ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA

“ESTUDIO DE SEGURIDADES EN UNA RED EXTREMO A EXTREMO, BASADA EN PROTOCOLO IPV6.”.

TESIS DE GRADO

PREVIA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN.

PRESENTADO POR:

GUSTAVO ENRIQUE SÁNCHEZ CHÁVEZ

RIOBAMBA - ECUADOR

2012

Agradezco a Dios, por darme la oportunidad de estudiar
y la gracia de aprovechar; a mis padres y familia,
por el apoyo incondicional; a mis tutores,
a quienes los considero pilar principal
de la EIE-TC y agradezco a mis
amigos, por sus valiosas
palabras de aliento.

El camino ha sido largo, la compañía continua por esto y
mucho más este trabajo lo dedico a mi familia.
A mis padres incansables e incondicionales
pilares de mi vida y a mis hermanos,
que son mi gran fortaleza
y fiel compañía.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO DE LA FACULTAD** **DE INFORMÁTICA Y** **ELECTRÓNICA**	……	……
Ing. Pedro Infante **DIRECTOR DE LA** **ESCUELA DE INGENIERÍA** **ELECTRÓNICA Y** **TECNOLOGÍA EN** **COMPUTACIÓN.**	……	……
Ing. Alberto Arellano **DIRECTOR DE TESIS**	……	……
Ing. Daniel Aro **MIEMBRO DEL TRIBUNAL**	……	……
Tlgo. Carlos Rodríguez **DIRECTOR DPTO.** **DOCUMENTACIÓN**	……	……
NOTA DE LA TESIS	……	

"Yo, **GUSTAVO ENRIQUE SÁNCHEZ CHÁVEZ**, soy el responsable de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado, y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo"

_____

Gustavo Enrique Sánchez

ÍNDICE GENERAL

CAPITULO III

3. SEGURIDADES IPV6

CAPITULO IV

4. COMPARACIÓN DE AMENAZAS PARA IPV4 E IPV6

CAPITULO V

5. FASE DE PRUEBAS

ÍNDICE DE ABREVIATURAS

ANSNET	Advanced Networks and Services
APNIC	Asia-Pacific Network Information Centre Network
ARPANET	Advanced Research Proyects Agency Net
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DOI	Domain of Interpretation
DoS	Denial of Service
GNU	General Public License
IANA	Internet Assigned Numbers Authority
IAPD	Identity Association for Prefix Delegation
IDEA	International Data Encryption Algorithm
IDS	Instrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	Abreviatura de Internet Protocol security
ISAKMP	Internet Security Association and Key Management Protocol
MTU	Maximum Transfer Unit
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NRO	Organización de recursos numéricos
NSF	National Science Fundation
NTP	Network Time Protocol

OpenVAS	Open Vulnerability Assessment System
OSI	Open System Interconnection
OSSIM	Open Source Security Information Management
PGP	Pretty Good Privacy
PMTUD	Path maximum transmission unit discovery
RIR	Regional Internet Registry
SA	Security associations
SAD	Security Association Database
SADB	Security Association Database
SPD	Security Policy Database
SPI	Security parameters index
UDP	User Datagram Protocol
VPN	Virtual Private Networks

ÍNDICE DE FIGURAS

CAPITULO IV

CAPITULO V

ÍNDICE DE TABLAS

INTRODUCCIÓN

Dado que las redes de computadores se han introducido en todos los ámbitos de nuestras vidas y debido a su imparable crecimiento, la versión 4 del protocolo de Internet (Ipv4) se está quedando obsoleta. Por ello, el IETF (Internet Engineering Task Forcé, organización encargada de la evolución de la arquitectura en la Red) ha diseñado una nueva interpretación, denominada IPv6 (Internet Protocolo versión 6). Este nuevo modelo se erigirá como sucesor de la versión 4 puesto que resuelve sus deficiencias y aporta nuevas funciones acordes a la evolución actual de la red.

Dada que la migración al protocolo IPv6 parece ser inevitable, resulta de gran importancia el entender este protocolo, sus ventajas y desventajas al momento de implementarlo, así como las soluciones que presenta en especial a problemas de seguridad, por lo que es primordial crear una sólida base de conocimiento y evitar así las respuestas caóticas que han caracterizado en muchos casos a las soluciones dadas a los problemas que se han presentado en IPV4, con el objetivo de garantizar una información más segura, con un protocolo que se presenta como virtualmente invulnerable.

Se ha hecho un estudio de las principales características de IPv6 tanto en sus aspectos más generales como en su arquitectura pero en especial en el funcionamiento de IPsec como base de su seguridad. Con el objetivo de realizar un análisis comparativo entre las dos versiones del protocolo IP en primer término se analizó las diferentes amenazas a las que está expuesta una red, sus consideraciones tanto en IPv4 como en IPv6, las capacidades de la tecnología actual y la recomendación de las mejores prácticas de seguridad y en segundo término se montó un escenario de pruebas donde usando herramientas de auditoría informática, se hizo ataques de reconocimiento, sniffing, y hombre en el medio.

Como resultado de este estudio se pudo conocer aspectos importantes como la aplicación de políticas de seguridad, herramientas de auditoría informática, complejidad, información disponible, tendencias, facilidades, configuraciones, limitaciones entre otros, los cuales son indispensables a la hora de decidir si migrar una red a IPv6 y en caso de hacerlo las implicaciones que este proceso tendrá en el ámbito de la seguridad de la red.

CAPITULO I

PROTOCOLO IPV6

En este capítulo se hará un recorrido por las características generales de IPv6, los mecanismos de transición disponibles y la situación actual de asignación de direcciones IPv4 e IPv6.

1.1. Introducción

El espacio de direcciones de IPV4 se ha usado por años para el crecimiento de internet, cuando fue desarrollado en 1981 cuatro billones de direcciones IP parecían suficientes y virtualmente inagotables pero cuando el mundo descubrió las posibilidades comerciales que podría encontrar en la red, el número de direcciones IP simplemente no era suficiente para todas las laptops, dispositivos móviles, servidores web, ruteadores, y otros dispositivos con la perspectiva de entrar en línea. Como resultado se desarrolló IPV6, un nuevo protocolo que cubre esta carencia de direcciones e incorpora además muchas características mejoradas, es así que la primera asignación

de direcciones de espacio IPv6 hecha por el RIR (Registro Regional de Internet - Regional Internet Registry) a un proveedor de internet se realizó en abril de 1999, comenzando de esta manera una relativamente lenta transición a IPV6, mientras tanto mucho del contenido del Internet correrá IPV4 e IPV6 simultáneamente de tal manera que los usuarios tengan acceso a todos los contenidos, sin importar la versión del protocolo que se esté usando.

A agosto del 2010 ya se habian asignado el 80.87% de las direcciones de IPV4 y si tomamos en cuenta que hay un 13.67% que son direcciones no disponibles se tenía tan solo un 5.46% de disponibilidad, pero la NRO (Number Resource Organization - Organización de Recursos numéricos) creada en el 2003 para proteger el espacio de direcciones IP no asignadas, anunció el 3 de febrero del 2011 que las direcciones disponibles de IPV4 estaban ya completamente agotadas. El 31 de enero del 2011 la IANA (Agencia de Asignación de Números de Internet - Internet Assigned Numbers Authority) asignó dos bloques de espacios de direcciones IPV4 a la APNIC (Centro de Información de redes para Asia y la Región Pacífica - Asia-Pacific Network Information Centre Network), la RIR para Asia y la Región Pacífica, lo cual disparó una política global para asignar las direcciones restantes de la IANA de manera equitativa entre las cinco RIR, lo que significa que ya no existe una dirección IPV4 disponible para asignar a ninguna RIR.

Los Registros Regionales de Internet deben, desde ahora, manejarse con sus propias reservas, que se estima, alcanzaran hasta Septiembre de 2011. Bajo las actuales circunstancias adoptar IPV6 ya no es una opción, es un requisito que permitirá a Internet seguir su asombroso crecimiento fomentando la innovación global que ha tenido en la red un imprescindible aliado.

1.2. Historia IPv4 a IPv6

El Protocolo de Internet versión 4 (IPv4) es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala. Durante la primera década de operación de Internet basada en TCP/IP, a fines de los 80s, se hizo aparente que se necesitaba desarrollar métodos para conservar el espacio de direcciones.

IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPV4. A continuación se detalla las causas de este problema:

- **Dispositivos móviles**

  En el momento en que IPv4 se convirtió en el estándar de la comunicación mediante redes, el coste de integración de capacidades informáticas en dispositivos portátiles ha caído en picada. Como consecuencia, los antiguos dispositivos simples de masas tales como los teléfonos móviles se han convertido en posibles terminales de IPv4. A medida que se implanta al 100% el teléfono móvil a nivel mundial, el resultado es un escenario verosímil en el que cabe la posibilidad de que cada persona del planeta tenga asignada una dirección IP.

- **Conexiones Always-on**

  Durante la década de los 90, el modo predominante del consumidor de acceso a Internet era el telefónico dial-up. Este acceso reduce la presión en las direcciones IP porque los enlaces dial-up están normalmente desconectados y, por lo tanto, no se necesitan direcciones IP permanentes. Sin embargo, en 2007, el acceso de banda ancha superó el 50% de la penetración en el mercado. Las conexiones de banda ancha permanecen activas completamente e, incluso cuando tienen asignadas dinámicamente una dirección, necesitan de una IP continua.

- **Demografía de Internet**

  Existen millones de hogares en el mundo desarrollado. En 1990, únicamente una mínima parte tenía conectividad a Internet. Tan sólo 15 años más tarde, casi la mitad de estos hogares tenían conexiones de banda ancha.

- **Uso ineficiente de direcciones**

  A las organizaciones que obtuvieron direcciones IP en los años 80 se les asignaron muchas más direcciones de las que realmente necesitaban. Por ejemplo, a las grandes empresas y universidades se les dieron bloques de direcciones de clase A, con 16 millones de direcciones IPv4 cada uno. Muchas organizaciones siguen utilizando direcciones IP públicas para dispositivos que no son accesibles fuera de sus redes locales y que podrían servirse de la implementación basada en NAT, cediendo un alto rango de direcciones IP para su reasignación. Algunas de las antedichas organizaciones también poseen direcciones IP que, actualmente, no se

utilizan pero que no se han devuelto a las autoridades de asignación por varias razones.

A principios de los 90s, incluso después de la introducción del rediseño de redes sin clase, se hizo claro que no sería suficiente para prevenir el agotamiento de las direcciones IPv4 y que se necesitaban cambios adicionales. Entre los principales atenuantes que se han usado tenemos:

- NAT (Network Address Translation, traducción de direcciones de red): es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. Su uso más común es permitir utilizar direcciones privadas para acceder a Internet.
- Uso de redes privadas.
- DHCP (Dynamic Host Configuration Protocol, Protocolo para la configuración dinámica del terminal): es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.
- Hosting virtual basado en nombres: solo necesita configurar el servidor de DNS para que localice la dirección IP correcta y entonces configurar el servidor por ejemplo Apache para que reconozca los diferentes nombres de host reduciendo la demanda de direcciones IP.

- Control exhaustivo de registros de Internet regional en la asignación de direcciones a los registros locales.
- Reenumeración de redes para recuperar amplios bloques de espacio de direcciones asignados en los primeros días de Internet.
- Conservación: A la hora de concebir Internet, nunca se previó que se fueran a necesitar tantas direcciones IP como se demandan en la actualidad. Por lo tanto, se asignaban con frecuencia en bloques de direcciones de 255, 65.536 ó 16.777.216 direcciones para su uso. Hasta ahora, a varias organizaciones se les había asignado cerca de 16 millones de direcciones IP, de las que utilizaban relativamente pocas. Actualmente, las empresas responsables de asignar direcciones IP públicas son mucho más reticentes a proporcionar grupos de direcciones.
- Subredes: Son otro método de sacar un mayor provecho de las direcciones IP en general. Esto permite que el mismo número se utilice en múltiples ubicaciones con una mínima consideración extra.
- Reclamación de espacio IPV4 sin utilizar: En los primeros días de Internet, antes de la creación de las redes y las posteriores direcciones CIDR, se asignaron amplios bloques de direcciones IP a empresas individuales y organizaciones e incluso algunas que ya han desaparecido o que nunca las utilizaron. IANA podría reclamar estos rangos y volver a expedir las direcciones a otras personas. Sin embargo, puede suponer mucho tiempo y dinero volver a numerar una red y probablemente, muchas organizaciones se opondrían hasta el punto de emprender acciones legales y por otro lado supondría un gran esfuerzo realizar el seguimiento de qué direcciones no se utilizan. Además, la tasa actual de consumo de direcciones IP, incluso con una eventual recuperación de bloques infrausados, derivarían en retrasar tan sólo en uno o dos años la fecha de agotamiento de las direcciones IP.

- Uso de direcciones IP que, en la actualidad, están reservadas por IANA. Existen propuestas para reclamar las direcciones de red de la clase E, lamentablemente, muchos sistemas operativos y tipos de routers necesitarían ser modificados o actualizados para poder hacer uso de estas direcciones. Muchas pilas de TCP/IP de los sistemas operativos, entre los que se incluyen la de los ordenadores personales de Microsoft, no permiten el uso de las direcciones IP de clase E, lo que deriva en errores de configuración cuando se intenta asignar direcciones IP a un terminal y produce el rechazo de comunicación con aquellos terminales que utilizan tales direcciones. Las implementaciones de TCP/IP en muchos conmutadores y ruteadores también prohíben el uso de espacio de clase E. Por esta razón, la propuesta no busca volver a designar espacio de clase E para asignación pública, sino que pretende cambiar el estado del campo de clase E de “reservado” a “uso limitado para grandes redes de Internet privadas”. Esto podría permitir el uso de espacio de clase E en grandes redes privadas que necesitan más espacio de direcciones del que se dispone actualmente.
- NAT amplia de los proveedores de internet: Del mismo modo que las empresas utilizan la NAT para la mayoría de los ordenadores de sus empleados, los ISP pueden utilizar NAT para la mayoría de los clientes, en vez de proporcionarles direcciones IP asignadas dinámicamente mediante ruteadores públicos. Esto genera un ahorro a través de menores costes para el proveedor. Entre estos costes se incluyen la reducción drástica de la necesidad de direcciones IPv4, el bloqueo más sencillo de servidores no autorizados que se ejecutan en los ordenadores de los usuarios (por ejemplo, sistemas de intercambio de archivos), el empleo de proxies web para reducir el uso de banda ancha y la publicidad indeseada, control de qué servicios mejorados se permiten (tales como VoIP o juegos), beneficios de

los cortafuegos de los clientes, el cumplimiento de las leyes que tratan contenidos y localizadores, etc. Los proveedores permitirían a los clientes adquirir, con un coste adicional, direcciones IP estáticas.

Por otro lado, esto crea una carga para que el ISP pueda ejecutar los servicios NAT de modo que se cumpla con la ley. Muchos países cuentan con leyes muy estrictas que controlan el tráfico (ley de protección de datos) y el comportamiento de los usuarios. La implementación de cualquier servicio diferente a una NAT pura, incluso si sólo se trata de la prestación de registro de tráfico básico, podría situar al ISP en el límite de la legalidad. El ISP no pretende erigirse como la policía de internet ni tampoco tiene la autoridad para hacerlo. Su papel es el de transporte de paquetes de datos, al igual que las compañías de telecomunicaciones tradicionales realizan para las llamadas telefónicas. La implementación de una NAT amplia requeriría una cantidad considerable de asesoría legal para salvaguardar la actuación del proveedor. Por estos motivos la NAT amplia es difícil de llevar a la práctica.

- Mercados de direcciones IP: La creación de mercados para vender y comprar direcciones IPv4 se ha propuesto numerosas veces como un medio de asignación eficiente. El beneficio primario de un mercado de direcciones sería que las direcciones IPv4 seguirían estando disponibles, aunque el precio de mercado de las mismas siempre tendería a incrementarse con el tiempo. Estos esquemas tienen muchos inconvenientes que han evitado su implementación:

  - ✓ La creación de un mercado de direcciones IPv4 sólo retrasaría el agotamiento práctico del espacio de direcciones IPv4 en un tiempo relativamente corto, ya que el agotamiento total de espacio de IPv4

seguiría durante, como mucho, un par de años tras el fin de direcciones para nuevos asignaciones.

- ✓ El concepto de “propiedad” legal de direcciones IP entendido como bienes es cuestionable e incluso no está el sistema legal de qué país resolvería cualquier controversia.
- ✓ La administración de un esquema así sería incompatible con las prácticas actuales.
- ✓ El comercio de direcciones desembocaría en diseños de asignaciones que expandirían infinitamente la tabla de routing, lo que desembocaría en serios problemas de elección de rutas para muchas redes que aún utilizan routers antiguos como memoria FIB limitada o procesadores de poca potencia. Si los vendedores y compradores de direcciones IP aplicaran este coste tan amplio a todos los usuarios de Internet provocarían un factor externo negativo que dichos mercados tendrían que corregir.
- ✓ El comercio de direcciones IP en bloques suficientemente grandes para evitar problemas de fragmentación reduciría el número de bienes comercializables a alrededor de un millón.
- ✓ El coste de cambio de un juego de direcciones IP a otro es muy elevado, lo que reduce la liquidez del mercado. Las organizaciones que posiblemente podrían reorganizar el uso de sus direcciones IP para liberarlas de modo que se pudieran comercializar demandarían un precio alto y, una vez compradas, estas direcciones no se venderían hasta no sacar un beneficio alto. El coste de enumeración del espacio de direcciones IP de una organización es comparable al coste de cambiar a direcciones IPv6.
- ✓ Las direcciones IP son sólo números por lo que no hay ningún valor intrínseco en ellas. El comercio de bienes sin valor intrínseco (por

ejemplo, billetes) en lugar de bienes con valor intrínseco (monedas de oro) puede ser arriesgado y necesita un mercado estable. La creación de un mercado necesita tener asegurado un número de compradores y vendedores. Sin ellos, no existirá estabilidad de precios y sin estabilidad de precios es muy poco probable que las empresas apoyen la formación de este tipo de mercado.

A comienzos de 1992, circulaban varias propuestas de sistemas y a finales de ese mismo año, la IETF (*Internet Engineering Task Force* – Grupo Especial sobre Ingeniería de Internet) anunció el llamado para white papers (RFC 1550) y la creación de los grupos de trabajo de "IP de próxima generación" *("IP Next Generation")* o (IPng) ya que se predijo que el agotamiento de IPV4 se daría entre el 2010 y el 2017. IPng fue propuesto por el IETF el 25 de julio de 1994, con la formación de varios grupos de trabajo IPng. Hasta 1996, se publicaron varios RFCs definiendo IPv6, empezando con el RFC 2460.

