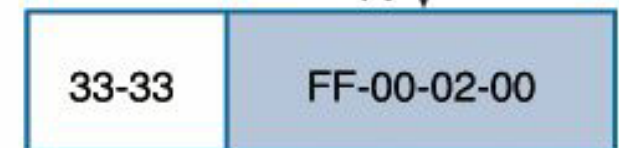
PC2's Global Unicast Address



PC2's IPv6 Solicited-Node Multicast Address



Solicited-node Multicast address mapped to Ethernet destination MAC address

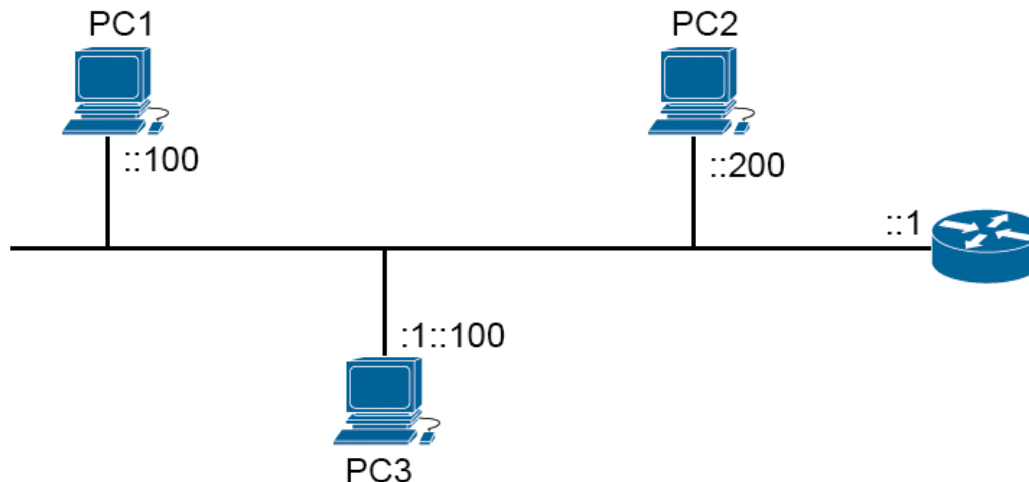


PC2's IPv6 Solicited-node multicast address: FF02::1:FF00:200

PC2's mapped solicited-node Ethernet multicast address: 33-33-FF-00-02-00

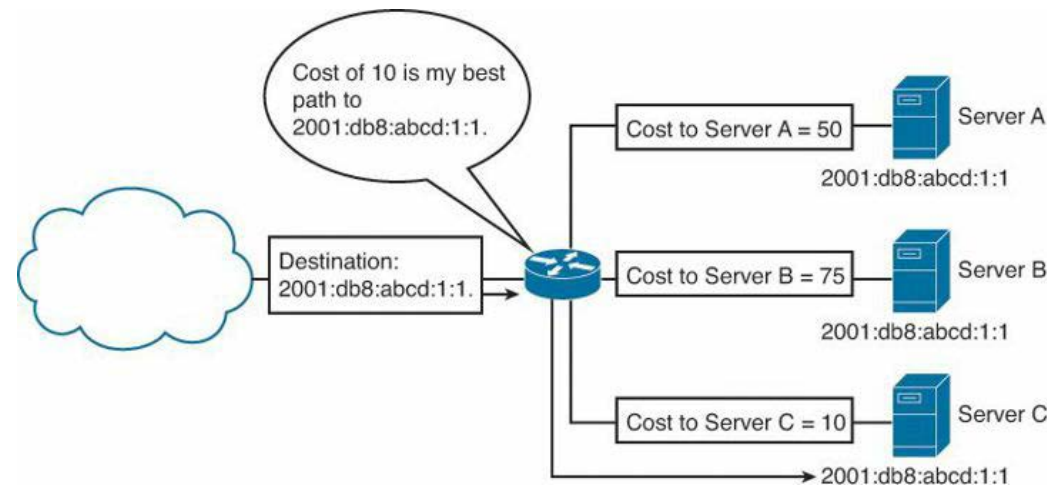
Multicast Solicited Node

- Ventaja sobre Broadcast: Pocos nodos capturan (y procesan) las direcciones Multicast Solicited Node.
- Ejemplo:
 - Prefijo de Subred: 2001:db8:aaaa:2::/64
 - Si la PC1 necesita traducir la dirección de la PC2, solamente PC2 procesa el paquete



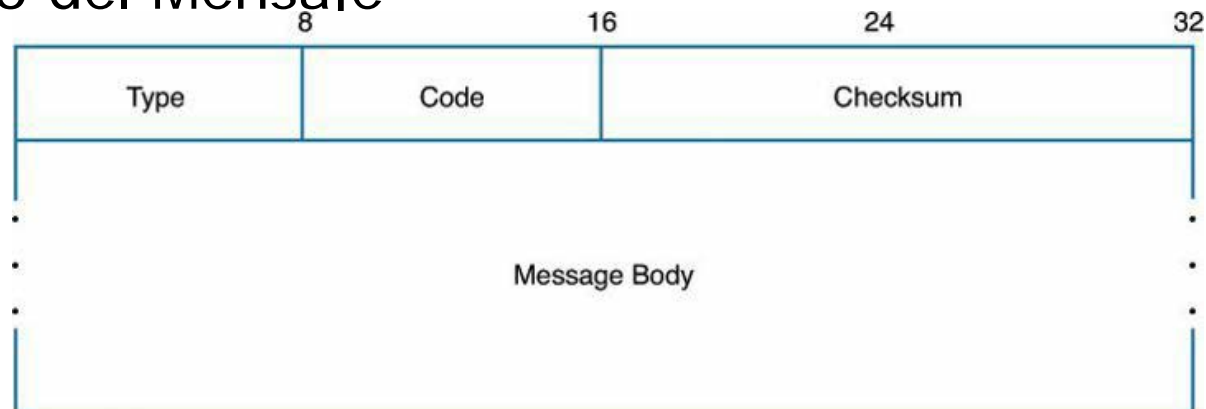
Direcciones Anycast

- Puede ser asignada a mas de una interfaz.
- Generalmente corresponde a dispositivos diferentes: Varios dispositivos pueden tener la misma dirección anycast.
- Un paquete enviado a una dirección anycast es ruteado a la interfaz mas cercana que tiene esa dirección (de acuerdo a la tabla de ruteo de los routers).
- No hay ningún prefijo especial usado para las direcciones anycast. Usan el mismo rango que las direcciones globales.
- RFC 1546 – Anycast Addresses



ICMPv6 y Neighbor Discovery Protocol

- Descripto en RFC 4443
- ICMPv6 es mucho mas robusto que ICMPv4.
 - Contiene nuevas funcionalidades y mejoras.
 - Uso Obligatorio.
- Formato del Mensaje



- Campo Type
 - Mensajes de Error: **0 a 127**
 - Mensajes Informativos: **128 a 255**

ICMPv6: Mensajes de Error

Type	Type Description	Code and Code Description
1	Destination Unreachable	0: No route to destination 1: Communication with 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
2	Packet Too Big	0: Ignored by receiver
3	Time Exceeded	0: Hop limit exceeded in transit 1: Fragment reassembly time exceeded
4	Parameter Problem	0: Erroneous header field encountered 1: Unrecognized Next Header type encountered 2: Unrecognized IPv6 option encountered
101	Private Experimentation	—
107	Private Experimentation	—
127	Reserved for expansion of ICMPv6 error messages	—

ICMP: Algunos Mensajes Informativos

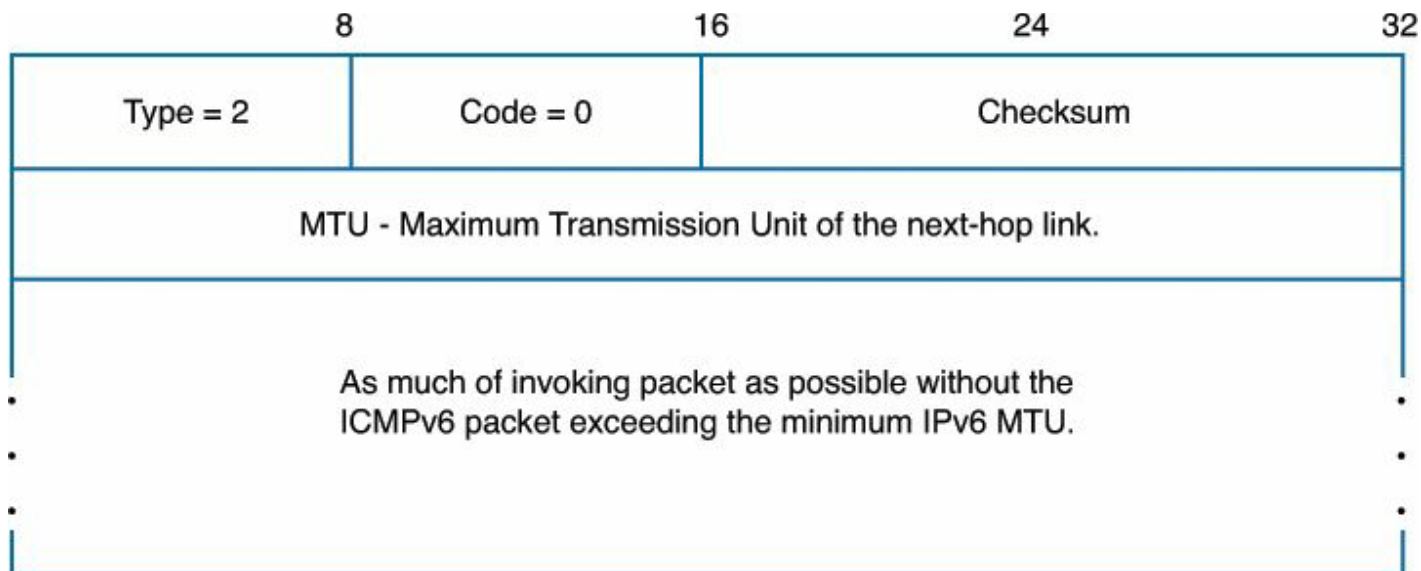
Type	Type Description	Code and Code Description
<i>Used by the ping command (RFC 4443)</i>		
128	Echo Request	0: Ignored by receiver
129	Echo Reply	0: Ignored by receiver
<i>Used for Multicast Listener Discovery (RFC 2710)</i>		
130	Multicast Listener Query	0: Ignored by receiver
131	Multicast Listener Report	0: Ignored by receiver
132	Multicast Listener Done	0: Ignored by receiver
<i>Used by Neighbor Discovery (RFC 4861)</i>		
133	Router Solicitation message	0: Ignored by receiver
134	Router Advertisement message	0: Ignored by receiver
135	Neighbor Solicitation message	0: Ignored by receiver
136	Neighbor Advertisement message	0: Ignored by receiver
137	Redirect message	0: Ignored by receiver

Ex IGMP IPv4 →

NDP →

Packet too big

- Los routers en IPv6 no fragmentan.
- Cuando reciben un paquete mas grande que el MTU de la interfaz de salida, el router descarta el paquete y envía un mensaje ICMPv6 **Packet Too Big** al origen
- Este mensaje incluye el MTU del enlace (en Bytes).
- Se utiliza para MTU Path Discovery (RFC 1981)

