

IP versión 6 (Parte 01) - Sus componentes.

Madrid, abril de 2013.

Por: Alejandro Corletti Estrada (acorletti@darFe.es - acorletti@hotmail.com)

1. Presentación.

Con este primer artículo, damos inicio a una **serie** cuya intención es la de completarla poco a poco hasta agotar el tema de IP versión 6 (también llamado IP Next Generation: IPNG).

No desarrollaremos aspectos históricos o evolución del mismo, pues ya está suficientemente documentado este aspecto, sino su explicación eminente técnica, basándonos en las **RFCs** (Request for Comments) que lo describen y sobre todo en el "**análisis de tráfico**" presentando tramas, ejemplos concretos y casos prácticos de su funcionamiento.

Una vez más hacemos este sencillo aporte para la libre descarga y difusión en Internet, con la única intención de colaborar en el conocimiento detallado de esta nueva tecnología y con mucha (*pero mucha...*) esperanza que en esta parte del mundo de habla hispana seamos capaces de "mojarnos", involucrarnos y aunar esfuerzos para demostrar que somos capaces de liderar o al menos formar parte activa en los avances tecnológicos (*este será el lema y objetivo de toda esta serie*).

Como se menciona en el pie de página, esta vez no es cuestión de inversiones monetarias, ya la gran mayoría de dispositivos soportan este conjunto de normas, sólo es necesario ponernos de acuerdo, presionar a las operadoras de telecomunicaciones, a los organismos oficiales y sobre todo poner nuestro esfuerzo (tal vez también desinteresadamente) para lograr esta vez lo que no fuimos capaces con la versión 4 de "participar" en las decisiones globales demostrando que este ENORME porcentaje de población mundial sabe a lo que está enfrentando, posee los conocimientos y experiencia necesaria, y desea verse involucrado compartiendo lo que tiene instalado y en producción..... en vez de recibir las migajas (aunque suene duro) que estén dispuestos a ofrecernos.

Os invitamos a *unir esfuerzos, voluntades y FE para lograrlo*

La población de habla hispana nativa es un 1,3% mayor que la de habla inglesa

Todos los artículos estarán estructurados de la siguiente forma:

1. Presentación.
2. Introducción.
3. Desarrollo.
4. Capturas de tráfico – ejemplos.



2. Introducción.

Si tuviéramos que enfrentar el desafío de realizar una reforma estructural, por ejemplo en el tercer piso de un gran edificio de cinco plantas de unos 30 años de antigüedad. Si en esa planta fuéramos a colocar el doble de oficinas, muros de separación, maquinarias, cableado, servicios, acondicionadores de aire, etc... es indudable que semejante reforma impactaría en varios aspectos del resto del edificio, por ejemplo debería contemplarse:

- ⊗ Reforzar los muros de las plantas inferiores (pues soportarían mucho más peso).
- ⊗ Cambiar la dimensión de su cableado desde el cuadro central.
- ⊗ Ampliar los accesos de voz y datos del edificio.
- ⊗ Modificar escaleras, ascensores, vías de evacuación.
- ⊗ Es posible también que si, supongamos, en las plantas superiores, existe personal que deba comunicarse con los del tercer piso y ahora esos son cuatro veces más, pues a estos superiores deberíamos de alguna forma permitirles interactuar o asignar tareas a una planta con 4 veces más personas.
- ⊗ Podríamos seguir bastante más con este supuesto.....

Si profundizáramos detalladamente en esta reforma, la conclusión evidente es que cuando se lanza un desafío de este tipo, el mismo no queda acotado únicamente a esa planta sino que impacta en mayor o menor medida en las inferiores y superiores.

Cuando hablamos del desafío que nos propone esta nueva versión del protocolo IP, el resultado es exactamente el mismo. Es decir, un cambio radical sobre la estructura de una nueva versión de un protocolo fundamental como es IP, sí o sí debe generar algunos cambios en los pisos superiores e inferiores de esta pila, familia o modelo TCP/IP (o también llamado Darpa).

Como el nombre de este artículo lo indica, comenzaremos esta serie, describiendo brevemente todo el conjunto de “componentes” (o protocolos) que también necesitan sufrir modificaciones en virtud de esta nueva versión, todos ellos también reciben la denominación de “Versión 6” y son los que presentaremos en el desarrollo de este texto.

Al igual que en el ejemplo de la reforma de construcción, decidimos iniciar estos artículos, con la visión global del edificio, para poder comprender todo el conjunto que se ve implicado, una vez tenida esta visión lejana del problema, seguiremos adelante entrando en el detalle de cada uno de ellos durante los próximos artículos.

3. Desarrollo.

Recordando el modelo de cinco capas que siempre hemos propuesto (ver y/o descargar por Internet el libro “**Seguridad por Niveles**”), encontramos los siguientes niveles:

- ⊗ Nivel 1: Físico.
- ⊗ Nivel 2: Enlace.





- ⊗ Nivel 3: Red.
- ⊗ Nivel 4: Transporte.
- ⊗ Nivel 5: Aplicación.

La nueva versión del protocolo IP presenta los siguientes cambios principales:

- ⊗ Encabezado mínimo de 40 Bytes (frente al mínimo de 20 de la versión 4).
- ⊗ Campo de direcciones de 128 bits (frente a los 32 de la versión 4).
- ⊗ Responsable de la determinación MTU (Unidad de transporte máximo) (Tema que se encargaba TCP en la versión 4).
- ⊗ Diferentes opciones para la asignación dinámica de direcciones (No solo DHCP: Dynamic Host Configuration Protocol).
- ⊗ No existe el concepto de Broadcast y aparece uno nuevo llamado "Anycast" (y esto afecta el nivel de enlace)
- ⊗ Nueva funcionalidad para determinar la unidad máxima de transmisión de información (MTU) para evitar la fragmentación en nodos intermedios.
- ⊗ IPSec como funcionalidad nativa de IPv6 (Es la única metodología de túnel aprobada por IETF (Internet Engineering Task Force).
- ⊗ Agrega 20 bytes más para QoS ("Flow level"), que se suman a los 8 bits originales de IPv4 que sólo cambian de nombre y ahora se llaman "Traffic class".
- ⊗ Elimina:
 - La capacidad de fragmentación que tenía IPv4, por lo tanto elimina todos estos campos (Ahora es una cabecera en extensión y solo se puede realizar en origen y destino, NO en nodos intermedios).
 - Longitud de cabecera (Ahora se llama "payload Length" y es la longitud del campo de datos, incluyendo cabeceras de extensión).
 - Control de errores de cabecera
 - Opciones

A continuación presentaremos los protocolos y recomendaciones que están asociadas a este nuevo diseño. Tal cual se expresó al principio, en este primer artículo sólo se hará la presentación inicial con el objetivo de comprender todos los "Componentes" de este cambio, en los próximos artículos se irá profundizando en cada uno de ellos.

Cada uno de estos cambios impacta a sus vecinos, concretamente en los siguientes aspectos:

a. Nivel de transporte

El encabezado mínimo de 40 Bytes, (el doble que la versión 4) afecta principalmente dos temas del nivel de transporte, su primer problema está



relacionado con el control de ventana de envío y recepción para el caso de TCP, el segundo al control de errores por una especie de “apaño” que se puede ejecutar sobre los protocolos de nivel 4 TCP y UDP a través del concepto de “pseudo encabezado”, en el cual se solapaban bits del encabezado de IP con TCP o UDP, al modificar el tamaño del encabezado IP, esto afecta concretamente a TCP y UDP y se consideran estas nuevas metodologías como:

- ⊗ UDPv6:
- ⊗ TCPv6:

Si bien se debe aclarar que no existen RFC que los proclamen como versión 6.

