Seguridad en los nuevos escenarios basados en IPv6

Pedro M. Ruiz
Director de I+D
Agora Systems S.A.

Sevilla, 5 de Marzo de 2003

Índice

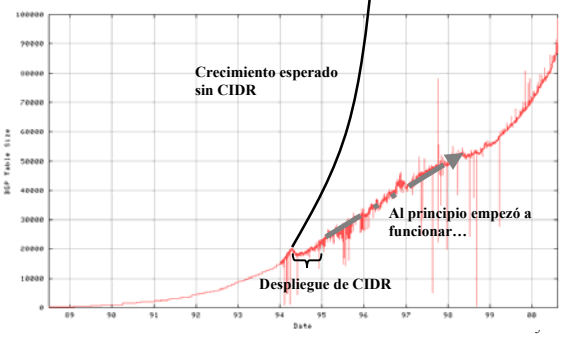
¿Por qué un nuevo IP?

- 1991 – ALE WG proyectó un agotamiento de direcciones IPv4 según la tasa actual para 2008.
- En mitad de 1994 se elige el enfoque de un nuevo protocolo.
- Las tablas de rutas BGP crecen de un modo exponencial

¿Hay tecnologías para paliar estos problemas?

- Dial-access / PPP / DHCP
  - –Ofrece asignación temporal de direcciones (Ej: Infovía).
- Políticas estrictas de asignación de direcciones
  - –Se pasa a asignar las 'current-need' frente al enfoque anterior basado en 'projected-maximum-size'.
- CIDR
  - –Se hace asignación geográfica para minimizar el tamaño de las tablas de encaminamiento de los routers.
- NAT
  - –Esconde a varios nodos detras de una única (o varias) IPs públicas.

IPv6 Facilita Agregación de rutas



¿Es adecuado incrementar el uso de NATs?

¡NO!

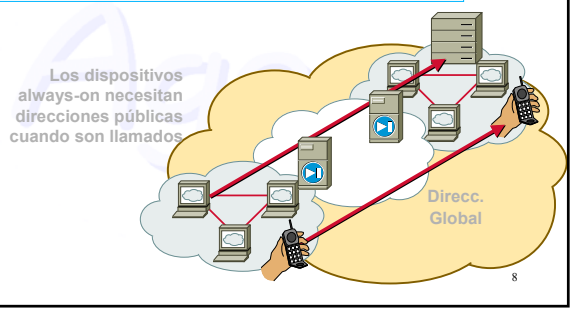
- NAT obliga a un modelo 'cliente-servidor' con restricciones sobre la topología del servidor
  - No se soportan conexiones P2P (Ej, VoIP)
  - Impiden el desarrollo de nuevas aplicaciones y servicios (requieren modificaciones a la configuración de todos los NATs del camino)
- NAT compromete el rendimiento y la fiabilidad de Internet.
- NAT incrementa la complejidad y reduce dificulta la gestión de la red.
- Las direcciones públicas siguen agotándose incluso usando NATs.

¿Cuáles fueron los objetivos del diseño del nuevo protocolo IP?

- Esperanza de resurgir tecnologías "allways-on"
  - xDSL, cable, Ethernet-to-the-home, Teléfonos móviles, etc.
- Se esperan nuevos usuarios con múltiples dispositivos.
  - China, India, etc. están creciendo muy rápidamente
  - Uso de todo tipo de dispositivos con conexión a Internet
- Se espera un incremento en el número de redes.
  - Mayor competición y delegación estructurada.

Vuelta al modelo End-to-End

Nuevas tecnologías/servicios para los usuarios
'Always-on'—Cable, DSL, Ethernet@home, Wireless,…

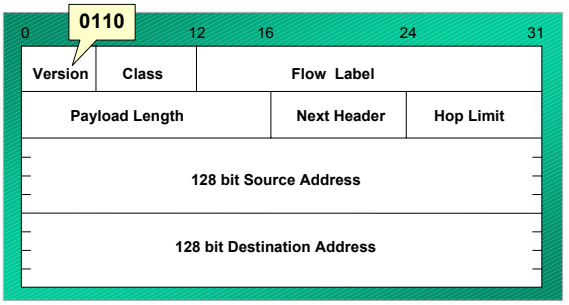


Resumen de ventajas de IPv6

- Mayor rango de direcciones
- Jerarquía estructurada para disminuir tamaño de tablas de routing
- Mecanismos de autoconfiguración
- Mejora en el formato de la cabecera e indentificación de flujos
- Mejor soporte de opciones y extensiones