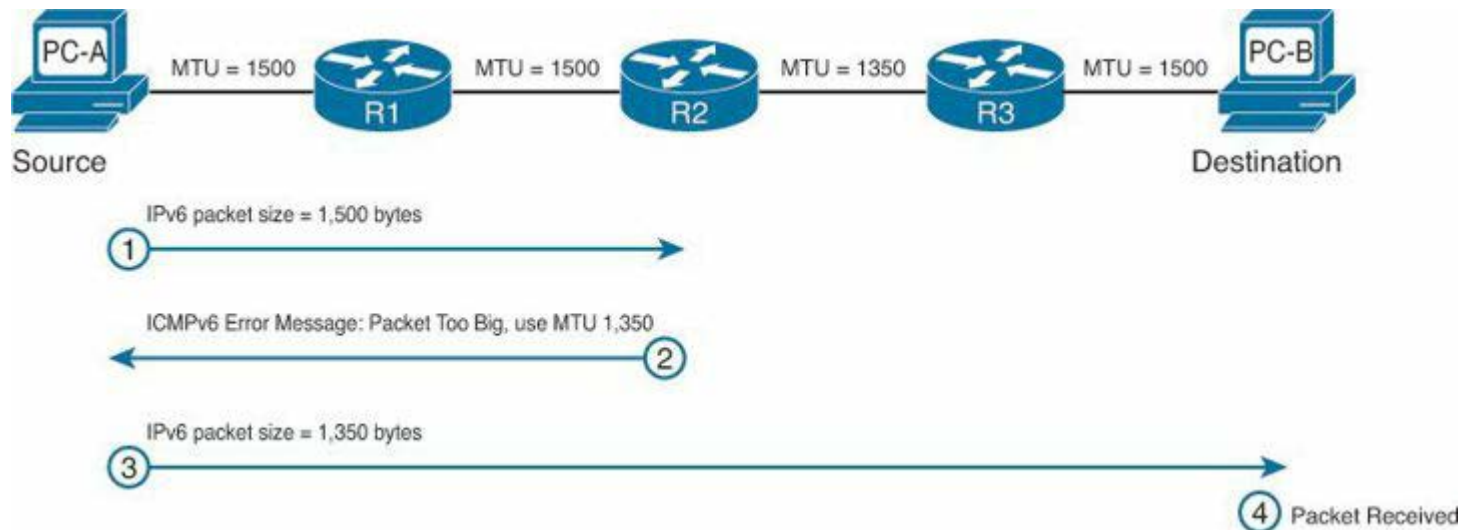


MTU Path Discovery



- Definido en RFC 1981
- Permite al origen transmitir el paquete de mayor tamaño posible sin fragmentación y sin que un router descarte un paquete por MTU pequeño.
 - IPv6 requiere que todo link en la Internet tenga un mínimo MTU de 1280 bytes (comparado con 68 bytes para IPv4).
- El tamaño de ese paquete se llama "Path MTU" (PMTU).

MTU Path Discovery



➤ Observaciones:

- El mensaje de Error ICMP contiene encapsulado el valor del MTU del próximo link
- Ya que el camino desde un origen puede cambiar, también puede cambiar el PMTU.
- Los dispositivos **no** están obligados a implementar Path MTU, pero es recomendado por el RFC 4443.
- Path MTU Discovery soporta destinos **multicast** o unicast.

Neighbor Discovery Protocol (ND ó NDP): RFC 4861

- Juega un rol importante en la configuración de direcciones IPv6
- Se usa para:
 - Stateless Address Autoconfiguration (SLAAC)
 - Determinación automática del Prefijo de Red, Default Gateway y otras configuraciones.
 - Determinar si una dirección link-local o global unicast está en uso por otro dispositivo (DAD).
 - Determinar la dirección de hardware (MAC) de un dispositivo a partir de la dirección IPv6 (equivalente a ARP)
 - Saber que vecinos son alcanzables (NUD).
 - Buscar camino alternativo al caerse un router o un camino al mismo.

Mensajes ICMPv6 para NDP



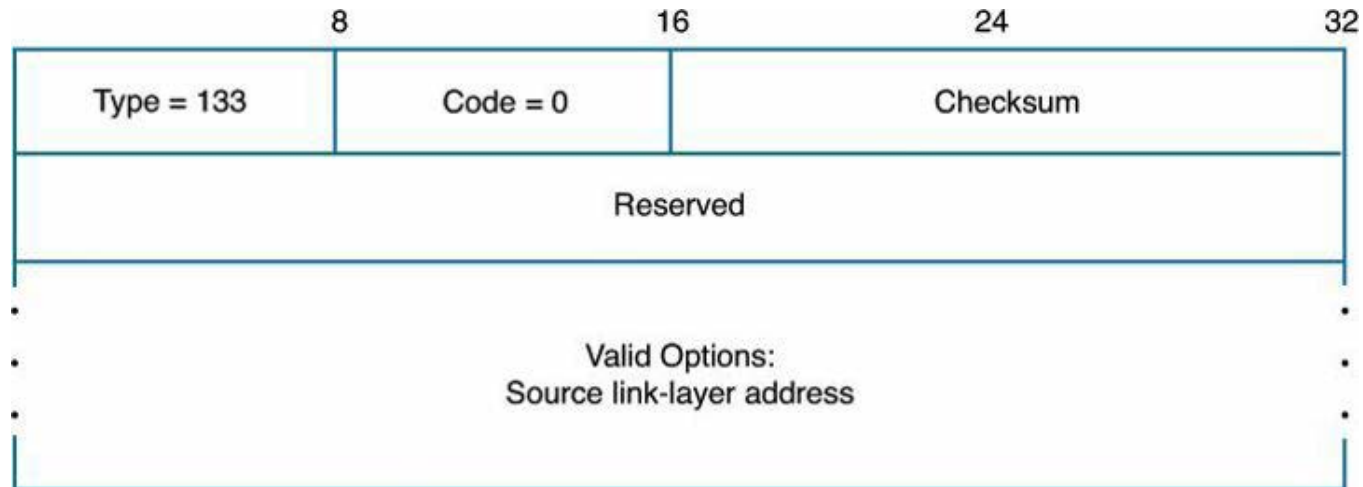
- Para NDP se usan 5 mensajes ICMPv6
 - Mensaje de Router Solicitation
 - Mensaje de Router Advertisement
 - Mensaje de Neighbor Solicitation
 - Mensaje de Neighbor Advertisement
 - Mensaje de Redirect
- Se verán estos mensajes y su uso con NDP.

Mensajes de Router Solicitation (RS) y Router Advertisement (RA)

- Los Routers envían periódicamente mensajes de “Router Advertisement” o responden a un mensaje de “Router Solicitation” de un host.
- Hosts envían un mensaje de “Router Solicitation” para solicitar una respuesta **“inmediata”** del router y que envíe el mensaje de “Router Advertisement”.
- Un host envía un mensaje Router Solicitation (RS) cuando necesita un prefijo, long. de prefijo, default gateway y otra información para SLAAC
 - Típicamente cuando se enciende una computadora y se configuró la opción de obtener IP en forma automática.
 - El host obtiene prefijo y longitud del mensaje Router Advertisement (RA)
 - La interfaz ID la genera el Host (EUI-64 Modified o Random).

Mensaje RS

➤ Formato



➤ Campos destacados en Header IPv6:

➤ Dirección origen:

- La previamente asignada o **no especificada** (si no tiene asignada dirección).

➤ Dirección destino:

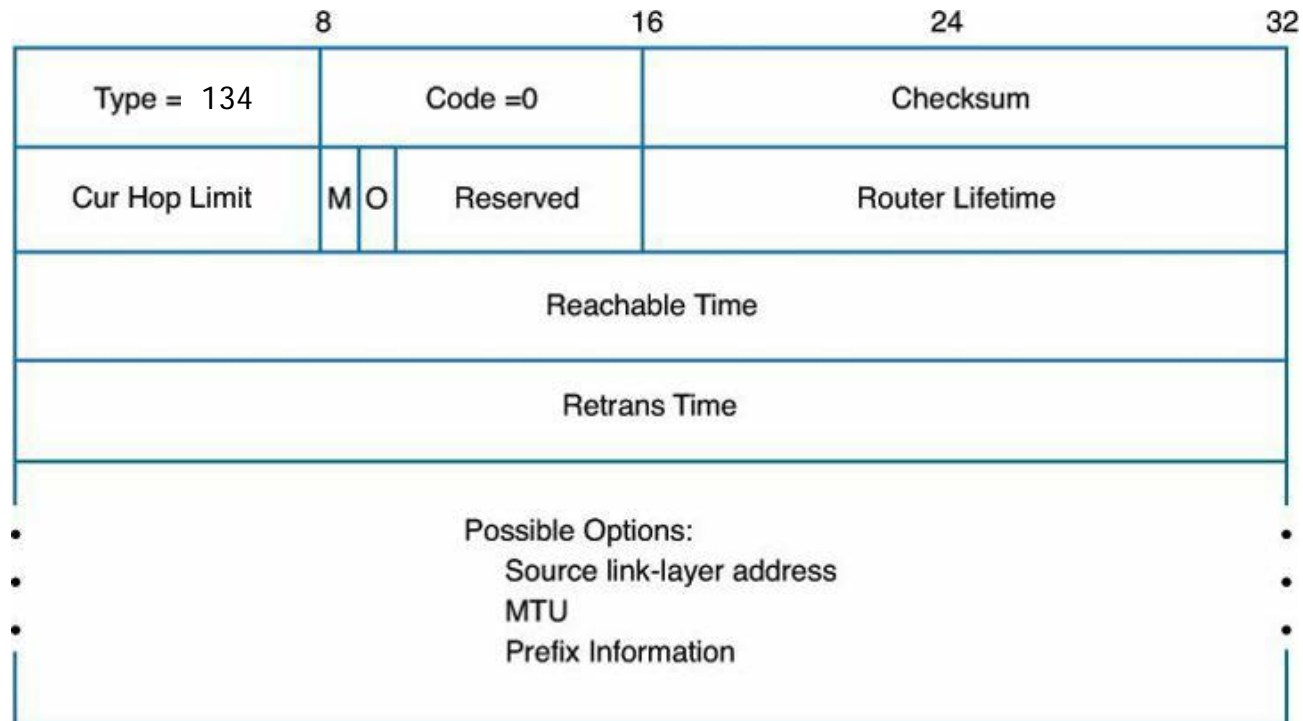
- Típicamente "All Router Multicast Address": **FF02::2**

➤ Campo destacado de ICMPv6

- **Source** link-layer add: Dirección de Capa 2 (MAC Address) del que envía el mensaje ICMP

Mensaje RA

➤ Formato:



➤ Campos destacados en **Header IPv6**:

- Dirección origen: **Link Local** asignada a la interface del router.
- Dirección destino: All nodes multicast address (**FF02::1**)

