Capacitación: Despliegue de IPv6

Teoría Día 2

Alvaro Vives (alvaro.vives@consulintel.es)

ALICE2 – CLARA Technical Training
July 6 to 8, 2020
San Salvador, El Salvador

This project is funded by the European Union

A project implemented by CLARA

Agenda

5. Gestión de Red sobre IPv6
6. DNS IPv6
7. Seguridad IPv6

5. Gestión de Red sobre IPv6

Gestión de Red

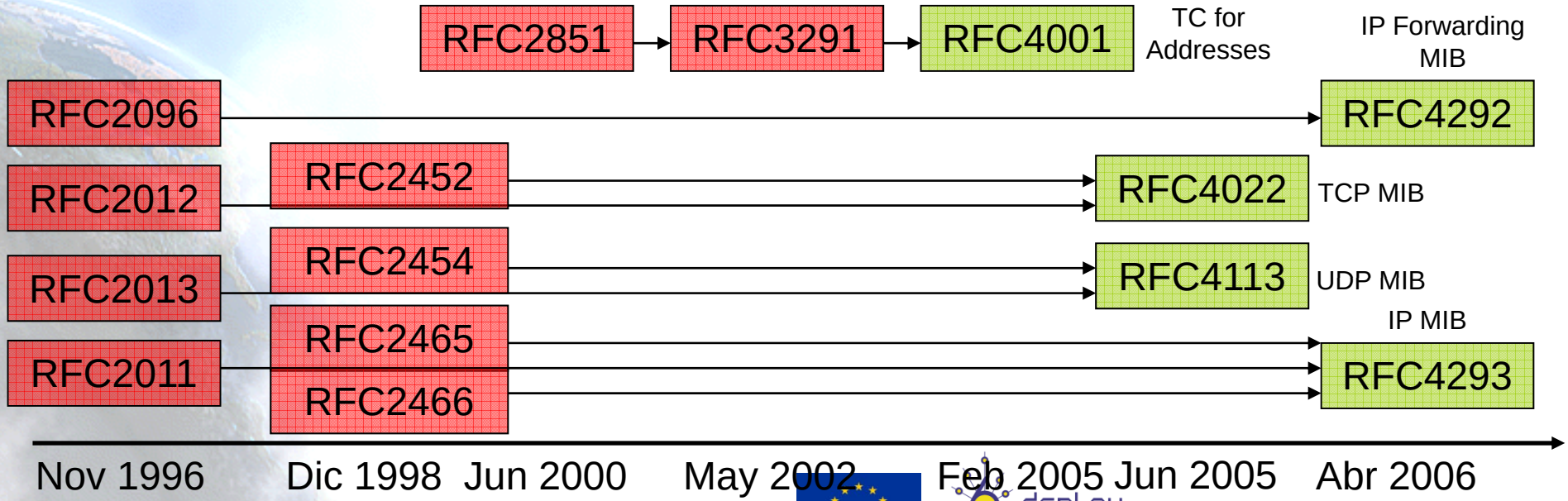
- La gestión de una o más redes estará compuesta de muchas partes:
  - Monitorización, Configuración, Inventariado, Topología, Gestión de incidencias, Seguridad, Contabilidad, etc.
- Lo “normal” ahora mismo son las redes doble-pila, se pueden hacer cosas sobre ambos protocolos, complementándose
- Algún día habrá sólo IPv6, ¿porque hacer doble trabajo en redes/implementación de herramientas nuevas?

SMNP e IPv6

- Para IPv6 desde muy temprano se ha actualizado el estándar “de facto”, SNMP [RFC4293], Transporte y MIB para IP:
  - Define un solo conjunto de objetos para describir y manejar módulos IP de una manera independiente de la versión de IP
  - Se añaden nuevos objetos para mejorar la gestión de IPv6
- La mayoría de los fabricantes importantes soportan ya IPv6 en sus implementaciones de SNMP, tanto el transporte sobre IPv6 como la propia MIB para IPv6
  - Cisco, Juniper, Hitachi, Huawey, 6Wind, etc.
- Las aplicaciones basadas en el paquete netSNMP Open Source, también

Actualización de las MIBs

- Con el fin de evitar duplicar las MIBs de IPv4 para IPv6, se han introducido algunas modificaciones
  - Se define la estructura IP {inetAddressType, inetAddress} que permite tanto direcciones IPv4 como IPv6
  - Consecuentemente se modifican otras estructuras manejadas en las MIBs



SMNP sobre Transporte IPv6

- SNMP puede configurarse sobre transporte IPv6 para que un host IPv6 pueda hacer peticiones y recibir notificaciones SNMP
- Cisco:
  - SNMP over IPv6 is available in 12.0(27)S and 12.3(14)T
  - IOS 12.4 & 12.4T too
  - More features available from 12.0(30)S
- Juniper, Hitachi, 6wind:
  - SNMP sobre IPv6 disponible

Monitorización Tráfico IPv6

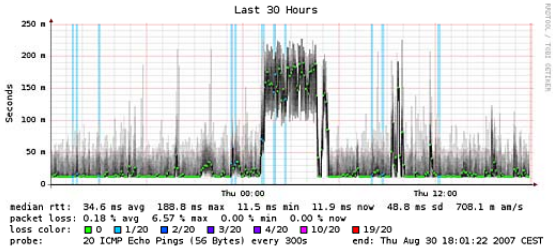
- Lo habitual es tener redes doble-pila donde circula tráfico IPv4 e IPv6 por el mismo cable
- Puede ser interesante diferenciar ambos tipos de tráfico para conocer la evolución del tráfico IPv6
- Se puede hacer de varias maneras:
  - Interfaces separadas para v4 y v6
  - Netflow [RFC3954] / IPFIX [RFC5101, RFC5102]
  - Captura de paquetes en sitios determinados (6meter)
- MRTG (http://oss.oetiker.ch/mrtg/), HP OpenView, CiscoWorks

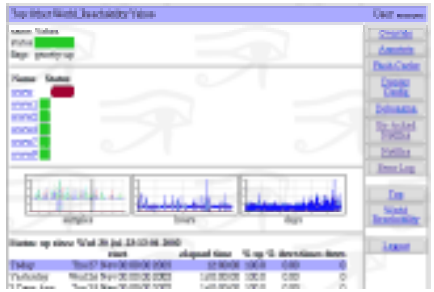
Gestión sobre IPv6

- Existen diversas herramientas para la gestión de equipos de red que funcionan sobre IPv6:
  - **SSH**: Para configuración CLI
  - **Telnet**: Para configuración CLI
  - **FTP**: Para gestión de imágenes o configuraciones
  - **TFTP**: Para gestión de imágenes o configuraciones
  - **HTTP**: Para configuración GUI

Monitorización sobre IPv6

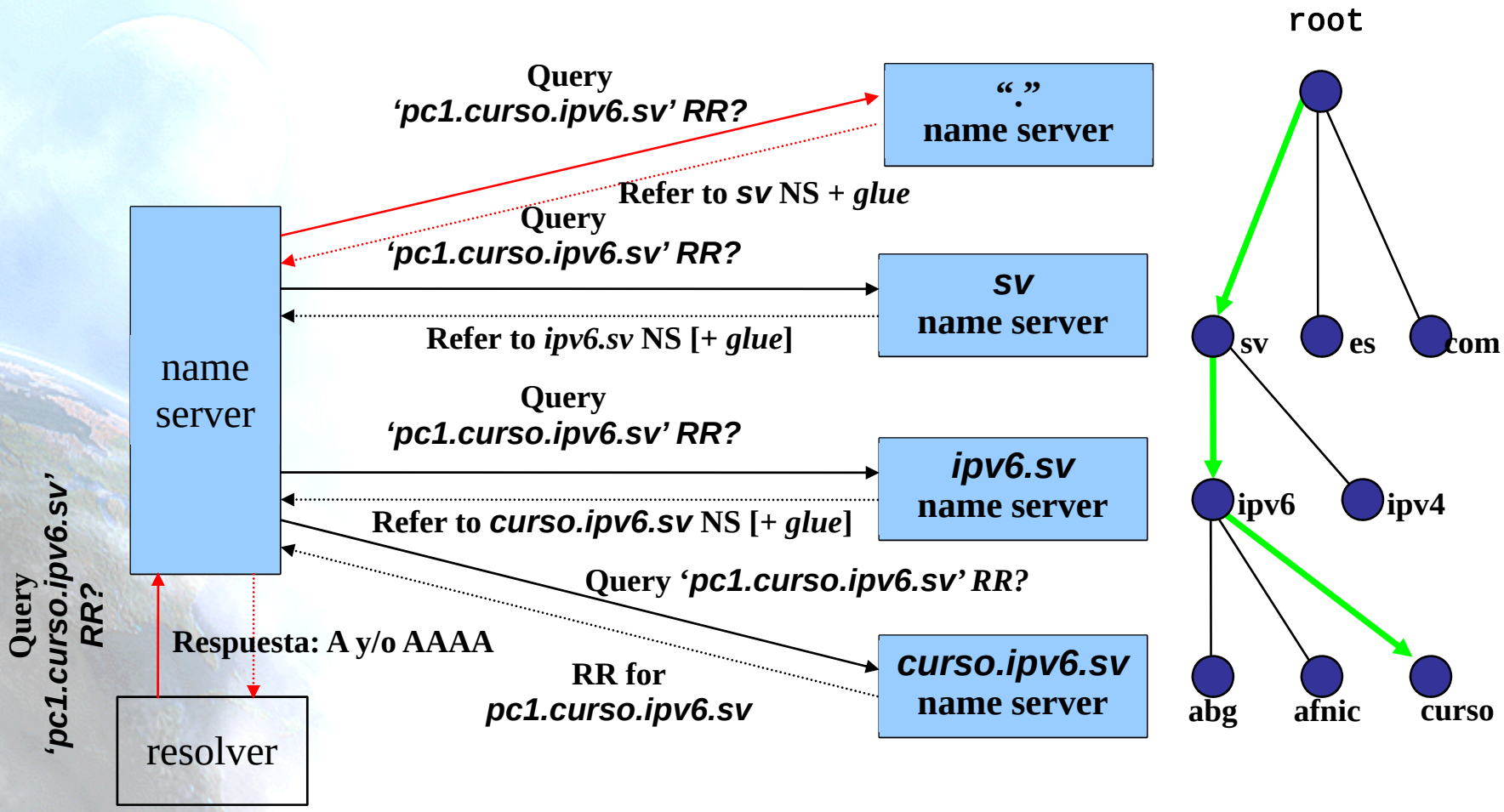
- Existen diversas herramientas de monitorización que pueden usar IPv6 como transporte:
  - **Ping6 / smokeping** (http://oss.oetiker.ch/smokeping/): para tener registro de alcanzabilidad y latencia
  - **ARGUS** (http://argus.tcp4me.com): software de monitorización de red y sistemas con interfaz web
  - **NAGIOS** (http://www.nagios.org): software de monitorización de red y sistemas con interfaz web