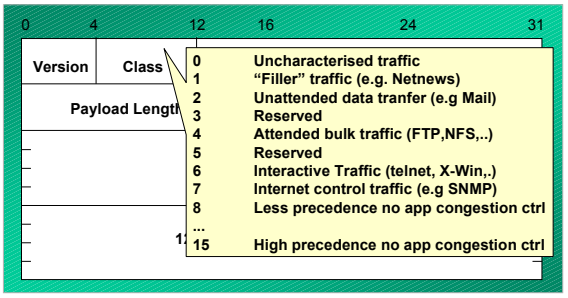
La cabecera IPv6

40 Octetos, 8 campos



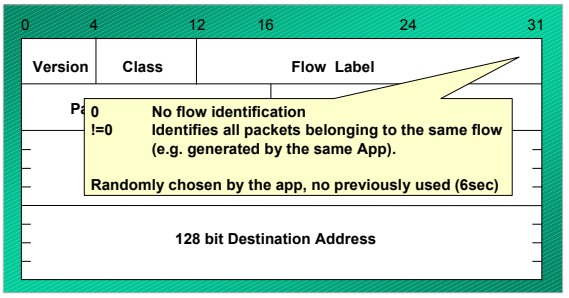
La cabecera IPv6

40 Octetos, 8 campos



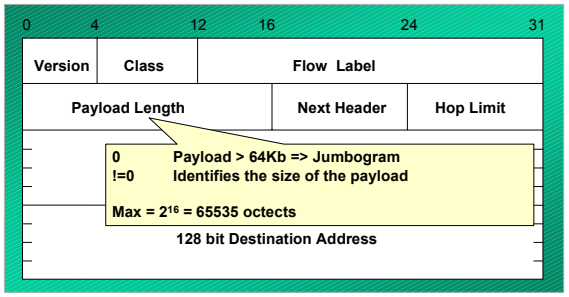
La cabecera IPv6

40 Octetos, 8 campos



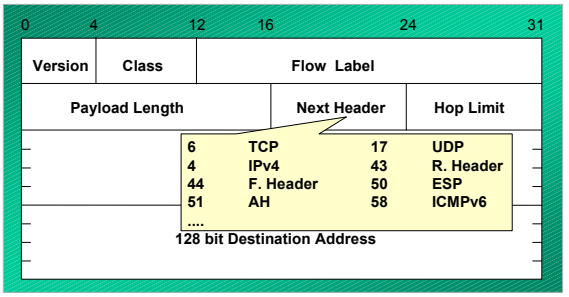
La cabecera IPv6

40 Octetos, 8 campos



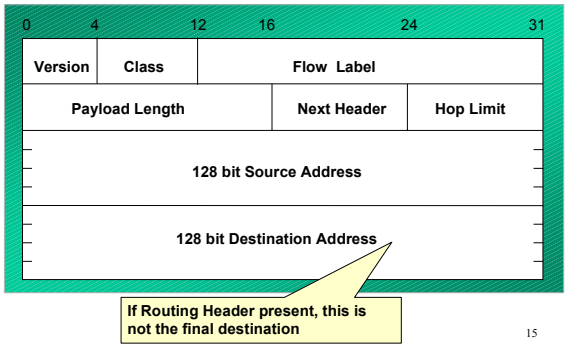
La cabecera IPv6

40 Octetos, 8 campos



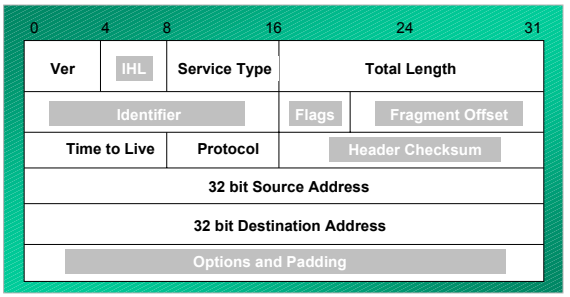
La cabecera IPv6

40 Octetos, 8 campos



Cabecera IPv4

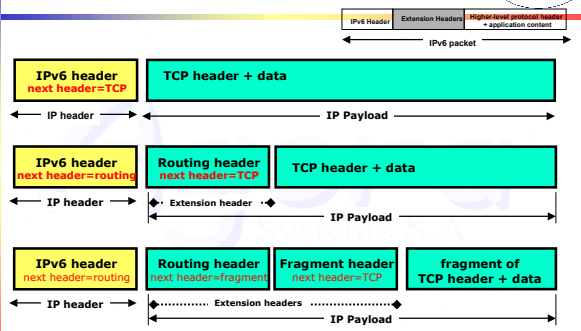
20 octetos + opciones : 13 campos, incluyendo 3 bits de flag



Resumen de cambios en las cabeceras IPv4/IPv6

- Mejorados
  - Los campos de fragmentación salen fuera de la cabecera básica
  - Las opciones IP salen fuera de la cabecera básica
  - Se elimina el checksum de la cabecera
  - Se elimina el campo con la longitud de la cabecera
  - El campo de longitud excluye la cabecera
  - La alineación se pasa de 32 a 64 bits
- Revisados
  - Time to Live → Hop Limit
  - Protocol → Next Header
  - Precedence & TOS → Traffic Class
  - Direcciones incrementadas 32 bits → 128 bits
- Extendidos
  - Campo "Flow Label" de identificación de flujos

Cabeceras de extensión



Espacio de direcciones

- **128-bit o 16 bytes**
- **2^128=340,282,366,920,938,463,463,374,607,431,768,211,456**
- **4.2 x 10^9** vs **3.4 x 10^38** addresses

  ← IPv4 → ← IPv6 →

Nota:
IPv4 ofrece 1 IP por cada 2 personas, e IPv6 ofrece ~5.6 x 10^28 por persona

Representación de las direcciones

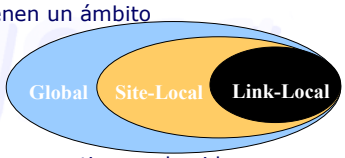
"Preferred" form:
1080:0:FF:0:8:800:200C:417A

Compressed form: FF01:0:0:0:0:0:0:43
se convierte en FF01::43

IPv4-compatible:
0:0:0:0:0:0:13.1.68.3
o ::13.1.68.3

Modelo de direccionamiento IPv6

- Las direcciones se asignan a interfaces
  - Igual que sucedía en IPv4
- Una interfaz puede tener múltiples direcciones
- Las direcciones tienen un ámbito
  - Link Local
  - Site Local
  - Global



- Las direcciones tienen un tiempo de vida
  - Valid y Preferred lifetime

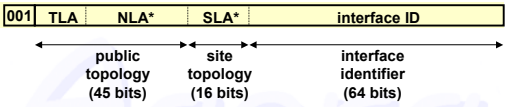
Prefijos para las direcciones

- El prefijo identifica el tipo de dirección IPv6; normalmente los primeros dos octetos.