Mensaje RA



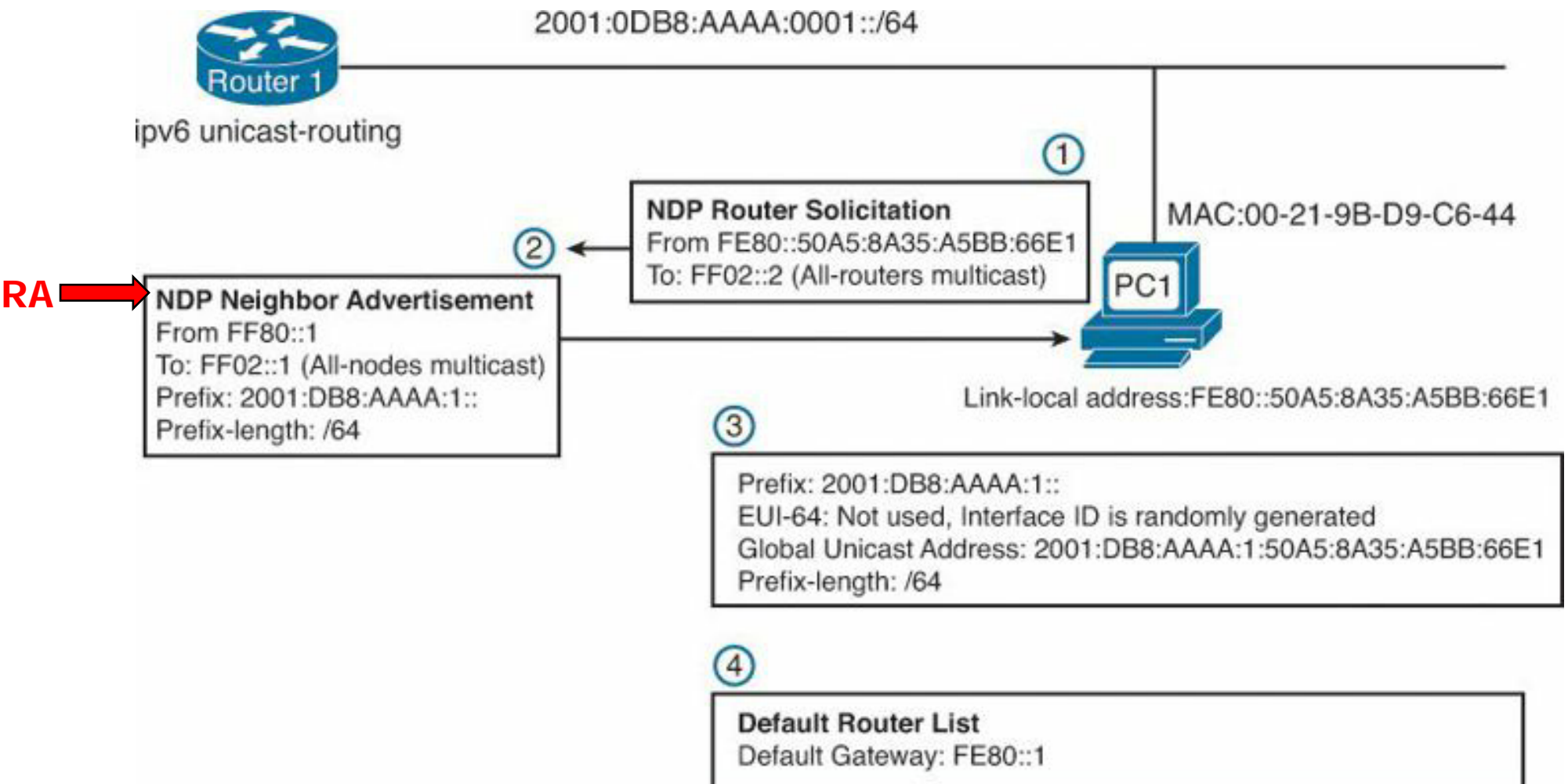
- Campos destacados de **ICMPv6**
 - Cur Hop Limit: Valor “recomendado” para TTL de los datagramas IP que enviará el host.
 - M Flag (Managed Add Configuration)
 - M = 0: Host usan SLAAC
 - M = 1: Host usan DHCPv6 (**stateful**)
 - O Flag (Other Configuration)
 - O = 0: No hay información adicional del servidor DHCPv6
 - O = 1: Deben usar DHCPv6 para parámetros que no incluyen a la dirección (como por ejemplo DNS servers)
 - Variaciones de M y O:
 - M=O=0 -> Stateless y usan otros métodos (manual) para opciones
 - M=O=1 -> Statefull (se usa DHCPv6)
 - M=0; O=1 -> Dirección obtenida desde el router (via SLAAC); opciones desde DHCPv6. Conocida como **DHCPv6 stateless**
 - M=1; O=0 -> DHCPv6 se usa para direcciones pero no para opciones. Poco usada

Mensaje RA



- Router Lifetime: Tiempo en **seg** que debe usarse este router como Default Gateway. **0** significa que no es el default router.
- Reachable Time: Tiempo en **mseg** en que un host puede asumir que un vecino es alcanzable después de recibir la confirmación. Se utiliza en **NUD** (Neighbor Unreachability Detection). **0** significa que el router no especifica un valor.
- Retrans Timer: Notifica al host intervalo de tiempo en **mseg** de retransmisión de mensajes **Neighbor Solicitation**. Se usa para resolución de direcciones y NUD
- Opciones:
 - Source Link Layer Address: MAC del router
 - MTU: Informa al host del MTU (usado para maximizar el MTU)
 - Prefix Info: Informa al host el prefijo y la longitud del prefijo de la red.
 - Incluye el **Preferred** y **Valid Lifetime** (usado por SLAAC para tiempo de vida de la dirección).

Ejemplo de uso RS y RA



Observaciones



➤ En el RS enviado por PC1:

- La dirección origen que se usa es la Link-Local (obtenida en forma automática al levantar IPv6)
- La Dirección Destino es all-routers multicast address FF02::2

➤ En el RA enviado por R1:

- Dirección Origen IPv6 es la Link Local (R1).
 - Esa dirección luego será usada como Default Gateway de PC1
- Dirección Destino All-Nodes Multicast Group
 - Pese que RA es respuesta al RS recibido de PC1 lo mismo envía el mensaje a todos los nodos.
- Los parámetros que envía el router y sus opciones dependen de la configuración del router en sí.
- Proxima transparencia muestra un ejemplo de un Mensaje ICMPv6 enviado por un router.

Ejemplo de Mensaje RA

Internet Control Message Protocol v6

Type: 134 (Router advertisement)

Code: 0

Checksum: 0x04d2 [correct]

Cur hop limit: 64 ! Hop Limit recomendado para hosts

Flags: 0x00 ! M y O flags indican que no hay
! información disponible via DHCPv6

Router lifetime: 1800 ! Este router es un gateway **válido** por los
! Próximos 1800 sec (30 min)

Reachable time: 0 ! No se especifica ningún valor

Retrans timer: 0 ! No se especifica ningún valor

Ejemplo de Mensaje RA (Opciones)

ICMPv6 Option (**Source link-layer address**)

Type: Source link-layer address (1)

Length: 8

Link-layer address: 00:03:6b:e9:d4:80 ! MAC add de R1

ICMPv6 Option (**MTU**)

Type: MTU (5)

Length: 8

MTU: 1500 ! MTU del enlace

ICMPv6 Option (**Prefix information**)

Type: Prefix information (3)

Length: 32

Prefix Length: 64 ! Long. del prefijo (/64) a ser usado en
! La autoconfiguración

Flags: 0xc0

Valid lifetime: 2592000 !Tiempo de Vida de Validez (seg)

Preferred lifetime: 604800 !Tiempo de Vida Preferido (seg)

Reserved

Prefix: 2001:db8:aaaa:1:: ! Prefijo de la red para ser usado
! por autoconfiguración

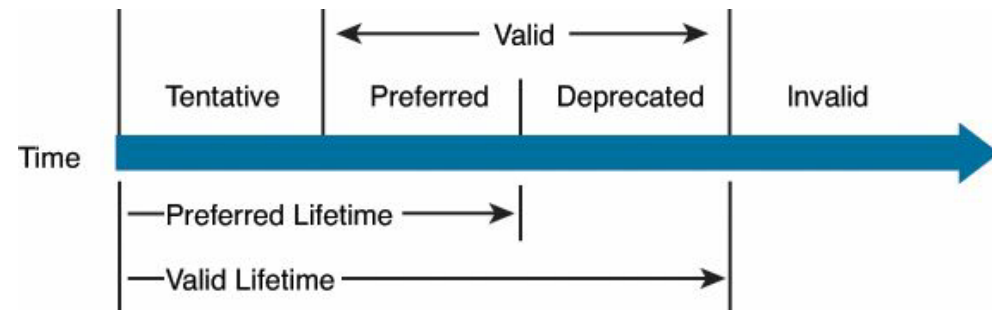
Valid Lifetime & Preferred Lifetime



- Usados por SLAAC.
- Preferred Lifetime: tiempo en que una dirección autoconfigurada permanece en el estado preferred. En ese estado puede ser usada sin restricciones.
- Expirado el Preferred Lifetime, la dirección puede seguir siendo utilizada hasta expirado el **Valid Lifetime** pero no puede crear nuevas conexiones.
- Un valor de 0xFFFFFFFF indica que el tiempo de vida es infinito.

Estado de Direcciones Autoconfiguradas

- Tentative: Siendo verificada como única por DAD
- Valid: Dirección válida pudiendo enviar y recibir paquetes unicast
- Preferred: Dirección totalmente válida para envío/recepción paquetes unicast (se pueden crear conexiones nuevas).
- Deprecated: **No** se recomienda el uso de la dirección para **comunicaciones** nuevas.
- Invalid: Dirección no puede ser usada.