En TCP, sin lugar a dudas el mayor impacto pasa por que se cuadruplica el trabajo sobre la técnica de “Ventana deslizante” (para profundizar, ver libro “**Seguridad por Niveles**”); sobre nodos que soportan muchas sesiones simultáneas, esto es un impacto importante, pues ahora debe analizar y almacenar “Sockets” compuestos por una concatenación de dirección IP + puerto (origen y destino) cuatro veces mayor, por lo tanto este incremento no es trivial, de hecho a mi juicio es donde mayor tarea de análisis de impacto de se deberá realizar y seguramente un nuevo dimensionamiento de estos servicios. Por otro lado (¿será para compensar?) se aliviana la tarea del cálculo de la MTU que es una actividad típica de TCP sobre IPv6.

Otro aspecto a mencionar en este nivel es un nuevo concepto que se denomina “**Jumbogramas**” definidos en la RFC 2675, esta recomendación tiene su base en la calidad de los vínculos de comunicaciones actuales (particularmente la fibra óptica) que en virtud de la bajísima tasa de errores, permite el empleo de “inmensas” unidades de información en un solo bloque pues la probabilidad de tener que retransmitirla es casi despreciable, por lo tanto se puede minimizar el empleo de muchos encabezados de paquetes pequeños y aprovechas para enviarlos todos en uno sólo “Enorme” → Jumbograma. Este hace uso de un campo de opciones y permite llevar el concepto de “Payload” con 32 bits, lo que equivale a unos 4.000.000 de Bytes en el campo de datos, de estos mensajes. Por ejemplo su uso es ideal en vínculos de sincronismo entre clusters, dispositivos de alta disponibilidad, backups internos, etc.

En el caso de UDP la idea es similar, exceptuando el tema de la ventana deslizante, que no aplica a este protocolo.

No hay cambios en los encabezados ni aparecen nuevas RFCs del tipo “TCPv6 y/o UDPv6”, pero como se acaba de desarrollar, sí implica cambios y ajustes en sus lógicas de funcionamiento. Una RFC que hace referencia a las nuevos puertos y opciones para TCP y UDP (también lo hace como se puede apreciar para ICMP e IP) es la que figura a continuación:

Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers	4727	Proposed Standard (PS)
---	----------------------	------------------------

b. Aspectos que impactan en el nivel de enlace/físico:



1) Protocolo ND (Network Discovery).

Este nuevo protocolo que aparece de la mano de IPv6, podríamos decir que es el que reemplaza el empleo de ARP (Address Resolution Protocol), pero también asume funciones de DHCP (Dynamic Host Configuration Protocol), se encuentra regulado por las siguientes RFC:

Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification	3122	Proposed Standard (PS)
Neighbor Discovery for IP version 6 (IPv6)	4861	Internet Standard (STD)
Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)	6494	Proposed Standard (PS)
Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND)	6495	Proposed Standard (PS)
Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	6775	Proposed Standard (PS)

Algunas de las funciones más importantes que realiza son:

- Descubrimiento de routers, prefijos de red, parámetros (como MTU).
- Participar en la obtención de direcciones IP de forma dinámica.
- Mapeos de direcciones MAC a direcciones IP.
- Determinación del próximo salto.
- Detección de direcciones IP duplicadas.
- Redirección de rutas.
- Muy importantes son los conceptos de SEND (RFCs: 6494 y 6495) pensados para evitar los conocidos ataques sobre direccionamiento MAC.

2) Especificaciones sobre protocolos de nivel enlace/físico ya existentes.

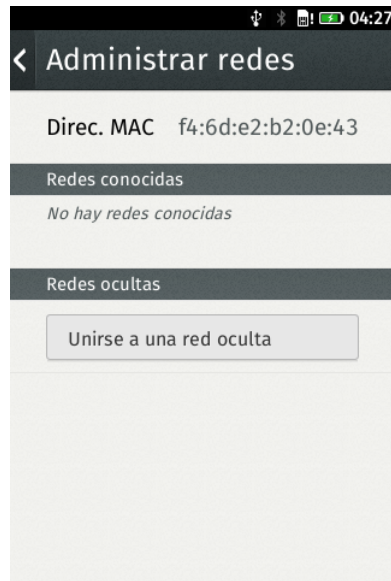
Tal cual iniciamos este artículo, podemos estar seguros que existen cambios en los “cimientos” de este modelo. Las diferentes metodologías de acceso al modelo de capas actualmente se encuentran todas definidas para soportar IPv6. En la actualidad la gran mayoría de las tarjetas de red ya vienen con funcionalidades para IPv6. En nuestra opinión, la parte física de estos elementos, no sufre modificaciones, las mismas en general van relacionadas a nuevos parámetros de diseño relacionados a la velocidad de ese vínculo físico (nuevos conectores, modulación, codificación de bits, multiplexación, etc.) pero no en el uso o no de IPv6. Dónde sí vemos cambios es en el nivel de enlace.

En particular, una de los mayores objetivos de IPv6 (y es tal vez su desencadenante) es la telefonía móvil, actualmente ha puesto en evidencia la escasez de direccionamiento IPv4. El primer paso sin duda fue que los dispositivos “Smart pone” pudieran acceder a la red con todo un modelo de capas TCP/IP y las mismas prestaciones que un ordenador, para ello crecieron de forma acelerada las generaciones de acceso a la red móvil (2G, 2.5G, 3G, 3.XG y ya está lista 4G=LTE [Long Term Evolution]). El protocolo IPv6 tiene como una de sus mayores fortalezas de direccionamiento, un fuerte vínculo con las direcciones MAC (lo veremos en detalle en artículos posteriores, bajo las normas relacionadas a **EUI-64**), por esa razón es que hoy cualquier “Smart





phone” ya trae su propia tarjeta MAC con su numeración única a nivel mundial, a continuación mostramos imágenes de dos de estos dispositivos:



Firefox.OS

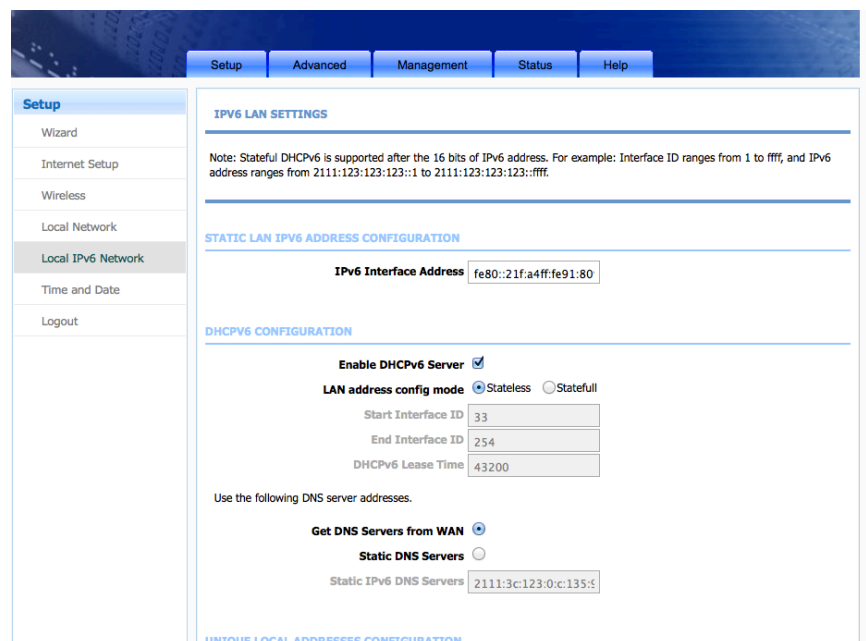


Nexus-Galaxy

Como pueda apreciarse en ambas imágenes su tarjeta y direccionamiento MAC ya la trae configurada y como estándar global de **IEEE**, este es único en el mundo (Para ampliar detalles ver libro “**Seguridad por Niveles**”).