La discusión técnica, el desarrollo e introducción de IPv6 no fue sin controversia. Incluso el diseño ha sido criticado por la falta de interoperabilidad con IPv4 y otros aspectos. Incidentalmente, IPng (Ping Pong) no pudo usar la versión número 5 (IPv5) como sucesor de IPv4, ya que ésta había sido asignada a un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio. Finalmente IPV6 se considera completamente testeado y disponible para producción desde 1999.

Actualmente no quedan direcciones IPv4 disponibles para compra, por ende se está en la forzosa y prioritaria obligación de migrar a IPv6, los sistemas operativos Windows Vista, 7, Unix/like (Gnu/linux, Unix, Mac OSX), BSD entre otros, tienen

soporte nato para IPv6, mientras que Windows XP requiere utilizar el prompt y digitar ipv6 install, para instalarlo, y sistemas anteriores no tienen soporte para este.

Se espera ampliamente que IPv6 sea soportado en conjunto con IPv4 en el futuro cercano. Los nodos solo-IPv4 no son capaces de comunicarse directamente con los nodos IPv6, y necesitarán ayuda de un intermediario. Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.

Mecanismos de transición a IPv6

Ante el agotamiento de las direcciones IPv4, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante 20 años y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. Actualmente existen alrededor de 20 mecanismos, los cuales de forma general pueden clasificarse en tres grupos:

- Doble pila
- Túneles
- Traducción

La **doble pila** hace referencia a una solución de nivel IP con doble pila, que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red.

Cada nodo con doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- **A favor**: Fácil de desplegar y extensamente soportado.
- **En contra**: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre proto-41. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

La traducción es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Este mecanismo de transición realiza una "traducción" similar a la que efectúa el NAT, donde es modificada la cabecera IPv4 a una cabecera IPv6. Se pueden dividir en dos grupos basados en si la información de estado está guardada o no:

- **Con estado**: NAT-PT (RFC 2766), TCP-UDP Relay (RFC 3142), Socks-based Gateway (RFC 3089)
- **Sin estado**: Bump-in-the-Stack, Bump-in-the-API (RFC_276)

1.3 La cabecera de IPV6

Para analizar el encabezado del protocolo de IPv6 es necesario también recordar el encabezado de su antecesor IPv4 porque ayudará a entender la evolución y las mejoras que ofrece IPv6.

La cabecera de IPv6, descrita principalmente en la RFC 2460, elimina o hace opcionales varios campos de la cabecera de IPv4, consiguiendo una cabecera de tamaño fijo y más simple, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6.

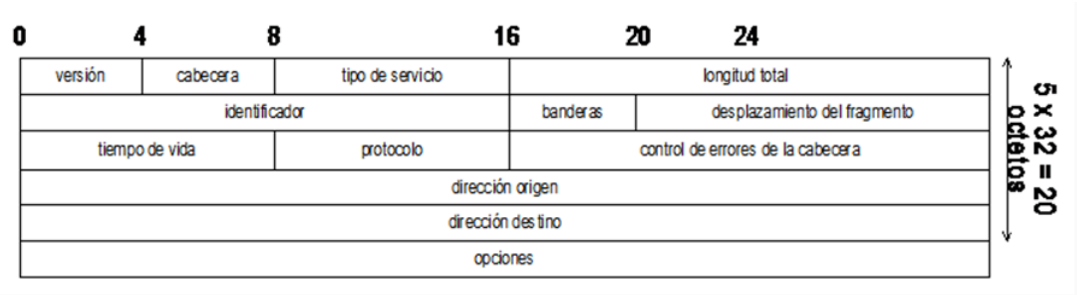


Figura 1.7: Cabecera IPv4

La cabecera de IPv4, mostrada en la Figura 1.7, tiene una longitud variable mínima de 20 octetos. El bit más significante se numera por 0 a la izquierda, y el menos significante se numera por 31 a la derecha. La forma de transmitir los diferentes bytes, sigue el orden conocido por big endian, es decir, de izquierda a derecha y de arriba abajo según la estructura presentada en la Figura 1.7. La cabecera consiste de los siguientes campos:

- Versión (4 bits): Es el número de versión de IP, es decir, 4.
- Cabecera (4 bits): Especifica la longitud total de la cabecera en palabras de 32 bits. El valor mínimo y más común es de 5, siendo la longitud de

cabecera mínima. Puesto que el campo es de 4 bits, se limita la longitud total de la cabecera a 60 bytes.

- Tipo de servicio (8 bits): Indica la calidad de servicio solicitada por el paquete IP. De los 8 bits, actualmente sólo se utilizan 4, que son: conseguir el retardo mínimo, maximizar caudal, maximizar la fiabilidad, y minimizar el coste monetario. Sólo uno de estos cuatro bits puede estar a 1. Su uso viene descrito en la RFC 1340 y RFC 1349.
- Longitud total (16 bits): Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes.
- Identificador (16 bits): Es un número único asignado por el dispositivo que envía el paquete, con el fin de que el destinatario pueda re ensamblar un paquete fragmentado por los nodos intermedios. La fragmentación es necesaria porque no todas las redes físicas tienen la misma longitud de trama máxima, por lo cual en muchos casos es necesario que los nodos intermedios dividan el datagrama en varios fragmentos. Cada uno de estos fragmentos podrá seguir rutas distintas al resto y, de perderse alguno de los fragmentos, el origen deberá retransmitir el paquete completo.
- Banderas (3 bits): Es un campo para el control de la fragmentación. El primer bit no es utilizado y está siempre puesto a 0. Si el segundo bit es 0, significa que puede haber fragmentación, y si es 1, significa que no puede haber fragmentación. Si el tercer bit es 0, indica que es el último fragmento, y si es 1, indica que aún hay más fragmentos.
- Desplazamiento del fragmento (13 bits): Es utilizado en los paquetes que han sido fragmentados, para posibilitar el re ensamblado total del paquete. Su valor indica el número de bloques de 8 bytes (sin contabilizar los bytes de la cabecera) que estaban contenidos en los fragmentos previos. En el primer fragmento, o en un único fragmento, este valor es siempre 0.

- Tiempo de vida (8 bits). Contiene el tiempo máximo que un paquete puede permanecer en una red. Cada dispositivo por el que pasa el paquete decrementa el valor de este campo en el tiempo que tarda en procesar la cabecera IP, siendo 1 el valor mínimo. Si el valor llega a 0, el paquete es descartado. Esto garantiza que los paquetes no viajan a través de una red haciendo bucles, incluso si las tablas de encaminamiento son erróneas.
- Protocolo (8 bits): Indica al protocolo de nivel superior al que IP deberá pasar los datos del paquete. Por ejemplo, UDP es 17 y TCP es 6.
- Control de errores de la cabecera (16 bits): Es un campo para controlar los errores únicamente en la cabecera IP, exceptuando este campo.
- Dirección origen (32 bits): Es la dirección del origen del paquete.
- Dirección destino (32 bits): Es la dirección del destino del paquete.
- Opciones (variable): No son requeridas en todos los paquetes.

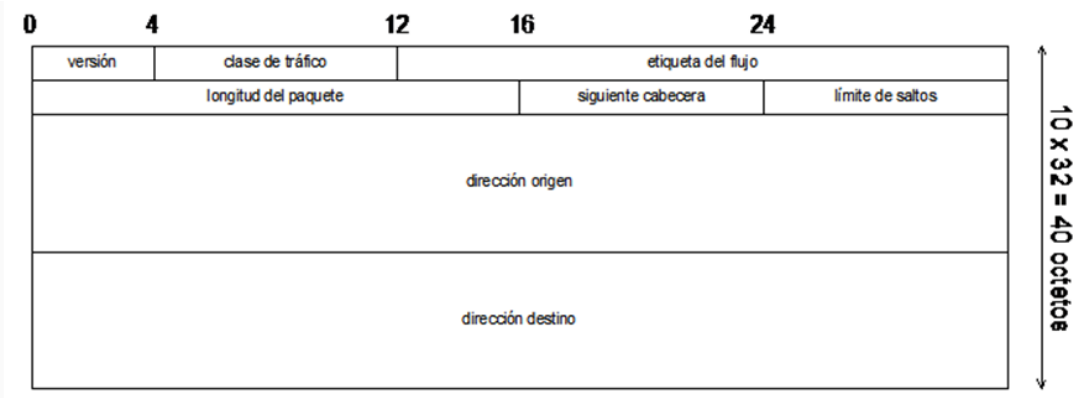


Figura 1.8: Cabecera de IPv6

La cabecera básica de IPv6, mostrada en la Figura 1.8, tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

- Versión (4 bits): Es el número de versión de IP, es decir, 6.

- Clase de tráfico (8 bits): El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de la congestión.
- Etiqueta del flujo (20 bits): El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino específico. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20 bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo. La utilización de esta etiqueta, que identifica un camino a lo largo de la red, posibilita encaminar conmutar en vez de encaminar. Su uso viene descrito en la RFC 1809.
- Longitud del paquete (16 bits): Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.
- Siguiente cabecera (8 bits): Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.
- Límite de saltos (8 bits): Es el número de saltos máximo que le quedan al paquete. El límite de saltos es establecido a un valor máximo por el origen y decrementado en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es decrementado y toma el valor 0, el paquete es descartado.
- Dirección origen (128 bits): Es la dirección del origen del paquete.
- Dirección destino (128 bits): Es la dirección del destino del paquete.

Como se puede observar, de los 12 campos de la cabecera de IPv4 se ha pasado a 8 campos en IPv6. El motivo fundamental por el que estos campos (tipo de

servicio, indicadores, identificación y control de errores) son eliminados, es la innecesaria redundancia; en IPv4 se está facilitando la misma información de diversas formas, como es el caso del campo de control de errores, pues otros mecanismos de encapsulado de capas inferiores, por ejemplo IEEE 802, ya realizan esta función. El campo de desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que se produce extremo a extremo. El único campo realmente nuevo en IPv6 es la etiqueta de flujo.

La información opcional a la estrictamente necesaria para encaminar los paquetes de datos, es codificada en cabeceras adicionales que pueden ubicarse entre la cabecera IPv6 y las cabeceras de niveles superiores, como por ejemplo la cabecera TCP/UDP. En la actualidad, hay un pequeño número de tales cabeceras de extensión (opciones de salto por salto, encaminamiento extendido, fragmentación y reensamblado, opciones del destino, autentificación, y encapsulación) estando cada una identificada por un valor distinto del valor del campo siguiente cabecera. Cada paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el valor del campo siguiente cabecera de la cabecera que la precede. Las cabeceras de extensión deben de ser procesadas en orden, ya que el contenido y semántica de cada una de ellas indican si se debe o no procesar la siguiente cabecera.

De esta forma, las cabeceras de extensión no son examinadas o procesadas por los nodos intermedios, sólo cuando lleguen al nodo que venga identificado por el campo de dirección de destino de la cabecera IPv6. La única excepción es la cabecera de opciones de salto por salto, que lleva información que debe ser procesada y examinada en todos los nodos por los que pasa el paquete, incluyendo

los nodos origen y destino. La cabecera de opciones de salto por salto, cuando esté presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia se indica por el valor 0 en el campo de siguiente cabecera de la cabecera IPv6.

Cada cabecera de extensión tiene una longitud múltiplo entero de 8 octetos, con el fin de mantener el alineamiento de 8 octetos en las cabeceras siguientes. La razón de que los distintos campos de la cabecera estén alineados a 64 bits, es que la nueva generación de procesadores, de 64 bits, puedan procesar dichos campos más eficientemente.

Resumiendo, las principales mejoras que ofrece la cabecera IPv6 son:

- Cabecera de tamaño fijo, de 40 bytes.
- Eliminación de campos redundantes en la cabecera, haciendo un total de 8.
- Cabeceras básicas y de extensión alineadas a un múltiplo entero de 64 bits.
- Procesamiento eficiente de las opciones, sólo en destino y cuando éstas se presentan.
- Fragmentación procesada en el origen y el destino de los paquetes, no en los routers.

1.4. Características y ventajas del protocolo IPv6

1.4.1. Gran espacio de direcciones

IPV6 incrementa el tamaño de la dirección IP de 32 a 128 bits, de este modo incrementa el número de direcciones enrutables globalmente de aproximadamente 4,300,000,000 a 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×1038). Incrementando el espacio de direcciones a 128 bits se tiene los siguientes beneficios adicionales:

- **Mayor funcionalidad de las aplicaciones:** Permite redes del tipo peer-to-peer (P2P) o redes punto a punto, que aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación.
- **Transparencia End-to-end:** Reduce motivaciones para tecnologías de translación de direcciones.

- **Direccionamiento jerárquico:** Resume y administra el crecimiento de las tablas de ruteo.

- **Multicast** la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

  IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse

enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.

Muchos ambientes no tienen, sin embargo, configuradas sus redes para rutear paquetes multicast, por lo que en éstas será posible hacer "multicasting" en la red local, pero no necesariamente en forma global.

El multicast IPv6 comparte protocolos y características comunes con IPv4, pero también incorpora cambios y mejoras. Incluso cuando se le asigne a una organización el más pequeño de los prefijos de ruteo global IPv6, ésta también recibe la posibilidad de usar uno de los 4.2 billones de grupos multicast IPv6 ruteables de fuente específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios (RFC 3306). En IPv4 era muy difícil para una organización conseguir incluso un único grupo multicast ruteable entre-dominios y la implementación de las soluciones entre-dominios eran anticuadas (RFC 2908). IPv6 también soporta nuevas soluciones multicast, incluyendo Embedded Rendezvous Point (RFC 3956), el que simplifica el despliegue de soluciones entre dominios.

1.4.2. Autoconfiguración

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red ruteada en IPv6 usando los mensajes de descubrimiento de

routers de ICMPv6. La primera vez que son conectados a una red, el nodo envía una solicitud de router de link-local usando multicast (router solicitación) pidiendo los parámetros de configuración; y si los routers están configurados para esto, responderán este requerimiento con un "anuncio de router" (router advertisement) que contiene los parámetros de configuración de capa de red.

Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o bien los nodos pueden ser configurados en forma estática. Esto crea un ambiente plug&play lo que simplifica significativamente la administración.

Los routers presentan un caso especial de requerimientos para la configuración de direcciones, ya que muchas veces son la fuente para información de autoconfiguración, como anuncios de prefijos de red y anuncios de router. La configuración sin estado para routers se logra con un protocolo especial de re numeración de routers.

1.4.3. Mejor formato de cabecera

El encabezado IPv6 tiene un nuevo formato que está diseñado para reducir al mínimo la sobrecarga del encabezado. Esto se consigue al mover los campos que no son esenciales y los campos de opciones a encabezados de extensión que se colocan a continuación del encabezado IPv6. La simplificación del encabezado IPv6 permite un procesamiento más eficaz en los enrutadores intermedios.

Los encabezados IPv4 y los encabezados IPv6 no son interoperables y el protocolo IPv6 no es compatible con el protocolo IPv4. Un host o un enrutador debe utilizar simultáneamente una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. Estas son sus características:

- El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

- Los routers IPv6 no hacen fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU, realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes.
- El encabezado IPv6 no está protegido por una suma de comprobación (checksum); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP, etc.). En efecto, los routers IPv6 no necesitan recalcular la suma de comprobación cada vez que algún campo del encabezado (como el contador de saltos o Tiempo de Vida) cambian. Esta mejora puede ser menos necesaria en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de línea (wirespeed), pero es relevante para routers por software.
- El campo Tiempo de Vida de IPv4 se llama ahora Límite de Saltos (Hop Limit), reflejando el hecho de que ya no se espera que los routers computen el tiempo que específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios (RFC 3306).

1.4.4. Provisión para extensiones

IPV6 ha sido diseñado de tal modo que el protocolo pueda ser extendido fácilmente para encontrar requerimientos de nuevas tecnologías o nuevas aplicaciones. IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a continuación del encabezado IPv6. A diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

Hasta el momento, existen 8 tipos de cabeceras de extensión, donde la cabecera fija y las de extensión opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Luego las cabeceras de extensión se van encadenando utilizando el campo de cabecera siguiente que aparece tanto en la cabecera fija como en cada una de las citadas cabeceras de extensión. Como resultado de la secuencia anterior, dichas cabeceras de extensión se tienen que procesar en el mismo orden en el que aparecen en el datagrama. La Cabecera principal, tiene a diferencia de la cabecera de la versión IPv4 un tamaño fijo de 40 octetos.

1.4.5. Mejora de la compatibilidad para la calidad de servicio (QoS)

Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo Flow Label (etiqueta de

flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec. Este mecanismo es realmente útil en transmisiones en tiempo real de audio y video

1.4.6. Movilidad

A diferencia de IPv4 móvil, IPv6 móvil (MIPv6) evita el ruteo triangular y por lo tanto es tan eficiente como el IPv6 normal. Los routers IPv6 pueden soportar también Movilidad de Red (NEMO, por Network Mobility) (RFC 3963), que permite que redes enteras se muevan a nuevos puntos de conexión de routers sin reasignación de numeración. Sin embargo, ni MIPv6 ni MIPv4 o NEMO son ampliamente difundidos hoy, por lo que esta ventaja es más bien teórica.

1.4.7. Jumbogramas

IPv4 limita los paquetes a 64 KiB de carga útil. IPv6 tiene soporte opcional para que los paquetes puedan superar este límite, los llamados jumbogramas, que pueden ser de hasta 4 GiB. El uso de jumbogramas puede mejorar mucho la eficiencia en redes de altos MTU. El uso de jumbogramas está indicado en el encabezado opcional Jumbo Payload Option.

1.4.8. Nuevo protocolo para la interacción de nodos vecinos

En IPv6, el protocolo semejante a ARP en IPv4, es el llamado protocolo de descubrimiento del vecino (ND, Neighbor Discovery). Este protocolo es el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros en su mismo enlace, determina sus direcciones en la capa de enlace, localiza los routers y mantiene la información de conectividad acerca de las rutas a los vecinos activos.

El protocolo ND se emplea también para mantener limpios los caches donde se almacena la información relativa al contexto de la red a la que está conectada un servidor o un router, y para detectar cualquier cambio en la misma. Si un router o una ruta falla, el servidor buscará alternativas funcionales.

ND emplea los mensajes ICMPv6 para algunos de sus servicios, este protocolo es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define varios mecanismos, entre ellos descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos inalcanzables, detección de direcciones duplicadas o campos, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies.

1.4.9. Características de seguridad

El apoyo para IPSec es una exigencia del protocolo IPv6, este requerimiento provee una solución estándar para las seguridades de red y promueve interoperabilidad entre diferentes implementaciones de IPv6. IPsec consiste en dos tipos de cabeceras de extensión y un protocolo que negocia las configuraciones de seguridad.

La autenticación en la cabecera provee integridad en los datos, autentificación en los datos, protección para la repetición de paquetes enteros en IPv6 (excluyendo campos en la cabecera ipv6 que deben cambiar en el recorrido).