Allocation	Binary prefix	Example (the first 16-bit)
Global unicast	001	2xxx or 3xxx
Link-local unicast	1111 1110 10	FE8x ... FEBx
Site-local unicast	1111 1110 11	FECx .... FEFx
IPv4-compatible unicast	000...0(96 zero bits)	0:0:0:0:0:0:n.n.n.n
IPv4-mapped unicast	000..FFFF(80 zero bits)	0:0:0:0:0:FFFF:n.n.n.n
Multicast	1111 1111	FFxx
Reserved IPX	0000 010	04xx or 05xx

- El resto de prefijos (85%) se reservan para uso futuro
- Las direcciones anycast se obtienen de prefijos unicast

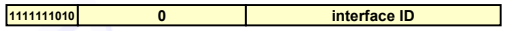
Global Unicast Addresses



- TLA = Top-Level Aggregator
  NLA* = Next-Level Aggregator(s)
  SLA* = Site-Level Aggregator(s)
- all subfields variable-length, non-self-encoding (like CIDR)
- TLAs may be assigned to providers or exchanges

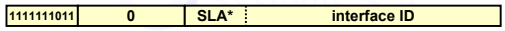
Link-Local & Site-Local Unicast Addresses

Link-local addresses se usan para autoconfiguración y cuando no hay routers presentes:



e.g=>fe80::2d0:b7ff:fe11:5d36

Site-local addresses mantienen independencia de cambios de TLA / NLA*:



e.g=>fec0::90:234:ffde:1098

Formato de direcciones multicast

FP (8bits)	Flags (4bits)	Scope (4bits)	Group ID (80+32bits)
11111111	000T	Lcl/Sit/Gbl	Locally administered

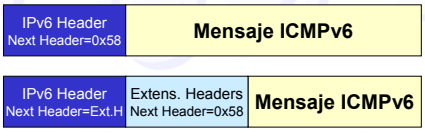
- flag field
  - **T=0 => dirección bien conocida asignada por IANA**
  - **T=1 => dirección disponible para ser usada por aplicaciones**
- scope field:
  - **1 – nodo local**
  - **2 – enlace local**
  - **5 – site local**
  - **8 – organización local**
  - **B – comunidad local**
  - **E – global**
  - **(el resto de valores están reservados)**
- Se mapean las direcciones IPv6 multicast directamente a los 32 bits del nivel IEEE 802 MAC

Índice

- Introducción a IPv6
- ICMPv6, ND y Autoconfiguración
- Seguridad en el nivel de red (IPsec)
- Seguridad de los mecanismos básicos
- Conclusiones y Trabajo Futuro

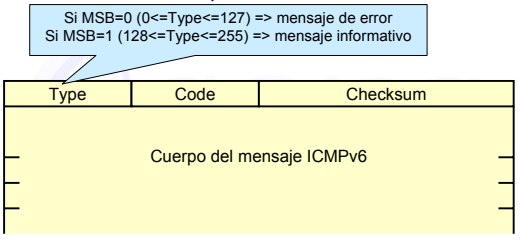
Introducción a ICMPv6

- Realiza funciones de ICMP, IGMP y ARP
- Dos tipos de mensajes
  - Mensajes de error
  - Mensajes de información
- Todos ellos van en un paquete IPv6 que puede contener también "extension headers".



Formato de los mensajes ICMPv6

El formato es común para todos ellos:

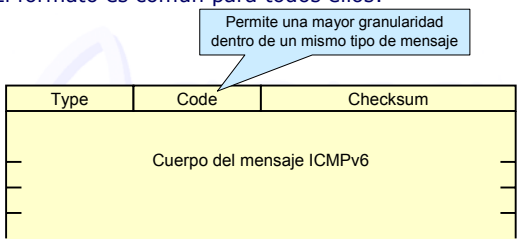


Tipos de mensajes ICMPv6

Type	Mensaje ICMPv6
1	Destination Unreachable
2	Paket Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

Formato de los mensajes ICMPv6

El formato es común para todos ellos:



Opciones de mensajes ICMPv6

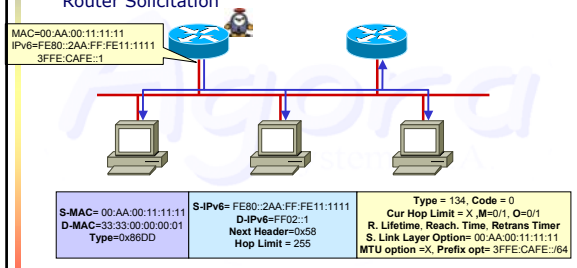
- Source/Target Link Layer
- Prefix Information Option
- Redirect Header Option
- MTU Option

Neighbor Discovery

- Proceso que realizan los nodos IPv6 para entre otras cosas:
  - Localizar routers vecinos
  - Aprender prefijos y parámetros de configuración
  - Autoconfigurar sus direcciones
  - Determinar si un vecino ya no está alcanzable (NUD)
  - Descubrir direcciones duplicadas (DAD)
  - Descubrir direcciones de nivel de enlace
  - Redirección de primer salto
- Se usan 5 mensjes ICMPv6 diferentes
  - Router Solicitation
  - Router Advertisement
  - Neighbour Solicitation
  - Neighbour Advertisement
  - Redirect

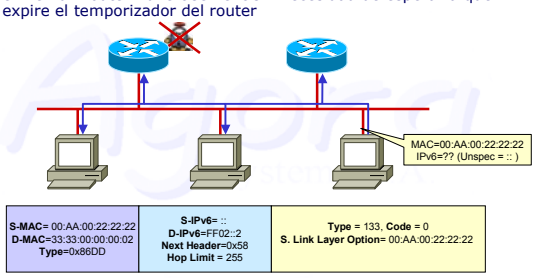
Router Advertisements

- Los routers se anuncian periódicamente enviando un ICMPv6 Router Advertisement, o como respuesta a un Router Solicitation



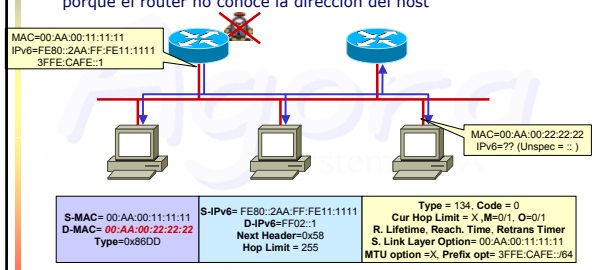
Router Solicitations

- Un host que acaba de arrancar, puede hacer que los routers le envíen un router Advertisement sin necesidad de esperar a que expire el temporizador del router