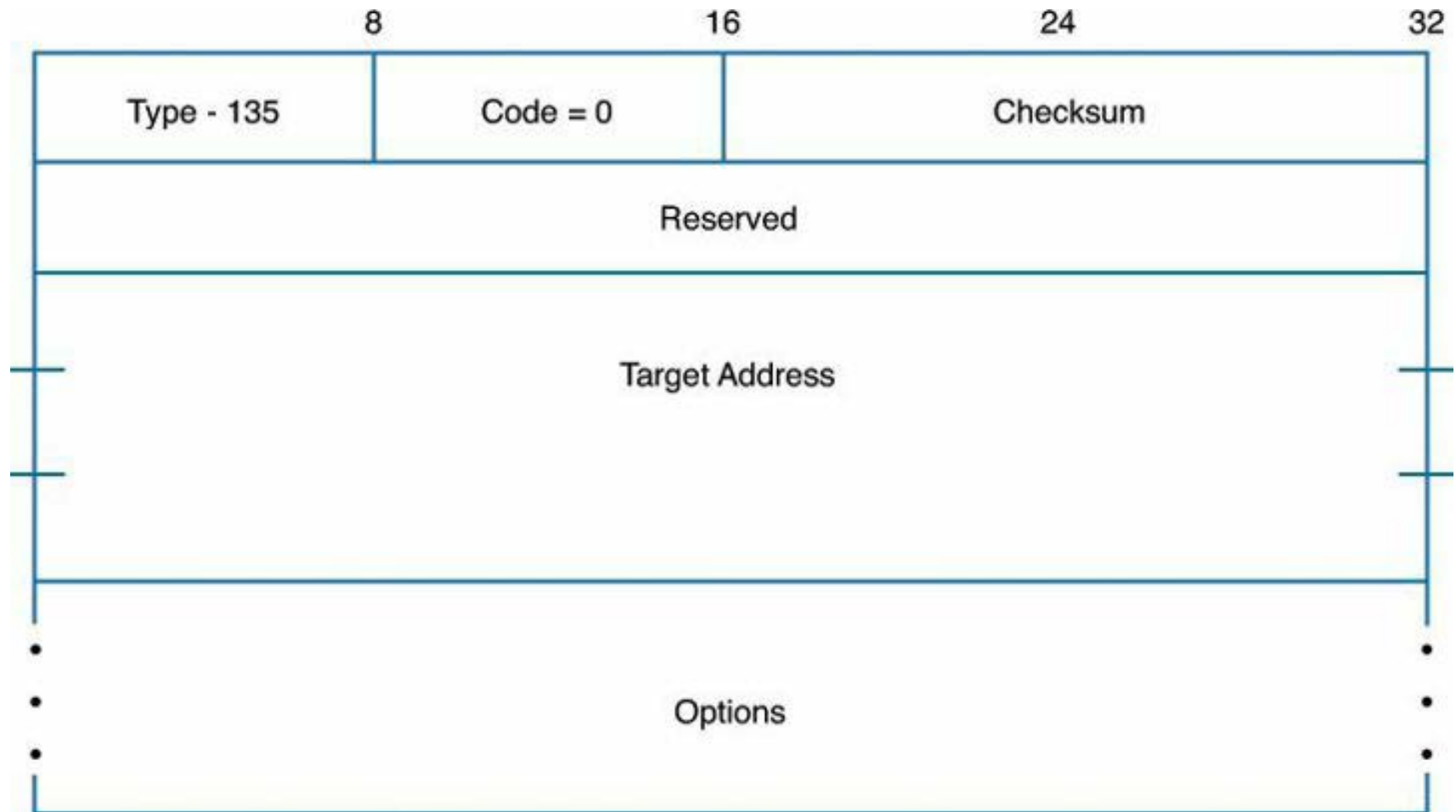


Mensajes Neighbor Solicitation y Neighbor Advertisement

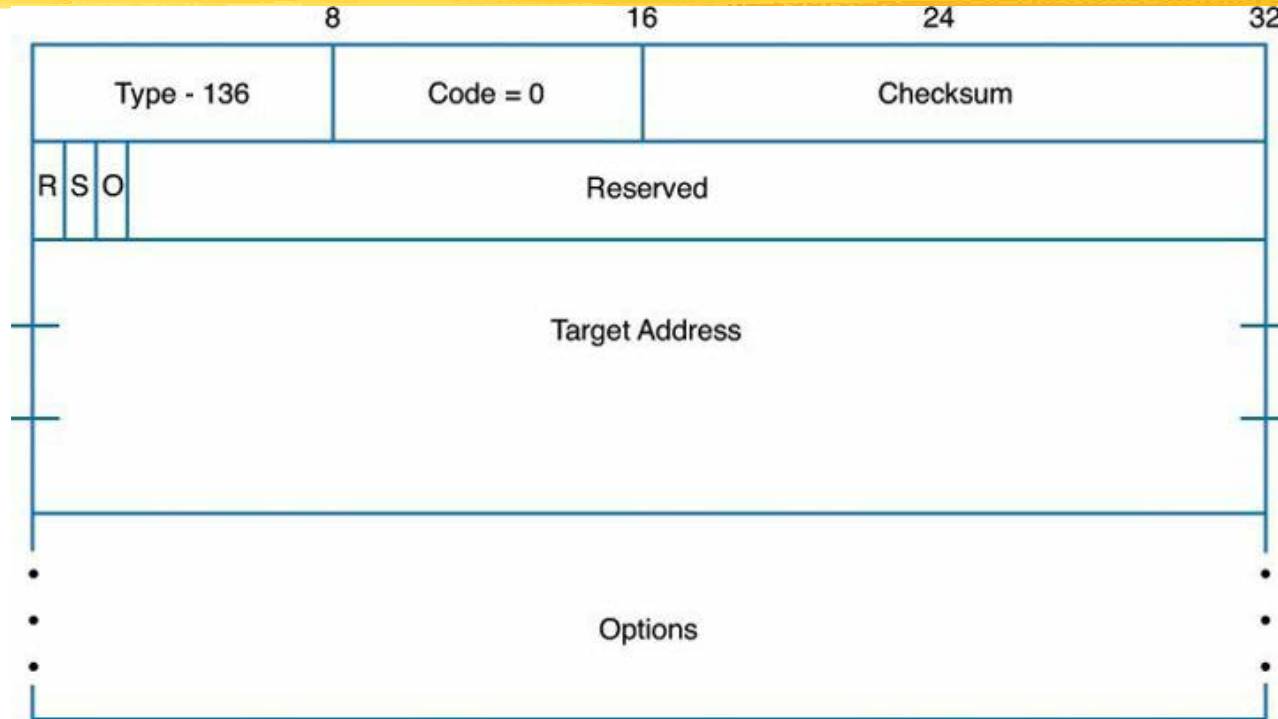


- Utilizados para solicitar dirección de Hardware (o entregar dicha dirección)
- Similares a ARP Request y Reply
- Empleados en 3 procesos:
 1. Resolución de Direcciones
 2. DAD
 3. NUD (Neighbor Unreachability Detection)

Mensaje Neighbor Solicitation



Mensaje Neighbor Advertisement



- R (Router Flag): R=1 significa que es un **router** el que envía el mensaje. Usado por **NUD**.
- S (Solicited Flag): S=1 significa que este mensaje de Advertisement es en respuesta a uno de Solicitation. Usado por **NUD**.
- O: (Override Flag): con O=1 el Neighbor Adv. debería sobrescribir el Neighbor Cache (equivalente al ARP Cache). Si O=0 se crea una entrada nueva solamente

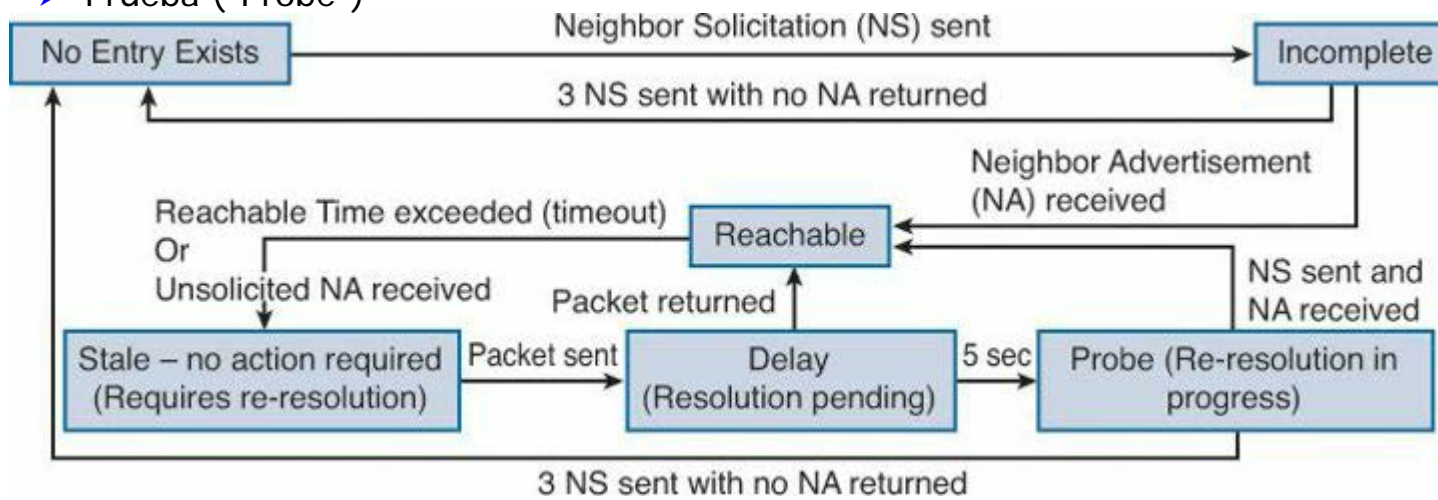
Cache Vecino y Destino



- RFC 4861 describe Estructuras de Datos que debe mantener un nodo para el uso de NDP.
- Entre ellas:
 - Cache vecino (Neighbor cache)
 - Equivalente al cache ARP en IPv4.
 - Construido con recepción de NA (y NS en cierta medida)
 - Cache destino (Destination cache)
 - Contiene una entrada por cada paquete enviado sea este local o **remoto**.
 - La diferencia con el cache vecino es **éste** (cache vecino) solo contiene entradas de nodos directamente alcanzables (vecinos).
 - El cache destino es actualizado por mensajes de redirección (no por NA).

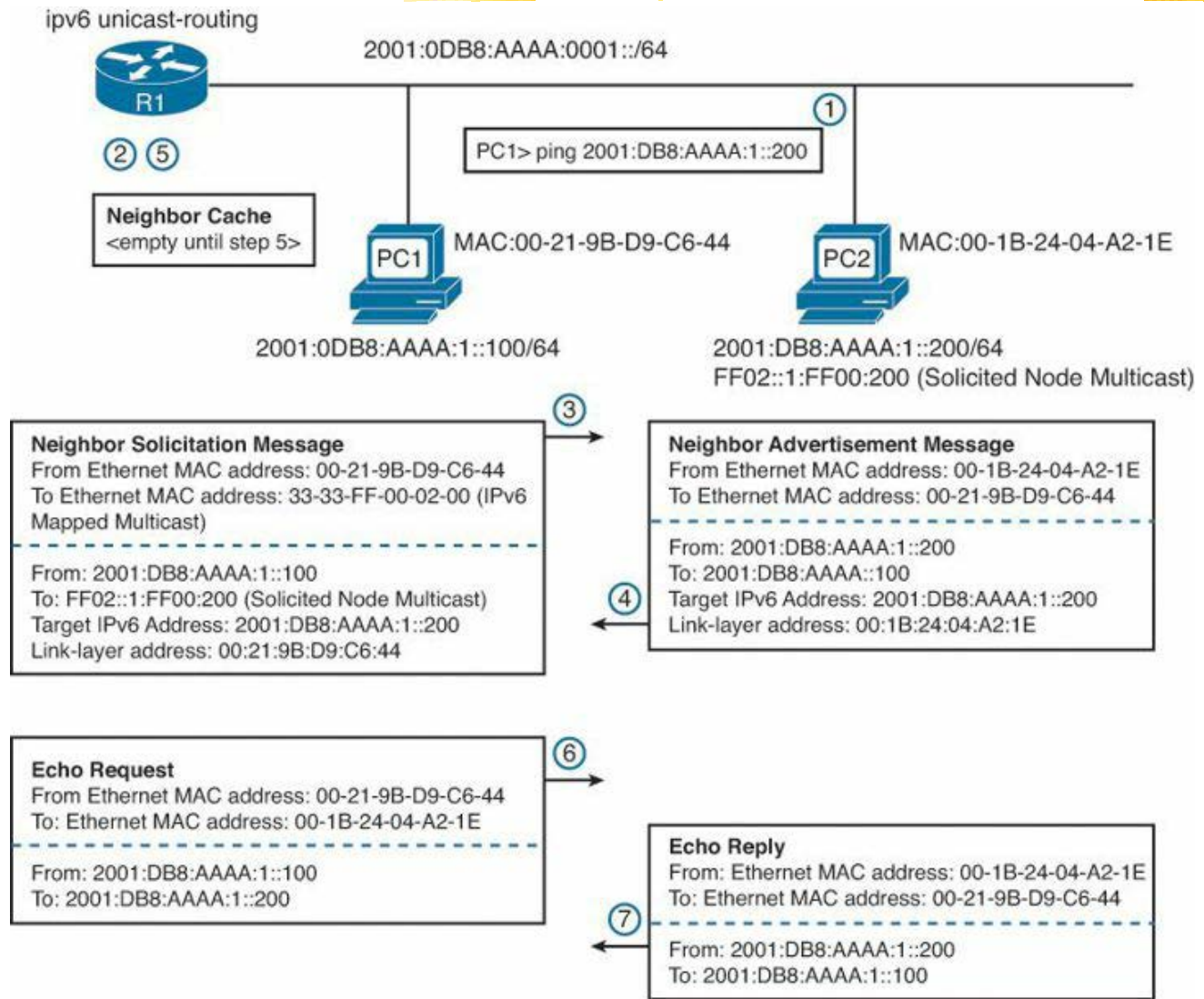
Cache de Vecinos (Neighbor Cache) y Cache Destino

- El host mantiene dos caches por interface:
 - Neighbor Cache – Equivalente a ARP Cache (subconjunto del neighbor cache)
 - Destination Cache – Lista de destinos recientes (local o remoto)
 - No contiene traducciones IPv6-MAC sino direccion de proximo salto.
- Neighbor cache
 - Una entrada en el cache puede estar en uno de 5 estados:
 - Incompleta ("Incomplete")
 - Alcanzable ("Reachable")
 - Caduca ("Stale")
 - Demorado ("Delay")
 - Prueba ("Probe")



Resolución de Direcciones

➤ Ejemplo:



Mensaje Neighbor Solicitation

MAC LAYER

! MAC Add Multicast Mapeada para PC2

Ethernet II, Src: 00:21:9b:d9:c6:44, Dst: **33:33:ff:00:02:00**

Internet Protocol Version 6

0110 = Version: 6

.... 0000 0000 = Traffic class: 0x00000000

.... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000

Payload length: 32

Next header: ICMPv6 (0x3a) ! Next header es ICMPv6

Hop limit: 255

Source: 2001:db8:aaaa:1::100 ! Global unicast add

Destination: **ff02::1:ff00:200** ! Solicited-node multicast add

Internet Control Message Protocol v6

Type: 135 (Neighbor solicitation) ! Mensaje Neighbor solicitation

Code: 0

Checksum: 0xbbab [correct]

Reserved: 0 (debería ser siempre cero)

Target: 2001:db8:aaaa:1::200 ! Add IPv6 solicitada,

! Se necesita MAC Add correspondiente

ICMPv6 **Option** (Dirección link-layer **origen**)

Type: Source link-layer address (1)

Length: 8

Link-layer address: 00:21:9b:d9:c6:44 ! MAC address **origen**

Mensaje Neighbor Advertisement

MAC LAYER

! Unicast MAC address of PC2

Ethernet II, Src: 00:1b:24:04:a2:1e, Dst: 00:21:9b:d9:c6:44

Internet Protocol Version 6

. . .

Next header: ICMPv6 (0x3a) ! Next header es ICMPv6

Hop limit: 255

Source: 2001:db8:aaaa:1::200 ! Global unicast add

Destination: 2001:db8:aaaa:1::100 ! Global unicast add

Internet Control Message Protocol v6

Type: 136 (Neighbor advertisement) ! Mensaje Neighbor Adv
!