La cabecera de Encapsulamiento seguridad de carga provee integridad en los datos, autenticación de datos, confidencialidad y protección para datos.

El protocolo típicamente usado para negociar configuraciones de seguridad de IPSec para comunicaciones unicast es el protocolo IKE (Intercambio de llave de Internet).

CAPÍTULO II

ARQUITECTURA DE IPV6

En este capítulo se revisa la arquitectura básica de IPv6, los diferentes tipos de direcciones que se manejan y la utilidad de las mismas.

2.1. Representación de direcciones en IPV6

Se ha definido una nueva notación para describir las direcciones de 16 bytes IPv6. Comprende de 8 grupos de 4 números hexadecimales separados por dos puntos, los dígitos hexadecimales no son sensibles a mayúsculas/minúsculas.

Se tiene tres formas comunes de representar direcciones IPv6 en texto:

- x:x:x:x:x:x:x:x donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.

- x:x::x en el caso de que haya grupos contiguos de 16 bits todos cero. Es una abreviatura que servirá para hacer más cómodo el uso de algunas direcciones. Además el primer cero de un grupo puede descartarse. Por ejemplo:

2001:0db8:85a3:0000:0000:8a2e:0370:7334	*dirección no simplificada*
2001:db8:85a3:0:0:8a2e:370:7334	*sin ceros iniciales*
2001:db8:85a3::8a2e:370:7334	*abreviando grupos de ceros*

  La sustitución con puntos puede realizarse únicamente una vez en la dirección. En caso contrario, se obtendría una representación ambigua. Si pueden hacerse varias sustituciones, se debe hacer la de mayor número de grupos; si el número de grupos es igual, se debe hacer la situada más a la izquierda.

- x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bis de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4.

2.2. Prefijos de direcciones

Una red IPv6 utiliza un grupo de direcciones IPv6 contiguas, de un tamaño potencia de dos. La parte inicial de las direcciones son idénticas para todos los hosts de una red, y se llama dirección de red o prefijo de encaminamiento *(*routing prefix*)*. Las direcciones de red se escriben en notación CIDR (Classless Inter-Domain Routing -

Enrutamiento entre dominios sin Clases), una red se representa por la primera dirección del grupo (que debe terminar en ceros), una barra invertida (/), y el número de bits del prefijo en decimal. Es posible indicar directamente el prefijo de encaminamiento de una dirección de interface mediante notación CIDR.

El tamaño del grupo de direcciones se representa únicamente con una barra invertida (/) y el tamaño del prefijo de red en decimal, sin indicar qué direcciones específicas están en el grupo.

Tabla I: Direcciones IPv6 reservadas

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	Sin especificar	Como 0.0.0.0 en Pv4
::1	128 bits	Dirección de bucle local (loopback)	Como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96 bits	Direcciónes IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones “empotradas.”
::ff:xx:xx:xx:xx	96 bits	Direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
fe80:: - feb::	10 bits	Direcciones link-local	equivalentes a la dirección de loopback de IPv4
fec0:: - fef::	10 bits	Direcciones site-local	Equivalentes al direccionamiento privado de IPv4
ff::	8 bits	Multicast	
001 (base 2)	3 bits	Direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son “001”.

2.3. Tipos de direcciones (Unicast, Multícast, Anycast)

Las direcciones IPv6 se clasifican según las políticas de direccionamiento y encaminamiento más comunes en redes: direcciones unicast, anycast y multicast. En IPv6 no existe la dirección de broadcast. Su función es reemplazada por el direccionamiento multicast. Por otro lado las direcciones todo ceros y todo unos son valores legales para cualquier campo, a menos que esté específicamente excluido.

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos (scope), lo que quiere decir que se tendrán direcciones globales y no globales. Si bien con IPv4 ya se había empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento.

Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador único de uno o varios interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que se va a poder diferenciarlos a simple vista.

Cualquier tipo de dirección se asigna a interfaces, no a nodos. Todos los interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito. Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no hacen falta direcciones IPv6 globales, sino que se tiene más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto. Respecto a los prefijos de

subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

2.3.1 Direcciones Unicast

Una dirección Unicast identificará un solo interfaz. Un paquete enviado a una dirección unicast se entregará a un solo interfaz. Son agrupables gracias a los prefijos de dirección, como ocurría con las direcciones IPv4 con CIDR.

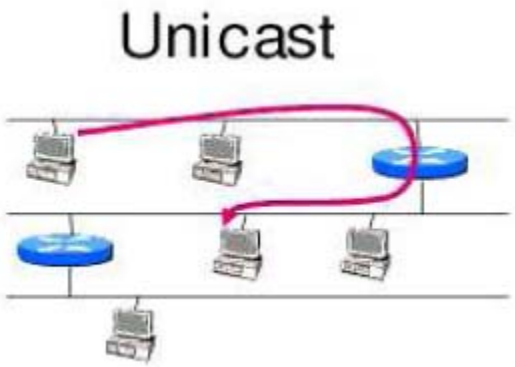


Figura 2.1: Comportamiento Unicast

Los nodos IPv6 pueden tener mucho o poco conocimiento de la estructura interna de las direcciones IPv6 según su papel (ej. host, router). El mínimo conocimiento implica que un nodo considere que las direcciones unicast (incluyendo la suya) no tienen estructura interna:

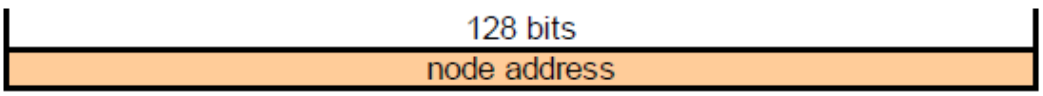


Figura 2.2: Mínimo conocimiento de un nodo

Un host algo más sofisticado puede conocer los prefijos de subred (“subnet prefix”) de los enlaces a los que está unido, donde diferentes direcciones pueden tener diferentes longitudes de “subnet prefix”:

Figura 2.3: Conocimiento de un nodo

Donde el identificador de interfaz (“interface ID”) identifica los distintos interfaces de un enlace.

En cuanto a los routers, si bien pueden no tener ningún conocimiento sobre la estructura interna de la dirección unicast, normalmente conocerán los límites jerárquicos para la operación de los protocolos de enrutamiento. El conocimiento de dichos límites variará de un router a otro, según la posición que ocupen en la jerarquía de enrutamiento.

2.3.1.1 Identificador de Interfaz (Interface ID)

Como se comentó en el punto anterior, los “Interface ID” son usados para identificar los interfaces de un enlace y por tanto, es un requisito indispensable que sea único en el ámbito delimitado por un “subnet prefix”. Además, es recomendable que sean únicos en el enlace o incluso en un alcance más amplio. En algunos casos, el identificado de interfaz se obtendrá a partir de la dirección de enlace del interfaz (su MAC).

Para las direcciones unicast (excepto las que empiezan con los bits 000) los “Interface ID” deben ser de 64 bits, por lo que, para convertir una dirección de enlace IEEE 802 48-bit MAC (la que incorporan las tarjetas ethernet), es necesaria una conversión.

2.3.1.2 Dirección Unspecified (::)

La dirección todo ceros es llamada Unspecified. Indica la ausencia de direcciones y no puede ser asignada a ningún nodo. Un ejemplo de uso de esta dirección es en el campo dirección origen de un paquete IPv6 enviado por un host durante su proceso de inicialización, antes de que haya obtenido su propia dirección.

2.3.1.3 Dirección de Loopback (::1)

La dirección 0:0:0:0:0:0:0:1 es llamada dirección de loopback. Ésta sirve para enviar un paquete de IPv6 de un nodo a si mismo. No puede ser asignada a ningún interfaz físico, sino que debe entenderse como la dirección link-local asignada a un interfaz virtual unido a un enlace que no va a ninguna parte.

2.3.1.4 Dirección IPv6 con Dirección IPv4 Embebida

Existen dos tipos de direcciones IPv6 que contienen en sus últimos 32 bits direcciones de IPv4. La primera de ellas, denominada “IPv4-compatible IPv6 address” fue definida para ayudar en los mecanismos de transición. Su formato es:

Figura 2.6: Dirección IPv6 compatible con IPv4

El segundo tipo de direcciones IPv6 que contienen direcciones IPv4, son las que representan las direcciones de nodos que sólo soportan IPv4 en formato IPv6. Este tipo de direcciones es conocida como “IPv4-mapped IPv6 address” y su formato es:

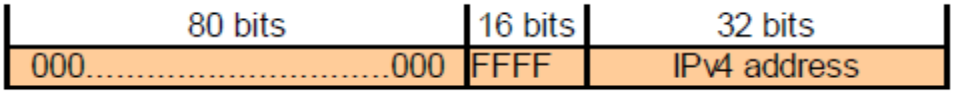


Figura 2.7: Dirección IPv4-mapped IPv6

2.3.1.5 Direcciones Global Unicast

El formato general para las direcciones global unicast es el siguiente:

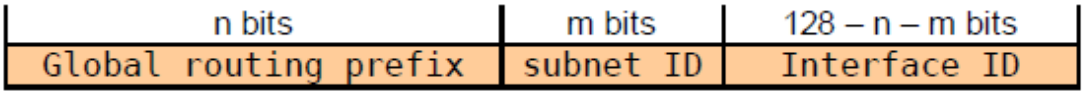


Figura 2.8: Formato dirección Unicast Globales

Donde el “global routing prefix” (prefijo de enrutamiento global) es un valor asignado a un “site” (un conjunto de subredes o enlaces), el campo “subnet ID” es el identificador de cada una de las subredes dentro del “site”, y el “interface ID” es el identificador de interface.

El prefijo de enrutamiento global ha sido diseñado para ser estructurado jerárquicamente por los RIR's (Regional Internet Registries) y los ISP's (Internet

Service provider). El “Subnet ID” ha de ser asignado de manera jerárquica por los administradores del “site”.

2.3.1.6 Direcciones Local-use unicast

Existen dos tipos de direcciones unicast de uso local: Link-local y Site-local.

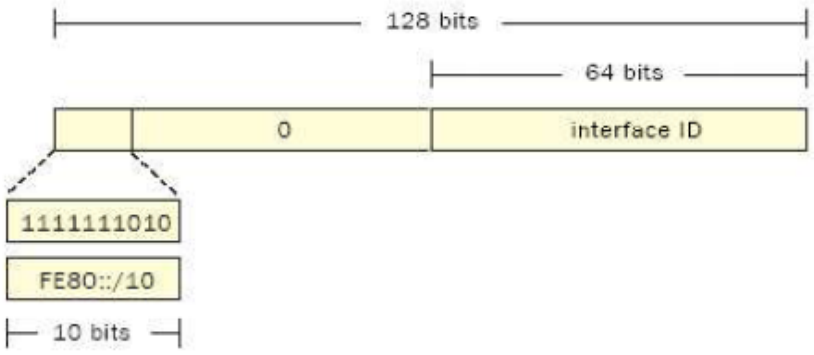


Figura 2.9: Formato de una dirección Link-Local

Estas direcciones están diseñadas para comunicaciones dentro de un solo enlace, para ofrecer funcionalidades como la autoconfiguración de dirección, neighbor discovery o para permitir la comunicación entre hosts cuando no hay routers presentes. Los routers no reenvían ningún paquete con dirección local como fuente.

El otro tipo de direcciones de uso local, denominadas site-local, definidas para ser utilizadas dentro de una red local con diferentes enlaces (en un site), han sido desaprobadas debido a que, pese a quedar definidas teóricamente, en la práctica su definición es ambigua, lo que supone un problema tanto para los desarrolladores de aplicaciones como para los routers.

Aunque hayan sido desaprobadas, esto no ha impedido su uso, por lo menos hasta que se haya estandarizado el cambio y estas hayan sido reemplazadas. Tienen el siguiente formato:

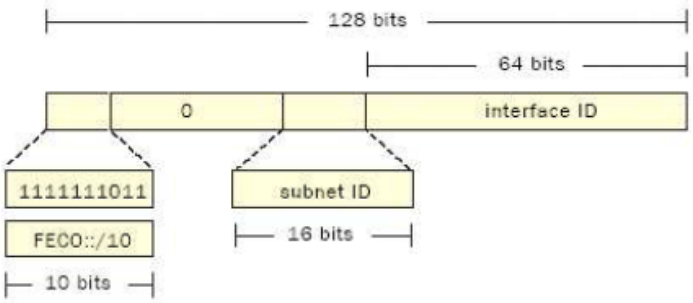


Figura 2.10: Formato de una dirección Site-Local

Las direcciones site-local se pensaron para ser usadas dentro de un site sin necesidad de prefijo global, pero cuando se produzca el cambio, el prefijo que utilizaban este tipo de direcciones (FEC0::/10) pasará a formar parte del espacio de direcciones global. Los routers no reenvían los paquetes con dirección origen local o de site fuera de éste.

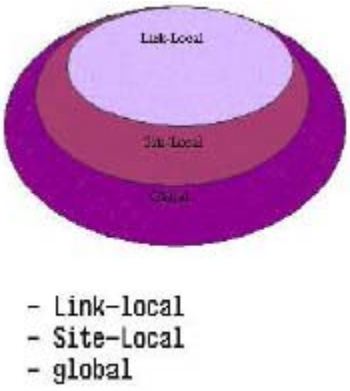


Figura 2.11: Ambito de direcciones IPv6

2.3.2 Direcciones Anycast

Una dirección anycast es una dirección asignada a más de un interfaz (generalmente de diferentes nodos), con el propósito de que un paquete que sea enviado a una de estas direcciones sea encaminado hasta el interfaz más cercano que responda a dicha dirección.

Las direcciones anycast ocupan parte del espacio de direcciones unicast, usando alguno de los formatos definidos para el mismo. Así, un paquete anycast es sintácticamente indistinguible de un paquete unicast. Cuando una dirección unicast es asignada a más de un interfaz se convierte inmediatamente en anycast, y los nodos a los que se les asigna deben ser explícitamente configurados para saber que se trata de una dirección anycast.

Para cada dirección anycast asignada, hay un largo prefijo de dirección (P), que identifica la región topológica en la que residen todos los interfaces con una dirección anycast concreta. Dentro de la región identificada con P, cada dirección anycast debe escribirse como una entrada diferente en el sistema de enrutamiento (comúnmente denominado “host route”); fuera de la región P, las direcciones anycast deben ser englobadas en las entradas de rutas bajo el prefijo P.

Un uso esperado de las direcciones anycast es identificar conjuntos de routers pertenecientes a una organización que provea servicios de Internet (ISP). Estas direcciones podrán ser usadas como direcciones intermedias en una “Cabecera de encaminamiento” para provocar que el flujo de paquetes sea encaminado a través de un ISP particular o una secuencia de estos.

En un funcionamiento similar, las direcciones anycast pueden ser utilizadas también para identificar el conjunto de routers unidos a una determinada subred.

2.3.3 Direcciones Multicast

Una dirección multicast en IPv6, identifica a un grupo de interfaces. Además, un interfaz puede pertenecer a cualquier número de grupos multicast. Estas direcciones tienen el siguiente formato:

Figura 2.12: Formato de una dirección Multicast

Donde el prefijo 11111111 ó 0xFF identifica la dirección como multicast, el campo flag es un conjunto de 4 flags, el campo scope (ámbito) indica el alcance de cada dirección multicast en concreto (desde alcance de interfaz hasta alcance global) y el group ID identifica al grupo multicast.

Las direcciones multicast no pueden aparecer como dirección origen en un paquete, y tampoco pueden ser utilizadas en el campo “Cabecera de encaminamiento” comentado para las direcciones anycast.

2.4 IPv6 sobre la capa de enlace

La independencia de IPv6 del medio físico de red es muy importante. Cuando un paquete es enviado de una red a otra, usualmente no se conoce de antemano el tipo de redes físicas por el cual el paquete viajará. El protocolo de internet (IP) solo se preocupa acerca de la dirección de destino y encontrar una manera de llegar ahí sin importar el hardware de red usado. Es ahí cuando entonces IP pasa el paquete a la capa de Enlace de Datos. En redes 802, el controlador de interfaz en la capa de enlace de datos aplica un encabezado MAC (Media Access Control) al diagrama y lo envía a la red física. El controlador de interfaz necesita estar consciente de los requerimientos físicos para la transmisión. Cada tecnología de hardware de red define un mecanismo de direccionamiento específico, es aquí donde *Neightbor Discovery* (ND) (combina ARP, descubrimiento y redireccionamiento ICMP) es usado para mapear direcciones IPv6 con direcciones MAC.

2.4.1 IPV6 Sobre Ethernet

Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, hay que basarse en la dirección MAC de 48 bits (IEEE802). Se toman los 3 primeros bytes (los de mayor orden), y se les agregan "FFFE" (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor Valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso).

Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

48 bits	48 bits	16 bits	
Ethernet Destination Address	Ethernet Source Address	1000011011011101 (86DD)	IPv6 Header and Data

Figura 2.13: Cabecera Ethernet

2.4.2 Mapeo Multicast sobre Ethernet

Cuando se envían paquetes IPv6 Multicast sobre una red Ethernet, la dirección MAC correspondiente al destino es **33-33-mm-mm-mm-mm** donde **mm-mm-mm-mm** representa los últimos 32 bits de la dirección Multicast IPv6 correspondiente.

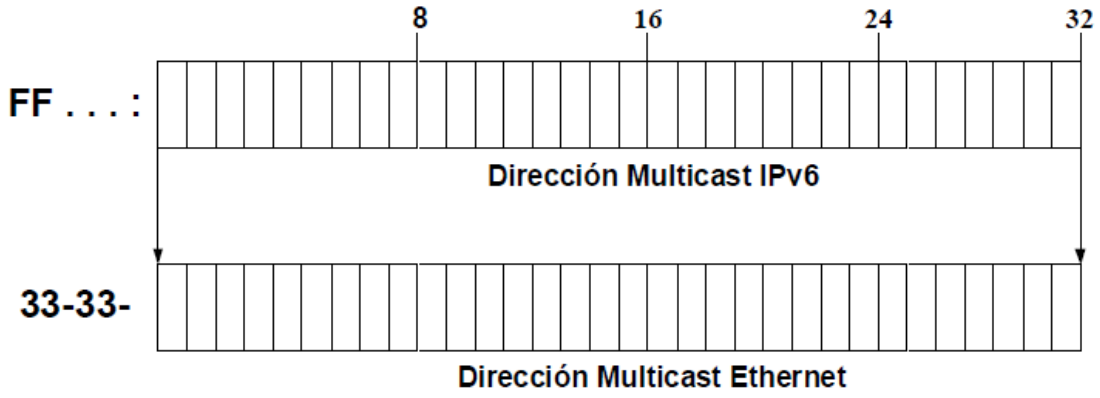


Figura 2.14: Mapeo multicast sobre ethernet

Esta conversión permite que la interfaz reconozca como propios tramas destinadas a las direcciones Ethernet multicast correspondientes. Como el mapeado no es único (1 dirección Ethernet multicast para 32 direcciones IP multicast) es necesario realizar un filtrado posterior para eliminar las tramas no importantes.