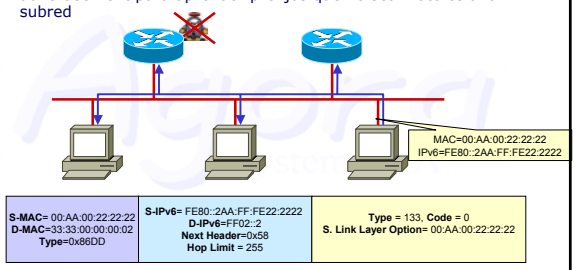
Router Solicitation Response

- En este caso el router responde a la dirección MAC unicast del nodo que envió el router solicitation. La IPv6 destino es FF02::1 porque el router no conoce la dirección del host



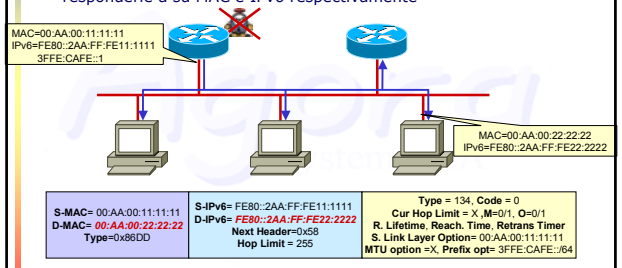
Router Solicitation (2)

- Aunque no acabe de arrancar, el host puede solicitar un router advertisement para aprender prefijos que no sean locales a la subred



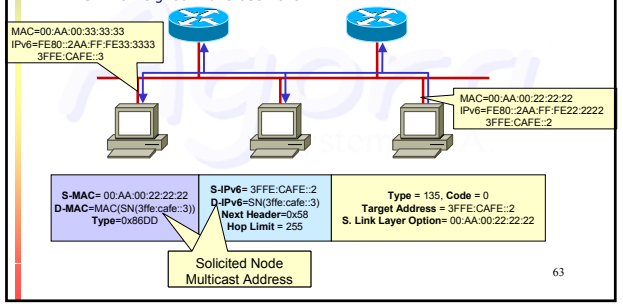
Router Solicitation Response (2)

- Como en este caso, el router conoce la dirección IPv6 de enlace local del nodo que solicitó el router advertisement, puede responderle a su MAC e IPv6 respectivamente



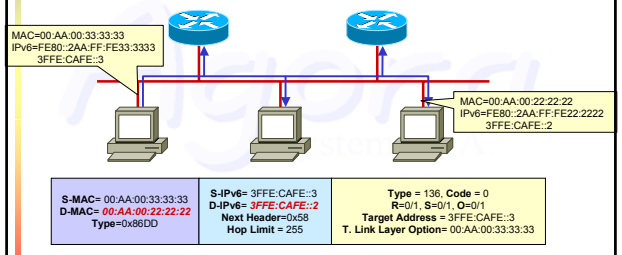
Resolución de direcciones

- Mientras que en IPv4 se usa ARP, en IPv6 esta función se incorpora en ICMPv6.
  - ICMPv6 Neighbor Solicitation
  - ICMPv6 Neighbor Advertisement



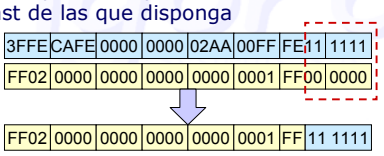
Resolución de direcciones (2)

- El destino, contesta con su dirección de enlace en un mensaje unicast (Neighbor Advertisement) dirigido a la dirección unicast que venía en el Neighbour Solicitation



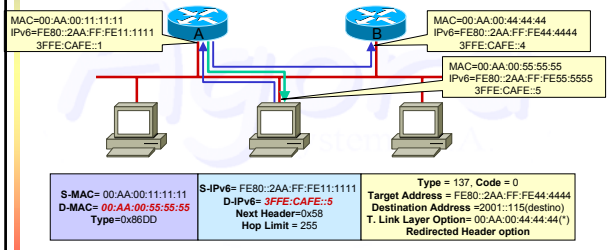
Solicited Node Multicast Address

- En el rango FF02:0:0:0:0:1:FF00::/104
- Se obtiene añadiendo los 24 LSB de la dirección unicast o anycast
- Todo nodo esta obligado a unirse a ese grupo multicast para cualquier dirección unicast o anycast de las que disponga



Función de Redirect

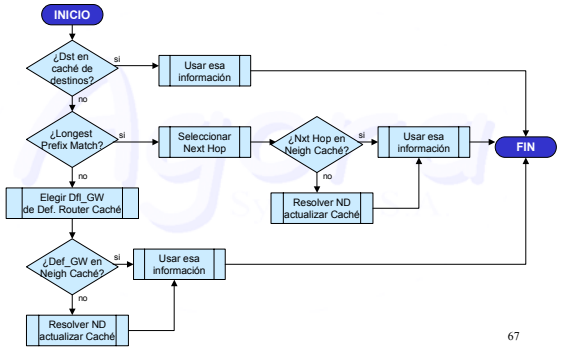
- El router por defecto no tiene por que ser el mejor camino hacia un destino de otra subred externa. **También útil para dos subredes sobre el mismo enlace físico**
- Ej: Si A para enrutar un datagrama ha de enviarlo otra vez por la misma interfaz por la que le llegó, => que hay un mejor camino si el nodo, envía directamente el datagrama al siguiente salto



S-MAC= 00:AA:00:11:11:11 **D-MAC**= ***00:AA:00:55:55:55*** **Type**=0x86DD	**S-IPv6**= FE80::2AA:FF:FE11:1111 **D-IPv6**= ***3FFE:CAFE::5*** **Next Header**=0x58 **Hop Limit** = 255	**Type** = 137, **Code** = 0 **Target Address** = FE80::2AA:FF:FE44:4444 **Destination Address** =2001::115(destino) **T. Link Layer Option**= 00:AA:00:44:44:44(*) **Redirected Header option**