6. DNS IPv6

DNS IPv6: Introducción (1)



DNS IPv6: Introducción (2)

- Se **definieron** varios elementos para dar soporte IPv6 al DNS:
  - Para resolución directa RRs: **AAAA** y A6
  - Para resolución inversa: dominios IP6.INT e **IP6.ARPA**, DNAME y PTR RR, además de las notaciones **nibble** y bit-string

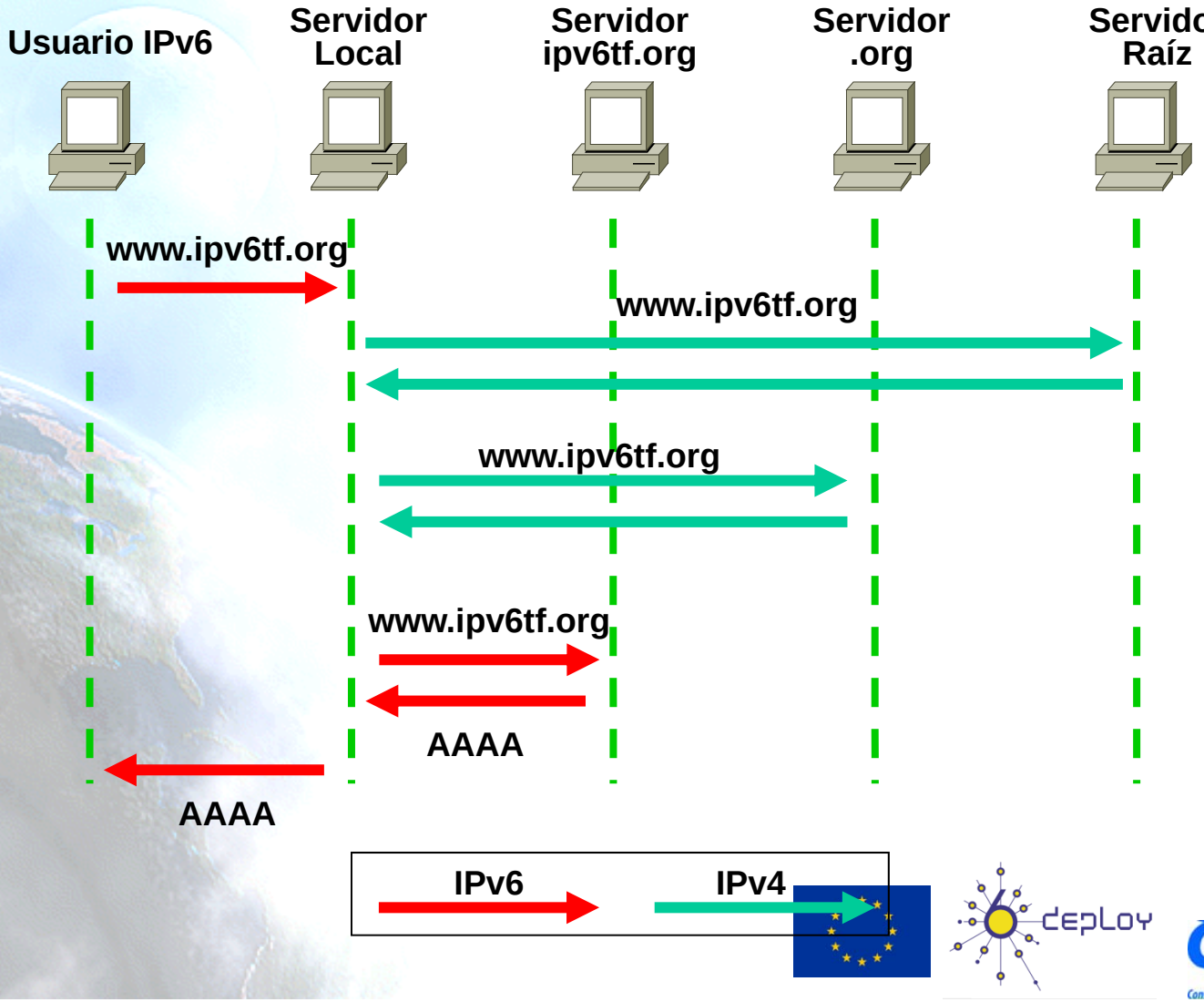
- 1995: AAAA, nibble e IP6.INT (RFC1886)
- 2000: A6, bit-string e IP6.ARPA (RFC2874)
- 2002: A6 y bit-string -> Experimental y DNAME -> Deprecado (RFC3363)

DNS IPv6: Introducción (3)

- Nos centraremos en los elementos usados hoy en día (RFC3596):
  - AAAA
  - IP6.ARPA
  - PTR
  - Notación con nibbles (4 bits en hex)

DNS IPv6: Transporte vs. Contenido

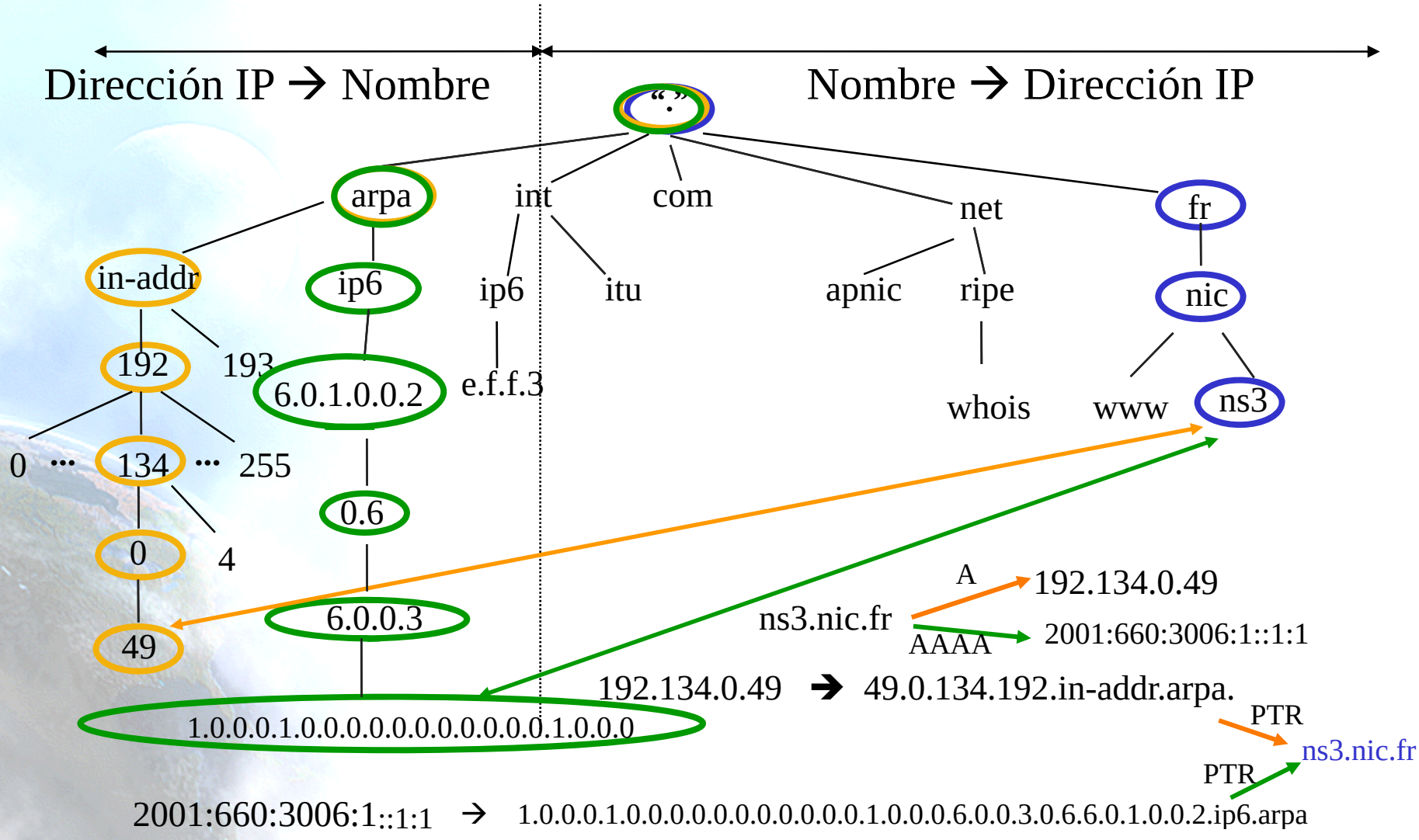
- Diferencia entre transporte y contenido



DNS IPv6: Recomendaciones

- IPv4 e IPv6 coexistirán, 3 tipos de servidores:
  - Solo IPv4 -> alcanzable sólo por IPv4
  - Solo IPv6 -> alcanzable sólo por IPv6
  - Doble-pila -> alcanzable por ambos
- **Evitar la fragmentación del espacio de nombres**: el proceso de resolución recursiva se rompe (e.g. cuando solo un NS IPv6 es autoritativo para un dominio, resultando que un servidor DNS solo IPv4 no podrá seguir la cadena de resolución).
- IDEA: **compatibilidad hacia atrás**.
- Políticas administrativas (RFC3901)
  - Todo servidor recursivo debe ser solo IPv4 o doble-pila.
  - Toda zona DNS debe ser servida al menos por un servidor autoritativo alcanzable sobre IPv4.