Code: 0

Checksum: 0x1b4d [correct]

Flags: 0x40000000 ! (010) Router Flag = 0,
! Solicitation Flag = 1, Override Flag = 0

Target: 2001:db8:aaaa:1::200 ! IPv6 add del transmisor(PC2)

ICMPv6 Option (Link-layer add)

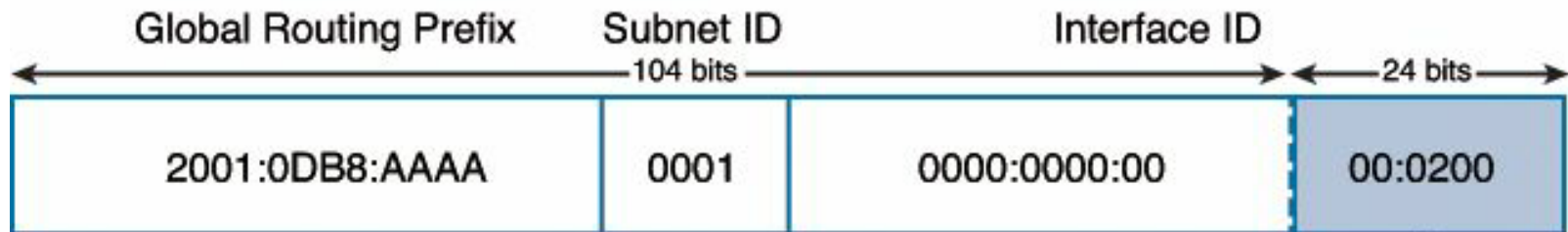
Type: Target link-layer address (2)

Length: 8

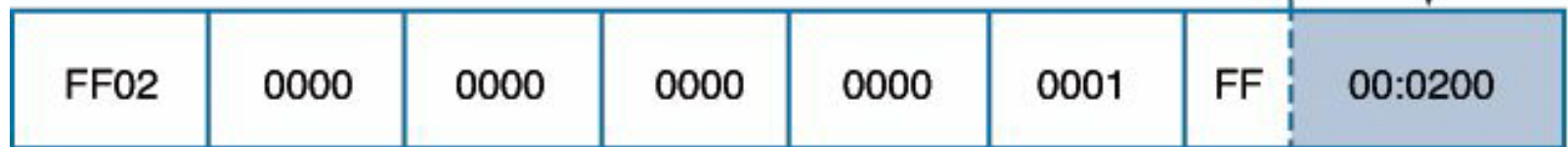
Link-layer address: 00:1b:24:04:a2:1e ! MAC add de PC2

Solicited-Node Multicast Address (PC2) (recordatorio)

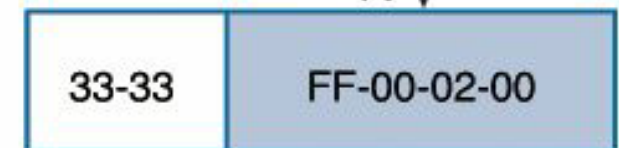
PC2's Global Unicast Address



PC2's IPv6 Solicited-Node Multicast Address



Solicited-node Multicast address mapped to Ethernet destination MAC address



PC2's IPv6 Solicited-node multicast address: FF02::1:FF00:200

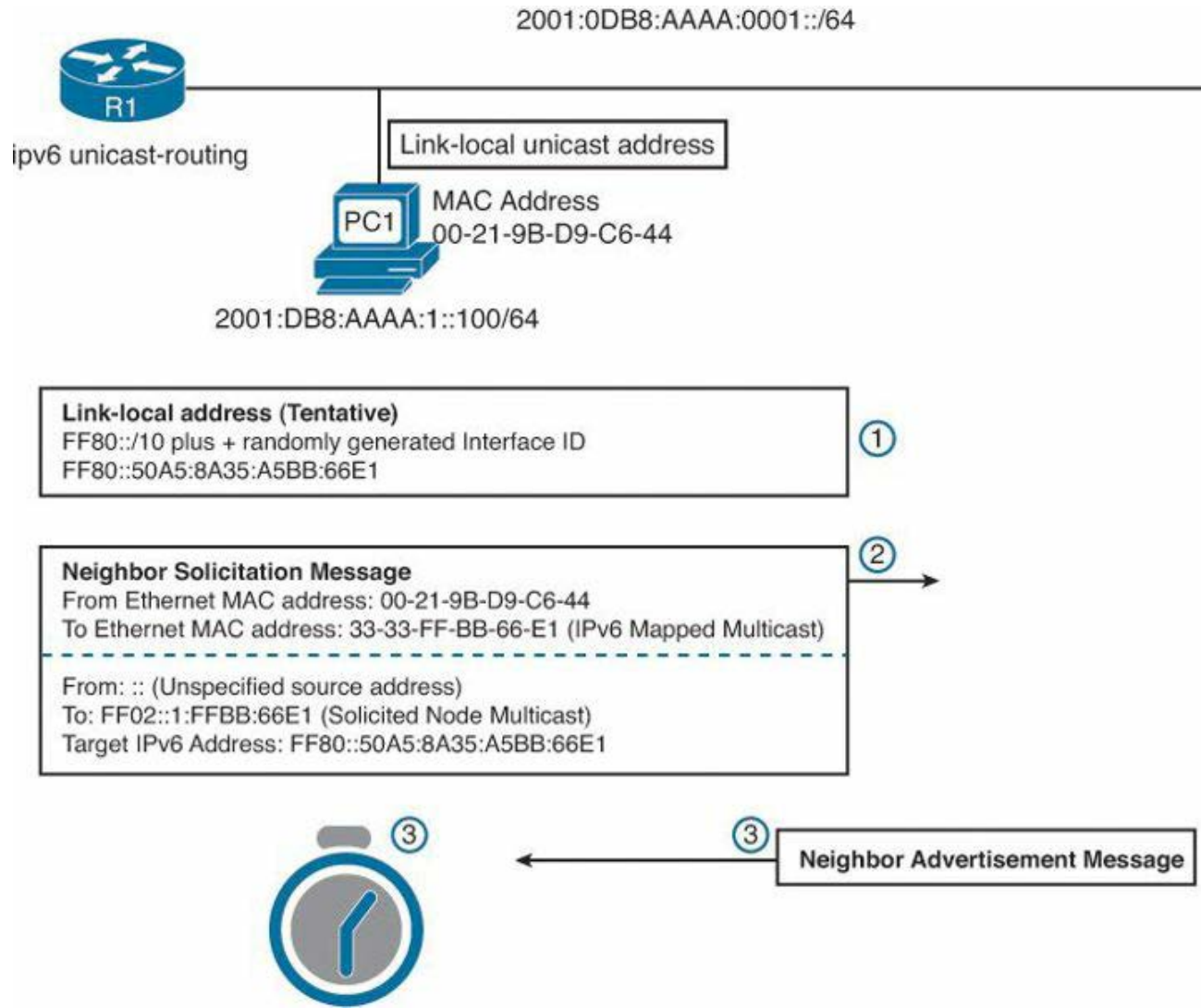
PC2's mapped solicited-node Ethernet multicast address: 33-33-FF-00-02-00

Duplicate Address Detection (DAD)



- Detecta duplicidad de direcciones (antes de confirmar su uso)
- Recomendado usar en todo tipo de Unicast Add (Link-Local o Global) independientemente de si es asignada por SLAAC, DHCPv6 o Manualmente.
- Si se detecta Dirección Duplicada **no** puede ser usada
- DAD usa mensajes de Neighbor Solicitation y Advertisement

Proceso DAD

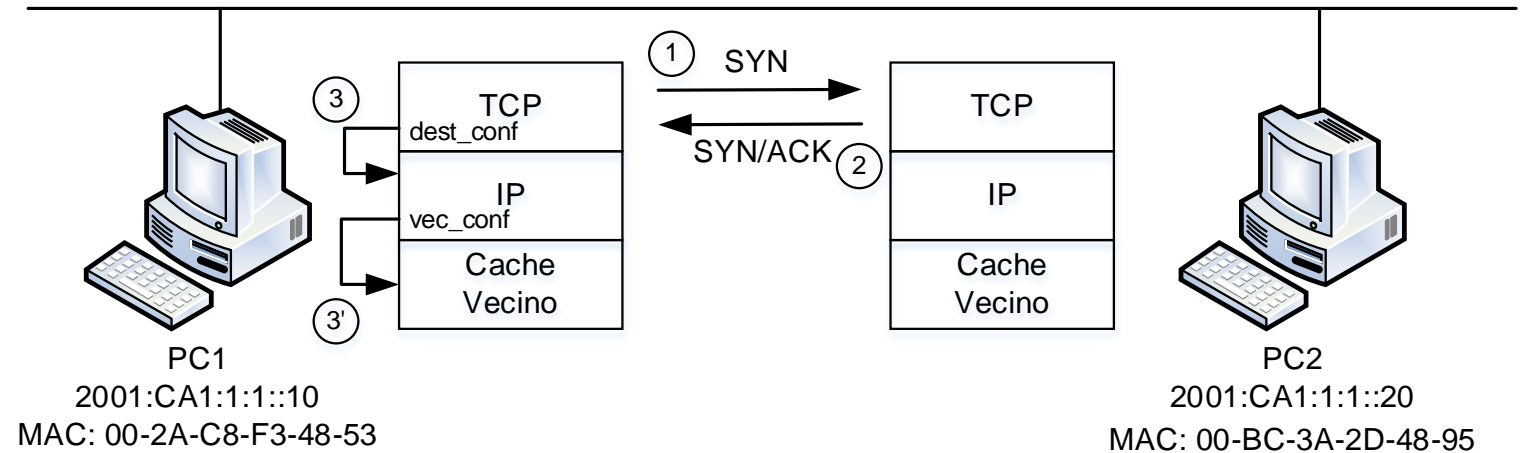


Network Unreachability Detection (NUD)



- Definido en RFC 4861
- Dispositivos continuamente chequean si los dispositivos directamente conectados son alcanzables (están activos o no)
- Válido para nodos/routers del **enlace local**.
- Si son alcanzables se desprende de:
 - Se recibe un mensaje de NA en respuesta a un mensaje de NS.
 - Proceso NUD Explícito (no se cubre en el curso)
 - Se reciben mensajes de protocolos de nivel superior (por ejemplo ACK de TCP)
 - Proceso NUD Implícito
 - (Ver ejemplo con TCP)

Ejemplo de NUD (transparente)