Cuando desarrollemos este tema se profundizará, por ahora podemos ir anticipando que las pruebas que realizamos desde diferentes dispositivos móviles fueron las siguientes:

Instalamos un punto de acceso WiFi, habilitando IPv6, deshabilitando DHCPv4 y habilitando DHCPv6 como se presenta en la siguiente imagen:



Fuimos probando conexiones con diferentes teléfonos móviles con el siguiente resultado:

Nº	Equipo	Estado
1	Teléfono: Galaxy-Nexus SO: Android 4.2 – Kernel 3.0.31 Aplicación WiFi por defecto	No conectó
2	Teléfono: Samsung GT-S5830i SO: Android 2.3.6 – Kernel 2.6.35.7 Aplicación WiFi: Ipv6 Config (no permitió su instalación : kernel no lo soportaba)	No conectó
3	Teléfono: i pone 4	No conectó
4	Teléfono: Samsung Galaxy SIII SO: Android 4.1.2 – Kernel 3.0.31 Aplicación WiFi por defecto	No conectó
5	Teléfono: Nokia N-900 SO: Linux – Kernel 2.6.28.10-Power50 Aplicación WiFi por defecto	Conectó sin problemas y se le asignó una IP v6

En el caso de una conexión también WiFi a este mismo punto de acceso, pero desde una máquina Windows, se puede ver a continuación que no ha habido ningún inconveniente:

Adaptador de LAN inalámbrica Conexión de red inalámbrica:
 Sufijo DNS específico para la conexión. . . :
 Descripción Qualcomm Atheros QCA9565 802.11b/
 g/n WiFi Adapter
 Dirección física. : 20-68-9D-09-70-75
 DHCP habilitado : sí
 Configuración automática habilitada . . . : sí
 Vínculo: dirección Ipv6 local. . . : fe80::f192:133b:6680:d632%13(Preferido)
 Puerta de enlace predeterminada : fe80::21f:a4ff:fe91:8092%13
 IAID DHCPv6 : 287336605
 DUID de cliente DHCPv6. . . : 00-01-00-01-18-80-38-73-28-92-4^a-28-E6-13
 Servidores DNS. : fe80::21f:a4ff:fe91:8092%13
 NetBIOS sobre TCP/IP. : habilitado

(más adelante explicaremos todos los campos)

En realidad lo que queremos presentar con estas pruebas es el hecho que, tal cual vemos en el trabajo realizado, la tecnología SOPORTA Ipv6 pero hace falta: voluntad y esfuerzo en actualizarlos, instalar aplicaciones, configurar dispositivos, etc. Nos pareció oportuno incluir estas pruebas en este primer artículo, sólo para despertar el interés, en este caso con la telefonía móvil. Cuando publiquemos el artículo referente al nivel de enlace con IPv6 estarán en el mismo todos los detalles y el trabajo completo que hemos realizado.

Sobre la base de este direccionamiento (MAC) en los dispositivos móviles a nivel de enlace, es que se puede seguir avanzando para su total adaptación, primero hacia IPv4 de forma no tan dependiente (entre IP y MAC) y luego sobre IPv6 con una relación mucho más estrecha.

Al sólo efecto de presentar brevemente estas novedades de IPv6 respecto al nivel de enlace (reiteramos, todo el detalle será desarrollada en artículos posteriores), tomemos por ejemplo la primera de la RFC que figuran más abajo: **RFC-2464**, la misma al principio ya define (en su punto 3. “*Frame Format*”) que el formato de las tramas Ethernet seguirá siendo el mismo, pero introduce un nuevo valor para su campo “*Ethertype*” que será “**86Ddh**” (100001011011101). Luego en el punto 4 (“*Stateless Autoconfiguration*”) describe al detalle cómo esta dirección MAC (EUI-48) se trabaja para transformarla en lo necesario para dar origen a una dirección IPv6 (se transforma a formato EUI-64) y sobre esto a su vez (tratado en el punto 5. “*Link Local Addresses*”) se elabora la dirección de enlace local, que bajo este tipo de configuración se convertirá (tal cual lo expresa en el punto 6. “*Address Mapping Unicast*”) en este caso en su dirección IPv6 (para los que ya conocen algo del tema, será un prefijo del tipo FE80::/64), y en el punto 7. “*Address Mapping Multicast*” describe como se constituye esta dirección IPv6 para las transmisiones Multicast.

En resumen, lo que intentamos explicar en este punto es que para cada tipo de nivel de enlace/físico, existen una serie de recomendaciones que describen cómo deberá ser tratado el mismo para poder entregar su “payload” de forma efectiva al nivel superior cuando este sea IPv6.

A continuación presentamos las RFCs que se relacionan con cada uno de ellos:

Transmission of Ipv6 Packets over Ethernet Networks	2464	Proposed Standard (PS)
Transmission of Ipv6 Packets over FDDI Networks	2467	Proposed Standard (PS)
Transmission of Ipv6 Packets over Token Ring Networks	2470	Proposed Standard (PS)
Ipv6 over ATM Networks	2492	Proposed Standard (PS)
Transmission of Ipv6 Packets over Frame Relay Networks Specification	2590	Proposed Standard (PS)
Transmission of Ipv6 Packets over IEEE 1394 Networks	3146	Proposed Standard (PS)
IP Version 6 over PPP	5072	Internet Standard (STD)
Address Mapping of Ipv6 Multicast Packets on Ethernet	6085	Proposed Standard (PS)

c. Protocolo ICMP (Internet Control Message Protocol) versión 6.

Este protocolo, como su nombre lo indica se emplea para el envío y recepción de mensajes de control, en particular de errores, conectividad, rutas, etc.

En el caso de la versión 6, se trata del protocolo que más modificaciones sufre dentro de este modelo (junto con DHCP). Su funcionamiento y encabezado sigue la misma lógica de la versión anterior, una pequeña diferencia es que ahora el campo “Protocol” del paquete IP que invoca al protocolo de nivel superior se define con un nuevo valor “**58**” (para ICMPv4 este valor era “01”). Podríamos decir que su funcionamiento se continúa basando en los dos campos: “**tipo**” y “**código**”, pero sobre estos dos mismos campos presenta o define un importante número de opciones que antes no existían, en general todos estos los engloba en dos “tipos”: Mensajes tipo “error” (valores del campo “Type” entre 0 y 127) y mensajes tipo “información” (valores del campo “Type” entre 128 y 255). Lo nuevo en ellos está



relacionado a escuchas de multicast, solicitudes y advertencias de rutas y de vecinos, información de nodos, prefijos móviles y caminos de certificación.

El empleo del protocolo ND (mencionado anteriormente) está soportado a través de ICMPv6, y justamente aquí es donde también introduce esta funcionalidad de SEND (Secure Neighbor Discovery).

Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (Ipv6) Specification	4443	Internet Standard (STD)
Stateless Source Address Mapping for ICMPv6 Packets	6791 *	Proposed Standard (PS)

d. Protocolos de enrutado.

Es natural que si el campo de direccionamiento es el que mayor diferencia presenta en el protocolo IPv6, todo lo relacionado a rutas y direcciones sea el área donde mayor trabajo se encuentra.

Respecto a los protocolos de enrutado, podemos mencionar las siguientes recomendaciones:

RIPng for Ipv6	2080	Proposed Standard (PS)
BGP-MPLS IP Virtual Private Network (VPN) Extension for Ipv6 VPN	4659	Proposed Standard (PS)
Multiprotocol Extensions for BGP-4	4760	Draft Standard (DS)
Routing Ipv6 with IS-IS	5308	Proposed Standard (PS)
OSPF for Ipv6	5340	Proposed Standard (PS)
IANA Considerations for the Ipv4 and Ipv6 Router Alert Options	5350	Proposed Standard (PS)
Virtual Router Redundancy Protocol (VRRP) Version 3 for Ipv4 and Ipv6	5798	Proposed Standard (PS)
Ipv6 Traffic Engineering in IS-IS	6119	Proposed Standard (PS)
Ipv4 and Ipv6 Infrastructure Addresses in BGP Updates for Multicast VPN	6515	Proposed Standard (PS)
Ipv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages	6516	Proposed Standard (PS)

En general estas nuevas versiones de protocolos de enrutado, ofrecen mayores funcionalidades para descubrimiento de routers (parte de ND), de distancias, saltos, por supuesto soporte para los nuevos 128 bits de direccionamiento (frente a los 32 anteriores), nuevos puertos (para que permitan convivir ambas versiones), interacción/integración directa con IPsec para seguridad (Autenticación, acceso, integridad, confidencialidad, trazabilidad, no repudio).