2.4.3 Interface PPP

El Protocolo Punto a Punto (PPP) proporciona un método estándar de encapsulado de la información del protocolo de la Capa de Red sobre los enlaces punto a punto. PPP también define un Protocolo de Control de Enlace extensible, y propone una familia de Protocolos de Control de Red (NCPs) para establecer y configurar diferentes protocolos de la capa de red.

A continuación se va a definir el método para la transmisión de los paquetes IP Versión 6 sobre los enlaces PPP así como el Protocolo de control de Red (NCP) para establecer y configurar los IPv6 sobre PPP. También especificará el método de formar direcciones de enlace locales IPv6 en enlaces PPP.

En el establecimiento de las comunicaciones sobre un enlace punto a punto, cada extremo del enlace PPP debe enviar primero los paquetes del Protocolo de Control de Enlace (LCP) para configurar y probar el enlace de datos. Después de que el enlace se ha establecido y los medios opcionales se han negociado como necesidad para el LCP, PPP debe enviar los paquetes de Protocolo de Control de Red (NCP) para escoger y configurar uno o más protocolos de la capa de red. Una vez que cada uno de los protocolos de la capa de red escogidos se han configurado, pueden enviarse datagramas de cada protocolo de la capa de red sobre el enlace.

2.4.3.1 Envío de Datagramas IPv6

Antes que cualquier paquete IPv6 pueda ser comunicado, PPP debe alcanzar la fase Protocolo capa de red, y el Protocolo de Control IPv6 debe alcanzar el estado abierto.

Exactamente un paquete IPv6 se encapsula en el campo de Información de las tramas de la capa Enlace de Datos PPP donde el campo Protocolo indica el tipo hex 0057 (Internet Protocol Version 6).

La longitud máxima de un paquete IPv6 transmitido sobre un enlace PPP es igual que la longitud máxima del campo de Información de una trama de la capa Enlace de Datos PPP. PPP se enlaza soportando IPv6 debiendo permitir que el campo de información sea por lo menos tan grande como el tamaño mínimo del enlace MTU requerido para IPv6.

2.4.3.2 Un Protocolo de Control de Red PPP para IPv6

El Protocolo de Control IPv6 (IPV6CP) es responsable de configurar, habilitar, y desactivar los módulos del protocolo IPv6 en ambos extremos del enlace punto a punto. IPV6CP usa el mismo mecanismo de intercambio de paquete que el Protocolo de Control de Enlace (LCP). No pueden intercambiarse paquetes IPV6CP hasta que PPP haya alcanzado la fase Protocolo Capa de Red.

Los paquetes IPV6CP recibidos antes de alcanzar esta fase deben desecharse silenciosamente. El Protocolo de Control IPv6 es exactamente igual que el Protocolo de Control de Enlace con las excepciones siguientes:

- **Campo Protocolo Capa de Enlace de datos**

  Exactamente un paquete IPV6CP se encapsula en el campo de Información de la trama Capa de Enlace de Datos PPP donde el campo Protocolo indica el tipo hex 8057 (Protocolo del Control ipv6).

- **Campo Código**

  Sólo un Código de 7 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack and Code-Reject) se usa. Los otros Códigos deben tratarse como no reconocido y debe producirse un Código-Reject.

- **Interrupciones**

  No pueden intercambiarse paquetes IPV6CP hasta que el PPP ha alcanzado la fase Protocolo Capa de Red. Una aplicación debe prepararse para esperar por la Autenticación y Calidad del Enlace. Sin embargo, puede decidir terminar antes del tiempo de espera para un Configure-Ack u otra contestación. Se sugiere que una aplicación sólo se termine después de la intervención del usuario o una cantidad de tiempo configurable.

- **Tipos de Opción de configuración**

  IPV6CP tienen un juego distinto de Opciones de Configuración.

2.4.3.3 Opciones de configuración IPV6CP

Las opciones de configuración IPV6CP permiten negociación de parámetros IPv6 deseables. IPV6CP usa el mismo formato de Opción de Configuración definido para LCP, con un juego separado de Opciones. Si una Opción de Configuración no es

incluida en un paquete de Requerimiento de Configuración, el valor predefinido para esta Opción de Configuración es asumido.

Los valores actualizados del campo Tipo Opción IPV6CP se especifica en él más reciente "Assigned Numbers" RFC. Los valores actuales se asignan como sigue:

a. Identificador de Interfaz (interface-Identifier)
b. Protocolo de Compresión Ipv6 (IPv6-Compression-Protocol)

a. Identificador de Interfaz

Esta Opción de Configuración proporciona una manera de negociar un único Identificador de interfaz de 64-bit a ser usado para la autoconfiguración de la dirección al extremo local del enlace. Un Requerimiento de Configuración debe contener exactamente un caso de la opción Identificador de Interfaz. El Identificador de Interfaz debe ser único dentro del enlace PPP; en la terminación de la negociación de los diferentes valores del Identificador de Interfaz, serán seleccionados para los extremos del enlace PPP. El Identificador de Interfaz puede también ser único sobre un alcance más ancho.

Antes de que esta Opción de Configuración se requiera, una aplicación escoge su Identificador de Interfaz provisional. El valor no-cero del Identificador de Interfaz provisional debería escoger el valor tal que sea único en ambos para el enlace y, si es posible, reproducible de forma consistente por las iniciaciones de la máquina state finite IPV6CP (Cierre administrativo y reabrir, reboots, etc). La razón para preferir un Identificador de Interfaz único reproducible consistentemente, a un Identificador de Interfaz completamente aleatorio es para proporcionar estabilidad a direcciones de alcance global que pueden formarse del Identificador de Interfaz.

Asumiendo que los bits del Identificador de Interfaz son enumerados de 0 a 63 en orden de bit canónico donde el bit más significativo es el bit número 0, el bit número 6 es el bit "u" (bit universal/local en la terminología IEEE EUI-64) que indica si o no el Identificador de Interfaz está basado en un identificador IEEE único globalmente (EUI-48 o EUI-64). Se establece a uno (1) si un identificador IEEE único globalmente es usado para derivar el Identificador de Interfaz, y se establece a cero (0) en otro caso.

Los siguientes son métodos para escoger el Identificador de Interfaz provisional en el orden de preferencia:

1. Sí un identificador global IEEE (EUI-48 o EUI64) está disponible en cualquier parte en un nodo, el debe ser usado para construir el Identificador de Interfaz provisional debido a sus propiedades singulares. Cuando se extrae un identificador global IEEE de otro dispositivo en el nodo, se debe tener cuidado, para eso el identificador extraído se presenta en clasificación canónica.

   La única transformación de un identificador EUI-64 es invertir el bit "u" (bit universal/local en terminología IEEE EUI-64). Por ejemplo, para un identificador EUI-64 único globalmente de la forma:

   Donde "c" son los bits de la company_id asignados, "0" es el valor del bit universal/local para indicar el alcance global, "g" es el bit grupo/individual, y "e" son los bits de extensión del identificador. El único cambio es invertir el valor del bit universal/local.

En el caso de un identificador EUI-48, se convierte primero al formato EUI-64 para insertar dos bytes, con valores hexadecimales de 0xFF y 0xFE, en el medio del MAC de 48 bits (entre las parte company_id y la extensión del identificador del valor EUI-48).

2. Sí un identificador global IEEE no está disponible, una fuente diferente de singularidad debe usarse. Las fuentes sugeridas de singularidad incluyen la dirección de la capa de enlace, números de serie de la máquina, etcétera.

   En este caso el bit "u" del Identificador de Interfaz debe establecerse a cero (0).

3. Si una buena fuente de singularidad no puede encontrarse, se recomienda que un número aleatorio sea generado. En este caso el bit "u" del Identificador de Interfaz debe establecerse a cero (0).

Se requieren buenas fuentes de singularidad o aleatoriedad para que la negociación del Identificador de Interfaz suceda. Si ningún número único o un número aleatorio puede ser generado, se recomienda que un valor cero sea usado para transmitir un Identificador de Interfaz en el Requerimiento de Configure-Request. En este caso el par PPP puede proporcionar un Identificador de Interfaz no-cero válido, en su respuesta como se describe abajo. Si por lo menos uno de los pares de PPP puede generar números no-ceros separados para él y su par, la negociación del identificador tendrá éxito.

Cuando una Configure-Request es recibida con la Opción de Configuración de Identificador de Interfaz y esa opción recibe las herramientas del par, el

Identificador de Interfaz recibido es comparado con el Identificador de Interfaz de la última Configure-Request enviada al par. Dependiendo del resultado de la comparación una aplicación debe responde de una de las siguientes maneras:

- Si los dos Identificadores de Interfaz son diferentes pero el Identificador de Interfaz recibido es cero, un Configure-Nak es enviado con un valor Identificador de Interfaz no-cero sugerido para el uso del par remoto. Un Identificador de Interfaz sugerido debe ser diferente del Identificador de Interfaz de la última Configure-Request enviada al par. Se recomienda que el valor sugerido sea reproducido de forma consistente por las iniciaciones de la máquina de estados finitos IPV6CP (Cierre administrativo y reabrir, reboots, etc.). El bit "u" universal/local) del identificador sugerido debe ser establecido a cero (0) sin tener en cuenta su fuente a menos que el identificador derivado EUI-48/EUI-64 único globalmente sea proporcionado para el uso exclusivo del par remoto.

- Si los dos Identificadores de Interfaz son diferentes y los Identificadores de Interfaz recibidos no son ceros, el Identificador de Interfaz debe ser reconocido, una Configure-Ack se envía con el requerimiento Identificador de Interfaz significando que el par que respondió está de acuerdo con el requerimiento del Identificador de Interfaz. Si los dos Identificadores de Interfaz son iguales y no son ceros, un Configure-Nak debe ser enviado especificado un valor de Identificador de Interfaz no-cero diferente, sugerido para el uso por el par remoto.

  Se recomienda que el valor sugerido sea reproducible de forma consistente por las iniciaciones de la máquina state finite IPV6CP (Cierre administrativo

y reabrir, reboots, etc.). El bit "u" universal/local) del identificador sugerido debe ser establecido en cero (0) sin tener en cuenta su fuente a menos que el identificador derivado EUI-48/EUI-64 único globalmente es proporcionado para el uso exclusivo por el par remoto.

- Si los dos Identificador de Interfaz son iguales a cero, la negociación del Identificador de Interfaz debe ser terminada transmitiendo un Configure-Reject con el valor Identificador de Interfaz puesto a cero. En este caso un Identificador de Interfaz único no puede negociarse.

- Si una Configure-Request es recibida con la Opción de Configuración del Identificador de Interfaz y el par recibido no implementa esta opción, Configurar-Reject se envía.

Una nueva Configure-Request no debería ser enviada al par hasta que el proceso normal, cause que sea enviado (es decir, hasta que un Configurar-Nak se recibe o se Reinicie el cronómetro runs out).

Una nueva Configure-Request no debe contener la opción del Identificador de Interfaz si un Identificador de Interfaz válida se recibe un Configure-Reject.

Recepción de un Configure-Nak con un diferente Identificador de Interfaz sugerido del último Configurar-Nak enviado al par, indica un Identificador de Interfaz único. En este caso una nueva Configure-Request debe ser enviada con el valor identificador sugerido en el último Configure-Nak del par. Pero si el Identificador de Interfaz recibido es igual al enviado en el último Configurar-Nak, un nuevo Identificador de Interfaz debe ser escogido. En este caso, un nuevo Configure-

Request debería ser enviado con el nuevo Identificador de Interfaz provisional. Esta sucesión (transmitir un Configure-Request, recibir un Configure-Request, transmitir un Configure-Nak, recibir un Configure-Nak) podría ocurrir unas pocas veces, pero es sumamente improbable que ocurra repetidamente. Más probablemente, los Identificadores de Interfaz escogidos en cualquier extremo diferirá rápidamente, terminando la sesión.

Si la negociación del Identificador de Interfaz se requiere, y el par no proporcionó la opción en su Configure-Request, la opción debería añadir un Configure-Nak. El valor provisional del Identificador de Interfaz dado debe ser aceptado como el Identificador de Interfaz remoto; debe ser diferente del valor del identificador seleccionado para el extremo local del enlace PPP. La próxima Configure-Request del par puede incluir esta opción. Si la próxima Configure-Request no incluye esta opción el par no debe enviar otro Configure-Nak con esta opción incluida. Debe asumir que la implementación del par no soporta esta opción.

Por defecto, una implementación debería intentar negociar el Identificador de Interfaz para su extremo de la conexión PPP.

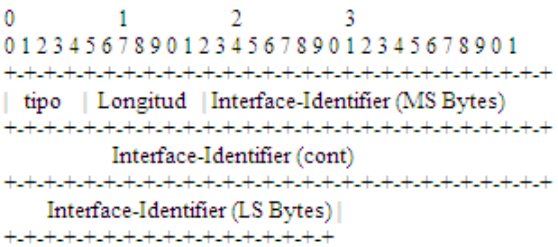


Figura 2.15: Resumen del formato de la Opción de Configuración del Identificador de Interfaz.

Identificador de Interfaz

El Identificador de Interfaz 64-bit que es muy probablemente el único en el enlace o es cero, sí una fuente de buena singularidad no puede encontrarse.

Valor por defecto

Si un Identificador de Interfaz no válido puede negociarse con éxito, ningún valor Identificador de Interfaz por defecto debe asumirse. Los procedimientos para recuperar de semejante caso no son especificados. Un acercamiento es configurar manualmente el Identificador de Interfaz de la interfaz.

b. Protocolo de Compresión IPv6

Esta Opción de Configuración proporciona una manera de negociar el uso de un protocolo de compresión de paquetes IPv6 específico. La Opción de Configuración del Protocolo de Compresión IPv6 se usa para indicar la habilidad de recibir paquetes comprimidos. Cada extremo del enlace debe pedir esta opción separadamente si la compresión bidireccional se desea. Por defecto, la compresión no se habilita.

La negociación de compresión IPv6 con esta opción es específica para Datagramas IPv6 y no será confundida con la compresión resultante de las negociaciones vía el Protocolo de Control de Compresión (CCP), qué potencialmente afecta a todos los Datagramas.

Un resumen del formato de Opción de Configuración del Protocolo de Compresión IPv6 es mostrado abajo. Los campos se transmiten de izquierda a derecha.

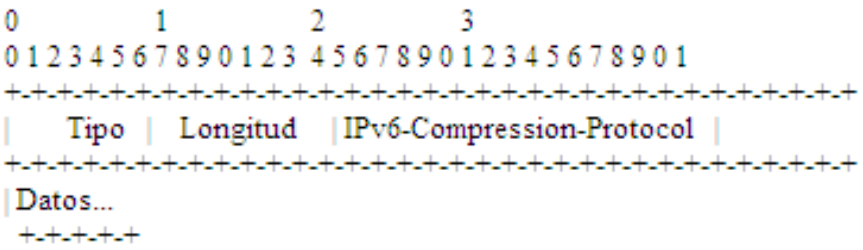


Figura 2.16: Resumen del formato de Opción de Configuración del Protocolo de Compresión IPv6

Protocolo de Compresión IPv6

El campo del Protocolo de Compresión IPv6 es de dos octetos e indica el protocolo de compresión deseado. Los valores para este campo siempre son iguales a los valores del campo Protocolo Capa Enlace de Datos PPP para ese mismo protocolo de compresión.

Ningún valor del campo Protocolo de Compresión IPv6 se asigna actualmente. Se harán asignaciones específicas en documentos que definen algoritmos de compresión específicos.

Datos

El campo de Datos es cero o más octetos y contiene datos adicionales determinado por el protocolo de compresión particular.

Valor por defecto

Ningún protocolo de compresión IPv6 disponible.

Autoconfiguración sin estado y Direcciones de Enlace-local

El Identificador de Interfaz de IPv6 de direccionamiento único de una Interfaz PPP, debe ser negociada en la fase IPV6CP del arreglo de conexión PPP. Si un Identificador de Interfaz no válida se ha negociado con éxito, los procedimientos para recuperar semejante caso no son especificados. Una forma es configurar manualmente el Identificador de interfaz de la interface.

Con tal de que el Identificador de interfaz sea negociada en la fase IPV6CP de arreglo de conexión PPP, es redundante para el desempeño la detección de dirección duplicada como una parte del protocolo de Autoconfiguración Sin estado IPv6. Por consiguiente se recomienda que para los enlaces PPP con la opción Identificador de interfaz IPV6CP habilitada el valor por defecto de la variable de autoconfiguración de DupAddrDetectTransmits sea cero.

Las direcciones enlace-local de interfaz PPP tienen el siguiente formato:

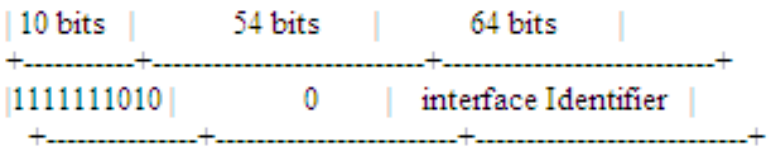


Figura 2.17: Formato de direcciones de enlace local de interfaz PPP

Los 10 bits más significativos de la dirección son el prefijo Enlace-local FE80::. 54 bits ceros rellenan la dirección entre el prefijo Enlace-local y el campo Identificador de interfaz.

c. Consideraciones de seguridad

El Protocolo de Control IPv6 extensión a PPP puede usarse con todos los mecanismos de autenticación y encriptación PPP definidos.

CAPÍTULO III

SEGURIDADES IPV6

3.1 Introducción a IPsec

IPsec como fue definido en el RFC 2401 provee una arquitectura de seguridad para el Protocolo de Internet (IP) - no una arquitectura de seguridad para Internet. Esta distinción es importante: IPsec define servicios de seguridad a ser usados en la capa IP tanto en IPv4 como en IPv6, con la diferencia de que IPsec es obligatorio en IPv6 y opcional en IPv4, lo que lleva a pensar que IPv6 es más seguro.

IPsec provee un estándar abierto e interoperable para construir seguridad en la capa de red en lugar de la capa de aplicación o la de transporte. Aunque las aplicaciones se benefician de la seguridad en la capa de red, la más importante capacidad de aplicación de IPsec es la creación de VPN (Redes privadas virtuales - Virtual Private Networks) para enviar de forma segura los datos de la empresa a través de un Internet abierto. IPsec permite lo siguiente:

Encriptación de datos que pasan entre dos nodos, usando claves públicas y privadas con algoritmos de encriptación muy seguras.