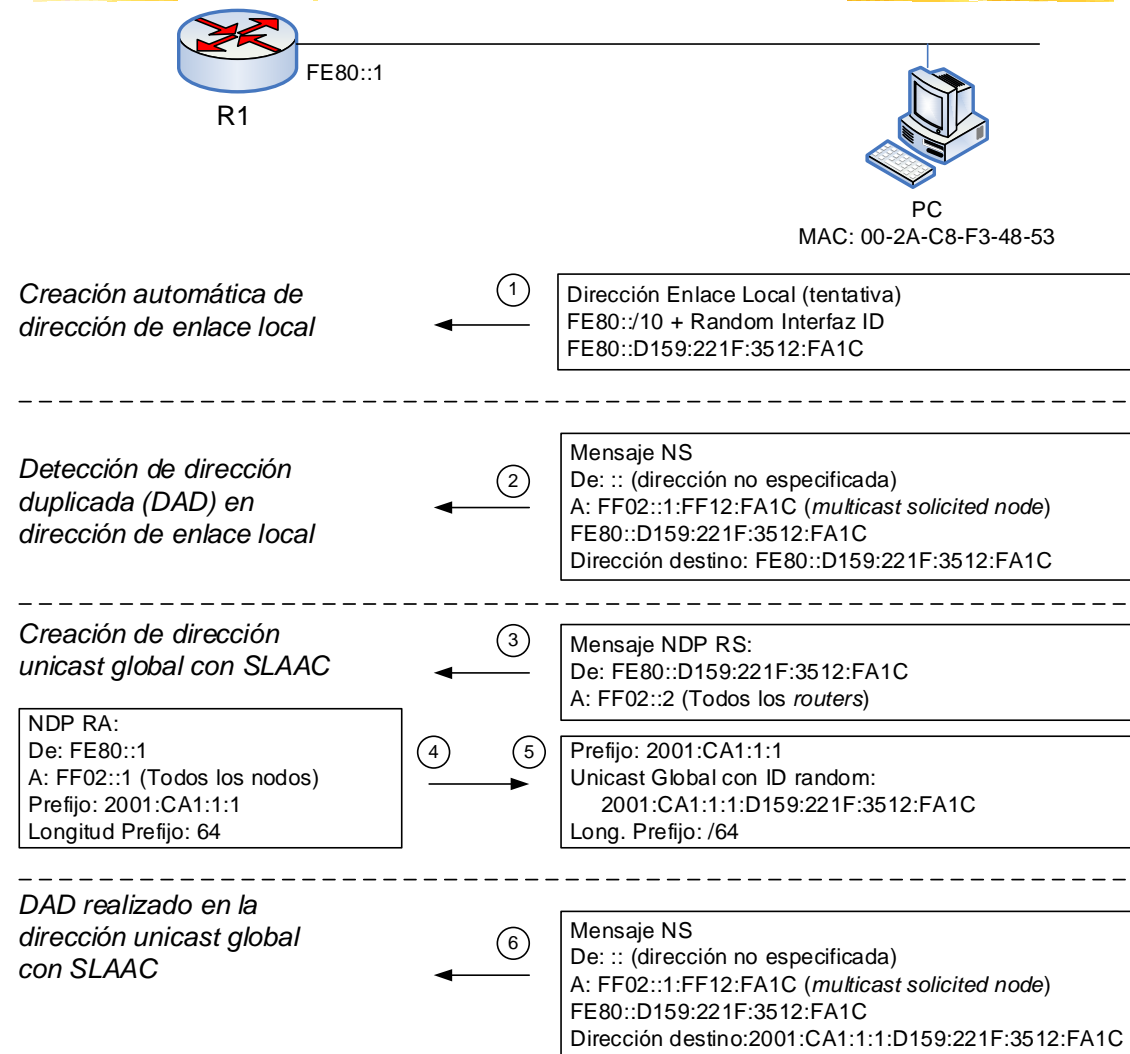


CACHE VECINO PC1

①	2001:CA1:1::20	00-BC-3A-2D-48-95	STALE (Caduco)	③
	2001:CA1:1::20	00-BC-3A-2D-48-95	DELAY (Demorado)	
	2001:CA1:1::20	00-BC-3A-2D-48-95	REACHABLE (Alcanzable)	

SLAAC (revisitado)

1. Creación de dirección Link-Local
2. DAD para link local
3. RS para obtener información del router para configuración de dirección unicast.
4. RA con Prefijo, Long. de Prefijo y opciones.
5. Concatenación del prefijo con InterfazID generado por el Nodo (EUI o Random)
6. DAD para dirección global unicast.



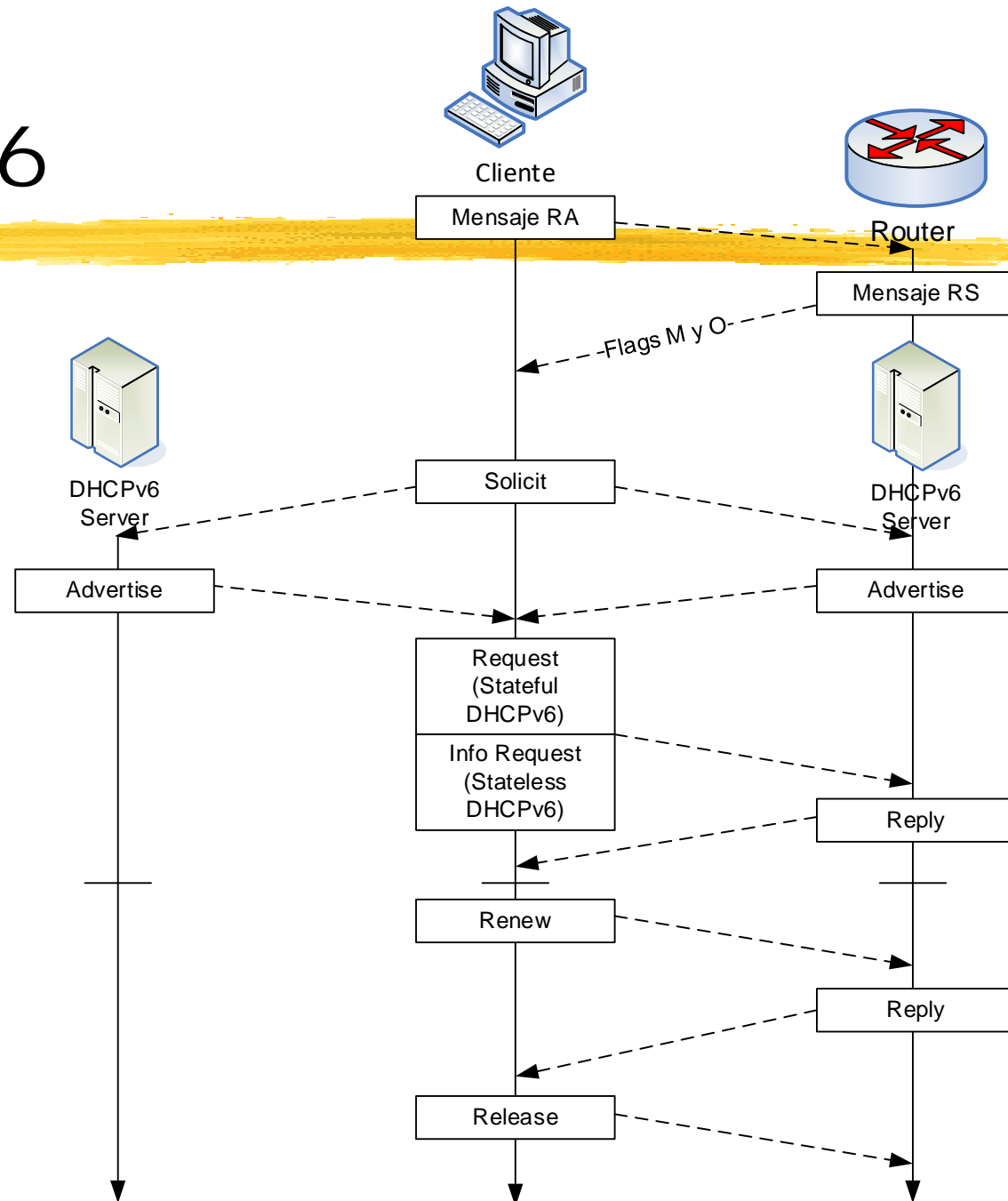
DHCPv6 vs. SLAAC

- Parecido a DHCPv4.
- Funciona sobre UDP utilizando los puertos 546 (cliente) y 547 (servidor)
- Dos RFC's:
 - RFC 3315 (2003): DHCPv6 **STATEFUL**
 - RFC 3736 (2004): DHCPv6 **STATELESS**

M	O	Tipo de Dirección	Opciones
0	0	SLAAC	Manual
0	1	SLAAC	DHCPv6 (Stateless)
1	0	DHCPv6	Sin opciones (sin uso)
1	1	DHCPv6	DHCPv6 (Stateful)

Proceso DHCPv6

- DHCPv6 Stateful (M=1 - O=1)
 - Envía mensaje **Solicit** a FF02::1:2 ("all DHCP Agent")
 - Servidores envían mensaje **Advertise**.
 - Cliente envía mensaje **Request** al servidor que le envió el advertise
 - Servidor envía **Reply** con opciones y confirmando dirección.
- Si DHCP Stateless (M=0 - O=1)
 - Envía mensaje **Information_Request**
 - Servidor envía **Reply** conteniendo opciones.
- El servidor contesta con un Reply enviado y confirmando la dirección



DHCPv6 vs. SLAAC



- DHCPv6 creado muchos años después de SLAAC (1998) con primeras implementaciones robustas en 2007.
 - Aún existe controversia si usar o no usar DHCPv6 en una red IPv6.
- Ventajas de DHCPv6:
 - Control y administración de direcciones otorgadas (stateful).
 - Se pueden establecer opciones a las direcciones.
 - Proceso de renovación establecido y predeterminado.
- Desventajas de DHCPv6:
 - No se puede otorgar router por defecto como opción (se configura a través del mensaje RA)
- Ventajas de SLAAC
 - Incluido genéricamente en IPv6. No necesita servidores externos para su funcionamiento.
 - Se autoconfigura la lista de routers por defecto
- Desventajas de SLAAC
 - No es posible configurar opciones, las que deben ser configuradas manualmente o con DHCPv6 (Stateless)

Diferencias entre DHCPv4 y DHCPv6

- Estándares e implementaciones independientes.
 - DHCPv4 evolución de BootP basado en broadcast.
 - DHCPv6 nuevo. Protocolo basado en Multicast
 - Servicios independientes en Sistemas Operativos.
- Formato del mensaje diferente
 - DHCPv6 mensaje simple, compuesto de 3 campos.

Tipo 8 bits	ID de Transacción 24 bits
Opciones (variable)	

- Usado por cliente/servidor
- Se introdujeron mensajes nuevos para hacer mas ordenado el funcionamiento del protocolo.
- Ejemplo:
 - *Renew*: renovación de dirección con el servidor que originalmente la otorgó.
 - *Rebind*: renovación de dirección con cualquier servidor.

DHCPv4 vs DHCPv6: Mensajes

DHCPv4	DHCPv6	Observaciones
DHCPDiscover	Solicit	
DHCPOffer	Advertise	
DHCPRequest	Request, Renew, Rebind	Nuevos mensajes para renovación con el mismo servidor (<i>renew</i>) o con cualquiera (<i>rebind</i>)
-	Confirm	Utilizado por cliente para saber si la dirección obtenida es válida en el enlace.
DHCPAck	Reply	Similar a ACK pero para múltiples tipos de mensajes DHCP (solicit, request, renew, etc.)
DHCPRelease	Release	
DHCPDecline	Decline	
DHCPForceRenew	Reconfigure	Cambios en el servidor. Cliente debe reconfigurar.
DHCPInform	Information-Request	Solicita parámetros al servidor (no dirección IP). Define a Stateless DHCPv6.
-	Relay-Forw	Forward desde un Relay Agent a un servidor o a otro relay agent.
-	Relay-Rep	Respuesta al Relay-forward

DHCPv6: Multicast



- Se reservaron las siguientes direcciones multicast para DHCPv6:
 - FF02::1:2
 - Todos los servidores y agentes de relay
 - Ámbito enlace local.
 - FF05::1:3
 - Todos los servidores del sitio.
 - Diseñada para que los agentes de relay envíen un mensaje de solicitud a todos los servidores DHCP del Sitio
 - Poco uso puesto que los agentes normalmente contactan a un servidor (o grupo de ellos).

Otras funciones de DHCPv6



- Delegación de prefijos de red.
 - Delegación de prefijo de un router a otros.
 - Útil para ISP
- Otorgamiento de Direcciones en Dos Fases
 - Opción Rapid Commit
 - Usada principalmente cuando hay un solo servidor DHCPv6 o se usa DHCPv6 Stateless.
 - Mensajes:
 - Solicit o Information-Request
 - Reply
 - Para usar esta opción se debe habilitar en el cliente (el mensaje Solicit incluye una opción de Rapid Commit en el mensaje)

Aspectos Misceláneos de IPv6



➤ Ruteo con IPv6

- Igual proceso que en IPv4
- Ruteo estático (manual) o dinámico
- Ruteo dinámico: Nuevos protocolos
 - Ruteo interior: RIPv3 – OSPFv3
 - Ruteo exterior: BGP-4
- Red mixta IPv4 – IPv6 se mantienen dos tablas de ruteo independientes

➤ Protocolos de Transporte

- Ningún cambio, excepto por el cálculo de los checksum ya que utiliza un pseudo-encabezamiento con direcciones IP

Otros aspectos de IPv6

➤ Resolución de nombre

➤ Se sigue utilizando la resolución estática y dinámica (DNS)

➤ DNS

➤ Se introduce el registro AAAA en lugar de A para especificar una dirección IPv6 asociada a un nombre.

➤ Se cambia el nombre del dominio raíz para la traducción inversa

- ip6.arpa

➤ Un nodo que posee dirección IPv4 e IPv6 deberá tener un registro A y AAAA

- Primero se devuelve el RR AAAA y en caso de que el nodo origen no tenga IPv6, luego de un tiempo de NO-CONEXIÓN se procede a solicitar el RR A.