DNS IPv6: Ejemplo



DNS IPv6: Estado actual (1)

- **Clientes**: Buen soporte DNS IPv6
- **Servidores**: Muy buen soporte: BIND, nsd, newbie, maradns and djbdns [5][6]
- Implantación extendida a nivel **TLD** (.fr, .uk, .jp, etc.), desde Julio 2004 con el anuncio de ICANN [1] sobre el soporte de direcciones IPv6 en los servidores raíz, muchos TLDs lo han añadido [2].
- **Servidores Raíz** (8/13)(root zone 2010061700) [3] implantación actualmente en curso. Se hizo el anuncio [4] y desde el 4 de Febrero de 2008 son alcanzables por IPv6.

DNS IPv6: Referencias

[1] Next-generation IPv6 Address Added to the Internet's Root DNS Zone: http://www.icann.org/announcements/announcement-20jul04.htm

[2] IANA Administrative Procedure for Root Zone Name Server Delegation and Glue Data: http://www.iana.org/procedures/delegation-data.html

[3] Root Zone Hints File in IANA Popular Links: http://www.iana.org/popular.htm

[4] IPv6 Address Added for Root Servers in the Root Zone: http://www.icann.org/announcements/announcement-04feb08.htm

[5] Internet Systems Consortium http://www.isc.org

[6] DeepSpace6 - Current Status of IPv6 Support for Networking Applications http://www.deepspace6.net/docs/ipv6_status_page_apps.html

7. Seguridad IPv6

- 7.1 IPsec
- 7.2 Extensiones de Privacidad
- 7.3 Amenazas a ND
- 7.4 SEND
- 7.5 Comparativa IPv4 vs. IPv6
- 7.6 Aspectos de seguridad con IPv6
- 7.7 Temas prácticos

Introducción

- Aunque el término Seguridad abarque gran cantidad de temas, en esta sección se abordarán solamente los relacionados con IPv6
- En primer lugar se dará una descripción de IPsec debido a que es obligatoria su implementación en todas las pilas IPv6, proporcionando la posibilidad de su uso a todos los dispositivos IPv6.
- A continuación se tratarán algunas soluciones de seguridad concretas desarrolladas en el contexto de IPv6: Extensiones de Privacidad y SEND.
- Se compararán IPv6 e IPv4 desde el punto de vista de las amenazas a la seguridad.
- Se expondrá un análisis general desde el punto de vista práctico, comparando elementos de seguridad IPv4 e IPv6.

7.1 IPsec

Seguridad IP (IPsec)

- **Objetivos**:
  - Proporcionar seguridad criptográfica, de calidad e interoperable para IPv4 e IPv6.
  - No afectar negativamente a usuarios, hosts u otros componentes de Internet que no usen IPsec para la protección del tráfico.
  - Los protocolos de seguridad (AH, ESP e IKE) se han diseñado para ser independientes de los algoritmos de cifrado usados. Se define un conjunto de algoritmos por defecto.
- **Conjunto de Servicios de Seguridad**:
  - Control de Acceso
  - Integridad sin-conexión
  - Autentificación del origen de los datos
  - Protección contra reactuación (un tipo de integridad de secuencia parcial)
  - Confidencialidad (cifrado)
  - Confidencialidad de flujo de tráfico limitado

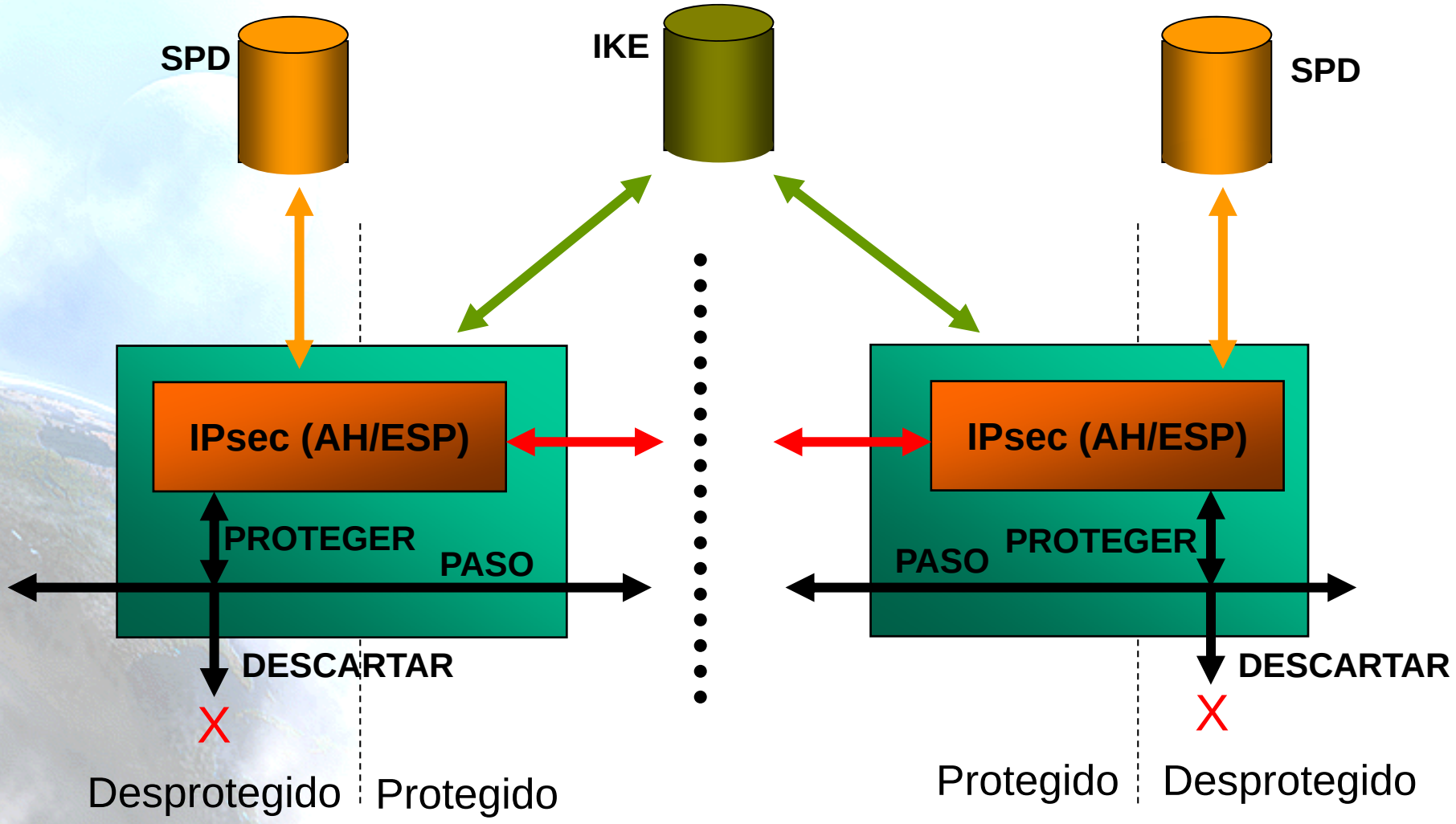
IPsec: Elementos Básicos

- Elementos básicos:
  - **Arquitectura Base** para sistemas conformes con IPsec (RFC4301)
  - **Protocolos de Seguridad:** Authentication Header (AH) (RFC4302) y Encapsulating Security Payload (ESP) (RFC4303)
  - **Asociaciones de Seguridad:** Qué son y como funcionan, cómo se gestionan (RFC4301)
  - **Gestión de Claves**: Manual y Automática (La Internet Key Exchange IKE) (RFC4306)
  - **Algoritmos para autentificación y cifrado**: Se definen algoritmos obligatorios, por defecto, para su uso con AH y ESP (RFC4835) y para IKEv2 (RFC4307)

Visión General (1)

- Una implementación IPsec opera en un host, como una pasarela de seguridad (SG) o como un dispositivo independiente.
- La protección ofrecida por IPsec se basa en los requerimientos definidos en la Security Policy Database (SPD).
- Los paquetes se clasifican basándose en información de las cabeceras IP y 'next layer', para buscar coincidencias en la SPD.
- Cada paquete puede ser DESCARTADO, PROTEGIDO usando los servicios IPsec o permitirse su PASO a través de la protección IPsec.
- IPsec se puede usar para proteger uno o más "caminos":
  - Entre un par de hosts.
  - Entre un par de pasarelas de seguridad.
  - Entre una pasarela de seguridad y un host.

Visión General (2)



Protocolos de Seguridad

- Las implementaciones IPsec DEBEN soportar ESP y PUEDEN soportar AH. AH y ESP pueden aplicarse solas o en combinación con la otra.
- **AH** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
- **ESP** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
  - Confidencialidad (NO recomendada sin integridad).
- Ambas ofrecen control de acceso, impuesta a través de la distribución de claves criptográficas y la gestión de flujos de tráfico según dicte la SPD.
- Estos mecanismos están diseñados para ser independientes de los algoritmos.

SA: El Concepto

- La Asociación de Seguridad (Security Association - SA) es un concepto fundamental para IPsec:
  - **Una “conexión” simple que proporciona servicios de seguridad al tráfico que transporta.**
- AH y ESP usan SAs, de forma que todas las implementaciones DEBEN soportar el concepto de Asociación de Seguridad.
- Una de las principales funciones de IKE es el establecimiento y mantenimiento de SAs.
- Para asegurar un comunicación bidireccional típica entre dos nodos con IPsec, se necesitan dos SAs (una para cada dirección). IKE crea pares de SAs.