Autenticación de datos y su fuente usando mecanismos de autenticación muy eficientes.

Control de acceso a datos sensibles en redes privadas

Verificación de integridad de los datos llevados por el protocolo (IP)

Protección de ataques de repetición en la cual un intruso intercepta paquetes enviados entre dos nodos IP y los reenvía después de desencriptarlos o modificarlos.

Limitación en ataques de análisis de tráfico, en el cual un intruso intercepta datos protegidos y analiza información de fuente y destino, tamaño y tipo de paquetes y otros aspectos de los datos, incluyendo los contenidos de la cabecera que podrían no estar protegidos por encriptación.

Seguridad extremo a extremo para paquetes IP proveyendo garantía para los usuarios de los extremos de los nodos de la privacidad e integridad de sus transmisiones.

Túneles seguros a través de redes inseguras como el Internet global y otras redes públicas.

Integración de algoritmos, protocolos e infraestructuras de seguridad.

3.2 Componentes de IPsec

Dentro del IETF, se estableció el IP Security Protocol Working Group, en donde se desarrolló la especificación completa de IPSec. Obteniendo siete componentes:

Arquitectura (Architecture): Establece los conceptos generales: requisitos de seguridad, definiciones y mecanismos característicos de la tecnología de IPSec.

Encapsulación de seguridad de la carga útil *(*Encapsulating Security Payload) ESP: Describe el formato del paquete y las definiciones generales relacionadas para el uso de ESP para el encriptamiento de paquetes, y opcionalmente la autentificación.

Cabecera de Autenticación (Authentication Header) AH: Describe el formato del paquete y las definiciones generales relacionadas para el uso de AH para la autentificación de paquetes, así como su algoritmo MAC (Message Authentication Code).

Algoritmo de encriptación (Encryption Algorithm): Documentos que describen cómo los diversos algoritmos de encriptamiento son utilizados por ESP, tales como DES, Triple-DES, RC5, IDEA,CAST, BLOWFISH y RC4.

Algoritmo de Autenticación (Authentication Algorithm): Documentos que describen cómo los diversos algoritmos son usados por AH y por la opción de autentificación de ESP.

Administración de Llaves (Key Management): Documentos que describen los esquemas para administración de las llaves.

Dominio de interpretación (*Domain of Interpretation*) DOI: Contiene parámetros necesarios para diversos documentos relacionados entre sí. Estos incluyen identificadores para algoritmos de autentificación y de encriptamiento aprobados, así como también parámetros operacionales tales como tiempos de vigencia de llaves (key lifetime).

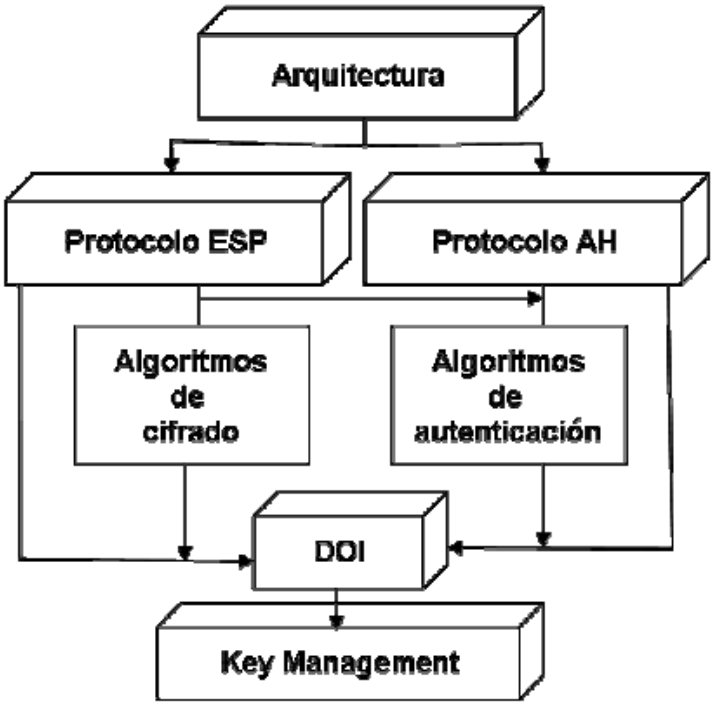


Figura 3.1: Componentes de IPsec

3.3 Objetivos de la seguridad

La seguridad informática se puede decir que tiene tres objetivos generales:

Autenticación: La capacidad de determinar de forma fiable que los datos han sido recibidos tal como fueron enviados y verificar que la entidad que envía los datos es la que se supone que sea. Una autenticación exitosa significa prevenir ataques de intrusos que se hacen pasar por entidades autorizadas.

Integridad: La capacidad para determinar realmente que los datos no han sido modificados durante la transmisión de la fuente al destino. El mantenimiento exitoso de la integridad significa tanto la prevención de ataques de datos auténticos modificados sin ser detectados así como prevenir la aceptación de datos que han sido corruptos en alguna nube de la red.

Confidencialidad: La capacidad de transmitir datos que puedan ser usados o leídos solo por su destinatario y no por otra entidad. Un exitoso mantenimiento de la confidencialidad de datos significa que nadie en absoluto que no sea el destinatario pueda acceder a los datos privados.

Desarrollos en criptografía moderna, específicamente en el uso de claves criptográficas públicas, hacen posible la combinación de estos tres objetivos en un conjunto de funciones:

Firmas digitales: inequívocamente enlazan al titular de un secreto en particular con datos representados como si hubieran sido firmados por esa entidad.

- **Hash seguros:** Un hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo. Dentro de este contexto un hash seguro digitalmente resume una secuencia de datos usando un proceso repetible que producirá idénticos resultados solo si la secuencia de datos siendo verificada coincide con la secuencia de datos producida por el remitente.

Encriptación: es el proceso de ejecutar una transformación reversible en datos legibles con el fin de hacerlos ilegibles para cualquier otro que no sea el titular de la clave de desencriptación apropiada.

Algunas o todas de estas funciones son posibles en combinación o individualmente en protocolos en cada capa TCP/IP, desde IP (a través de IPsec) a la capa de transporte (a través de TLS, el protocolo de seguridad de la capa de transporte) a las funciones de seguridad que se proveen a través de las aplicaciones.

3.4 Arquitectura de seguridad

IPsec está implementado por un conjunto de protocolos criptográficos para:

1. Asegurar el flujo de paquetes
2. Garantizar la autenticación mutua
3. Establecer parámetros criptográficos

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede necesitar saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

3.5 Algoritmos de Autenticación y Encriptación

En lugar de confiar en la discreción para proteger un esquema de encriptación o autenticación (un procedimiento conocido como "seguridad a través de la obscuridad") los protocolos de seguridad de TCP/IP siempre especifican qué algoritmos de criptografía serán bien conocidos y accesibles. Esto es hecho por algunas razones, una de las cuales es que es un protocolo abierto, las especificaciones TCP/IP deben ser publicadas libremente pero la razón más importante, sin embargo, es que confiar en el secretismo o discreción es una salvaguarda muy pobre hablando de seguridad.

Tratar de guardar en secreto un algoritmo de encriptación es casi imposible, particularmente si va a ser usado por alguien que no sea la persona que sabe el secreto. Los intrusos tienen muchas herramientas de análisis de criptología que están hechas para romper códigos y solo necesitan tener acceso a los textos cifrados para romperlos. Teniendo acceso al software usado para encriptar/desencriptar datos con el algoritmo secreto hace la tarea mucho más fácil: el intruso solo debe determinar que hace el software a los datos para hacer la operación correcta para revertirlo.

La gran ventaja que proveen los algoritmos publicados es el beneficio del escrutinio al que son sometidos por investigadores y otros buscadores para encontrar los caminos para mejorarlos o romper los algoritmos. Los expertos mejor entrenados examinan un algoritmo haciendo menos probables los ataques más obvios.

Los algoritmos y protocolos de seguridad son muy difíciles de diseñar debido a que hay muchos modos diferentes de atacarlos y los diseñadores no pueden siempre

imaginar todos ellos. Aunque las organizaciones de seguridad nacional tanto como las corporaciones pueden tener sus propios códigos “top-secret”, los secretos son difíciles de guardar. Espías y otros criminales son bien conocidos por sus habilidades de motivar (a través de la fuerza, extorsión u otros medios) a la gente que sabe los secretos para que los comparta con ellos.

En seguridad la predominante sabiduría dice que un buen algoritmo de encriptación o autenticación debe ser seguro aún si los atacantes saben qué algoritmo está siendo usado. Esto es particularmente importante para la seguridad de Internet, desde que un atacante con un sniffer puede ser capaz de determinar exactamente qué tipo de algoritmo está siendo usado escuchando como los sistemas negocian sus conexiones.

Entre las más importantes tipos de funciones de criptografía están:

Encriptación simétrica

Encriptación de clave pública

Intercambio de clave

Hashes seguros

Firma digital

3.5.1 Encriptación simétrica

La mayoría de la gente tiene familiaridad con la encriptación simétrica en un nivel muy intuitivo, textos planos son encriptados con una clave secreta y un conjunto de procedimientos y luego son desencriptados con la misma clave y el mismo conjunto

de procedimientos. Si se tiene la clave, se puede desencriptar todos los datos que fueron encriptados con esa clave. Algunas veces conocido como “encriptación con clave secreta”, la encriptación simétrica es computacionalmente eficiente y es el tipo más frecuente de encriptación para transmisión en redes de volúmenes de datos.

En octubre del 2000 el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology -NIST) anunció que el algoritmo de encriptación de datos Rijndae, ha sido seleccionado como el estándar de cifrado en los Estados Unidos, reemplazando al estándar de encriptación de datos (DES), desarrollado originalmente en los años 70 por IBM.

Usar una encriptación segura requiere que las claves sean largas porque mientras más cortas son más vulnerables a ataques, en los que los intrusos usan una computadora para tratar con todas las claves posibles. Claves largas en el orden de los 40 bits, por ejemplo, son consideradas inseguras porque pueden ser rotas en poco tiempo por computadoras relativamente baratas, en general se consideran seguras en un futuro inmediato claves de 128 bits.

Los algoritmos de encriptación simétrica pueden ser vulnerables a otros tipos de ataque. La mayoría de las aplicaciones que usan encriptación simétrica para las comunicaciones en Internet usan claves de sesión, lo que significa que la clave es usada solo para la transmisión de datos de una sesión. Perder la clave de la sesión por lo tanto compromete solo los datos que fueron enviados en esa sesión o en una porción de la misma.

A continuación se describen brevemente algunos algoritmos de encriptación simétrica que están siendo actualmente usados por aplicaciones de Internet:

RC2/RC4: Este algoritmo de encriptación simétrica fue desarrollado y comercializado por la firma de criptografía RSA.

CAST: Desarrollado en Canadá y usado por Nortel's Entrust products, soporta claves sobre los 128bits.

IDEA: El Algoritmo Internacional de Encriptación de Datos (International Data Encryption Algorithm) soporta claves de 128 bits. Fue patentado por la firma Suiza Ascom, la cual garantiza permisos para que IDEA pueda ser usado libremente de forma no comercial en el programa de código abierto de encriptación Pretty Good Privacy (PGP – Privacidad bastante buena), escrito por Philip Zimmermann y publicado por un tiempo por la Asociación de Redes, Inc.

GOST Este algoritmo fue desarrollado por la agencia de seguridad Soviética.

Blowfish Este algoritmo fue desarrollado por Bruce Schneier y liberado al dominio público.

Twofish Este fue la presentación de Bruce Schneier para la competencia de la AES.

Skipjack Este algoritmo fue desarrollado por la Agencia Nacional de Seguridad de los Estados Unidos para ser usado en el sistema Clipper chip's escrowed key.

3.5.2 Encriptación de Clave Pública

La Encriptación de Clave Pública también llamada "Encriptación Asimétrica" usa pares de claves: una, la clave pública, es asociada con la otra, la clave secreta. La clave pública está destinada a ser pública, cualquier dato encriptado con ella puede ser solo desencriptada con la clave secreta y cualquier dato encriptado con la clave secreta puede ser descifrada con la clave pública.

Cualquiera puede obtener la clave pública y encriptar datos con ella. Esos datos pueden ser desencriptados solo por el titular de la clave secreta. Tanto como la entidad pueda guardar su clave como un secreto, otras entidades pueden estar seguras que cualquier dato encriptado con la clave pública será solo accesible al titular asociado con la clave secreta. El titular de clave secreta puede encriptar algo usando la clave secreta y hacerlo accesible para otra entidad, la cual puede verificar la primera entidad como propietaria de la clave secreta de su clave particular pública desencriptando los datos con esa clave.

La encriptación con clave pública tiende a ser computacionalmente intensa y es la mayoría de las veces usada para encriptar claves de sesión tanto para transmisiones de red como firmas digitales. El más comúnmente utilizado para encriptación de clave pública es el algoritmo RSA desarrollado por Ron Rivest, Adi Shamir, and Len Adleman. Define un mecanismo para escoger y generar el par de claves (secreta y pública) así como una función matemática actual usada para encriptación.

3.5.3 Key Management

Uno de los más complejos problemas de los profesionales de seguridad de Internet es cómo manejar las claves. Esto incluye no solo la actual distribución de claves a través del protocolo de intercambio de claves también la negociación de tamaños, tiempos de vida y algoritmos de criptografía entre los sistemas de comunicación.

Un canal abierto como el Internet global complica el proceso de compartir un secreto. Este proceso es necesario cuando dos entidades necesitan compartir una clave para ser usado para encriptación. Algunos de los más importantes algoritmos criptográficos se relacionan con el proceso de compartir claves sobre un canal abierto seguro de tal forma que guarde el secreto de todos menos de los destinatarios.

Diffie-Hellman key exchange es un algoritmo que permite a las entidades intercambiar suficiente información para obtener una clave de encriptado de sesión. Alice (el acostumbrado nombre de la entidad, para la primera entidad participante en el protocolo de criptografía) calcula un valor usando el valor público de Bob y su propio valor secreto (Bob es el segundo participante en el protocolo de criptografía). Bob calcula su propio valor y lo envía a Alice, cada uno de ellos pueden entonces usar sus valores secretos para calcular sus claves compartidas. La matemática es relativamente simple; el punto central es que Bob y Alice pueden enviarse suficiente información para calcular sus claves compartidas pero eso no sería suficiente para que un atacante sea capaz de descifrarla.

Diffie-Hellman es algunas veces llamado un algoritmo de clave pública, pero no es un algoritmo de encriptación de clave pública, es usado para calcular la clave, pero esa clave debe ser usada con algún otro algoritmo de encriptación. Puede ser usado para autenticación sin embargo es también usado por PGP. El intercambio de claves es integral para cualquier arquitectura de seguridad de Internet y candidatos para la arquitectura de IPsec incluye el protocolo IKE (Internet Key Exchange-Intercambio de clave de Internet) y ISAKMP (Internet Security Association and Key Management Protocol-Asociación de seguridad de Internet y Protocolo de Administración de clave).

ISAKMP es un protocolo de aplicación que esa UDP como su transporte, lo cual define diferentes tipos de mensajes que los sistemas pueden enviarse entre ellos para negociar el intercambio de claves. Los mecanismos y algoritmos para hacer los actuales intercambios sin embargo no están definidos en ISAKMP –este es un marco para ser usado por mecanismos específicos. Los mecanismos, a menudo basados en el intercambio de claves de Diffie-Hellman, han sido definidos en un número de diferentes propósitos a través de los años. Algunos de ellos son: Photuris, SKIP, OAKLEY.

3.5.4 Secure Hashes

Un hash es un resumen digital de un segmento de datos de cualquier tamaño. Tipos simples de hash incluyen chequear dígitos; hash seguros producen resultados largos (algunas veces 128 bits o mayores). Un buen Hash seguro hace extremadamente difícil realizar una ingeniería inversa o revertirlo por otros medios, pueden ser usados con claves o no, pero su propósito es un resumen digital de un mensaje que puede ser usado para verificar si algunos datos que han sido recibidos son los mismos que han sido enviados. El remitente calcula el hash e incluye el valor con los datos, el receptor calcula el hash en los datos recibidos. Si el resultado coincide con el valor hash adjunto el receptor puede confiar de la integridad de los datos.

3.5.5 Firmas digitales

La encriptación de clave pública como se vio anteriormente se basa en pares de claves. Las Firmas digitales dependen de la propiedad de la encriptación de clave pública que permiten a los datos ser encriptados con la clave secreta de la entidad y ser desencriptados con su correspondiente clave pública. El remitente calcula un hash seguro sobre los datos a ser firmados y entonces encripta el resulta usando una clave secreta. El receptor calcula el mismo hash y entonces desencripta el valor adjunto encriptado por el remitente. Si los dos valores coinciden, el receptor sabe que el dueño de la clave pública fue la entidad que firma el mensaje y que el mensaje no fue modificado durante la transmisión.

El algoritmo de encriptación de clave pública RSA puede ser usado para firmas digitales: La entidad firmante crea un hash de los datos y entonces encripta ese hash con su propia clave secreta. La entidad certificada entonces calcula el mismo hash sobre los datos recibidos, desencripta la firma usando la clave pública de la entidad firmante y compara los dos valores. Si el hash es el mismo así como la firma desencriptada entonces los datos son certificados.

Las Firmas digitales traen algunas implicaciones:

Una firma que puede ser certificada indica que el mensaje fue recibido sin ninguna alteración desde el momento en que fue firmado hasta que fue recibido.

Si una firma no puede ser certificada, entonces el mensaje fue corrompido o manipulado dentro de la transmisión, la firma fue calculada incorrectamente, o la fue corrompida o manipulada en el transcurso. En cualquier caso, una firma no certificada no necesariamente implica algo mal hecho pero requiere que el mensaje sea refirmado y reenviado para ser aceptado.

Si una firma es certificada, esto significa que la entidad asociada con la clave pública es la única entidad que pudo haberla firmado. En otras palabras, la entidad asociada con la clave pública no puede negar que fue quien firmó el mensaje. Esto es llamado no repudiación y es una importante característica de las firmas digitales. Hay otros mecanismos para hacer firmas digitales, pero RSA es probablemente el más ampliamente usado, implementado y popular producto de Internet.

3.6 IP e IPsec

IPsec provee servicios de seguridad tanto para IPv4 como para IPv6, pero el modo de hacerlo es significantemente diferente para cada uno. Cuando se usa con IPv4, las cabeceras IPsec son insertadas después del encabezado IPv4 y después de la cabecera del protocolo de la siguiente capa. IPv6 simplifica ese proceso: cada cabecera de un paquete tiene la misma longitud, 40 octetos, pero cualquier opción puede ser acomodada en las cabeceras de extensión que siguen a la cabecera IPv6. El servicio IPsec es provisto a través de esas extensiones.