Un caso particular de denominación es OSPF (Open Short Path First) para IPv6 que es también conocido como OSPFv3 (en vez de ser "v6"), algo similar sucede con las extensiones de BGPv4+.

Con IPv6 pierde sentido todo concepto de NAT (Network Address Translation) y CIDR (Classless Inter Domain Routing), por lo tanto esto alivia de trabajo



sensiblemente a todos los elementos responsables del manejo de rutas y creación/mantenimiento de túneles.

e. DHCP (Dynamic Host Configuration Protocol)

Como ya hemos anticipado, este protocolo es tal vez el que mayor trabajo ha ocasionado con la aparición de IPv6. La aparición de DHCP fue la evolución natural del protocolo **Bootp** (Boot Trap Protocol, para profundizar sobre esto ver libro "**Seguridad por Niveles**"), luego también se relaciona con **R_ARP** (Reverse Address Resolution Protocol) y para simplificar, ampliar y hacer más amigable esta configuración nace DHCP. Esta sumatoria de ampliaciones (que hasta tal vez podríamos llamar "parches") es la que se optimiza considerablemente con DHCPv6. Se crean dos puertos nuevos para solicitudes y respuestas: UDP 546 y 547 (que en DHCPv4 son: UDP 67 y 68), con la convivencia de estos cuatro puertos se permite el funcionamiento de ambas versiones simultáneamente (para transición) pudiendo contar en la misma red con los dos esquemas de direccionamiento dinámico a la vez.

Cuando desarrollemos en detalle este protocolo, podremos comprender las diferentes opciones que ofrece, tanto en lo relacionado a "Autoconfiguración" de direcciones, como al nuevo concepto que propone llamado "Con y sin control de estados" que en definitiva permite que las configuraciones dinámicas puedan ser ofrecidas tanto por servidores DHCP, como por los mismos routers de red, sin llevar estos últimos un control de las direcciones asignadas (por eso viene lo de control de estados, o no).

La actividad de DHCPv6 guarda estrecha relación con el nuevo protocolo mencionado anteriormente "ND", y entre ambos ofrecen toda una gama de posibilidades anteriormente inexistentes con IPv4 que permiten solicitudes, respuestas y advertencias (información) de rutas, vecinos, parámetros, servicios, servidores, opciones de vendedores/fabricantes, etc.

El diálogo a través del protocolo DHCP, como hemos mencionado ofrece los dos nuevos puertos UDP y se realiza por medio de mensajes similares a la versión 4 (con la salvedad que ahora no existe el "Broadcast" por lo tanto este diálogo es bastante más dirigido) del tipo Solicitud/petición/respuestas/información todos ellos se identifican empleando el primer octeto de su encabezado. Hay que destacar que ahora aparecen dos tipos de solicitudes: "Solicit" y "Request" habrá que ponerse de acuerdo, como lo llamaremos en castellano: mi propuesta será "Solicitud" y "Petición". También tenemos mensajes de advertencia, confirmación, renegociación, re-enlace, liberación, rechazo, reconfiguración, solicitud de información, encaminamiento, relevo. Todos estos los desarrollaremos con máximo detalle en artículos posteriores.

Las RFCs que hacen referencia a este nuevo protocolo son las que figuran a continuación:

Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)	3315	Proposed Standard (PS)
---	----------------------	------------------------





Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers	3319	Proposed Standard (PS)
Ipv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) versión 6	3633	Proposed Standard (PS)
DNS Configuration options for Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)	3646	Proposed Standard (PS)
Stateless Dynamic Host Configuration Protocol (DHCP) Service for Ipv6	3736	Proposed Standard (PS)
Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)	3898	Proposed Standard (PS)
Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for Ipv6 (DHCPv6) T	4076	Informational
Information Refresh Time Option for Dynamic Host Configuration Protocol for Ipv6 (DHCPv6)	4242	Proposed Standard (PS)
Dynamic Host Configuration Protocol for Ipv6 (DHCPv6) Relay Agent Subscriber-ID Option	4580	Proposed Standard (PS)
Dynamic Host Configuration Protocol for Ipv6 (DHCPv6) Relay Agent Remote-ID Option	4649	Proposed Standard (PS)
The Dynamic Host Configuration Protocol for Ipv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option	4704	Proposed Standard (PS)
Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information	4776	Proposed Standard (PS)
DHCPv6 Relay Agent Echo Request Option	4994	Proposed Standard (PS)
DHCPv6 Leasequery	5007	Proposed Standard (PS)
DHCPv6 Bulk Leasequery	5460	Proposed Standard (PS)
Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery	5678	Proposed Standard (PS)
DHCPv6 Options for Network Boot	5970	Proposed Standard (PS)
DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery	6153	Proposed Standard (PS)
Lightweight DHCPv6 Relay Agent	6221	Proposed Standard (PS)
DHCPv6 Prefix Delegation for Network Mobility (NEMO)	6276	Proposed Standard (PS)
Dynamic Host Configuration Protocol for Ipv6 (DHCPv6) Option for Dual-Stack Lite	6334	Proposed Standard (PS)
Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)	6355	Proposed Standard (PS)
The EAP Re-authentication Protocol (ERP) Local Domain Name DHCPv6 Option	6440	Proposed Standard (PS)
Prefix Exclude Option for DHCPv6-based Prefix Delegation	6603	Proposed Standard (PS)
Virtual Subnet Selection Options for DHCPv4 and DHCPv6	6607	Proposed Standard (PS)
DHCP Options for Home Information Discovery in Mobile Ipv6 (MIPv6)	6610	Proposed Standard (PS)
Rebind Capability in DHCPv6 Reconfigure Messages	6644	Proposed Standard (PS)



DHCPv6 Redundancy Deployment Considerations	6853	Best Current Practice (BCP)
---	----------------------	-----------------------------

f. Relacionado a su nuevo rol de responsable de la determinación MTU.

Como hemos comentado al principio esta actividad que con IPv4 era responsabilidad del nivel de transporte, ahora recae en IPv6.

Se desarrolla con todo detalle en la RFC que mencionamos aquí debajo.

Path MTU Discovery for IP version 6	1981	Internet Standard (STD)
-------------------------------------	----------------------	-------------------------

Hemos querido hacer una breve referencia de la misma en este punto pues implica un cambio importante para este nuevo modelo. El funcionamiento se realiza aprovechando un nuevo "Tipo" del protocolo ICMPv6 que es el tipo "2" combinado con el código "0", a continuación presentamos este encabezado tal cual lo propone la RFC 1981 en el punto: 3.2. "**Packet Too Big Message**".

```
Type 2
Code Set to 0 (zero) by the originator and ignored by the receiver.
MTU The Maximum Transmission Unit of the next-hop link.
```

Como se puede apreciar el valor importante que viaja aquí es justamente el de MTU que es la máxima unidad de información que podrá soportar en el próximo salto.