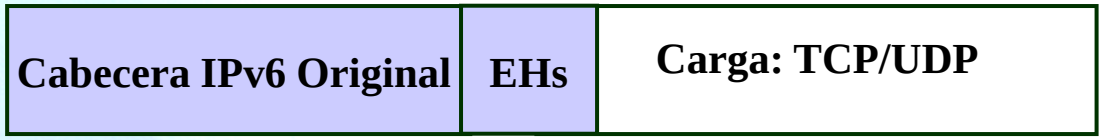
Identificación de SA

- Cada SA se identifica unívocamente por la terna:
  - Índice de Parámetros de Seguridad (Security Parameter Index - SPI)
    - Cadena de bits asignada a la SA (significado local), como puntero a una base de datos de SAs (SPD o Security Policy Database).
  - Dirección IP Destino
  - Identificador de protocolo de seguridad (AH o ESP)
- La dirección destino puede ser:
  - Dirección Unicast
  - Dirección Broadcast
  - Dirección Grupo Multicast

Modos de Uso

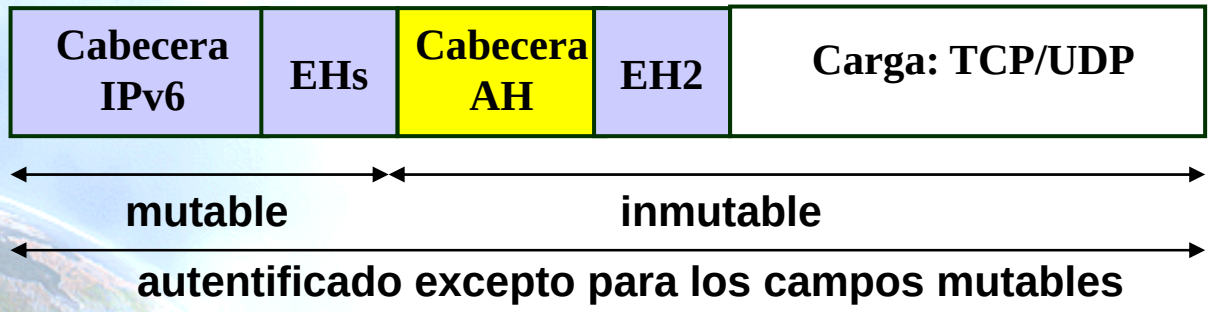
- Cada protocolo soporta dos modos de uso:
  - Modo Transporte (protege principalmente protocolos de capa superior)
    - Directo entre dos sistemas extremo-a-extremo
    - Los dos sistemas remotos deben soportar IPsec!
  - Modo Túnel (protocolos aplicados a paquetes IP encapsulados)
    - Túnel seguro para encapsular paquetes IP inseguros
    - Entre sistemas intermedios (no extremo-a-extremo)

AH en Modo Transporte y Túnel

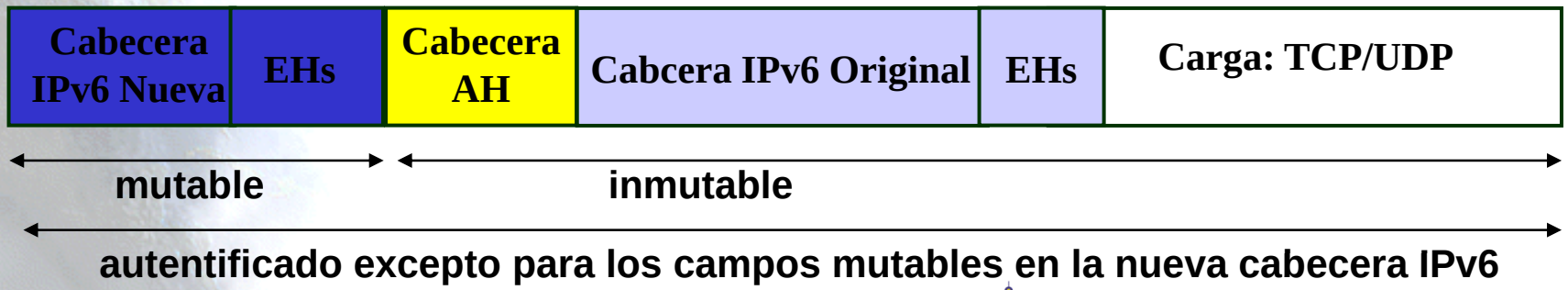


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

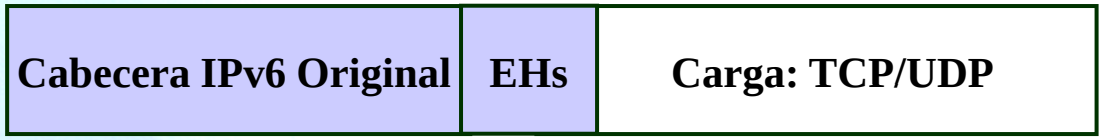
Modo Transporte



Modo Túnel

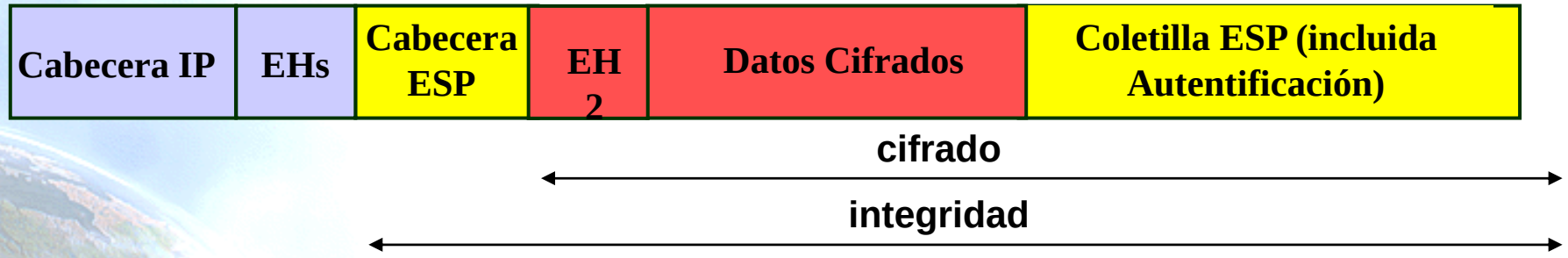


ESP en Modo Transporte y Túnel

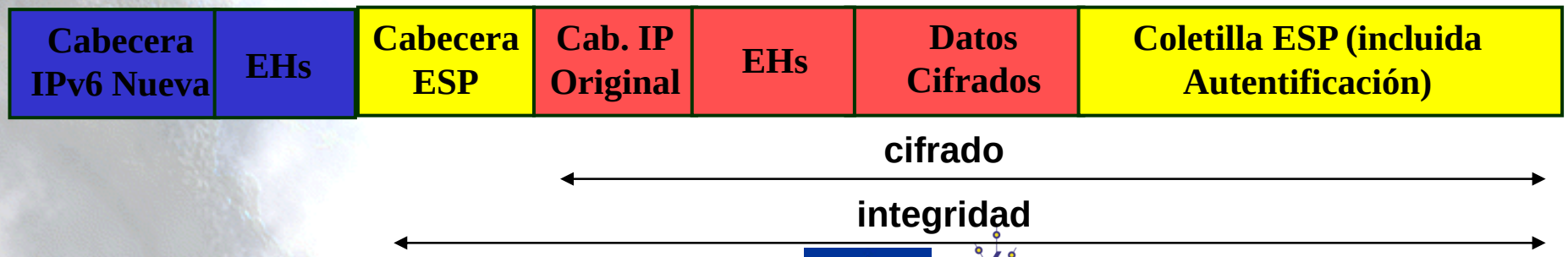


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

Modo Transporte

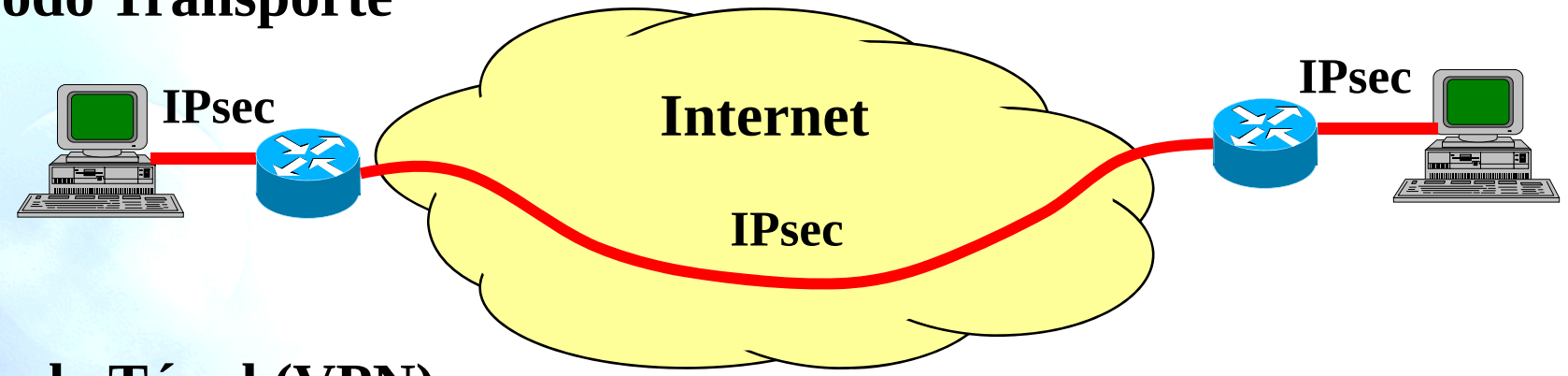


Modo Túnel

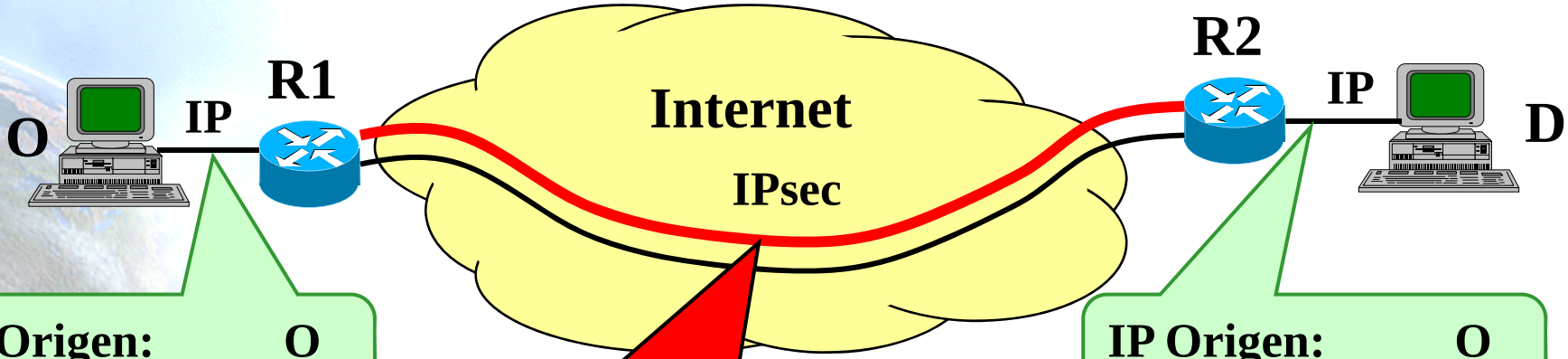


Modo Transporte vs. Túnel

Modo Transporte



Modo Túnel (VPN):