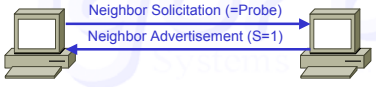
(*) Sólo si se conoce en ese momento

Algoritmo de transmisión de datos



Neighbor Unreachability Detection (NUD)

- Estados de una entrada en la neighbour caché:
  - Al introducirla, **"Reachable"**
  - A los 30 segs desde la última confirmación de alcanzabilidad **"Stale"**
  - Al enviar el primer mensaje hacia ese nodo cuya entrada está en estado "Stale", se activa un timer de 5 segs, y la entrada pasa a modo **"Probe"**
  - En modo "Probe" se envían tres mensajes "probe" (uno por segundo). Si no se ha confirmado la alcanzabilidad de nodo, la entrada **se elimina**.



- Es imprescindible que el "Neighbor Advertisement" lleve el bit "S" (Solicited) activo. En otro caso, sólo se podría asegurar conectividad de B a A, pero no se sabe si la hay de A a B.

Mecanismos de autoconfiguración

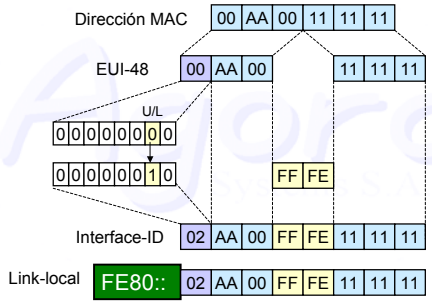
- Stateless (RFC 1791)
  - Parte integral de IPv6 (ICMPv6)
  - Creación de dirección de enlace local y global
  - Para la dirección de enlace local
    - Se asume que existe indentificador único de un interfaz
    - Se hace detección de duplicados (DAD)
- Stateful
  - Mecanismo tradiconal basado en DHCP
  - Adaptado a IPv6 (DHCPv6)
  - El servidor almacena información de
    - Direcciones a emplear
    - Otra infomación de configuración (DNS, etc.)

Autoconfiguración stateless

- Compendio de mecanismos que acabamos de estudiar

1. Generar dirección de enlace local
   1.a. Comprobar unicidad con detección de duplicados
2. Si la dirección de enlace no se ha podido crear, FIN
3. Encontrar los routers disponibles
   3.a. Esperar siguiente Router Advertisement
   3.b. Forzarlo enviando un Router Solicitation
4. Si no se recibe ningún RA, FIN (red aislada)
5. Autoconfigurar direcciones a partir del prefijo/s anunciado/s
   5.a. Bit "O" = 1 => Ir a DHCPv6 a por el resto de inform.
   5.b. Bit "M"= 1 => Ir a DHCPv6 a por más direcciones
6. Acabar autoconfiguración

Generación de dirección de enlace local



Duplicate Address Detection (DAD)

- Se usa para cualquier dirección unicast tanto manual como autoconfigurada
- El nodo envía un Neighbor Solicitation a su propia Solicited Node Multicast Address
  - Si no hay respuesta usa esta dirección (TODO OK)
  - Si alguien responde no usa esta dirección. El administrador de red ha de resolver esto manualmente

Dirección MAC		00	AA	00	11	11	11		
Interface-ID	02	AA	00	FF	FE	11	11	11	
IPv6 Source	FE80::	02	AA	00	FF	FE	11	11	11
IPv6 Dest	FF02::	00	00	00	01	FF	11	11	11
Target Addr	FE80::	02	AA	00	FF	FE	11	11	11

Solicited Node

Dirección a chequear

Autoconfiguración stateless

- Compendio de mecanismos que acabamos de estudiar

1. Generar dirección de enlace local
   1.a. Comprobar unicidad con detección de duplicados
2. Si la dirección de enlace no se ha podido crear, FIN
3. Encontrar los routers disponibles
   3.a. Esperar siguiente Router Advertisement
   3.b. Forzarlo enviando un Router Solicitation
4. Si no se recibe ningún RA, FIN (red aislada)
5. Autoconfigurar direcciones a partir del prefijo/s anunciado/s
   5.a. Bit "O" = 1 => Ir a DHCPv6 a por el resto de inform.
   5.b. Bit "M"= 1 => Ir a DHCPv6 a por más direcciones
6. Acabar autoconfiguración

Esta parte, tal cual vimos antes

Autoconfiguración Stateful (DHCP)

- Modelo cliente/servidor basado en UDP
  - Los servidores envían por el puerto 546
  - Los clientes envían por el puerto 547
- 6 tipos de mensajes
  - DHCPv6 Solicit
    - Enviado por el cliente a All-DHCP-Agents (FF02::C), sirve para localizar a los servidores DHCP disponibles (si no se conocen)
  - DHCPv6 Advertise
    - Enviado por unicast por el servidor al cliente que envió el **Solicit**
  - DHCPv6 Request
    - Mensaje unicast de cliente a servidor para solicitar parámetros de red
  - DHCPv6 Reply
    - Respuesta del servidor que contiene la información de la red
  - DHCPv6 Release
    - Mensaje de cliente a servidor para indicar que el cliente deja libres ciertos recursos de red, que el servidor puede reasignar
  - DHCPv6 Reconfigure
    - Mensaje unicast del servidor al cliente, para indicarle que ciertos parámetros deben reconfigurarse. Para esta reconfiguración el cliente enviará un mensaje **Request**