El encabezado de este tipo es el que figura a continuación:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Code      |      Checksum      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     MTU                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Por medio de este mensaje, la lógica de funcionamiento de IPv6, permite ir controlando el tamaño máximo de paquetes que entregará al nivel de enlace, manteniendo un control periódico tanto para evaluar si puede aumentarlos como si debe disminuirlos. Todo este detalle, también se desarrollará en artículos posteriores.

g. Autenticación/Control de acceso/Trazabilidad

El punto más robusto para este tema pasa por su nativo diseño sobre IPsec, que es el punto siguiente, pero tengamos en cuenta que existen protocolos de Autenticación/control de acceso/trazabilidad, que pueden interactuar entre la dirección IP de usuario, su nombre y las direcciones IP destino a las cuáles podrá o no acceder, por lo tanto, si este esquema de direccionamiento cambia, entonces necesariamente debe actualizarse su funcionamiento para poder mantener esta lógica con la máxima granularidad, es decir pudiendo segmentar perfectamente desde dónde se permite o no, a quién y hacia que direcciones IP, segmentos de red, grupos de dispositivos, servidores, servicios, aplicaciones, etc.





Todas estas nuevas características aplican a los siguientes protocolos y se definen en las RFC que figuran a continuación:

RADIUS and IPv6	3162	Proposed Standard (PS)
RADIUS Authentication Client MIB for IPv6	4668	Proposed Standard (PS)
RADIUS Authentication Server MIB for IPv6	4669	Proposed Standard (PS)
RADIUS Delegated-IPv6-Prefix Attribute	4818	Proposed Standard (PS)
RADIUS Support for Proxy Mobile IPv6	6572	Proposed Standard (PS)
Kerberos Options for DHCPv6	6784	Proposed Standard (PS)
Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction	5447	Proposed Standard (PS)
Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction	5778	Proposed Standard (PS)
Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server	5779	Proposed Standard (PS)

h. IPSec/túneles.

El tema IPSec es uno de los aspectos sobre los que más centraremos la atención en esta serie de artículos, pues justamente, desde el punto de vista de seguridad (que es lo que nos interesa) implica una nueva lógica de funcionamiento mucho más robusta. Sin desarrollar nada en esta primera presentación, sólo queremos dejar sembrada la semilla de su importancia, IPSec es un conjunto de normas que ofrece toda la gama de medidas necesarias para una verdadera comunicación segura de extremo a extremo, con certificados o sin ellos con clave pública y privada, con mecanismos sólidos de claves (ISAKMP e IKE), con un encabezado adicional para IP (AH) y con la posibilidad de criptografiar toda la información en el nivel superior a IP (ESP). La única reflexión que deseamos dejar pendiente es que a partir de ahora ¿qué rol ocuparán: toda la familias de TLS (SSL, https, sftp...)?, ¿SSH seguirá siendo necesario?.

Las RFCs que regulan esta familia son las siguientes:

Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	3776	Proposed Standard (PS)
Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	3898	Proposed Standard (PS)
Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	4877	Proposed Standard (PS)
IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)	5739 *	Experimental
Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6	5845 *	Proposed Standard (PS)
Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic	6054 *	Proposed Standard (PS)
Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels	6438 *	Proposed Standard (PS)

i. DNS (Domain Name System).





Todo el sistema de nombres de dominio se ve afectado, tanto en la resolución simple como en la inversa, se mantiene la misma lógica, pero ahora se está implantando este desafío a través de la convivencia de ambas versiones.

Las RFCs que lo regulan son las que figuran a continuación:

DNS Extensions to Support IPv6 Address Aggregation and Renumbering	2874	Historic
DNSSEC and IPv6 A6 aware server/resolver message size requirements	3226	Proposed Standard (PS)
Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)	3363	Informational
Nameservers for IPv4 and IPv6 Reverse Zones	5855	Best Current Practice (BCP)
IPv6 Router Advertisement Options for DNS Configuration	6106	Proposed Standard (PS)
DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	6147	Proposed Standard (PS)

j. NTP (Network Time Protocol)

La sincronización de tiempos es una actividad fundamental en los dispositivos de una red, a pesar que la experiencia nos demuestra que no se le suele dar importancia, la realidad es que a la hora de sufrir anomalías en una infraestructura, es increíble la cantidad de problemas que se presentan a la hora de analizarlos para obtener conclusiones o intentar restaurarlos, en particular cuando se debe hacer un análisis forense. Este será otro de los temas que le dedicaremos cierto espacio en nuestros artículos, pues una ventaja para montar una verdadera “jerarquía” (o estratos) de servidores de tiempo, es aprovechar el funcionamiento de DHCP. Desde el punto de vista de seguridad hay varias medidas que deben conocerse pues este también es un protocolo interesante para un intruso, por eso lo abordaremos con cierto detalle.

Las RFCs que lo describen son:

Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6	4075	Proposed Standard (PS)
Network Time Protocol (NTP) Server Option for DHCPv6	5908	Proposed Standard (PS)



4. Capturas de tráfico – ejemplos.

En esta sección presentaremos brevemente algunas capturas de tráfico relacionadas a los componentes que hemos descrito.

a. Neighbor Discovery

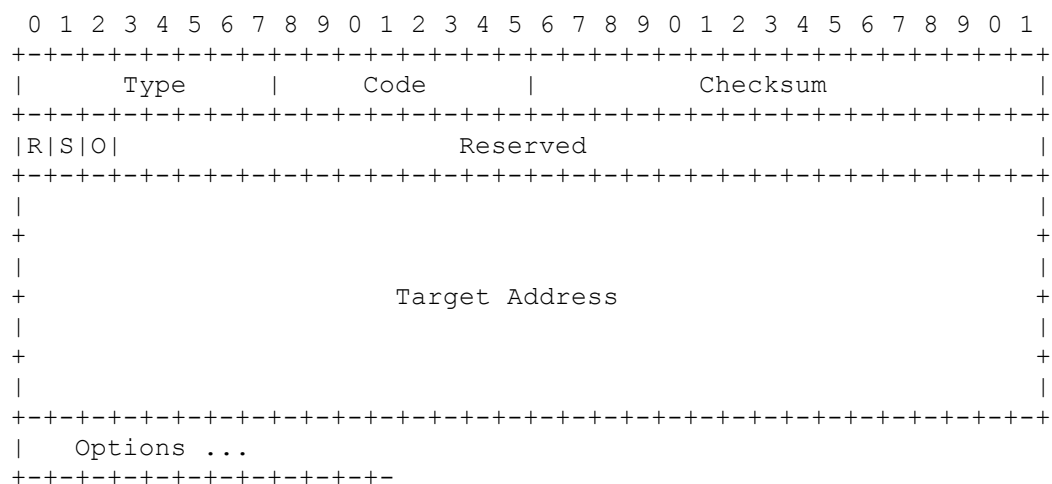
Como hemos mencionado, este es un nuevo protocolo que aparece con IPv6, trabaja en estrecha relación con ICMPv6, tanto es así que en la **RFC 4861** “Neighbor Discovery for IP version 6 (IPv6)” hace referencia a los nuevos “Tipos y códigos” de ICMPv6 que se definen para el funcionamiento de ND. En el punto “2.3. Addresses” de esta RFC nos menciona que “**Neighbor Discovery (ND)**” hace uso de un número de diferentes direcciones (definidas en [ADDR-ARCH]), que incluyen:

- ⊗ all-nodes multicast address (Las direcciones de ámbito local para alcanzar todos los nodos). Esta dirección es: **FF02::1**.

Más adelante describe que ND define cinco “Tipos” de paquetes: Solicitud de router – Advertencia de router – Solicitud de Neighbor (vecino) - Advertencia de vecino - mensaje de redirección

A Continuación presentamos un ejemplo de capturas justamente de este “Neighbor Advertisement” que la misma RFC lo describe como una respuesta a una “Solicitud de Neighbor” (que presentamos también como segunda imagen).