El orden de las cabeceras IPsec, ya sea IPv4 o IPv6, es importante. Por ejemplo esto tiene sentido para encriptar la carga útil con Encabezado ESP y entonces usar el Encabezado de Autenticación para proveer integridad de los datos en una carga útil encriptada. Revirtiendo el orden, haciendo integridad de los datos primero y entonces encriptando todo el lote, significa que se debe estar seguro de quién originó los datos pero no necesariamente de quien hizo la encriptación.

3.6.1 Security Associations

Las Asociaciones de Seguridad (SA) son un elemento fundamental de IPsec. El RFC 2401 define una SA como “una simple conexión que ofrece servicios de seguridad al tráfico que transporta”. Esta definición poco turbia se aclara con una descripción; una SA consta de tres cosas:

Un Indice de Parámetro de Seguridad (SPI)

Una dirección IP destino

Un identificador de protocolo de seguridad (AH or ESP)

Como una conexión simple, la SA asocia un solo destino con un SPI; por lo tanto, para un típico tráfico IP debe haber dos SAS: una en cada dirección que asegura el flujo de tráfico (una por cada host fuente y host destino).

Una SA provee servicios de seguridad usando AH o ESP pero no ambos (si un stream de tráfico usa ambos, debe tener dos o más SAS). El Indice de Parámetro de Seguridad (SPI) es un identificador que indica que tipo de encabezado IP la asociación de seguridad está usando (es decir AH o ESP). El SPI es un valor de 32 bits que identifica la SA diferenciándola de otras SAS enlazadas a la misma dirección de destino. Para una comunicación segura entre dos sistemas, debe haber dos diferentes asociaciones de seguridad, una para cada dirección destino. Cada asociación de seguridad incluye más información relacionada al tipo de seguridad negociada para esa conexión, así los sistemas deben guardar registro de sus SAS y el tipo de algoritmos de encriptación o autenticación, tamaño de las claves y tiempos de vida de las claves que deben hacer sido negociados con las SA de los host destino.

3.6.2 Usando las Asociaciones de Seguridad

Como se ha mencionado ISAKMP provee un protocolo generalizado para establecer SAs y administrar claves de encriptación dentro de un entorno de Internet. Los procedimientos y formatos de paquetes necesitan establecer, negociar, modificar y borrar SAs y están definidos dentro de ISAKMP, el cual también define cargas útiles para intercambio, generación y autenticación de datos. Estos formatos proveen un

marco consistente para transferir esos datos, independientemente de cómo la clave es generada o qué tipo de encriptación o autenticación está siendo usada.

ISAKMP fue diseñado para proveer un marco que puede ser usado por cualquier protocolo de seguridad que usa SAs, no solo IPsec. Para ser usado por un particular protocolo de seguridad un DOI (Dominio de Interpretación - Domain of Interpretation) debe ser definido. Un grupo de DOI debe estar relacionado con protocolos con el propósito de negociar asociaciones de seguridad – los protocolos de seguridad que comparte un DOI pueden escoger protocolos y transformaciones criptográficas desde un común nombre de espacio, tanto como la interpretación del contenido de la carga útil.

Mientras ISAKMP e IPsec DOI proveen un marco de autenticación e intercambio de claves, ISAKMP no define actualmente cómo estas funciones son llevadas a cabo. El protocolo IKE trabajando dentro del marco definido por ISAKMP define los mecanismos para los host que ejecutan estos intercambios.

El host que envía la información sabe qué tipo de seguridad aplicar al paquete chequeando en la SPD (Base de datos de Políticas de Seguridad - Security Policy Database), además puede determinar qué política de seguridad es apropiada para el paquete, dependiendo de varias selecciones (por ejemplo, dirección IP destino y /o puertos de la capa de transporte). La SPD indica que política es conveniente para un paquete particular; es decir si es procesado por el módulo de IPsec o es simplemente pasado a través de un proceso normal IP. Si los paquetes llegan a la red la SPD es chequeada para ver qué tipo de servicio de IPsec está presente en dichos paquetes.

Otra base de datos llamada SAD (Base de datos de Asociaciones de seguridad - Security Association Database, incluye todos los parámetros de seguridad asociados con las SAs activas. Cuando un host IPsec necesita enviar un paquete este chequea los selectores apropiados para ver que dice en la SAD acerca de las políticas de seguridad para ese destino/puerto/aplicación. La SAD puede referenciar una SA particular, para que el host pueda buscar la SA para identificar los parámetros de seguridades asociados para el paquete.

3.6.3. Modos en IPsec.

IPsec define dos modos para el intercambio seguro de la información: túnel y transporte. En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red o comunicaciones ordenador a red u ordenador a ordenador sobre Internet. En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

3.6.3.1 Modo Transporte

En la figura 3.2 se muestra un esquema en el cual se puede observar dos hosts en cada uno de los cuales está implementado IPSec que es lo que se necesita para que IPSec funcione en modo transporte, además se tiene dos routers con firewall con lo que se genera un conjunto que garantiza seguridad extremo a extremo.

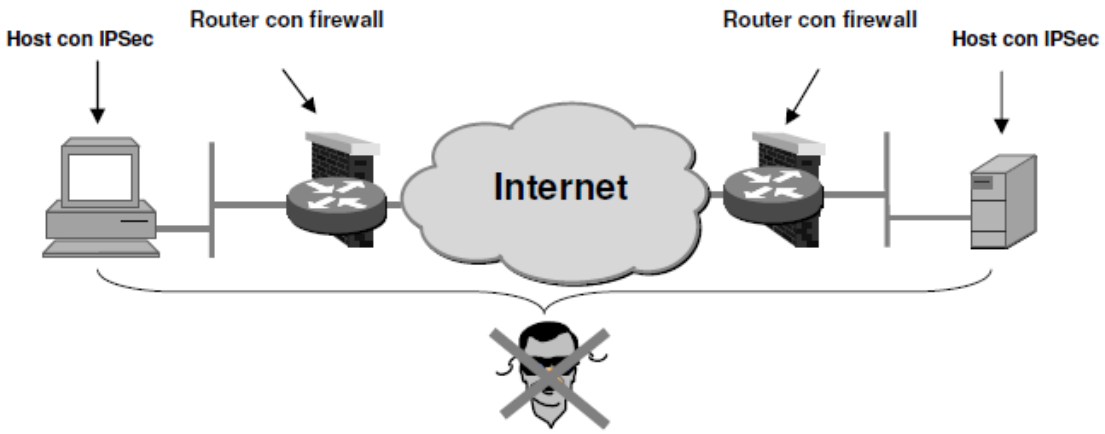


Figura 3.2: IPSec en Modo Transporte

El Modo transporte protege los protocolos de las capas superiores y es usado entre extremos de nodos. Este enfoque permite seguridad extremo a extremo porque los host que originan los paquetes son también seguros y el host destino es capaz de verificar la seguridad ya sea desencriptando el paquete o certificando la autenticación.

El modo transporte es bueno para dos host individuales que desean comunicarse de manera segura; el modo túnel es el fundamento de las redes privadas virtuales (VPN).

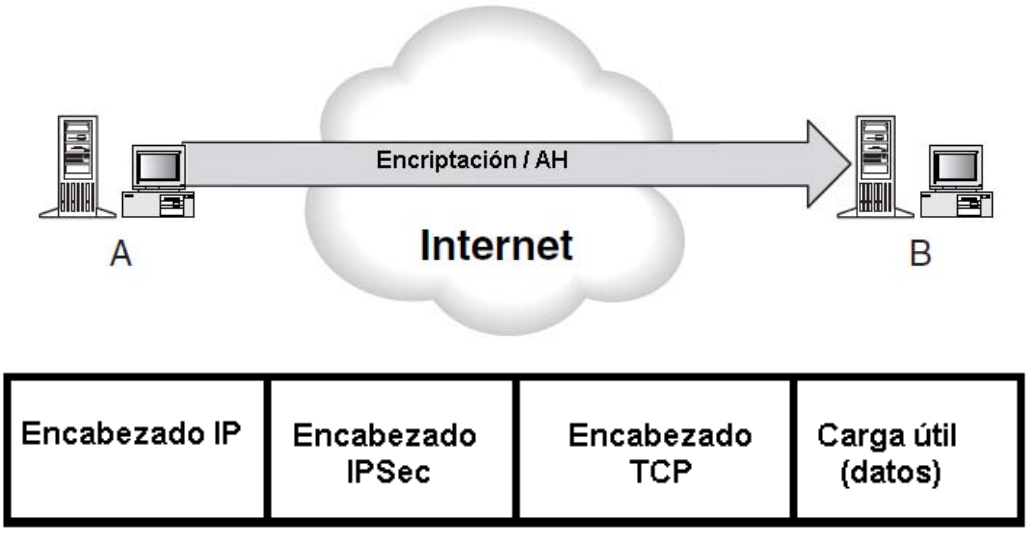


Figura 3.3: Modo Transporte

En modo transporte el contenido que se envía dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

3.6.3.2 Modo Túnel

El modo túnel protege el contenido completo del paquete. Los paquetes del túnel son aceptados por un sistema actuando como una puerta de enlace de seguridad, encapsulando dentro un conjunto de encabezado IP/IPsec, y reenviando al otro extremo del túnel, donde los paquetes originales son extraídos (después de que han sido desencriptados o certificados) y entonces se pasan a su destino final. Los paquetes son seguros siempre y cuando están dentro del túnel.

El modo túnel podría requerir en cualquier momento una puerta de enlace segura (un dispositivo ofreciendo servicios de IPsec a otros sistemas) que esté envuelto en cada extremo de una transmisión IPsec. Dos puertas de enlace seguras pueden siempre comunicarse por túneles, enviando paquetes IP dentro de paquetes IPsec; lo mismo sucede con un host individual al comunicarse con una puerta de enlace segura.

El la figura 3.4 se muestra un esquema en el cual se tiene dos hosts así como dos routers, donde para que funcione IPSec en modo túnel, se tiene que implementar en ambos routers los cuales ejecutan un túnel de seguridad. Este modo de funcionamiento de IPSec permite incorporarlo sin tener que modificar los hosts.

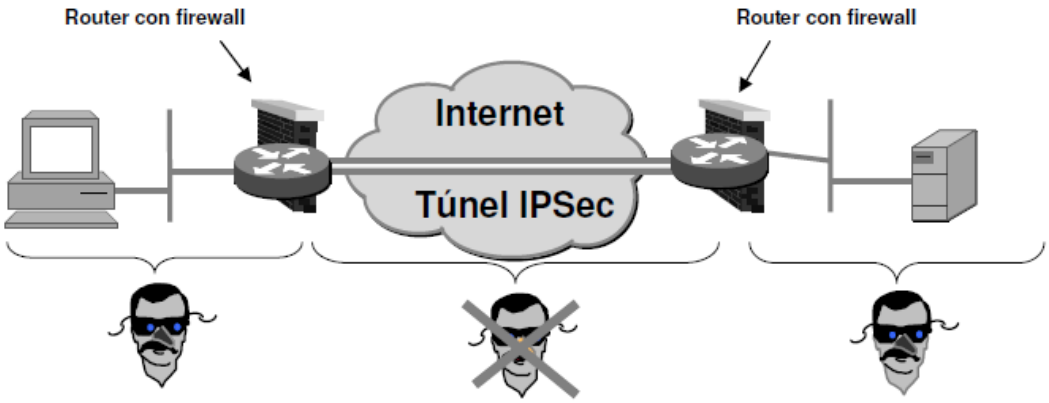


Figura 3.4: IPsec en Modo Túnel

El modo de túnel IPSec se utiliza para proteger el tráfico entre redes diferentes, cuando el tráfico debe pasar a través de una red intermedia que no es de confianza. El modo de túnel se utiliza principalmente para la interoperabilidad con puertas de enlace o sistemas finales que no admiten conexiones L2TP/IPSec o PPTP. Puede emplear el modo de túnel en las configuraciones siguientes:

- Puerta de enlace a puerta de enlace
- Servidor a puerta de enlace
- Servidor a servidor

El túnel que se ve en la figura 3.4 permite a dos sistemas setear las SAs para habilitar una comunicación segura sobre Internet. El tráfico de red que se origina en un sistema es encriptado o firmado y entonces es enviado al sistema de destino. En el receptor el datagrama es descifrado o autenticado y la carga útil es pasada a través de la pila de la red del sistema receptor donde finalmente es procesada por una aplicación usando datos. Este es un modo transparente de uso de asociaciones de seguridad, porque los dos host pueden comunicarse tan fácilmente como si no hubiera cabeceras de seguridad debido a que las actuales cabeceras IP de los datagramas deben ser descubiertas para permitir ser ruteadas a través de Internet.

Una SA también puede ser usada para pasar IP seguras a través de un túnel en una red interna. La figura 3.5 muestra cómo funciona esto. Todos los paquetes IP desde el sistema A son enviadas a la puerta de enlace segura X, lo cual crea un túnel IP a través del internet hacia la puerta de enlace segura Y la cual descubre los paquetes enviados y los reenvía. La puerta de enlace segura Y puede enviar los paquetes a cualquier host (B, C o D) dentro de su propia intranet local o los podría enviar a un host externo como M. Todo este depende de a donde el host original dirigió el paquete. Siempre que un nodo destino de SA es una puerta de enlace segura es por definición una asociación de túnel, en otras palabras un túnel puede ser hecho entre dos puertas de enlace seguras o puede ser hecha entre un nodo regular y una puerta de enlace segura. Por lo tanto el host M podría crear una conexión de túnel con las puertas de enlace seguras X o Y. Este es tuneleado en virtud de que los

datagramas enviados desde M han pasado primero por la puerta de enlace la cual entonces la reenvía apropiadamente después de desencriptar o autenticar.

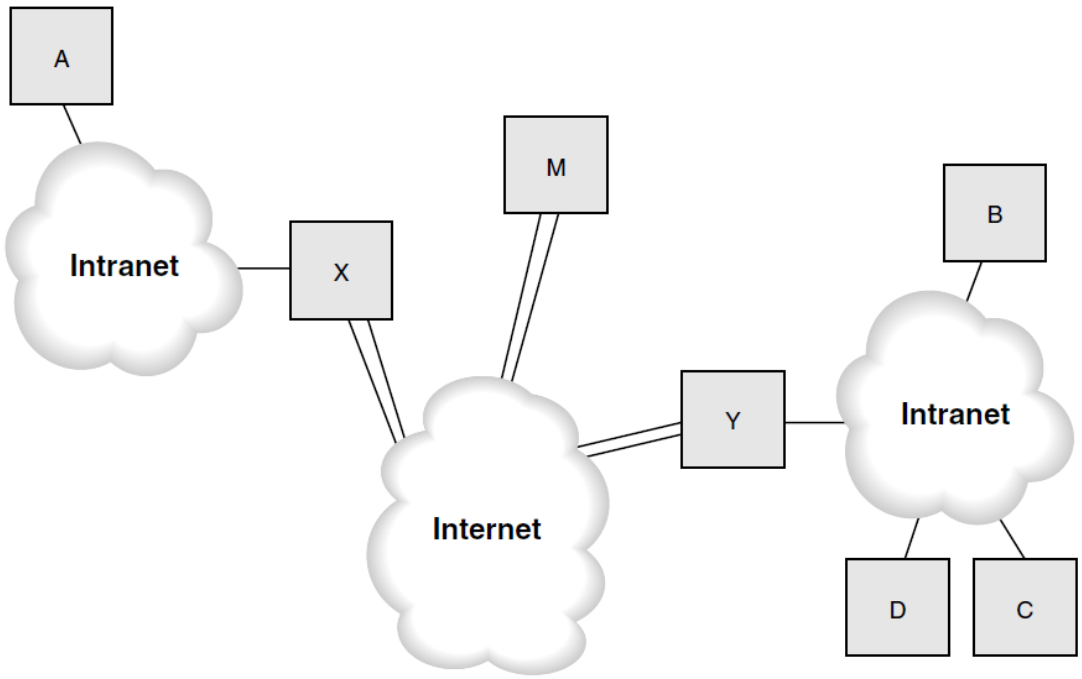


Figura 3.5: Dos host utilizando IPsec para comunicarse transparentemente a través de Internet

3.6.3.3 ESP (Encapsulating Security Payload)

La cabecera ESP está diseñada para proporcionar una combinación de servicios de seguridad en IPv4 e IPv6. El ESP se puede aplicar solo, en combinación con el AH, o de forma anidada. Los servicios de seguridad se pueden proporcionar entre un par de hosts en comunicación, entre un par de gateways de seguridad o entre un gateway de seguridad y un host. La cabecera ESP se inserta después de la cabecera IP y antes de la cabecera del protocolo de capa superior (modo transporte), o antes de una cabecera IP encapsulada (modo túnel). El protocolo ESP puede ser utilizado para proporcionar confidencialidad, autenticación del origen de los datos, integridad

sin conexión, un servicio anti-replay (una forma de integridad parcial de la secuencia) y confidencialidad (limitada) del flujo de tráfico. Por ejemplo, se puede ocultar la longitud del paquete, y así facilitar la eficiente generación y descarte de paquetes falsos. El conjunto de servicios depende de las opciones seleccionadas en el momento del establecimiento de la SA y la ubicación de la aplicación en una topología de red.

El ESP permite utilizar sólo cifrado para proporcionar confidencialidad. Sin embargo, cabe señalar que, en general, esto únicamente proporcionará defensa contra los atacantes pasivos. Utilizar el cifrado sin un mecanismo fuerte de integridad en la parte superior de este (ya sea con el ESP o por separado, a través del AH) puede hacer inseguro el servicio de confidencialidad ante algunas formas de ataque activo. Por otra parte, un servicio de integridad subyacente, como el AH, aplicado antes del cifrado no necesariamente lo protege contra los atacantes activos. El ESP permite el cifrado solo porque este puede ofrecer un rendimiento mucho mejor y todavía proporcionar una adecuada seguridad. Sin embargo, este estándar no exige que las implementaciones del ESP ofrezcan un servicio decifrado solo, ya que no es lo que más se suele usar.

La integridad sola en ESP debe ofrecerse como un servicio de selección opcional, por ejemplo, debe ser negociable en los protocolos de gestión de SAs, y debe ser configurable a través de interfaces de gestión. Se trata de una atractiva alternativa al AH en muchos contextos, por ejemplo, porque el proceso es más rápido y más sensible a la canalización en muchas implementaciones. A pesar de que la confidencialidad e integridad pueden ser ofrecidas de forma independiente, el ESP suele emplear ambos servicios, es decir, los paquetes serán protegidos con respecto a estas dos. Así, hay tres posibles combinaciones deservicios de seguridad con el ESP que incluyen estos servicios: Sólo confidencialidad (puede ser soportado,

sólo integridad (debe ser soportado), confidencialidad e integridad (debe ser soportado). El servicio de anti-replay puede ser seleccionado para una SA sólo si el servicio de integridad está seleccionado para esa SA. La selección de este servicio es exclusivamente a discreción del receptor y por lo tanto no tiene que ser negociado. Sin embargo, para hacer uso de la función de Número de Secuencia Extendido de una forma interoperable, el ESP obliga a los protocolos de gestión de SAs que sean capaces de negociar esta función.