- Para evitar espera conviene introducir dos nombres diferenciados:

- www6.unt.edu.ar. IN AAAA 2001:DB8::10:2aa:ff:fe21:5a88
- www.unt.edu.ar. IN A 200.45.169.29

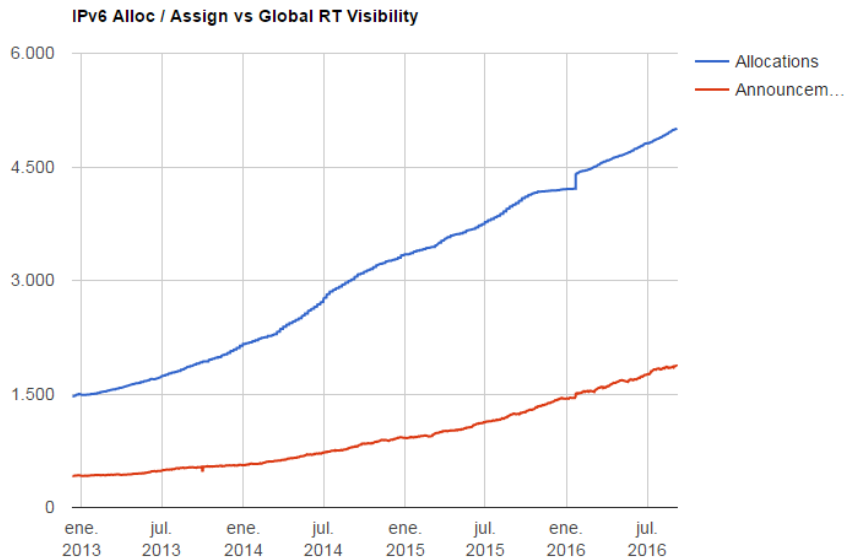
Coexistencia e Integración IPv4 – IPv6



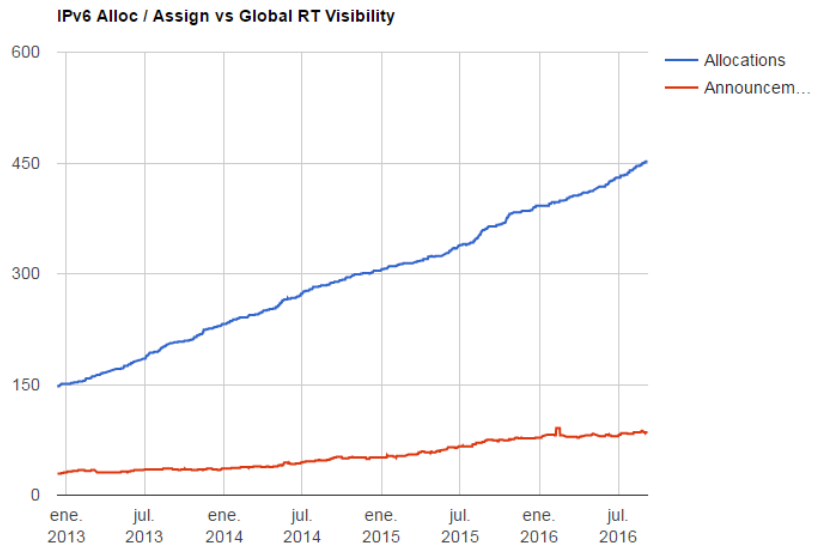
- Agotamiento de direcciones IPv4 reportado por la mayoría de los RIR's (entre ellos LacNic).
- Adopción de IPv6 a nivel mundial baja
- En Latinoamérica el país de mayor adopción acceso a Internet con IPv6 es Perú seguido de Ecuador.
- En Argentina el grado de adopción es casi nulo.
- En bloques asignados de direcciones IPv6 lidera Brasil seguido por Argentina.

IPv6 Argentina vs. Latinoamerica

➤ LACNIC Labs OpenData:: IPv6 Stats - Routing Table Evolution



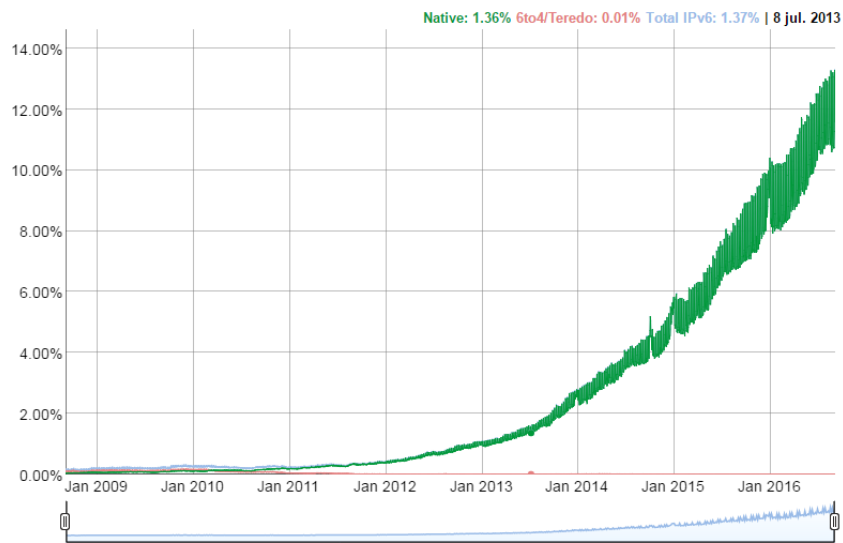
Latinoamérica



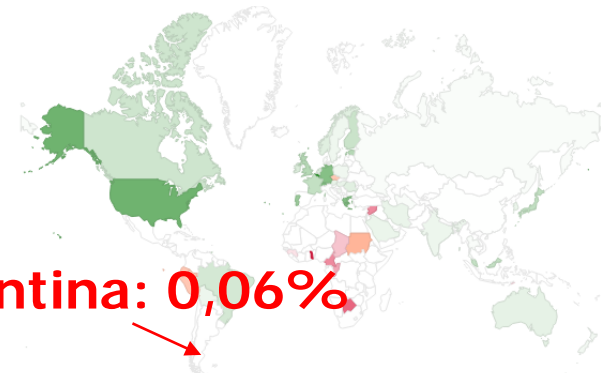
Argentina

IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



Per-Country IPv6 adoption



World | Africa | Asia | Europe | Oceania | North America | Central America | South America

The chart above shows the availability of IPv6 connectivity around the world.

- 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.

<https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption>

Coexistencia IPv4 – IPv6



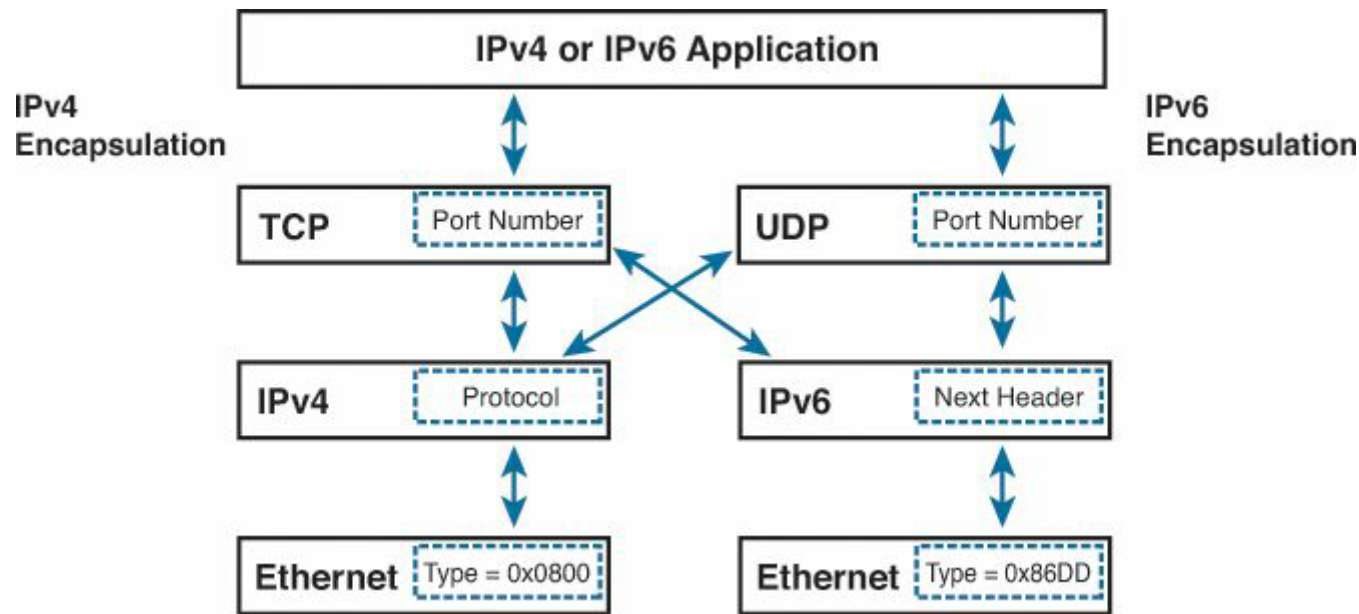
- En necesario la coexistencia y migración de IPv4 a IPv6
- IETF creó mecanismos y herramientas para la migración.
- Se pueden agrupar en 3 categorías:
 - Dual Stack: Coexistencia de IPv4 e IPv6 en un mismo host o router
 - Tunneling: Encapsulación de paquetes IPv6 dentro de IPv4
 - Traducción: NAT64 permite que dispositivos IPv6 se comuniquen con dispositivos IPv4

Dual Stack



- Un dispositivo dual stack tiene soporte completo para IPv4 e IPv6
- Puede ser una impresora, un computador, un **router**, o cualquier otro dispositivo.
- En IPv4 incluye:
 - Dirección IPv4 (4 octetos) – ARP – ICMP
 - En un router: soporte de ruteo estático o dinámico (RIP, OSPF...)
- En IPv6 incluye:
 - Direcciones Global y Link-Local
 - ICMPv6 y SLAAC con DAD
 - En un router: Ruteo estático y dinámico
 - También puede realizar tunneling y/o servicios de traducción.

Aplicaciones con Dual Stack



- La trama Ethernet que transporta IPv4 es idéntica a la que transporta IPv6. Observar campo **TYPE**
- **NOTA:** Que un switch L2 no soporte IPv6 no significa que no puede retransmitir paquetes que llevan encapsulado IPv6 sino que no puede ser **administrado** vía un host IPv6 (only)
- Se introdujeron extensiones para la interface de sockets (ver RFC 3493)

Dual Stack

- Una aplicación puede soportar IPv4 e IPv6
- El dispositivo con dual-stack **NO** elige aleatoriamente que protocolo usar.
- DNS:
 - Una aplicación que soporta ambos protocolos solicita todas las direcciones IP del servidor DNS
 - Si DNS envía direcciones IPv4 e IPv6 selecciona una (normalmente IPv6)
 - El dispositivo se comunica con una **única** dirección IP
 - El algoritmo de selección depende del Sistema Operativo
 - Ver RFC 4472 (Operational Considerations and Issues with IPv6 DNS)
- IP:
 - Si la aplicación utiliza una dirección IP en lugar de un nombre (FQDN) usará el protocolo correspondiente a la dirección IP
 - Ejemplo con IPv4: <http://192.168.1.1> – El browser usará IPv4
 - Con IPv6 existe conflicto porque el signo **:** es usado para indicar un puerto.
 - Se debe encerrar la dirección IPv6 entre corchetes.
 - Ejemplos con IPv6:
 - [http://\[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210\]:80/index.html](http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html)
 - [http://\[1080::8:800:2000C:417A\]/index.html](http://[1080::8:800:2000C:417A]/index.html)

Configuración de Dual-Stack



➤ Hosts:

- Cada interface se configura con una IPv4 y una IPv6 y parámetros opcionales (D. Gateway, DNS, etc.)