IP Origen: O
IP Destino: D

IP Origen: R1
IP Destino: R2

IP Origen: O
IP Destino: D

7.2 Extensiones de Privacidad

¿Por qué Extensiones de Privacidad?

- El problema (con identificadores IEEE)
  - Las direcciones IPv6 en un interfaz dado y generada via “Stateless Autoconfiguration” contienen el mismo ID de interfaz, con independencia del lugar de Internet en el que el dispositivo se conecta. Esto puede facilitar la trazabilidad de dispositivos y/o individuos.
- Posibles Soluciones
  - Usar DHCPv6 para obtener direcciones. El servidor DHCP podría asignar “direcciones temporales” que nunca se renuevan y tienen la condición de temporalidad necesaria
  - Cambiar el ID de interfaz de una dirección IPv6 cada cierto tiempo y generar por tanto nuevas direcciones IPv6 para determinados ámbitos

Extensiones de Privacidad

- El RFC4941 describe una extensión para la autoconfiguración “stateless” en IPv6 que hace que los nodos generen direcciones de ámbito global que cambian con el tiempo.
- El RFC4941 se basa en generar identificadores de interfaz aleatorios con un tiempo de vida limitado.

7.3 Amenazas a ND

Visión General

- El protocolo Neighbor Discovery (ND) (RFC4861) es vulnerable a diversos ataques (RFC3756)
- La especificación original del protocolo ND define el uso de IPsec para proteger los mensajes de ND. Por diversas razones en la práctica esta no es una solución
- SEcure Neighbor Discovery (SEND) (RFC3971) tiene como objetivo proteger ND

Amenazas a ND (1)

- Neighbor Solicitation/Advertisement Spoofing
  - Se hace o bien mandando un NS con una opción de dirección de capa de enlace origen cambiada, o enviando un NA con una opción de dirección de capa de enlace destino cambiada
  - Este es un ataque de redirección/DoS
- Fallo de Neighbor Unreachability Detection (NUD).
  - Un nodo malicioso puede permanecer enviando NAs hechos “a medida” como respuesta a mensajes NS de NUD. Si los mensajes NA no se protegen de alguna manera el atacante puede llevar a cabo el ataque por periodos muy largos de tiempo
  - Este es un ataque DoS (Denegación de Servicio)

Amenazas a ND (2)

- Ataque DoS usando DAD
  - Un nodo atacante puede lanzar un ataque DoS respondiendo a todos los intentos de DAD hecho por un host que llega a la red
  - El atacante puede reclamar la dirección de dos maneras: puede responder con un NS, simulando que también esta haciendo DAD, o bien puede responder con un NA, simulando que ya ha esta usando esa dirección
  - También puede estar presente cuando se use otro tipo de configuración de direcciones, es decir, siempre que se invoque DAD antes de configurar una dirección
  - Es un ataque de tipo DoS

Amenazas a ND (3)

- Encaminador de Último Salto Malicioso
  - Un nodo atacante en la misma subred que un host que intenta descubrir un encaminador de ultimo salto legítimo, se puede hacer pasar por un encaminador IPv6 enviando por multicast un RA o por unicast un RA como respuesta a un RS del nodo que llega a la red
  - El atacante se puede asegurar de que el nodo que llega a la red lo selecciona a él como el encaminador por defecto enviando periódicamente por multicast RAs para el encaminador verdadero pero con tiempo de vida cero. Esto haría que creyese que el router verdadero no quiere cursar tráfico
  - Esta amenaza es un ataque de redirección/DoS

Amenazas a ND (4)

- ‘Muerte’ del encaminador por defecto
  - Un atacante ‘mata’ el(los) encaminador(es) por defecto, haciendo que todos los nodos del enlace asuman que todos los nodos son locales
  - El atacante puede lanzar un ataque DoS clásico contra el encaminador de forma que parezca que no responde. Otra forma sería enviar un RA falso con tiempo de vida cero (zero Router Lifetime)
- El ‘buen’ encaminador se vuelve ‘malo’
  - Un router en el que previamente se confiaba queda comprometido
  - Se aplica el caso de ‘Encaminador de último salto malicioso’
  - Este es un ataque de redirección/DoS

Amenazas a ND (5)

- Mensaje Redirect Falso
  - El atacante usa la dirección en enlace-local del encaminador de primer salto actual para enviar un mensaje Redirect a un host legítimo
  - Debido a que el host identifica el mensaje como proveniente del encaminador por la dirección de enlace-local, acepta el Redirect
  - Siempre que el atacante responda a los mensajes NUD a la dirección de capa de enlace, el efecto de la redirección seguirá vigente
  - Este es un ataque de redirección/DoS

Amenazas a ND (6)

- Prefijo falso en el enlace
  - Un nodo atacante puede enviar un RA especificando que un prefijo de longitud arbitraria pertenece al enlace
  - Si un host que va a enviar un paquete piensa que ese prefijo pertenece al enlace, nunca enviará un paquete con destino a ese prefijo al encaminador. Por el contrario, usará un NS para resolver la dirección, pero el NS no tendrá respuesta, denegando de esta forma el servicio a ese host
  - Este ataque se puede extender a un ataque de redirección si el atacante responde al NS con NAs falsos
  - Este es un ataque DoS

Amenazas a ND (7)

- Prefijo falso para configuración de dirección
  - Un nodo atacante puede enviar un RA especificando un prefijo de red inválido para ser usado por un host para la autoconfiguración de direcciones
  - Como resultado, los paquetes de respuesta nunca llegan al host porque su dirección origen no es valida
  - Este ataque tiene el potencial de propagarse más allá del host atacado si el host realiza una actualización dinámica en el DNS usando la dirección construida con el prefijo falso
  - Este es un ataque DoS

Amenazas a ND (8)

- Parámetros falseados.
  - Un nodo atacante puede enviar RAs con significado válido que dupliquen los RAs enviados por el encaminador por defecto válido, excepto en que los parámetros incluidos están pensados para interrumpir el tráfico legítimo
  - Algunos ataques específicos:
    1. Incluir un 'Current Hop Limit' de uno u otro número pequeño que el atacante sepa causará que los paquetes legítimos se descartarán antes de llegar a su destino
    2. El atacante implementa un servidor o 'relay' DHCPv6 falso y los flags 'M' y/o 'O' están activados, indicando que la configuración 'stateful' de direcciones y/o otros parámetros de realizarse. El atacante puede responder a las peticiones de configuración 'stateful' de un host legítimo con sus respuestas falsas
  - Este es un ataque DoS

Amenazas a ND (9)

- Ataques de Reactuación (Replay)
  - Todos los mensajes de Neighbor Discovery y Router Discovery pueden sufrir ataques de reactuación
  - Un atacante podría capturar mensajes válidos y reenviarlos más tarde
  - En los intercambios de tipo petición-respuesta, como los de ‘Solicitation-Advertisement’, la petición puede contener un valor (nonce) que debe aparecer también en la respuesta. Las respuestas antiguas no son válidas ya que no contienen el valor correcto
  - Los mensajes ‘solitarios’, como los ‘Advertisements’ no solicitados o los mensajes ‘Redirect’, deben protegerse con sellos temporales o contadores

Amenazas a ND (10)

- Ataque DoS a Neighbor Discovery
  - El nodo atacante comienza a fabricar diversas direcciones a partir del prefijo de red y envía paquetes continuamente a esas direcciones. El encaminador de último salto se ve obligado a resolver esas direcciones enviando paquetes NS
  - Un host legítimo que intenta conectarse a la red no será capaz de obtener servicio de ND por parte del encaminador de último salto ya que estará ocupado enviando otras peticiones (NS)
  - Este ataque DoS es diferente de los otros en el sentido de que el atacante puede estar fuera del enlace