El servicio de Confidencialidad del Flujo de Tráfico (TFC), generalmente, es eficaz sólo si el ESP es empleado de manera que oculte las direcciones de origen y destino finales de los peers y suficientes flujos de tráfico entre ellos (ya sea de forma natural o como resultado de la generación de tráfico de enmascaramiento) ocultan las características específicas, los flujos de tráfico de suscriptores individuales. El ESP puede ser empleado como parte de un sistema TFC de capa superior. Nuevas características TFC presentes en el ESP facilitan la eficiente generación y descarte de tráfico ficticio y mejor carga del tráfico real, de manera compatible con versiones anteriores. La cabecera del protocolo IP que precede inmediatamente a la cabecera ESP deberá contener el valor 50 en el campo Protocol (IPv4) o Next Header (IPv6, IPv6 Extensión). La figura 3.6 ilustra el formato de la cabecera ESP utilizando autenticación y sin utilizarla.

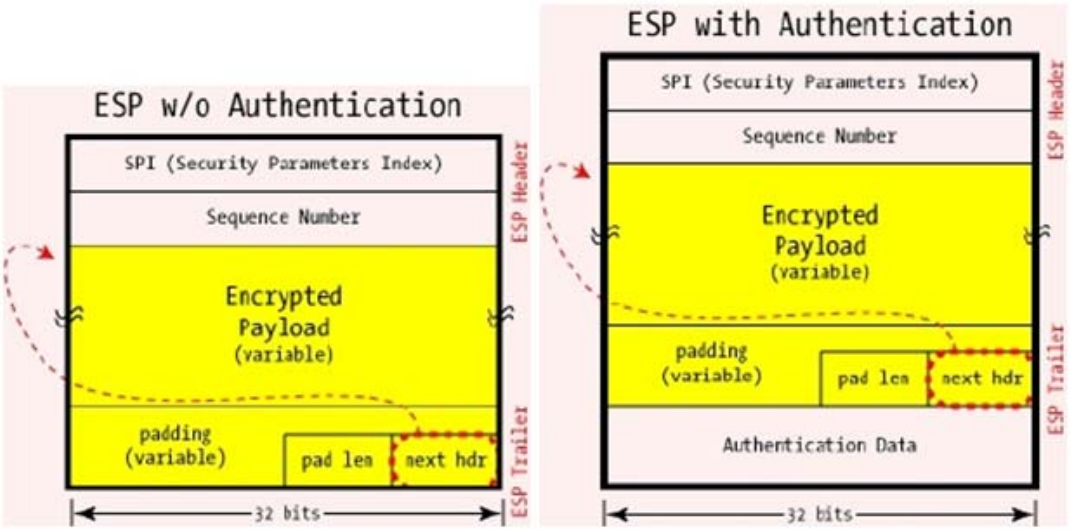


Figura 3.6: Paquete ESP con y sin autenticación

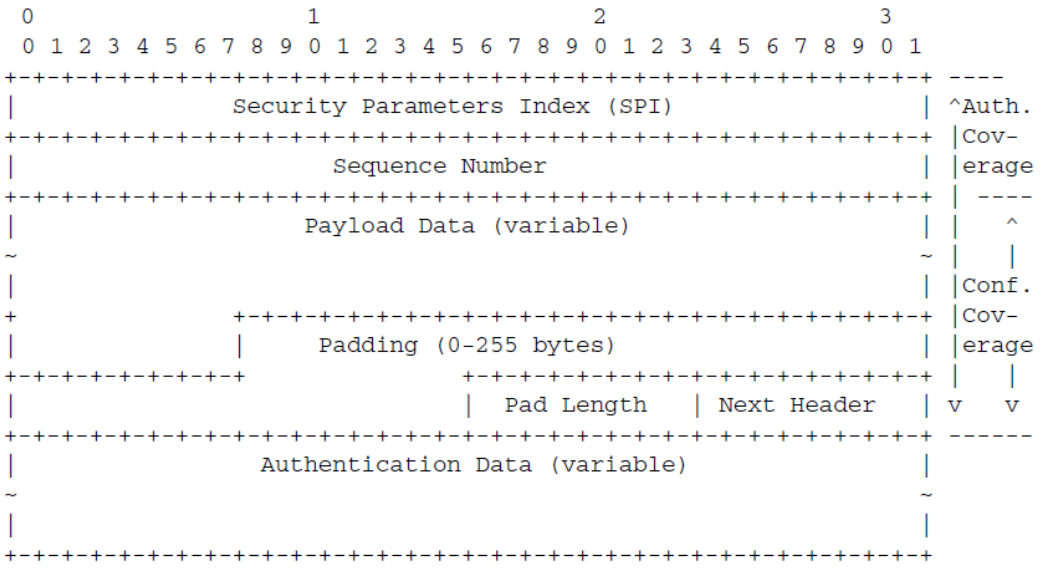


Figura 3.7: Cabecera ESP

La cabecera ESP consiste de lo siguiente:

Security parameters index (SPI)

Identifica los parámetros de seguridad en combinación con la dirección IP. Este valor es usado para la comunicación entre nodos referente a una asociación de

seguridad el cual puede ser usado para determinar cómo los datos pueden ser encriptados.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición. Este valor es siempre puesto en cero y se incrementa en uno con cada datagrama enviado.

Payload data

Los datos a transferir. Este es un campo de tamaño variable y contiene una porción del datagrama encriptado junto con datos suplementarios necesarios para el algoritmo de encriptación. El campo Payload comienza con un vector de inicialización, un valor que debe ser enviado en texto plano; los algoritmos de encriptación necesitan este valor para desencriptar los datos protegidos.

Padding

Usado por algunos algoritmos criptográficos para rellenar por completo los bloques. La porción encriptada de la cabecera (la carga útil) debe terminar en un límite asignado asi que a veces un relleno puede ser necesario.

Pad length

Tamaño del relleno en bytes. Este campo indica cuanto relleno debe ser añadido a la carga útil.

Next header

Identifica el protocolo de los datos transferidos. Este campo trabaja como normalmente lo hacen otras cabeceras de extensión de IPv6; solo aparece cerca del final de la cabecera (donde se le puede dar protección de confidencialidad) antes

que al comienzo de esta forma el protocolo de la siguiente capa puede esconderlo de terceras partes no autorizadas.

Authentication data

Contiene los datos utilizados para autenticar el paquete. Este es el ICV (Valor de chequeo de integridad) calculado sobre la cabecera ESP entera (excepto por los datos de autenticación). Este cálculo de autenticación es opcional.

3.6.3.4 Cabecera de autentificación (AH - Authentication Header)

La Cabecera de Autenticación IP (AH) se utiliza para proporcionar integridad sin conexión y autenticación del origen de los datos para datagramas IP (en lo sucesivo simplemente como integridad, ya que el cálculo realizado sobre el paquete proporciona directamente la integridad sin conexión e indirectamente la autenticación del origen de los datos como resultado del enlace realizado para obtener la clave utilizada para verificar la integridad de la identidad del peer IP-sec. Típicamente, este enlace se realiza mediante el uso de una clave compartida, simétrica y para proporcionar protección contra repeticiones.

El servicio anti-replay puede ser seleccionado opcionalmente por el receptor cuando se establece una SA (el protocolo, por defecto, requiere que el emisor incremente el número de secuencia utilizado para el antireplay, pero el servicio sólo es efectivo si el receptor comprueba el número de secuencia). El AH proporciona autenticación para tantos campos de la cabecera IP como sea posible, así como para los datos del protocolo de la capa superior. Sin embargo, algunos campos de cabecera IP pueden cambiar su valor en tránsito y el emisor no puede predecir cuál será cuando llegue

al receptor. Los valores de tales campos no pueden ser protegidos por el AH. Así, la protección prevista para el encabezado IP es por partes.

El AH se puede aplicar solo, en combinación con el ESP, o de forma anidada. Los servicios de seguridad se pueden proporcionar entre un par de Hosts en comunicación, entre un par de gateways de seguridad, o entre un gateway de seguridady un host. El ESP se puede utilizar para proporcionar el mismo anti-replay y servicios de integridad similares, además proporciona servicios de confidencialidad (cifrado). La principal diferencia entre la integridad que ofrece el ESP y la que ofrece el AH es la extensión de la cobertura. En concreto, el ESP no protege los campos de la cabecera IP, a menos que éstos sean encapsulados, por ejemplo, mediante el uso del modo de túnel. La figura 3.8 ilustra el formato de la cabecera AH. La cabecera del protocolo inmediatamente anterior a la cabecera AH (cabecera IP) contendrá el valor 51 en su campo Protocol (IPv4) o Next Header (IPv6,IPv6 Extension).

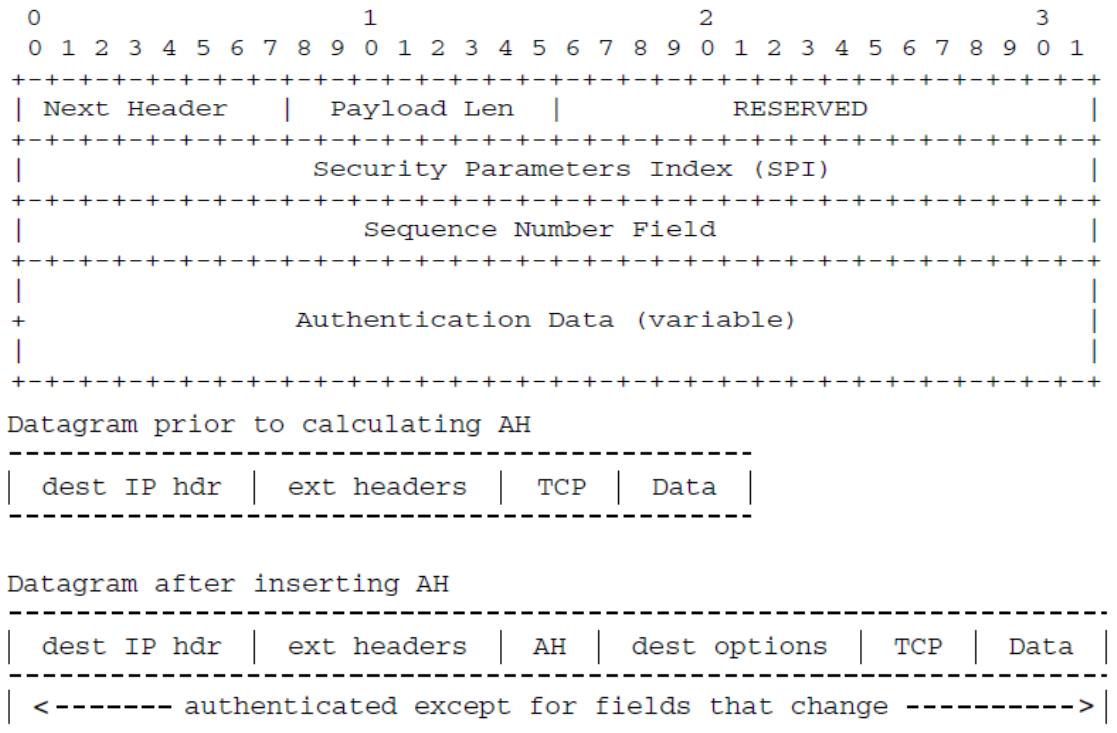


Figura 3.6: Añadiendo una Cabecera de Autenticación a un datagrama IP en modo transporte

Los campos de la cabecera AH incluyen lo siguiente:

Next header

Identifica el protocolo de los datos transferidos.

Payload length

Este campo de 8 bits indica la longitud de la Authentication Header en unidades de palabras de 32 bits, menos 2. Como originalmente fue definida, la AH consistía en 64 bits de cabecera, con el resto dedicada a la autenticación de datos. Por lo tanto la longitud de la carga útil meramente indica (en palabras de 32 bits) la longitud de los datos de autenticación. Con la adición del campo Sequence Number este valor es ahora igual a la longitud de de los datos de autenticación más la longitud del campo Sequence Number.

Reserved

Reservado para uso futuro (hasta entonces todo ceros).

Security parameters index (SPI)

Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete. Este valor de 32 bits es un valor arbitrario. Un valor SPI de cero indica que es para uso local solamente y que podría nunca ser transmitido; valores entre 1 y 255 son reservados por la IANA para uso futuro.

Sequence number

Un número siempre creciente, utilizado para evitar ataques de repetición. Este valor de de 32 bits es un contador obligatorio y es también incluido por el remitente, aunque este no siempre vaya a ser usado por el destinatario. Comenzando en cero,

este contador se incrementa con cada datagrama enviado lo que evita posibles ataques de repetición. Cuando el destinatario lo está usando para estos propósitos este descartará cualquier datagrama que duplique una secuencia de número que ya haya sido recibido. Esto significa que cuando el contador está listo para reiniciarse (cuando 2^{32} datagramas han sido recibidos) una nueva asociación de seguridad debe ser negociada de lo contrario el sistema del destinatario descartará todos los datagramas una vez que el contador se resetea.

Authentication Data

Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno. El contenido debe ser múltiplo de 32 bits en longitud.

3.6.3.5 IPsec Modo Transporte ESP

ESP se inserta después de la cabecera IP, y antes del protocolo de capa superior (TCP, UDP, ICMP) o antes de cualquier cabecera propia de IPSec que ya se haya incluido, la figura 3.9 describe ESP en modo trasporte para IPv6.

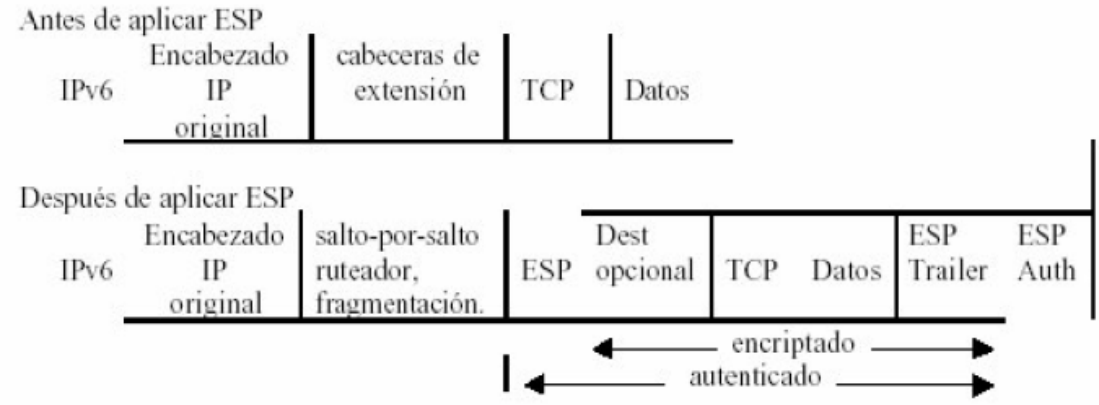


Figura 3.9: ESP en Modo Trasporte en IPv6

3.6.3.6 IPsec Modo Túnel ESP

En éste modo la cabecera interna posee el origen y destino finales, mientras que la cabecera interna posee direcciones distintas (las de las puertas de enlace). ESP protege a toda la cabecera interna, incluida la totalidad de la Cabecera IP interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transferencia. La figura 41 describe ESP en modo túnel para ipv6.

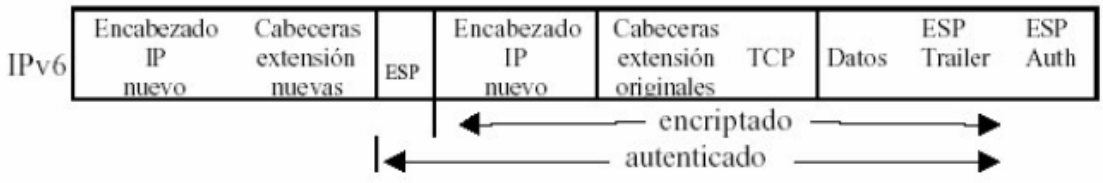


Figura 3.10: ESP en Modo Túnel en IPv6

3.6.3.7 IPsec Modo Transporte AH

AH se inserta después de la cabecera IP, y antes del protocolo de capa superior (TCP, UDP, ICMP, etc) o antes de cualquier cabecera propia de IPSec que ya se haya incluido. La figura 3.11 describe AH en modo trasporte para IPv6.

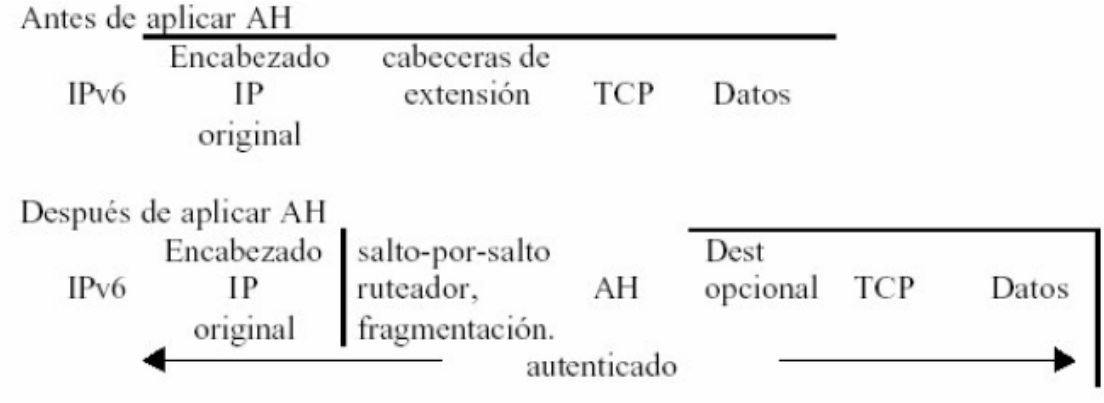


Figura 3.11: AH en Modo Trasporte en IPv6

3.6.3.8 IPsec Modo Túnel AH

En éste modo la cabecera interna posee el origen y destino finales, mientras que la cabecera interna posee direcciones distintas (las de las puertas de enlace). La cabecera AH protege a toda la cabecera interna, incluida la totalidad de la Cabecera IP interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transferencia. La figura 40 describe AH en modo túnel para ipv6.

Figura 3.12: AH en Modo Túnel en IPv6

3.7 Neighbor Discovery

En IPv6, los nodos (routers o hosts) de una red usan un nuevo protocolo denominado Neighbor Discovery (descubrimiento de vecinos) para determinar las direcciones de enlace de los nodos que residen en su mismo enlace (denominados vecinos) y para eliminar rápidamente los valores almacenados en caché que queden invalidados. Por tanto, son capaces de mantener un seguimiento sobre el estado de la conectividad con sus vecinos y detectar cambios en sus direcciones unicast link-local.