Índice

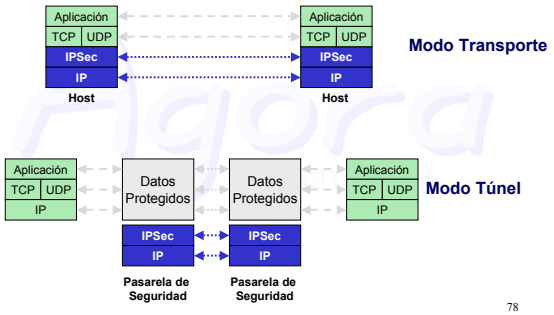
Seguridad en IPv6

- En general, la seguridad de IPv6 no es muy diferente de la de IPv4
- La implementación de IPsec en IPv6 es obligatoria, y su uso recomendado
- IPv6 permite seguridad e2e, que en IPv4 no se puede conseguir por culpa de los NATs
- En IPv6 se pueden emplear los mismos elementos que en IPv4
  - Firewalls
  - Filtrado de paquetes
  - ...
- Hay que desmitificar al NAT como elemento para ofrecer seguridad

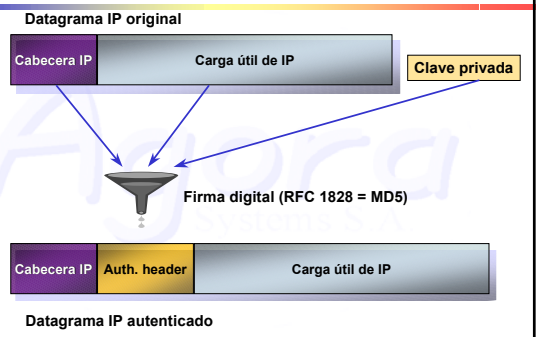
¿Qué es IPsec?

- Autenticación y cifrado a nivel de red
- Estandar abierto para proporcionar comunicaciones privadas y seguras
- Obligatorio en implementaciones IPv6
- Ofrece una solución flexible y basada en estándares para implementar una política de seguridad en toda una red
- Ventajas:
  - Estándar para privacidad, integridad y autenticación para comercio en la red
  - Se implementa de forma transparente en la infraestructura de red
  - Ofrece seguridad extremo a extremo incluyendo a routers, firewalls, PCs y servidores

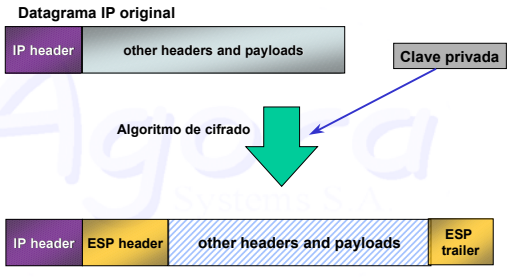
Modos en IPsec



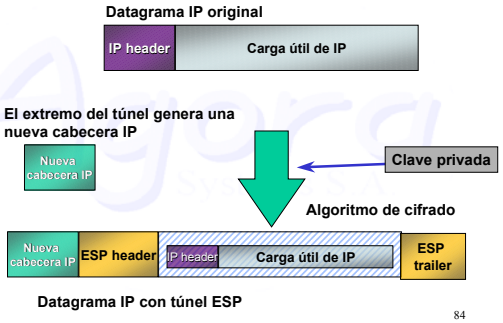
Authentication Header (AH)



IPsec ESP modo transporte



IPsec ESP Tunnel



IPSec Cabecera AH

- Authentication Header (AH)
- Se utiliza para obtener integridad y autenticación
  - Opcionalmente protege contra reenvío
- Autentica los campos del datagrama, salvo los mutables de IPv4
  - Type of Service (TOS)
  - Time to Live (TTL)
  - Flags
  - Header Checksum
  - Fragment Offset
  - Sólo autentica los mutables en el modo túnel
- Identificado como protocolo 51 (del IANA) en
  - IPv4: campo *Protocol*
  - IPv6: campo *Next Header*

Authentication Header

Next Header	Hdr Ext Len	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data		

- Codificada en cabecera IPv6 como Next Header = 0x51

IPSec Cabecera AH

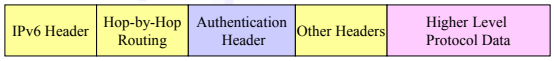
- Next Header (8 bits)
  - Tipo de datos tras la cabecera AH
  - Definido por IANA
- Payload Lenght (8 bits)
  - Longitud de la cabecera AH
  - En palabras de 32 bits menos 2
- Reserved (16 bits)
  - Actualmente se rellena a **0**
- Security Parameter Index (32 bits)
  - El SPI de una SA previamente definida

IPSec Cabecera AH

- Sequence Number (32 bits)
  - Contador con crecimiento monótono
  - Para protección contra reenvío de paquetes
  - Campo obligatorio, inicializado a **1** por la SA
  - Es responsabilidad del receptor usarlo o no
  - Si se llega al máximo (2^{32}-1), se negocia otra SA
- Authentication Data (múltiplo 32 bits)
  - Usado por el receptor para verificar la integridad
  - Para el cálculo, los campos mutables se suponen **0**
  - Se puede usar cualquier algoritmo de MAC
    - HMAC-MD5-96
    - HMAC-SHA-1-96

IPSec Cabecera AH

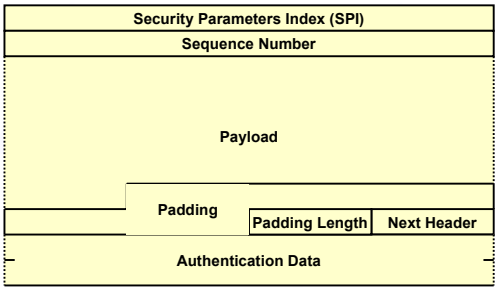
- AH en IPv6
  - AH es parte del protocolo IPv6, y se consideran datos de extremo a extremo
  - Aparece después de las cabeceras de extensión
  - Aparece antes o después de las opciones de destino



IPSec Cabecera ESP

- Encapsulating Security Payload (ESP)
- Se utiliza para integridad, autenticación, y cifrado
  - Opcionalmente protege contra reenvío
  - Servicios no orientados a conexión
  - Selección opcional de servicios
    - Al menos uno debe de estar activado
- Identificado como protocolo 50 (del IANA) en
  - IPv4: campo *Protocol*
  - IPv6: campo *Next Header*