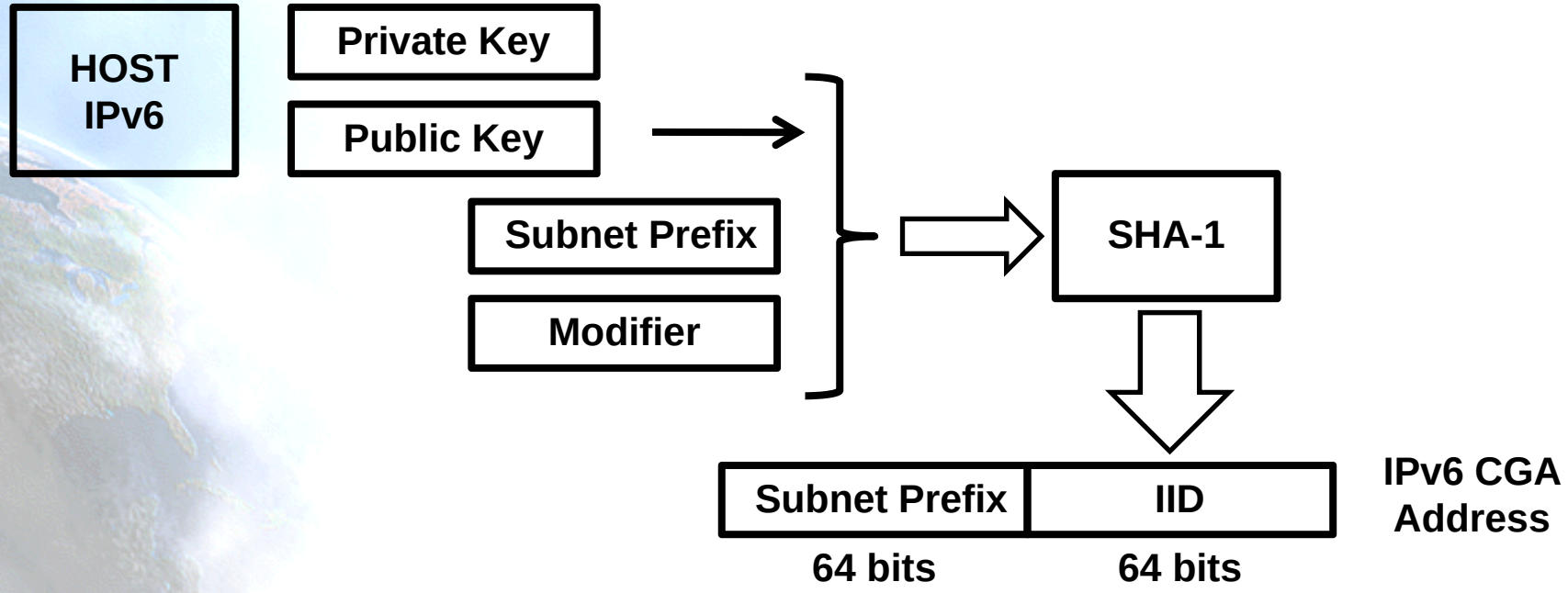
7.4 Secure Neighbor Discovery

Secure Neighbor Discovery - SEND (RFC3971)

- Los nodos IPv6 usan NDP para:
  - Descubrir otros nodos en el segmento de red o enlace
  - Determinar su dirección de nivel de enlace
  - Mantener información para saber si los vecinos siguen activos
- NDP es vulnerable a varios ataques si no se asegura
- El RFC3971 especifica ciertos mecanismos de seguridad para NDP
  - Estos mecanismos no usan IPSec, a diferencia de las especificaciones originales de NDP
  - SEND se aplica en entornos donde la seguridad física del enlace no está asegurado (como por ejemplo redes inalámbricas)
- De momento solo hay implementaciones de SEND para linux y *BSD
  - P.e. http://www.docomolabs-usa.com/lab_opensource.html

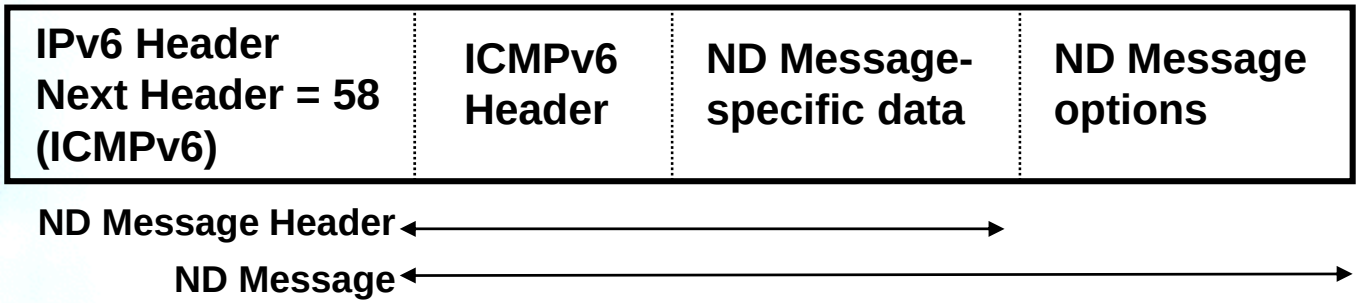
Funcionamiento de SEND y CGAs

- Un host que implemente SEND usa un par de claves **publica-privada**
- SEND se basa en el uso de CGAs [RFC3972]: dirección IPv6 con el IID generado criptográficamente a partir de la clave pública, el prefijo de red y un modificador



Elementos de SEND

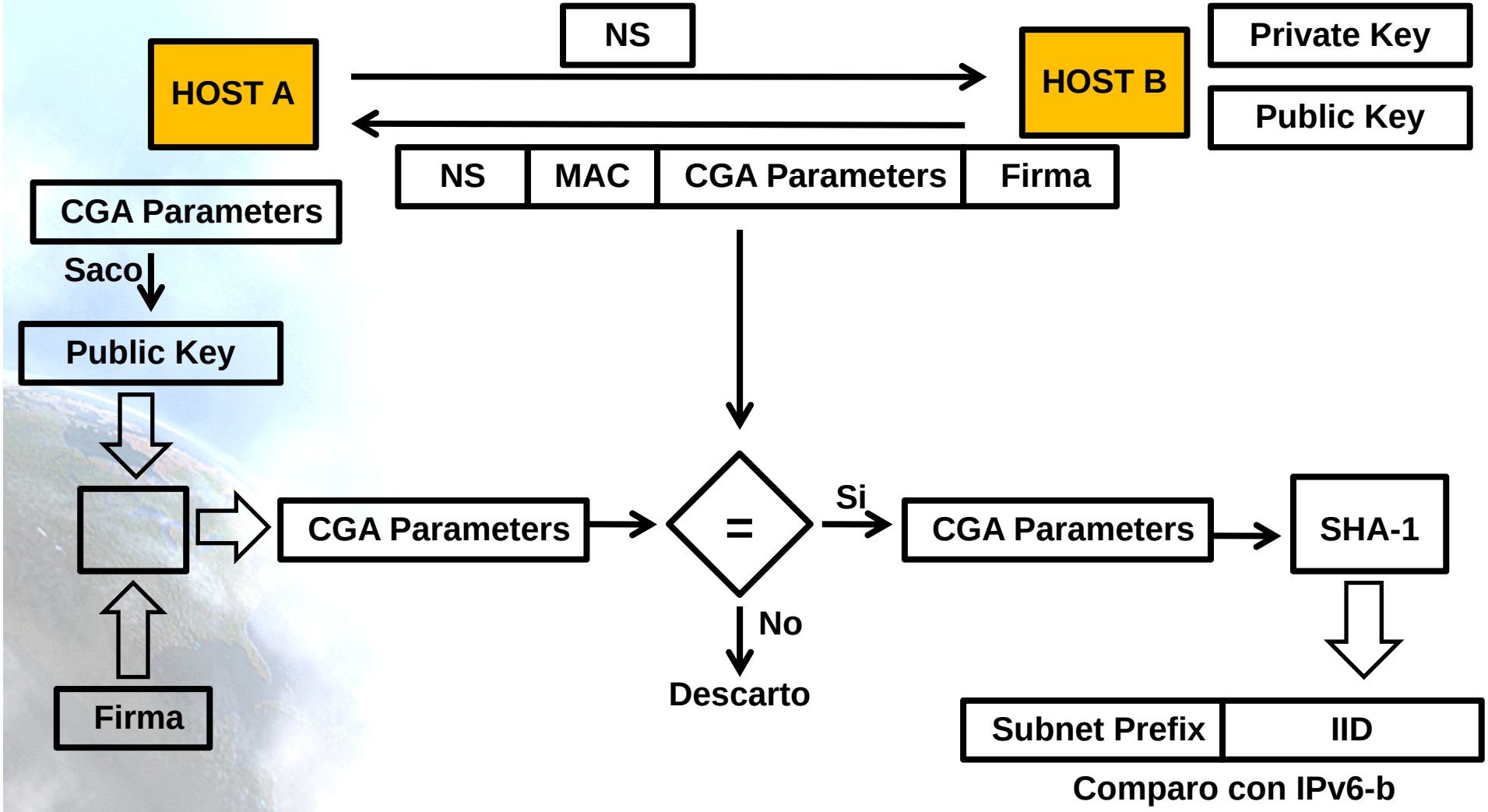
- Un mensaje NDP real incluye:
  - Cabecera del mensaje NDP
    - Cabecera ICMPv6
    - Datos específicos del mensaje ND
  - y cero o más opciones NDP, las cuales siguen el formato “Type-Length-Value”



- Se definen una serie de nuevas opciones ND para asegurar NDP y proteger sus mensajes:
  - **Parámetros CGA**: Modifier, Subnet Prefix, Public Key
  - **Nonce**: Número aleatorio para evitar ataques por reactuación
  - **Firma**: Parámetros CGA y Nonce firmados con la clave privada

Funcionamiento de SEND (1)

- Host A quiere saber MAC de IPv6-b (host B) -> envía NS



Funcionamiento de SEND (2)

- Los RA se pueden asegurar usando algo similar
- Los RA los firman los routers, que necesitan un certificado X.509 asociado a su par de claves para que los hosts confíen en ellos
- El certificado X.509 y la firma (signature) van en todos los RAs
- El certificado es expedido por una CA en la que los hosts deben confiar
- Se crean dos nuevos mensajes ICMPv6:
  - CPS (Certification Path Solicitation): Usado por el host para obtener el certificado del router
  - CPA (Certification Path Advertisement): Respuesta del router con el certificado

7.5 Comparativa IPv4 vs. IPv6

Visión General

- **Seguridad:** incluye diversos procedimientos, mecanismos, prácticas recomendadas y herramientas
- Con **IPv6** hay muchos puntos que serán los mismos que con IPv4, i.e., son “independientes de IP”. Ejemplo, actualizaciones de firmware y software o riesgos de seguridad a nivel de aplicación
- IPv6 introduce nuevos temas a tener en cuenta. Veremos que estos puntos pueden significar una ventaja o desventaja desde el punto de vista de la seguridad

Seguridad IPv6: primer contacto

- Las dos primeras ideas que vienen a la mente de un responsable de seguridad que despliega IPv6 son:
  1. Se utilizan direcciones globales (existe la excepción de las ULAs), i.e., son alcanzables desde cualquier sitio de Internet, en otras palabras, **no hay NAT**.
  2. Todas la pilas IPv6 deben soportar IPsec, como se ha visto.
- La primera puede dar la falsa impresión de peligro y la segunda la falsa impresión de protección. Se profundizará más en esto después.