En el punto “4.4. Neighbor Advertisement Message Format” la misma RFC describe el formato de este mensaje:



No es intención de este primer artículo entrar en este tipo de detalles, sencillamente comenzar a presentar el trabajo y la metodología de confrontación entre el desarrollo teórico y la parte práctica, como en este caso las capturas de tráfico, por esa razón presentamos a continuación una captura de este tipo de mensaje:





```

13:54:04.650118 fe80::da9e:3fff:fe2b:ff02::1 2302 ICMPv6 86 Neighbor Advertisement
<-----
|> Frame 2302: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
|> Ethernet II, Src: d8:9e:3f:2b:1f:57 (d8:9e:3f:2b:1f:57), Dst: 33:33:00:00:00:01 (33:33:00:00:00:01)
|> Internet Protocol Version 6, Src: fe80::da9e:3fff:fe2b:1f57 (fe80::da9e:3fff:fe2b:1f57), Dst: ff02::1 (ff02::1)
|> Internet Control Message Protocol v6
|   Type: Neighbor Advertisement (136)
|   Code: 0
|   Checksum: 0xb23a [correct]
|   Flags: 0x20000000
|       0... .. = Router: Not set
|       .0... .. = Solicited: Not set
|       ..1... .. = Override: Set
|       ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
|   Target Address: fe80::da9e:3fff:fe2b:1f57 (fe80::da9e:3fff:fe2b:1f57)
|   < ICMPv6 Option (Target link-layer address : d8:9e:3f:2b:1f:57)
|       Type: Target link-layer address (2)
|       Length: 1 (8 bytes)
|       Link-layer address: d8:9e:3f:2b:1f:57 (d8:9e:3f:2b:1f:57)
|-----|-----
0000 33 33 00 00 00 01 d8 9e 3f 2b 1f 57 86 dd 60 00 33..... ?+.W..
0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 da 9e ... ..
0020 3f ff fe 2b 1f 57 ff 02 00 00 00 00 00 00 00 00 ?..+.W..
0030 00 00 00 00 00 01 38 00 b2 3a 20 00 00 00 fe 80 .....:.....
0040 00 00 00 00 00 00 da 9e 3f ff fe 2b 1f 57 02 01 .....?+.W..
0050 d8 9e 3f 2b 1f 57 .....?+.W..
    
```

En la imagen anterior, podemos ver los puntos que destacamos de la RFC:

- ⊗ La dirección IPv6 Multicast: ff02::1
- ⊗ El protocolo ICMPv6
- ⊗ El type ICMPv6: Neighbor Advertisement (tipo 136)
- ⊗ Todos los campos presentados en el punto 4.4 de la RFC (formato del mensaje): Tipo, código, checksum, R S O....

Para ampliar un poco más este protocolo, presentamos otra captura con el mensaje relacionado al formato anterior : Tipo 135 “Neighbor Solicitation”.

```

13:49:58.816862 fe80::f192:133b:668d:ff02::1:ff91:8092 301 ICMPv6 86 Neighbor Solicitation for f
<-----
|> Frame 301: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
|> Ethernet II, Src: 20:68:9d:09:70:75 (20:68:9d:09:70:75), Dst: 33:33:ff:91:80:92 (33:33:ff:91:80:92)
|> Internet Protocol Version 6, Src: fe80::f192:133b:668d:d632 (fe80::f192:133b:668d:d632), Dst: ff02::1:ff91:8092 (ff02::1:ff91:8092)
|> Internet Control Message Protocol v6
|   Type: Neighbor Solicitation (135)
|   Code: 0
|   Checksum: 0x65ce [correct]
|   Reserved: 00000000
|   Target Address: fe80::21f:a4ff:fe91:8092 (fe80::21f:a4ff:fe91:8092)
|   < ICMPv6 Option (Source link-layer address : 20:68:9d:09:70:75)
|       Type: Source link-layer address (1)
|       Length: 1 (8 bytes)
|       Link-layer address: 20:68:9d:09:70:75 (20:68:9d:09:70:75)
|-----|-----
0000 33 33 ff 91 80 92 20 68 9d 09 70 75 86 dd 60 00 33.... h..pu..
0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 00 f1 92 ... ..
0020 13 3b 66 80 d6 32 ff 02 00 00 00 00 00 00 00 00 ;f.2... ..
0030 00 01 ff 91 80 92 37 00 65 ce 00 00 00 00 fe 80 .....e.....
0040 00 00 00 00 00 00 02 1f a4 ff fe 91 80 92 01 01 .....
0050 20 68 9d 09 70 75 .....h..pu..
    
```





Si alguien tiene intención de profundizar aún más sobre ND, dejamos a continuación un par de capturas, esta vez relacionadas a mensajes de router (Tipo 133 y 134):

```
12:36:19.881914 fe80::f66d:e2ff:feb2:ff02::2 1450 ICMPv6 70 Router Solicitation from f4:6d:e2:b2:0e:43
.....
┆ Frame 1450: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
┆ Ethernet II, Src: f4:6d:e2:b2:0e:43 (f4:6d:e2:b2:0e:43), Dst: 33:33:00:00:00:02 (33:33:00:00:00:02)
┆ Internet Protocol Version 6, Src: fe80::f66d:e2ff:feb2:e43 (fe80::f66d:e2ff:feb2:e43), Dst: ff02::2 (ff02::2)
┆ Internet Control Message Protocol v6
  Type: Router Solicitation (133)
  Code: 0
  Checksum: 0xb066 [correct]
  Reserved: 00000000
  ▾ ICMPv6 Option (Source link-layer address : f4:6d:e2:b2:0e:43)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: f4:6d:e2:b2:0e:43 (f4:6d:e2:b2:0e:43)

0000 33 33 00 00 00 02 f4 6d e2 b2 0e 43 86 dd 60 00 33.....m...C...
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 00 00 f6 6d .....m
0020 e2 ff fe b2 0e 43 ff 02 00 00 00 00 00 00 00 00 .....C.....
0030 00 00 00 00 00 02 85 00 60 66 00 00 00 00 01 01 .....f.....
0040 f4 6d e2 b2 0e 43 .....m...C
```