Encapsulating Security Payload (ESP)



IPSec Cabecera ESP

- Security Parameter Index (32 bits)
  - El SPI de una SA previamente definida
- Sequence Number (32 bits)
  - Contador con crecimiento monótono
  - Para protección contra reenvío de paquetes
  - Campo obligatorio, inicializado a **1** por la SA
  - Es responsabilidad del receptor usarlo o no
  - Si se llega al máximo (2^{32}-1), se negocia otra SA

IPSec Cabecera ESP

- Payload Data (variable)
  - Datos de usuario cifrados por el algoritmo de la SA
  - Se puede usar cualquier algoritmo de bloques
    - DES-CBC
    - 3DES
  - Definido por IANA
  - Si se requiere vector de inicialización, se incluye aquí
- Padding (0-255 bytes)
  - Para ajustar los datos al tamaño de bloque de cifrado
  - Puede ocultar la longitud del mensaje original
  - Puede afectar negativamente en el ancho de banda

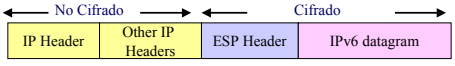
IPSec Cabecera ESP

- Pad Lenght (8 bits)
  - Tamaño del campo *Padding*
  - Medido en bytes (**0** significa sin relleno)
- Next Header (8 bits)
  - Tipo de datos contenido en el *Payload Data*
  - Definido por IANA
- Authentication Data (múltiplo 32 bits)
  - Usado por el receptor para verificar la integridad
  - Similar al campo de la cabecera AH

IPSec Cabecera ESP

- ESP en modo de Transporte
  - La cabecera ESP es insertada justo después de la IP
  - Si ya hay cabecera IPSec, se inserta justo antes

- ESP en modo de Túnel
  - La cabecera ESP es insertada justo antes del datagrama a cifrar



IPSec ¿Por qué dos cabeceras?

- ESP requiere criptografía fuerte, se use o no, mientras que AH sólo requiere hashing
  - La criptografía está regulada en muchos países
  - La firma no suele estar regulada
- Si sólo se requiere autenticación, AH es mejor
  - Formato más simple
  - Menor tiempo de procesamiento
- Al tener dos cabeceras se tiene un mejor control sobre la red IPSec, así como opciones flexibles

Índice

- Introducción a IPv6
- ICMPv6, ND y Autoconfiguración
- Seguridad en el nivel de red (IPsec)
- Seguridad de los mecanismos básicos
- Conclusiones y Trabajo Futuro

Seguridad de ND & Autoconf.

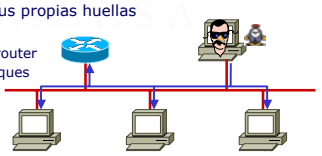
- Aparecen problemas incluso con un nivel de enlace seguro.
- En RFC 2461 y RFC 2462 se comenta la posibilidad de usar cabeceras AH para autenticar estos mensajes
- No se explica como
- Problemas de usar AH
  - No siempre es posible. El host podría no tener a SA necesaria (Ej: movilidad)
  - Para poder establecerla automáticamente, ya necesitaría acceso a la red
  - Se haría necesario el establecimiento manual de SAs entre todos los hosts y routers de la LAN
  - Imposible pre-configurar SAs para más de 4 billones de posibles "Solicited Node" multicast addresses.

Posibles ataques

- Malicious Last Hop Router
- Good Router Goes Bad
- Neighbor Solicitation/Adv Spoofing
- Spoofed Redirect Message
- Bogus On-Link Prefix
- Bogus Address Configuration Prefix
- Duplicate Address Detection DoS Attack
- Neighbor Discovery DoS Attack (desde fuera)
- Parameter Spoofing

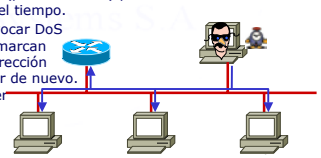
Malicious Last Hop Router

- Un nodo en la LAN podría hacerse pasar por un router enviando RAdv (tanto multicast de anuncio como unicast de resspuesta a RSol).
- Si cualquier host selecciona a este router como por defecto, éste podría provocar un DoS o incluso un Man in the Middle.
- El nodo maligno puede asegurarse que le van a elegir a él, enviando un RAdv haciéndose pasar por el router con un Lifetime = 0.
- Una vez hecho el ataque, podría enviar un Redirect hacia el verdadero router, borrando sus propias huellas
- Good Router Goes Bad
  - Se compromete un last hop router
  - Exáctamente los mismos ataques



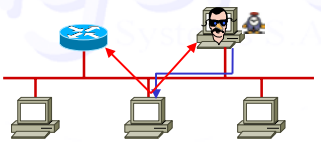
Neighbor Solicitation / Advertisement Spoofing

- El atacante puede hacer que datagramas dirigidos a nodos legítimos se envíen a otra dirección de enlace
  - Enviando un Neigh. Solicitation con Source Link-Layer Option
  - Enviando un Neigh. Advertisement con Target Link-Layer Option
- Esto sobre-escribirá las cachés del resto de nodos (incluso puede forzarse activando el bit 'O' – Override)
- Variedades del ataque
  - Usar una dirección de enlace válida. El atacante simplemente repondiendo a los unicast NS (parte del NUD) puede mantener el ataque indefinidadmente en el tiempo.
  - Usar una no válida para provocar DoS
    A los (30-50 seg) los nodos marcan como no válida (NUD) esa dirección de enlace, e intentan resolver de nuevo. El atacante tendría que volver a repetir el ataque



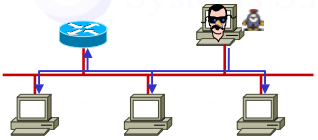
Spoofed Redirect Message

- El atacante usa la dirección "link-local" del legítimo First-hop router y envía un mensaje Redirect a un nodo legítimo
- El nodo acepta el mensaje Redirect porque viene de la dirección "link-local" de su router por defecto, y comienza a enviar sus datagramas a la nueva dirección de enlace que aparece en el redirect
- Mientras el atacante responda a los NUD-Probes dirigidos a la nueva dirección de enlace, el ataque seguirá teniendo efecto.