Clasificación de las Amenazas de Seguridad

- Se pueden establecer tres categorías para las amenazas de seguridad en IPv6:
  1. Amenazas que ya existían con IPv4 y que tienen un comportamiento similar con IPv6.
  2. Amenazas que ya existían con IPv4 y que presentan novedades con IPv6.
  3. Nuevas amenazas que aparecen con IPv6.

Amenazas IPv4 con comportamiento similar con IPv6

- **Sniffing:** IPsec puede ayudar.
- **Ataques a Nivel de Aplicación**: IPsec puede usarse para perseguir al atacante, aunque introduce problemas para los IDS. También puede usarse protección en el nivel de Aplicación.
- **Dispositivos no autorizados**: Se hacen pasar por conmutadores, encaminadores, puntos de acceso o recursos como servidores DNS, DHCP o AAA.
- **Ataques de 'Hombre-en-el-medio'**: IPsec puede ayudar.
- **Ataques por inundación**.

Amenazas IPv4 con diferente comportamiento con IPv6 (1)

- **Escaneo de Red**: El escaneo de una red típica (/64) en la práctica es más difícil. También los ataques automatizados, por ejemplo gusanos que seleccionan direcciones aleatorias para propagarse, se ven dificultados => cambio métodos escaneo
- **Ataques de Amplificación Broadcast (Smurf)**: Ataque DoS. Un mensaje echo ICMP se envía a la dirección de broadcast de un prefijo de red con la dirección de origen falseada a la del host víctima. Todos los nodos del prefijo destino envían una echo reply a la víctima. E**n IPv6, no existe el concepto de broadcast** -> Multicast => no respuesta ICMP

Amenazas IPv4 con diferente comportamiento con IPv6 (2)

- **Ataques relacionados con Mecanismos de Transición**: No se utilizan nuevas tecnologías, el mismo tipo de vulnerabilidades que con IPv4:
  - Redes doble-pila pueden ser atacadas usando ambos protocolos.
  - Los túneles IPv6 necesitan nuevos puertos abiertos en los firewalls.

  Recomendaciones:
  - En redes/hosts de doble-pila usar medidas de seguridad similares para IPv4 e IPv6.
  - Controlar el uso de túneles cuando sea posible.
  - Habilitar que los firewalls inspeccionen el tráfico encapsulado.

Nuevas Amenazas IPv6

- Amenazas a ND
- Routing Header Type 0 (RFC5095)
- Mecanismos de Transición, en el sentido de que funcionan encapsulando tráfico y los firewalls y otros dispositivos/software de seguridad deben ser capaces de procesarlos.
- IPsec, en el sentido de enviar datos cifrados que los firewalls no pueden inspeccionar, especialmente firewalls ‘full-state’.

7.6 Aspectos de seguridad con IPv6

Aspectos de Seguridad con IPv6 (1)

- **IPsec**: Obligatorio en todas las implementaciones de IPv6. Esto puede proporcionar una falsa sensación de seguridad, porque la seguridad la proporciona solamente si se usa IPsec. En la práctica IPsec no se encuentra ampliamente desplegado y en uso debido a la falta de un mecanismo de intercambio de claves a nivel de todo Internet.

  IPsec se configura manualmente para algunas configuraciones concretas y controladas, esto no es escalable.

  Otro aspecto a tener en cuenta es que el tráfico IPsec (ESP) no puede ser inspeccionado por los firewalls.

Aspectos de Seguridad con IPv6 (2)

- **Extremo-a-extremo**: El uso de direcciones IPv6 globales **permite pero no obliga** a todos los nodos a ser alcanzables. El administrador de seguridad/red debe decidir si todos, algunos o ningún tráfico puede alcanzar cada parte de la red.

  Diversos escenarios:

  – **Usuario DSL**: El tráfico debe alcanzar el CPE sin interferencias. El usuario tiene la responsabilidad de filtrar en el CPE.

  – **Centro de Datos**: Entorno controlado donde solo los servicios permitidos deben desplegarse.

Aspectos de Seguridad con IPv6 (3)

- El **nuevo esquema de direccionamiento** implica:
  - El **número de direcciones e**s REALMENTE grande. No tiene sentido el escaneo aleatorio o por fuerza bruta (RFC5157)
  - Cada nodo puede tener **varias direcciones** e incluso identificadores de interfaz aleatorios (RFC4941). Esto dificulta el control sobre un host por medio de su IP
  - El uso de direcciones de enlace-local en una interfaz IPv6, proporciona conectividad IP en un segmento de LAN sin ayuda externa. Como guía, no debe confiarse en sesiones que vengan de direcciones de enlace-local y permitirlas solo para servicios básicos
  - Se han definido direcciones multicast bien conocidas para facilitar la localización de servicios. Esto también facilita la localización de servicios para atacarlos (FF05::2 All routers, FF05::1:3 All DHCP Servers)

Aspectos de Seguridad con IPv6 (4)

- **Cabeceras de Extension (EH)**: este potente y flexible mecanismo debe tenerse en cuenta por los dispositivos de seguridad, es decir, deben ser capaces de inspeccionar la ‘cadena’ de cabeceras.
- **Fragmentación**: En IPv6 solo los hosts finales pueden fragmentar paquetes. Esto reduce los ataques posibles utilizando solapamiento de fragmentos o fragmentos muy pequeños. Las consideraciones para fragmentos desordenados son las mismas que en IPv4 pero en los nodos finales. Los firewalls no deben filtrar fragmentos de paquetes.

Aspectos de Seguridad con IPv6 (5)

- **Autoconfiguración:** En IPv6 se definen distintos medios para la autoconfiguración. DHCP tiene las mismas consideraciones en IPv4 e IPv6. Neighbor Discovery Protocol tiene varias amenazas (como ARP en IPv4), e IPsec y SEND se pueden usar para añadir seguridad.
- **Movilidad IPv6**: IPv6 facilita el despliegue de Movilidad IP aunque algunos elementos necesarios para un despliegue ‘en el mundo real’ están siendo definidos, incluyendo temas de seguridad.

Aspectos de Seguridad con IPv6 (6)

- **Routing Header:** Type 0 Routing Header (RH0) puede ser usada para lograr amplificación de tráfico sobre un camino remoto con el propósito de generar tráfico DoS.

  Se puede construir un paquete que ‘oscile’ entre dos hosts/routers que procesen RH0 muchas veces. Esto permite que un flujo de paquetes de un atacante se amplifique en el camino entre dos encaminadores remotos. Esto puede usarse para causar congestión sobre un camino remoto arbitrario y por lo tanto actuar como un mecanismo de DoS.

Aspectos de Seguridad con IPv6 (7)

- La gravedad de esta amenaza se consideró suficiente para prohibir el uso de RH0 (RFC5095)
- Sólo afecta a la cabecera de extensión Routing Type 0, de manera que las especificaciones para la Type 2 siguen siendo válidas, usada en MIPv6

7.7 Temas prácticos

Temas Prácticos (1)

- **ICMPv6 es una parte fundamental de IPv6**. Con IPv4 un filtrado de tipo ‘deny_all_ICMP’ podía usarse, pero con IPv6 significaría que funcionalidades básicas dejasen de funcionar.

Type - Code	Descripción	Acción
Type 1	Destination unreachable	ALLOW, de entrada para detectar algunos errores
Type 2	Packet too big	ALLOW, necesario para PMTU discovery
Type 3 - Code 0	Time Exceeded	ALLOW
Type 4 - Code 1 y 2	Parameter problem	ALLOW, para detectar algunos errores
Type 128	Echo reply	ALLOW para **depurar la red** o **Teredo**. De entrada se puede permitir limitando la frecuencia. De salida permitir para algunos **servicios conocidos**.
Type 129	Echo request	ALLOW para **depurar la red** o **Teredo**. De salida se puede permitir limitando la frecuencia. De entrada permitir para algunos **servicios conocidos**.
Type 130,131,132,143	Multicast listener	ALLOW si se despliega Multicast y MLD debe atravesar el firewall
Type 133	Router Solicitation	ALLOW si el firewall interfiere en ND
Type 134	Router Advertisement	ALLOW si el firewall interfiere en ND
Type 135	Neighbor Solicitation	ALLOW si el firewall interfiere en ND
Type 136	Neighbor Advertisement	ALLOW si el firewall interfiere en ND
Type 137	Redirect	NOT ALLOW
Type 138	Renumbering	NO TALLOW
Type 139	Node information Query	NOT ALLOW
Type 140	Node information Reply	NOT ALLOW

Temas Prácticos (2)

- Dependiendo del nivel de control y seguimiento que se requiera se deben usar distintos métodos de configuración de direcciones. De más a menos:
  - Direcciones estáticas.
  - Autoconfiguración ‘Stateful’: DHCPv6.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz a partir de la dirección MAC.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz utilizando las extensiones de privacidad.
- No se puede hacer un filtrado “ciego” de las cabeceras de extensión (en IPv4 sí se podía hacer con las “IP options”)

Temas Prácticos (3)

- Se recomienda
  - **Filtrar los prefijos no asignados**: más facil deny all + allow legitimate. Filtrado ‘grueso’ (Permitir 2000::/3 Global Unicast) o fino (2600:0000::/12, 2400:0000::/12, etc.)
  - Filtrar ULA a la “salida/entrada” de la red, no debe atravesar Internet
  - Filtrar al borde del sitio site-scoped multicast
  - Si se despliega Multicast permitir prefijos

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
deny	3ffe::/16	host/net	any	service
deny	any	any		

Temas Prácticos (4)

- Filtrado de **paquetes fragmentados**:
  - Filtrar fragmentos dirigidos a dispositivos de red (DoS a la infraestructura)
  - Asegurarse de capacidades de filtrado de fragmentos adecuadas
  - Filtrar todos los fragmentos de menos de 1280 bytes, excepto el último
  - Todos los fragmentos deben entregarse en 60 segundos, en caso contrario descartarlos

Temas Prácticos (5)

- **Utilizar direcciones difíciles de adivinar**, por ejemplo no usar ::1 para encaminadores o servidores, para dificultar el trabajo del atacante.