➤ Routers:

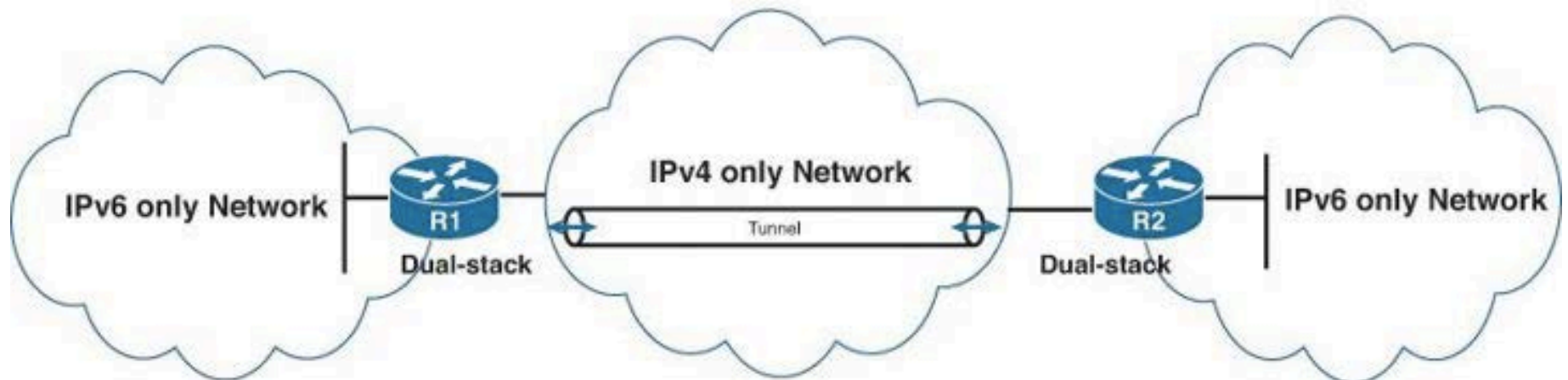
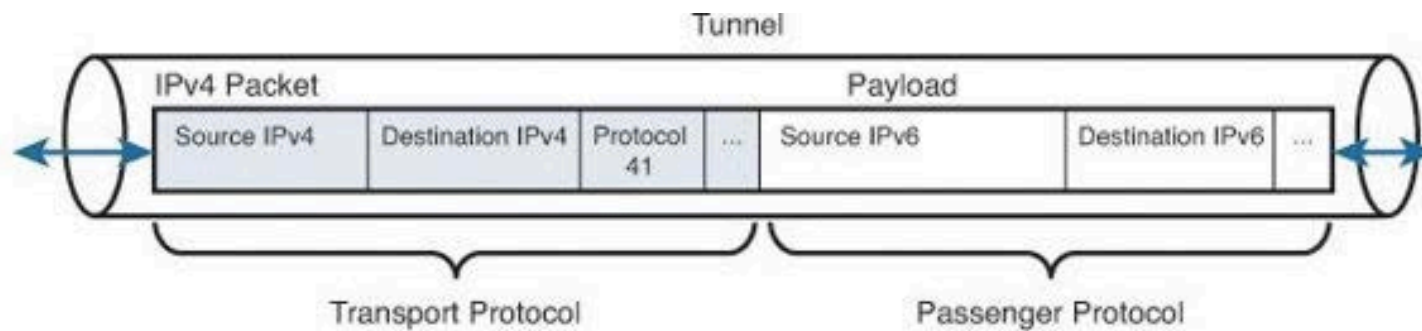
- Interfaces idem a un hosts
- Tablas de ruteo:
 - Una para IPv4
 - Una para IPv6
- Protocolos de Ruteo (dinámico)
 - Habilitar la versión para cada protocolo. Ejemplo
 - IPv4: OSPFv2
 - IPv6: OSPFv3

Tunneling



- Encapsulación de un paquete **IPv6 dentro** de un paquete **IPv4**
- Solución **temporaria** hasta implementación definitiva de IPv6
- Un tunel posee dos tipos de protocolos:
 - Protocolo de Transporte:
 - IPv4. Protocol Number: 41 (denota IPv6 encapsulado)
 - Protocolo Pasajero (Passenger Protocol):
 - IPv6

Tunneling

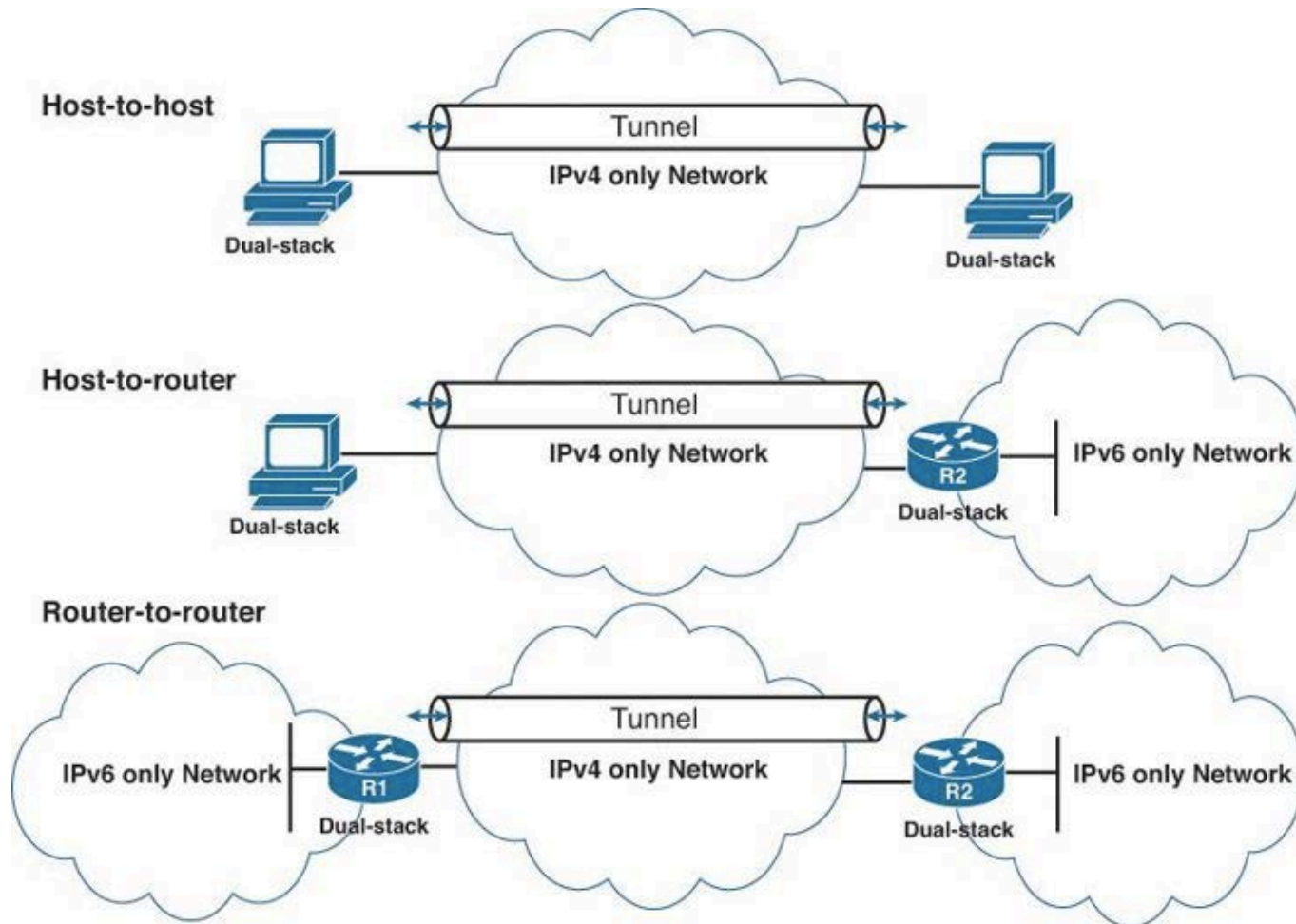


Tunneling: Componentes



- Un tunel involucra 2 dispositivos, puntos finales del tunel y un protocolo de administración
- Componentes:
 - Punto de entrada al tunel: Dispositivo **dual-stack** donde se encapsula IPv6
 - Punto de salida del tunel: Otro dispositivo **dual-stack** donde se desencapsula IPv6
 - Administración del tunel: Se realiza en el punto de entrada y salida. Involucra encapsulación/desencapsulación, direccionamiento, MTU, fragmentación y procesamiento de error.

Tunneling: Escenarios



Tipos de Túneles

Tipo de Túnel	Origen del Túnel	Destino del Túnel	Observaciones
Manual	Dirección IPv4 o referencia a interface con IPv4	Dirección IPv4	Solo puede transportar tramas IPv6
IPv4 Compatible	Dirección IPv4 o referencia a interface con IPv4	No requerido. Se genera automáticamente	Cisco recomienda NO usar este tipo de Túnel.
ISATAP	Dirección IPv4 o referencia a interface con IPv4.	-	Túneles punto a multipunto usado para conectar sistemas dentro de un sitio.
6to4	Dirección IPv4 o referencia a interface con IPv4	Se calcula la IPv4 por paquete usando la dirección IPv6 destino	

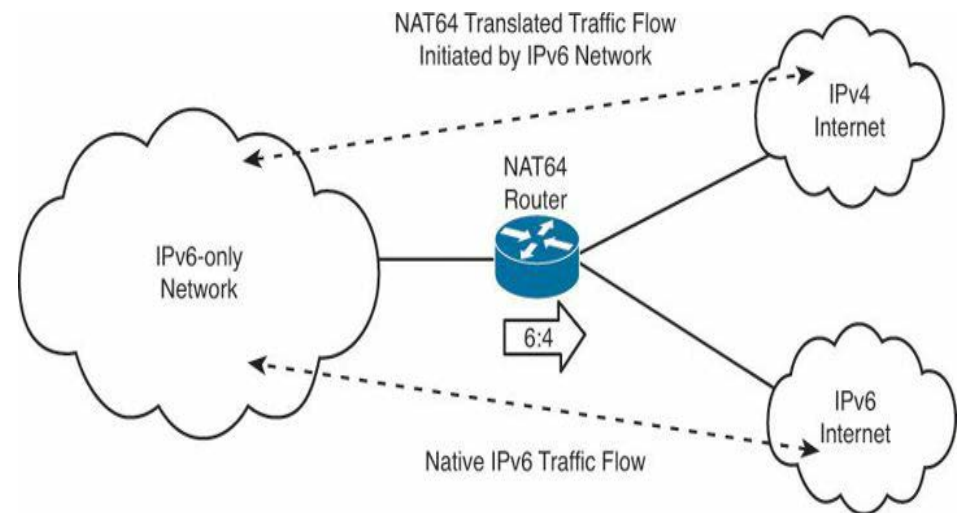
Tipos de Túneles



- Otros túneles:
 - GRE
 - 6RD
 - Teredo
 - ...
- Los más comunes son:
 - Manual
 - 6to4
 - ISATAP

Translation: NAT64 (RFC 6146)

- NAT64 es un mecanismo para transición IPv4 a IPv6 y además para coexistencia entre IPv4 – IPv6
- Objetivo de NAT64:
 - Permitir comunicación de un cliente IPv6 (**only**) a un Servidor IPv4 (**only**)
 - Necesita **DNS64**
 - También comunicación de un cliente IPv4 (**only**) a un servidor IPv6 (**only**)
 - Necesita intervención manual.



NAT64

- (Stateful) NAT64 realiza traducción entre IPv6 e IPv4:
 - Traducción de “Headers” entre ambos protocolos (RFC 6145)
 - Traducción de “Direcciones” entre ambos protocolos (RFC 6052)
- Existen 3 Componentes en NAT64:
 1. Prefijo NAT64
 - Puede ser /32, /40, /48, /56, /64 ó /96 usado para la conversión
 - Puede ser NSP (Network-Specific Prefix) o un WKP (Well-Know Prefix)
 - NSP: Asignado por la organización (gralmente una subnet del prefijo IPv6 de la organización)
 - WKP: 64:FF9B::/96. Utilizado cuando no se configura un NSP.
 - Con este prefijo IPv6 se mapearán las direcciones IPv4
 2. Servidor DNS64
 - Obtiene registro AAAA para IPv6 ó en caso que no se encuentre, obtiene el registro A para IPv4 y lo convierte usando el prefijo NAT64 a una dirección IPv6.
 3. Router NAT64
 - Anuncia el prefijo NAT64 en la red IPv6 (Only)
 - Convierte datagramas IPv6 \leftrightarrow IPv4

NAT64: Ejemplo