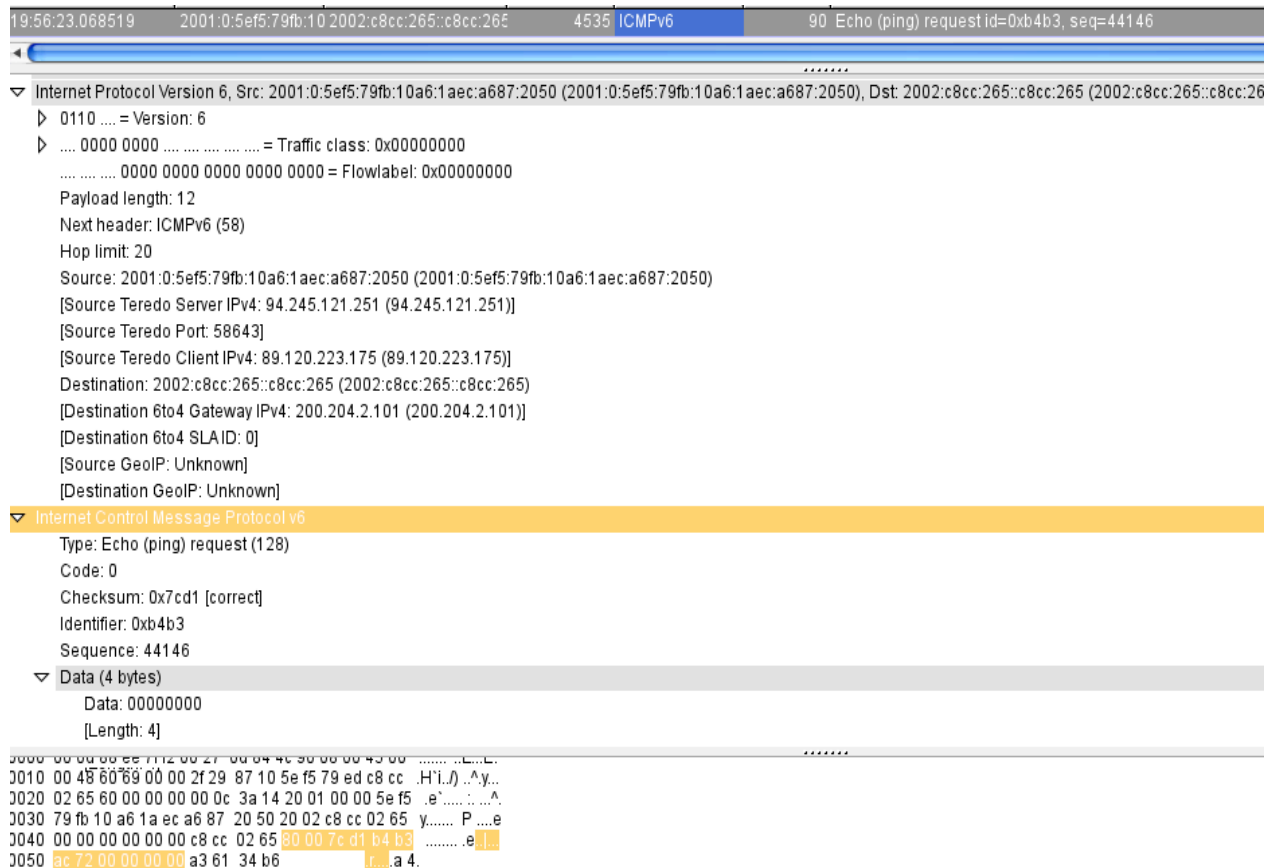
```
12:31:50.382093 fe80::21f:a4ff:fe91:ff02::1 6 ICMPv6 78 Router Advertisement
.....
┆ Frame 6: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
┆ Ethernet II, Src: 00:1f:a4:91:80:92 (00:1f:a4:91:80:92), Dst: 33:33:00:00:00:01 (33:33:00:00:00:01)
┆ Internet Protocol Version 6, Src: fe80::21f:a4ff:fe91:8092 (fe80::21f:a4ff:fe91:8092), Dst: ff02::1 (ff02::1)
┆ Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xeeaa [correct]
  Cur hop limit: 64
  ▾ Flags: 0xd8
    1... .. = Managed address configuration: Set
    .1.. .. = Other configuration: Set
    ..0. .... = Home Agent: Not set
    ...1 1... = Prf (Default Router Preference): Low (3)
    ....0.. = Proxy: Not set
    ....0. = Reserved: 0
  Router lifetime (s): 30
  Reachable time (ms): 0
  Retrans timer (ms): 0
  ▾ ICMPv6 Option (Source link-layer address : 00:1f:a4:91:80:92)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: 00:1f:a4:91:80:92 (00:1f:a4:91:80:92)

0000 33 33 00 00 00 01 00 1f a4 91 80 92 86 dd 60 00 33.....
0010 00 00 00 18 3a ff fe 80 00 00 00 00 00 00 02 1f .....
0020 a4 ff fe 91 80 92 ff 02 00 00 00 00 00 00 00 00 .....
0030 00 00 00 00 00 01 36 00 ee aa 40 d8 00 1e 00 00 .....@.....
0040 00 00 00 00 00 00 01 01 00 1f a4 91 80 92 .....m...C
```



b. ICMPv6

Para cerrar un poco más el punto anterior, presentamos algunas capturas también de ICMPv6. En la siguiente imagen podemos apreciar una trama típica de ICMP como es la solicitud de eco (comando PING), que opera exactamente igual que la versión previa, pero esta vez sobre ICMPv6:



```

19:56:23.068519 2001:0:5ef5:79fb:10:2002:c8cc:265::c8cc:265 4535 ICMPv6 90 Echo (ping) request id=0xb4b3, seq=44146
-----
Internet Protocol Version 6, Src: 2001:0:5ef5:79fb:10a6:1aec:a687:2050 (2001:0:5ef5:79fb:10a6:1aec:a687:2050), Dst: 2002:c8cc:265::c8cc:265 (2002:c8cc:265::c8cc:265)
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic class: 0x00000000
  .... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 12
  Next header: ICMPv6 (58)
  Hop limit: 20
  Source: 2001:0:5ef5:79fb:10a6:1aec:a687:2050 (2001:0:5ef5:79fb:10a6:1aec:a687:2050)
  [Source Teredo Server IPv4: 94.245.121.251 (94.245.121.251)]
  [Source Teredo Port: 58643]
  [Source Teredo Client IPv4: 89.120.223.175 (89.120.223.175)]
  Destination: 2002:c8cc:265::c8cc:265 (2002:c8cc:265::c8cc:265)
  [Destination 6to4 Gateway IPv4: 200.204.2.101 (200.204.2.101)]
  [Destination 6to4 SLAID: 0]
  [Source GeolIP: Unknown]
  [Destination GeolIP: Unknown]
Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0x7cd1 [correct]
  Identifier: 0xb4b3
  Sequence: 44146
  Data (4 bytes)
    Data: 00000000
    [Length: 4]
0000 00 00 00 00 e2 71 2 00 2f 00 04 4c 30 00 00 43 00 .....L...
0010 00 48 60 60 00 00 2f 29 87 10 5e f5 79 ed c8 cc .H'i..) .Ay...
0020 02 65 60 00 00 00 00 0c 3a 14 20 01 00 00 5e f5 .e.....A
0030 79 fb 10 a6 1a ec a6 87 20 50 20 02 c8 cc 02 65 y..... P...e
0040 00 00 00 00 00 00 c8 cc 02 65 80 00 7c d1 b4 b3 .....e..
0050 ac 72 00 00 00 00 a3 61 34 b6 .....a 4.
    
```

Como podemos ver en la imagen anterior, el protocolo ICMP mantiene su formato original, este vez sobre IPv6 y con la salvedad de este nuevo “**Tipo: 128**” para la solicitud, que en ICMPv4 es el tipo: 8. Reiteramos que estos nuevos valores son definidos para mantener la convivencia entre ambas versiones y que no se solapen.

c. Nivel de enlace:

En la próxima captura presentamos como trabaja el nivel de enlace, en esta caso una trama Ethernet, la cual, como hemos mencionado en el desarrollo no sufre ningún tipo de cambios, excepto la asignación de nuevos valores para el campo “Ethertype” que tal cual podemos apreciar responde al valor “**86**” que hemos destacado en color naranja, y por este solo aspecto es que deseábamos incorporar esta captura.



18:43:06.738545 fe80::108:3030:af6:ff02::1:3 67 LLMNR 84 Standard query 0x9813 A wpa

Frame 67: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)

Ethernet II, Src: 00:23:24:12:f8:0d (00:23:24:12:f8:0d), Dst: 33:33:00:01:00:03 (33:33:00:01:00:03)

- Destination: 33:33:00:01:00:03 (33:33:00:01:00:03)
Address: 33:33:00:01:00:03 (33:33:00:01:00:03)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
- Source: 00:23:24:12:f8:0d (00:23:24:12:f8:0d)
Address: 00:23:24:12:f8:0d (00:23:24:12:f8:0d)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)

Type: IPv6 (0x86dd)

Internet Protocol Version 6, Src: fe80::108:3030:af65:1cb5 (fe80::108:3030:af65:1cb5), Dst: ff02::1:3 (ff02::1:3)

0000 33 33 00 01 00 03 00 23 24 12 f8 0d 86 dd 60 00 33.....#\$....

d. DNSv6

Presentamos una solicitud y una respuesta DNS, en la segunda de ellas hemos dejado visibles los campos de UDP donde nos muestra el valor 5353 como protocolo de nivel superior, lo que abre el acceso a DNSv6. Este protocolo requerirá varias páginas en artículos posteriores.