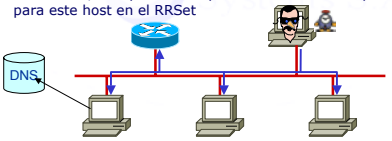
Bogus on-link Prefix

- El atacante envía un RAdv indicando que un prefijo de una cierta longitud es "on-link". (esta longitud podría ser incluso /128)
- Los nodos que reciben dicho mensaje, nunca enviarán al router datagramas dirigidos a direcciones dentro de estos prefijos. Intentarán hacer ND enviando Neigh. Sol.
- Al no haber respuesta, se produce un ataque de DoS
- El atacante puede controlar el tiempo del ataque con el "lifetime" asociado al anuncio del prefijo.
  - Si este fuese infinito, un host no podría recuperarse hasta que no perdiese el estado (e.g. Reboot, o anuncio similar con lifetime=0)



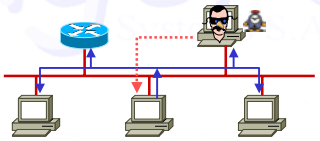
Bogus Address Configuration Prefix

- El atacante envía un RAdv anunciando un prefijo no válido para la subred
- Los nodos que reciben dicho mensaje, se autoconfiguran con una dirección no válida en la subred
- Como resultado, los mensajes de vuelta nunca serán recibidos porque la dirección fuente del host no es válida
- Este ataque podría incluso propagarse fuera de la subred:
  - Si el host actualiza dinámicamente su registro AAAA o A6 del DNS, el cambio podría propagarse
  - Con suerte, las aplicaciones podrían intentar otras posibles direcciones para este host en el RRSet



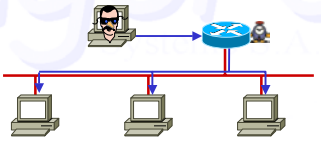
Duplicate Address Detection DoS Attack

- Un atacante puede provocar un ataque de DoS respondiendo a todos los intentos de DAD que haga un nuevo hosts que intenta autoconfigurarse
- Si el atacante dice estar usando esa dirección, el atacado nunca conseguiría una dirección
- Podría evitarse haciendo que el router controlase qué hosts se han configurado qué direcciones. Sin embargo, estos posibles mecanismos no están estandarizados



Neighbor Discovery DoS Attack

- El atacante, desde fuera de la subred, fabrica direcciones de dentro de la subred, y envía los datagramas
- El router de acceso deberá resolver esas direcciones
- Un nodo legítimo de dentro de la subred podría no llegar a obtener un servicio de descubrimiento de vecinos, por estar el router cursando otros ND.
- El ataque en este caso se dirige al Neighbor Caché.



Parameter Spoofing

- El atacante envía un RAdv igual al del router pero cambiando los parámetros del mensaje (hop limit, preferred lifetime, etc.) de forma que se interrumpa el tráfico legítimo.
- Si incluye un "Current Hop Limit" de 1 u otro número pequeño, los paquetes de los nodos legítimos de la subred serían eliminados antes de llegar al destino
- Si el atacante implementa un DHCP server trucado, y activa los flags 'M' y 'O' en el mensaje, éste estaría en disposición de gestionar la autoconfiguración de todos los nodos

RFC 3041.- Extensions to IPv6 Address Autoconfiguration

- El uso de identificadores permanentes únicos daña la privacidad del usuario
  - En IPv6, las direcciones construidas a partir de identificadores únicos (e.g. IEEE MACs) se pueden tracear simplemente
- RFC 3041 define un mecanismo para la generación de direcciones IPv6 que cambian temporalmente a partir de identificadores pseudoaleatorios
- En el art. 29 de la EC (data protection) claramente va en contra de esta falta de privacidad
  - Por ejemplo, con MIPv6, a partir de los datagramas que recibo de un nodo móvil, puede saber donde está (por su direccionamiento jerárquico).
- Este es uno de los problemas básicos del modelo e2e, y posiblemente siga habiendo más debate...

Índice

- Introducción a IPv6
- ICMPv6, ND y Autoconfiguración
- Seguridad en el nivel de red (IPsec)
- Seguridad de los mecanismos básicos
- Conclusiones y Trabajo Futuro

Conclusiones

- Se ha avanzado mucho en la madurez de IPv6
  - Operadores, productos, equipos, software...
- Cada vez se ve más cercano un posible despliegue de IPv6
- Hay que prestar especial atención a la seguridad de IPv6
  - Aunque IPv6 se haya diseñado con muchas lecciones aprendidas de IPv4, las implementaciones de IPv6 no llevan 20 años de refinamiento frente a ataques
- En los nuevos mecanismos de IPv6, aún quedan aspectos importantes por resolver
  - Seguridad en la autoconfiguración
  - Seguridad en la resolución de direcciones
  - Seguridad en Mobile IPv6
  - Adecuación a normativas Europeas
- Solución a los problemas aquí planteados, estudiándose en el grupo SEND de IETF

Trabajo Futuro

- La transición a IPv6 se ve como un largo (aprox 20 años) periodo de coexistencia
- El despliegue de este tipo de escenarios de transición no es simple en absoluto
  - Multitud de mecanismos
  - Múltiples requerimientos (no compatibles en algunos casos)
  - Sin poder presuponerse conectividad e2e
- En este tipo de entornos heterogéneos, la seguridad va a ser complicada de garantizar
  - Escenarios complejos => C(IPv4)+C(IPv6)+C(IPv4&6)
  - Diferentes topologías a las acostumbradas
    - Un usuario final (e.g. ADSL) recibiría un /48 o /64
    - El operador en lugar de conectar usuarios sin conocimientos, conectará redes inseguras de usuarios sin conocimientos