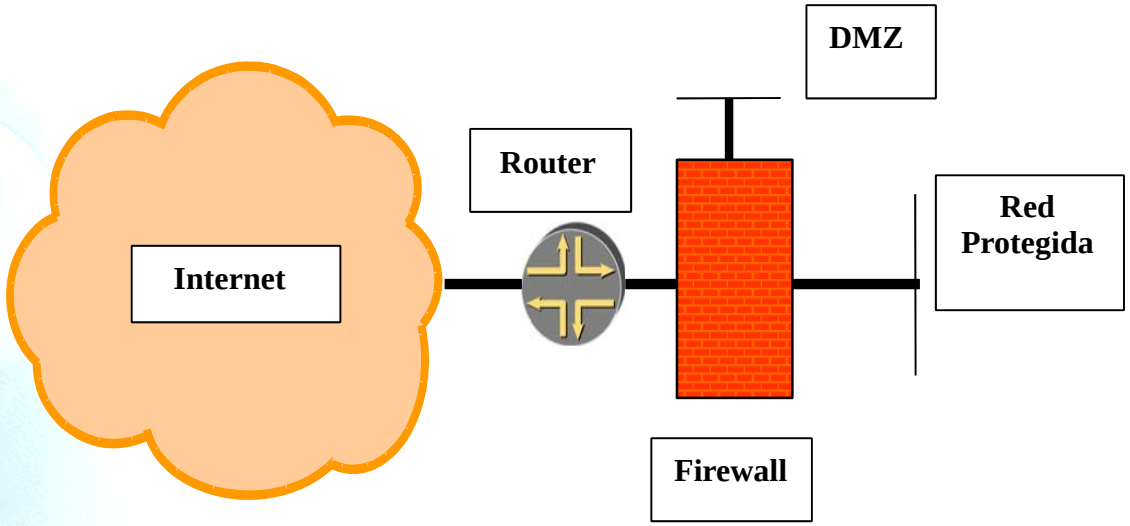
  Un ejemplo sería, habilitar la autoconfiguración steteless y después usar esa dirección autoconfigurada en una asignación estática. Esta dirección también se configuraría en el DNS

- **Desplegar Ingress Filtering** (RFC2827, RFC3074) de una manera similar a como se hace para IPv4

Temas Prácticos (6)

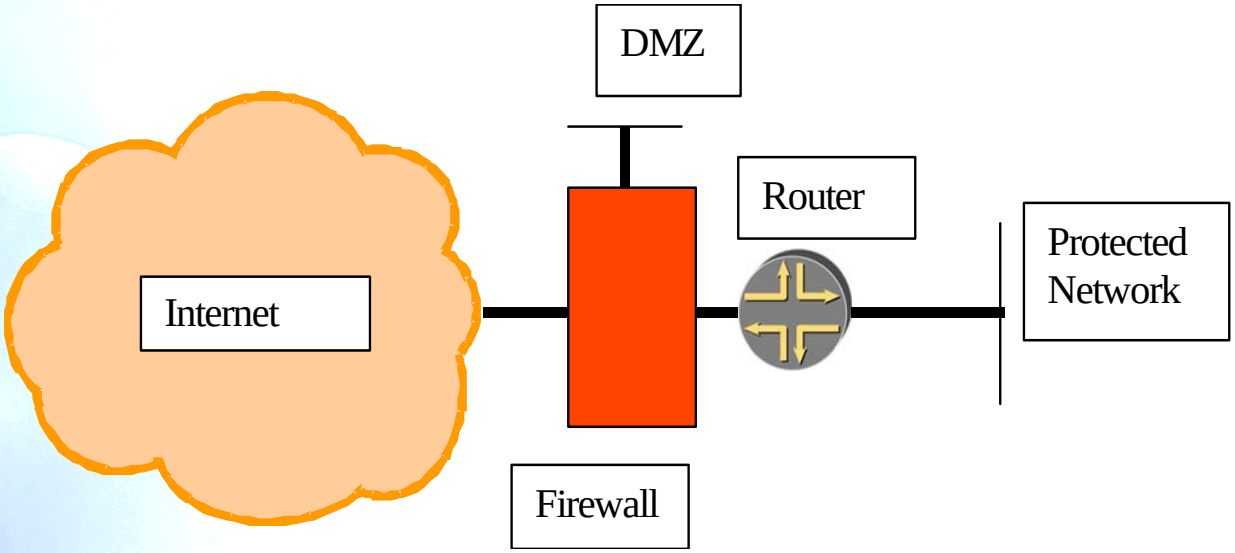
- Si se utilizan **Mecanismos de Transición**, asegurarse de que el prefijo correspondiente se anuncia y que su tráfico no se filtra
- IPv4 e IPv6 coexistirán, las redes IPv6 seguirán diseño de redes IPv4, compartiendo dispositivos si es posible. Hacer coherentes reglas IPv4 e IPv6 (no permitir todo con IPv6/nada con IPv4)
- Asegurarse de que el firewall soporta:
  - Filtrado por dirección origen y destino
  - Procesado de cabeceras de extensión IPv6 (incluida RH0)
  - Filtrado por información de protocolo de capa superior
  - Inspección de tráfico encapsulado

Firewalls (1)



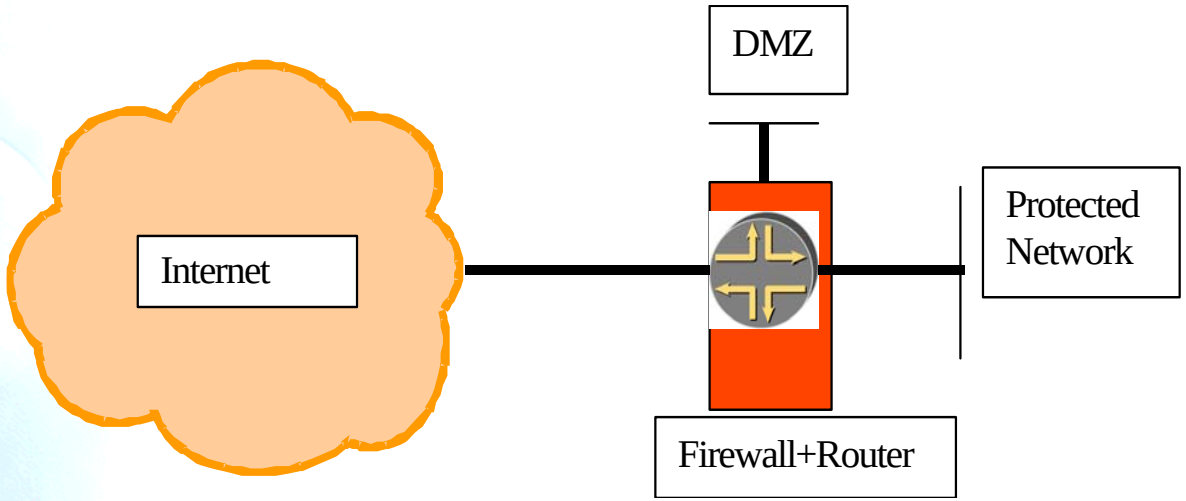
- Internet ↔router↔firewall↔red(es)
- Requisitos:
  - Firewall debe soportar/reconocer filtrado ND/NA
  - Firewall debe soportar RS/RA si se usa SLAAC
  - Firewall debe soportar mensajes MLD si se requiere Multicast

Firewalls (2)



- Internet ↔ firewall ↔ router ↔ red(es)
- Requisitos:
  - Firewall debe soportar ND/NA
  - Firewall debe soportar filtrado de protocolo encaminamiento dinámico
  - Firewall debe tener una gran variedad de tipos de interfaz

Firewalls (3)



- Internet ↔ firewall/router(edge device) ↔ red(es)
- Requisitos:
  - Puede ser potente – único punto para encaminamiento y políticas de seguridad – muy común en routers SOHO (DSL/cable)
  - Debe soportar lo que normalmente soportan los routers y firewalls

Firewalls (4)

	IPFilter 4.1	PF 3.6	IP6fw	Iptables	Cisco ACL	Cisco PIX 7.0	Juniper firewall	Juniper NetScreen	Windows XP SP2
Portability	Excellent	Good	Average	Weak	Weak	Weak	Weak	Weak	Weak
ICMPv6 support	Good	Good	Good	Good	Good	Good	Good	Good	Good
Neighbor Dissovery	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Good	Excellent	Weak
RS /RA support	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Excellent	Excellent	Good
Extension header support	Good	Good	Good	Excellent	Good	Good	Good	Good	Weak
Fragmantation support	Weak	Complete block	Weak	Good	Weak	Average	Weak	Average	Weak
Stateful firewall	Yes	Yes	No	Csak USAGI	Reflexive firewall	Yes	ASP necessary	Yes	No
FTP proxy	No	Next version	No	No	since 12.3 (11)T	?	No	No	No
Other	QOS support	QoS support, checking packet vailidity	Predefined rules in *BSD	EUI64 check,	Time based ACL		No TCP flag support today, HW based	IPSec VPN, routing support	Graphical and central configuration

Preguntas?

Gracias!

ALICE2: http://alice2.redclara.net/

6DEPLOY: http://www.6deploy.eu

The IPv6 Portal:http://www.ipv6tf.org