18:39:53.823900 fe80::3e07:54ff:fe6c:ff02::fb 24 MDNS 233 Standard query

Domain Name System (query)

Transaction ID: 0x0000

Flags: 0x0000 Standard query

- 0... = Response: Message is a query
- .000 0... = Opcode: Standard query (0)
-0..... = Truncated: Message is not truncated
-0..... = Recursion desired: Don't do query recursively
-0..... = Z: reserved (0)
-0..... = Non-authenticated data: Unacceptable

Questions: 11
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries

- _afpovertcp._tcp.local: type PTR, class IN, "QM" question
Name: _afpovertcp._tcp.local
Type: PTR (Domain name pointer)
.000 0000 0000 0001 = Class: IN (0x0001)
0... = "QU" question: False
- _smb._tcp.local: type PTR, class IN, "QM" question
Name: _smb._tcp.local
Type: PTR (Domain name pointer)
.000 0000 0000 0001 = Class: IN (0x0001)
0... = "QU" question: False
- _rfb._tcp.local: type PTR, class IN, "QM" question
Name: _rfb._tcp.local
Type: PTR (Domain name pointer)
.000 0000 0000 0001 = Class: IN (0x0001)
0... = "QU" question: False
- _adisk._tcp.local: type PTR, class IN, "QM" question
Name: _adisk._tcp.local
Type: PTR (Domain name pointer)





```

13:54:07.999732 fe80::da9e:3fff:fe2b:fd2::fb 2447 MDNS 266 Standard query response 0x0000 PTR, cache flush David.local AA
User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)
Domain Name System (response)
  [Request In: 4200]
  [Time: -152.542068000 seconds]
  Transaction ID: 0x0000
  Flags: 0x8400 Standard query response, No error
    1..... = Response: Message is a response
    .000 0..... = Opcode: Standard query (0)
    .....1..... = Authoritative: Server is an authority for domain
    .....0..... = Truncated: Message is not truncated
    .....0..... = Recursion desired: Don't do query recursively
    .....0..... = Recursion available: Server can't do recursive queries
    .....0..... = Z: reserved (0)
    .....0..... = Answer authenticated: Answer/authority portion was not authenticated by the server
    .....0..... = Non-authenticated data: Unacceptable
    .....0000 = Reply code: No error (0)
  Questions: 0
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 3
  Answers
    7.5.F.1.B.2.E.F.F.F.F.3.E.9.A.D.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.ip6.arpa: type PTR, class IN, cache flush, David.local
    Name: 7.5.F.1.B.2.E.F.F.F.F.3.E.9.A.D.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.ip6.arpa
    Type: PTR (Domain name pointer)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1..... = Cache flush: True
    Time to live: 2 minutes
    Data length: 13
  
```

e. DHCPv6

Las próximas dos capturas son del protocolos DHCPv6, en la primera hemos dejado la imagen del nivel de transporte para que se puedan ver esos nuevos valores (546 y 547) que se definieron para el acceso a DHCPv6 y poder mantener el 67 y 68 para la versión 4 tal cal mencionamos en el desarrollo.

```

13:54:35.631508 fe80::da9e:3fff:fe2b:fd2::1:2 2632 DHCPv6 98 Information-reqe
Internet Protocol Version 6, Src: fe80::da9e:3fff:fe2b:1f57 (fe80::da9e:3fff:fe2b:1f57), Dst: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
DHCPv6
  Message type: Information-request (11)
  Transaction ID: 0x37bfdc
  Client Identifier: 0001000118e5a71fd89e3f2b1f57
    Option: Client Identifier (1)
      Length: 14
      Value: 0001000118e5a71fd89e3f2b1f57
      DUID type: link-layer address plus time (1)
      Hardware type: Ethernet (1)
      Time: Mar 27, 2013 13:48:31 CET
      Link-layer address: d8:9e:3f:2b:1f:57
  Option Request
    Option: Option Request (6)
      Length: 4
      Value: 00170018
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Domain Search List (24)
  Elapsed time
    Option: Elapsed time (8)
      Length: 2
      Value: 0000
      elapsed-time: 0 ms
  
```

```

3030 00 00 00 01 00 02 02 22 02 23 00 2c 03 1c 0b 37 .....".#...7
3040 bf dc 00 01 00 0e 00 01 00 01 18 e5 a7 1f d8 9e .....
3050 3f 2b 1f 57 00 06 00 04 00 17 00 18 00 08 00 02 ?+.W.....
3060 00 00
  
```





18:39:44.843703 fe80::a8fc:9d55:e8a:f02::1:2 7 DHCPv6 166 Soli

▼ DHCPv6

- Message type: Solicit (1)
- Transaction ID: 0x674e6d
- ▼ Elapsed time
 - Option: Elapsed time (8)
 - Length: 2
 - Value: 05dc
 - elapsed-time: 15000 ms
- ▼ Client Identifier: 000100011617c8f0001a6b5e186c
 - Option: Client Identifier (1)
 - Length: 14
 - Value: 000100011617c8f0001a6b5e186c
 - DUID type: link-layer address plus time (1)
 - Hardware type: Ethernet (1)
 - Time: Sep 30, 2011 02:25:20 CEST
 - Link-layer address: 00:1a:6b:5e:18:6c
- ▼ Identity Association for Non-temporary Address
 - Option: Identity Association for Non-temporary Address (3)
 - Length: 12
 - Value: 0e001a6b0000000000000000
 - IAID: 0e001a6b
 - T1: 0
 - T2: 0
- ▼ Fully Qualified Domain Name
 - Option: Fully Qualified Domain Name (39)
 - Length: 26
 - Value: 000c49424d3932303030303832353004746d7665056c6f6361...
0000 0... = Reserved: 0x00
....0.. = N bit: Server should perform DNS updates
....0. = O bit: Server has not overridden client's S bit preference
....0 = S bit: Server should not perform forward DNS updates
Domain: IBM920008250.tmve.local

f. http (Hiper Text Transfer Protocol)

Si bien sobre este protocolo no existen cambios, nuevamente encontramos “ciertos aspectos” que guardan relación con IPv6, como por ejemplo una URI para poder llamar una dirección IPv6 a través de http, y este es el aspecto que quisimos destacar en esta captura. Prestad atención a que en el campo “Location”, se está llamando una dirección IPv6, que tal cual está definido al invocar la versión 6, su dirección debe quedar entre “[“]”, en esta captura http://[fe80::9d1.....]:2869/.....





```
17:58:38.566076 fe80::9d1a:9e27:a3ff02::c 10 SSDP 506 NOTIFY * HTTP/1.1
<
▶ Frame 10: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits)
▶ Ethernet II, Src: 00:1a:6b:5e:0d:71 (00:1a:6b:5e:0d:71), Dst: 33:33:00:00:00:0c (33:33:00:00:00:0c)
▶ Internet Protocol Version 6, Src: fe80::9d1a:9e27:a3df:d6c9 (fe80::9d1a:9e27:a3df:d6c9), Dst: ff02::c (ff02::c)
▶ User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
▼ Hypertext Transfer Protocol
  ▶ NOTIFY * HTTP/1.1\r\n
    Host:[FF02::C]:1900\r\n
    NT:upnp:rootdevice\r\n
    NTS:ssdp:alive\r\n
    Location:http://[fe80::9d1a:9e27:a3df:d6c9]:2869/upnpghost/udhisapi.dll?content=uuid:9eeb3fa1-24eb-4f12-aa00-45ff9c8f2900\r\n
    USN:uuid:9eeb3fa1-24eb-4f12-aa00-45ff9c8f2900::upnp:rootdevice\r\n
    Cache-Control:max-age=1800\r\n
    Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
    OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n
    01-NLS:5266dbd90602c574dbea94619017dfcd\r\n
    \r\n
    [Full request URI: http://[FF02::C]:1900*]
```