Este protocolo proporciona además un mecanismo a los hosts que les permite encontrar los routers que han de encaminar sus paquetes, por lo que, teniendo en

cuenta su facultad de seguimiento de estado del enlace, serán capaces de encontrar nuevas rutas ante fallos de enlaces o routers.

3.7.1 Formato del Mensaje Neighbor Discovery

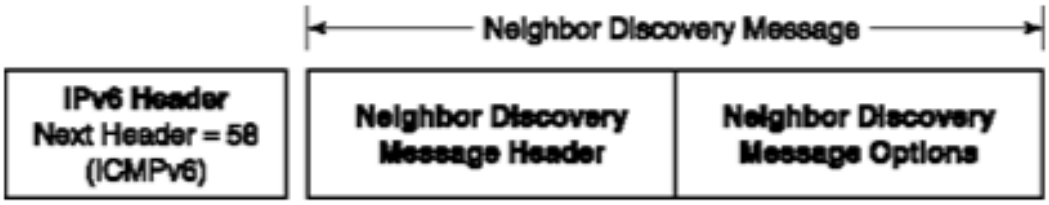


Figura 3.13: Formato de mensajes de Neighbor Discovery

Los mensajes ND usan la estructura de mensajes ICMPv6 y sus tipos del 133 al 137. Consiste de un encabezado ND, compuesto de una cabecera ICMPv6 y Mensajes ND específicos, cero o más opciones ND. La figura 3.13 muestra el formato del mensaje ND.

Las opciones de los mensajes proveen información adicional, indicando dirección MAC, prefijos de red on-link, información MTU on-link, redirección de datos, información de mobilidad y rutas específicas.

Para asegurarse de que los mensajes ND recibidos provienen de un nodo de la red local, todos los mensajes ND son enviados con un límite de saltos de 255. Cuando un mensaje ND es recibido, el campo de Hop Limit en la cabecera IPv6 es chequeado. Si este no está puesto dentro de 255 el mensaje es simplemente descartado. Verificar que los mensajes ND tienen un límite de 255 saltos provee protección contra ataques que son lanzados por nodos off-link. Con un límite de saltos de 255 un router no tiene que reenviar el mensaje ND a un off-link.

3.7.2 Direcciones utilizadas por Neighbor Discovery

Neighbor Discovery utiliza los siguientes tipos direcciones para ofrecer sus servicios:

All-nodes multicast address (FF02::1): Para comunicación con todos los nodos del enlace.

All-routers multicast address (FF02::2): Para mensajes dirigidos a todos los routers del enlace.

Solicited-node multicast address: Para referirse a un nodo en concreto.

Link-local unicast address: La dirección unicast que identifica cada interfaz.

Unspecified address (0::0): Utilizada como dirección de origen cuando aún no se posea ninguna

3.7.3 Terminología

on-link: Un destino se considera on-link cuando se encuentra en el mismo enlace y el prefijo de su dirección coincide con alguno de los definidos en el interfaz del origen. Además, los hosts considerarán un destino como on-link cuando un router se lo anuncie como siguiente salto sin realizar ninguna comprobación.

off-link: Lo contrario a on-link, es decir está fuera del enlace.

3.7.4 Funcionalidades

ND facilita la interacción entre los nodos unidos en un mismo enlace. Define para ello mecanismos que hacen uso de cinco nuevos paquetes recogidos en ICMPv6:

Solicitud de Router (Router Solicitation): Peticiones a los routers. Tienen el mensaje ICMPv6 tipo 133.

Aviso de Router (Router Advertisement): Enviado por los routers periódicamente y en respuesta un mensaje de Router Solicitation. El tiempo entre avisos periódicos debe ser suficientemente frecuente para que los hosts conozcan la presencia de los routers en unos pocos minutos, pero no es necesario que sean capaces de detectar fallos de los routers por la ausencia de estos paquetes. Tienen el mensaje ICMPv6 tipo 134.

Solicitud a Vecino (Neighbor Solicitation): Peticiones a los hosts. Tienen el mensaje ICMPv6 tipo 135.

Aviso de Vecino (Neighbor Advertisement): Se usa en respuesta a un mensaje de Neighbor Solicitation, o también cuando un nodo cambia su dirección de enlace, en cuyo caso enviará los avisos inmediatamente sin esperar a que le sean solicitados. Tienen el mensaje ICMPv6 tipo 136.

Redirección (Redirect): Utilizados por los routers para informar de mejores rutas a los hosts. El siguiente salto proporcionado por estos paquetes será considerado automáticamente como un destino on-link por parte de los nodos. Tienen el mensaje ICMPv6 tipo 137.

Algunas de las funcionalidades cubiertas por este protocolo son:

Descubrimiento de los routers vecinos por parte de los hosts

Cuando un interfaz de un host es habilitado, este debe mandar mensajes de Router Solicitation para invocar inmediatamente mensajes de Router Advertisement provenientes de los routers del enlace. Estos mensajes contienen, entre otras cosas, información sobre los routers.

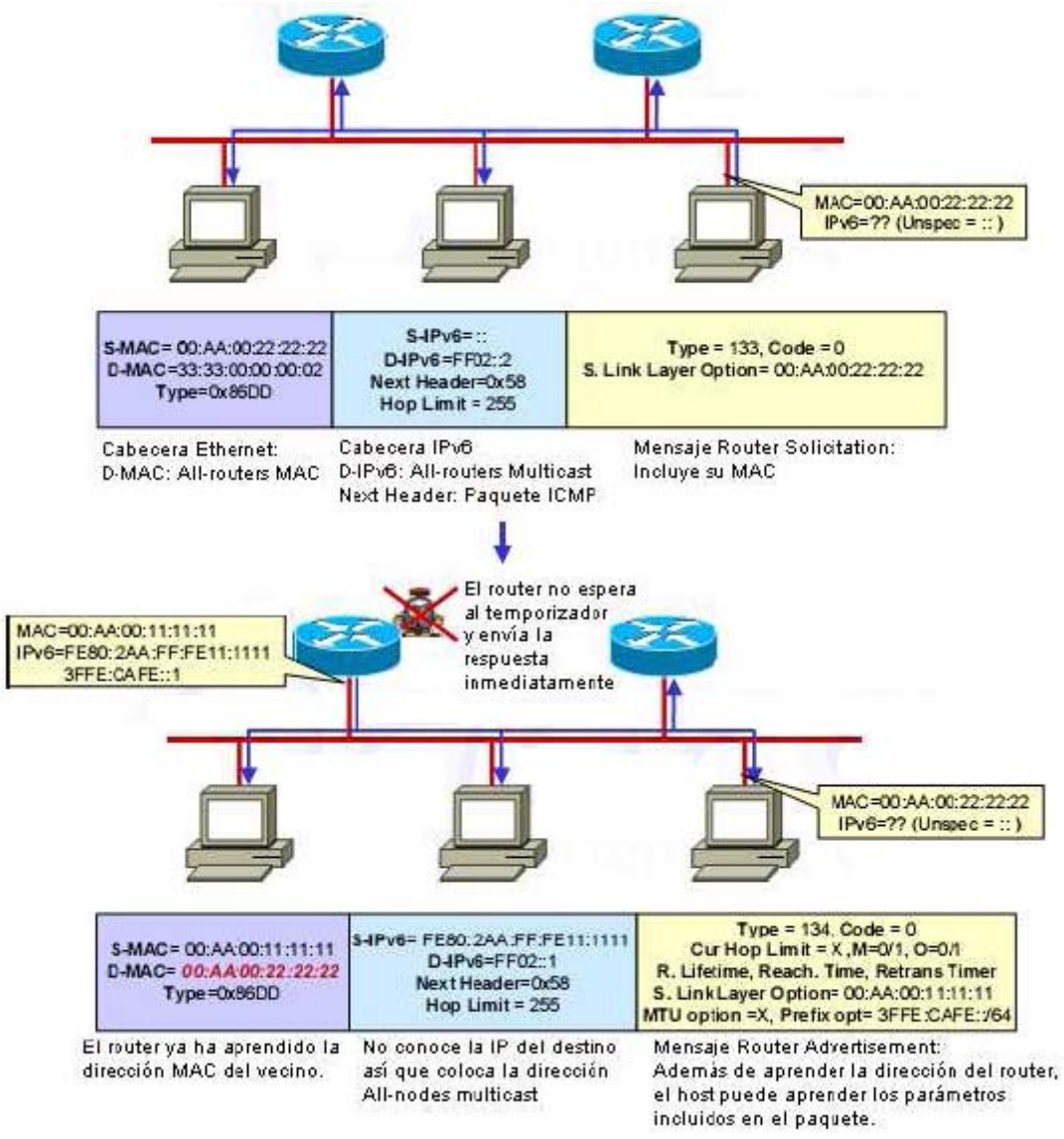


Figura 3.14: Descubrimiento de los routers vecinos por parte de los hosts

Descubrimiento del prefijo (dirección de la subred)

La información sobre el prefijo puede encontrarse también en los mensajes Router Advertisement (aunque opcionalmente los routers podrán optar por no anunciar uno, varios o todos los prefijos de la red). Con esta información, los nodos podrán diferenciar los destinos on-link de los off-link.

Figura 3.15: Descubrimiento del prefijo de red

Descubrimiento de parámetros de enlace (MTU, etc.) o de Internet (Hop-Limit, etc.)

Estos parámetros se encuentran también en los paquetes Router Advertisement repartidos por los routers. Este mecanismo facilita la administración centralizada de parámetros críticos, que pueden ser configurados en routers y, automáticamente, propagados al resto de hosts pertenecientes al enlace. A partir de esta información los hosts fijarán los parámetros de sus paquetes salientes.

Figura 3.16: Descubrimiento de parámetros de enlace

Autoconfiguración de dirección de los interfaces de los nodos

Los paquetes Router Advertisement servirán también a los routers para informar a los hosts sobre cómo llevar a cabo la autoconfiguración de dirección. Por ejemplo, los routers pueden especificar si los hosts deberán usar una configuración de dirección stateful (DHCPv6) o stateless.

Resolución de la dirección de enlace de los vecinos a partir de su dirección IP

Los nodos aprenden la dirección de enlace de un vecino mandando un mensaje Neighbor Solicitation a la dirección solicited-node multicast (construida a partir de la dirección unicast) del destino. El nodo destino devolverá su dirección a través de un mensaje unicast de Neighbor Advertisement, y en una sola comunicación petición-respuesta, ambos (origen y destino) resolverán la dirección de enlace del otro, ya que el nodo origen incluye en su mensaje de Neighbor Solicitation su propia dirección de enlace. Se puede ver que el funcionamiento es parecido a ARP en IPv4.

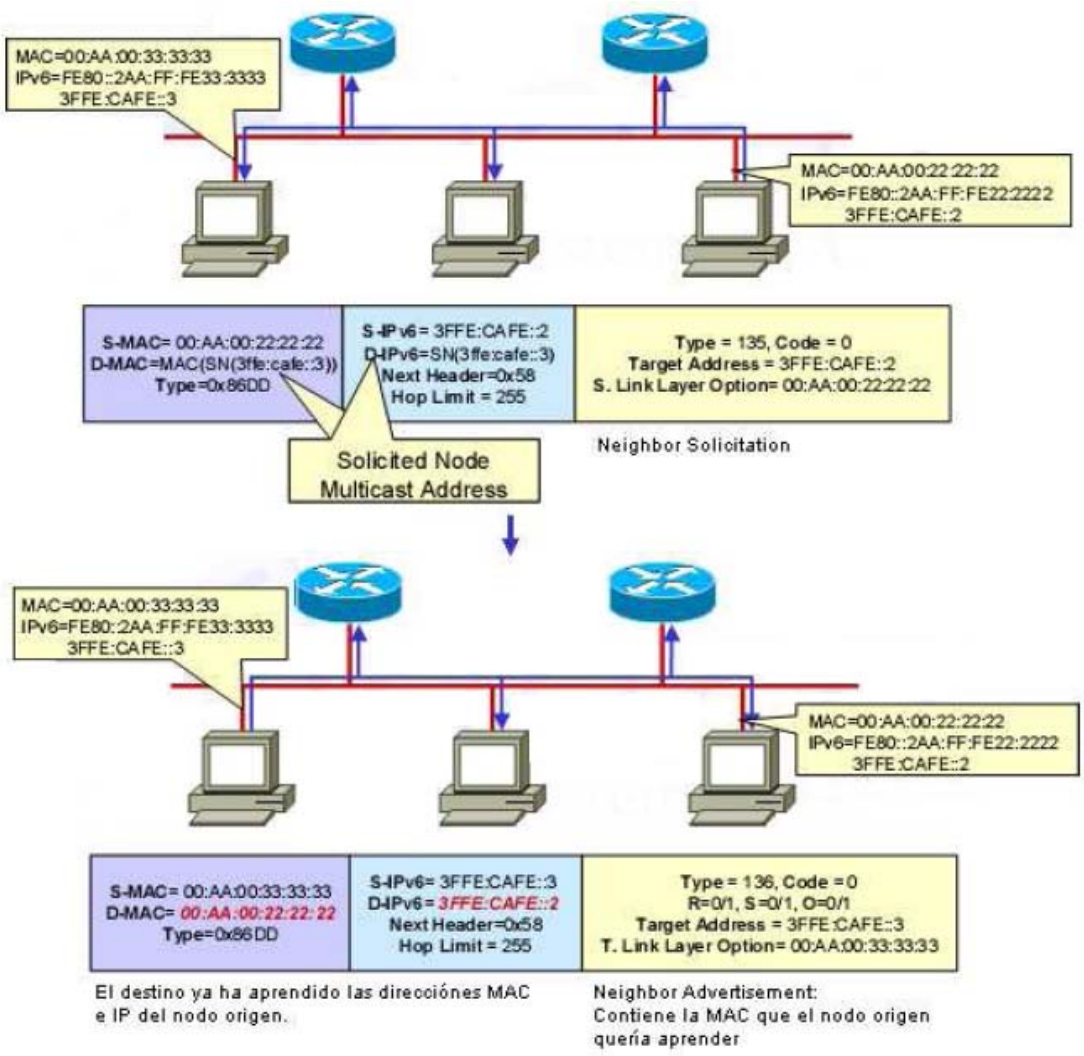


Figura 3.17: Resolución de la dirección de enlace de los vecinos a partir de su dirección IP

Construcción de una tabla de siguiente salto que mapee las direcciones IP de los destinos con las de los vecinos hacia los que enviar el tráfico

Los mensajes Router Advertisement contendrán prefijos con los que el nodo será capaz de discernir si el destino se encuentra en su mismo enlace y así mapear en la tabla el destino como siguiente salto. Además, gracias a estos mismos mensajes, el nodo será capaz de guardar una relación de los routers a los que dirigir cada uno de los distintos destinos a los que no tenga conectividad directa.

Detección de vecinos inalcanzables.

El algoritmo “Neighbor Unreachability Detection” proporciona un mecanismo de detección de fallos en los vecinos o en los caminos hacia ellos. Esto requiere confirmación de los paquetes enviados a los vecinos para asegurar que llegan y se procesan correctamente. Este mecanismo utiliza dos tipos de confirmación: si es posible, obtiene la confirmación de protocolos de capas superiores que sepan que los datos enviados anteriormente han sido entregados correctamente (por ejemplo si se han recibido confirmaciones recientemente). Si esto no es posible, el nodo envía un mensaje de Neighbor Solicitation (a la dirección unicast almacenada en caché) para obtener un Neighbor Advertisement que confirme que el siguiente salto está activo.

Para no llenar la red con tráfico innecesario, estos mensajes de prueba son enviados solamente a vecinos con los cuales el nodo tiene una comunicación frecuente. En caso de que un router quede inalcanzable el nodo tratará de elegir una nueva ruta, y en caso de que sea un host el que quede inalcanzable, se procederá a una nueva resolución de dirección de enlace (por si el destino hubiera cambiado su dirección de enlace).

Detección de direcciones duplicadas

Los nodos son capaces de evitar la utilización de una dirección ya en uso en la autoconfiguración de dirección de su interfaz. Se envía para ello un mensaje de Neighbor Solicitation y si nadie lo responde, el nodo asumirá que la dirección que desea colocar en su interfaz no está ocupada.

Redirección de los paquetes provenientes de un nodo hacia otro mejor primer salto.

Los routers utilizan mensajes de Redirect para avisar a los hosts sobre mejores primeros saltos hacia un determinado destino. Además, puede darse el caso en que un nodo del enlace no quede “cubierto” por ninguno de los prefijos anunciados por los routers, de manera que será considerado por el resto de nodos como un destino offlink. En este caso, los routers podrán enviar paquetes de redirección para informar a los nodos que intenten comunicar con este de que se trata de un destino on-link.

Actualización de direcciones inválidas

Un nodo cuya dirección de enlace haya sido cambiada puede enviar a la dirección all-nodes multicast unos pocos paquetes de Aviso de Vecino (no solicitados por ningún otro vecino de la red) para actualizar rápidamente la dirección de enlace inválida en la caché del vecindario. Sin embargo, esto es tan solo un funcionamiento añadido que no asegura que todos los vecinos actualicen su caché. El algoritmo “Neighbor Unreachability Detection” será el encargado de asegurar que todos los nodos descubran la nueva dirección, aunque el retardo será algo mayor.

3.7.5 Estructuras de datos en los hosts

Cada host deberá mantener en memoria ciertos datos para interactuar con los nodos vecinos:

Caché de vecinos. Una lista de los vecinos hacia los que se ha enviado tráfico recientemente. Para cada vecino se guarda información sobre su dirección unicast link-local, una flag para distinguir entre hosts y routers, etc. Contiene además información utilizada por el algoritmo “Neighbor Unreachability Detection”.

Caché de destinos. Una lista de los destinos a los que se ha enviado tráfico recientemente. Se almacenan tanto destinos on-link como off-link, mapeando cada dirección IP de destino junto con la dirección IP del siguiente salto (que podrá ser el propio destino).

Lista de Prefijos. Una lista generada a partir de los avisos de los routers contiene cada uno de los prefijos anunciados para el enlace junto con un tiempo de expiración. Una vez agotado el temporizador, el prefijo quedará invalidado. El valor del temporizador puede fijarse como "infinito" y permanecer así a no ser que se modifique con un posterior aviso de router.

Lista de Routers por defecto. Una lista de los routers hacia los que los paquetes pueden ser enviados. Esta lista está enlazada con la caché de vecinos. Cada entrada tendrá asociado un contador de expiración para borrar las entradas no anunciadas en un periodo largo de tiempo.

Dada esta información, el diagrama de estados para cada intento de transmisión por parte de un host, quedará como muestra la siguiente figura:

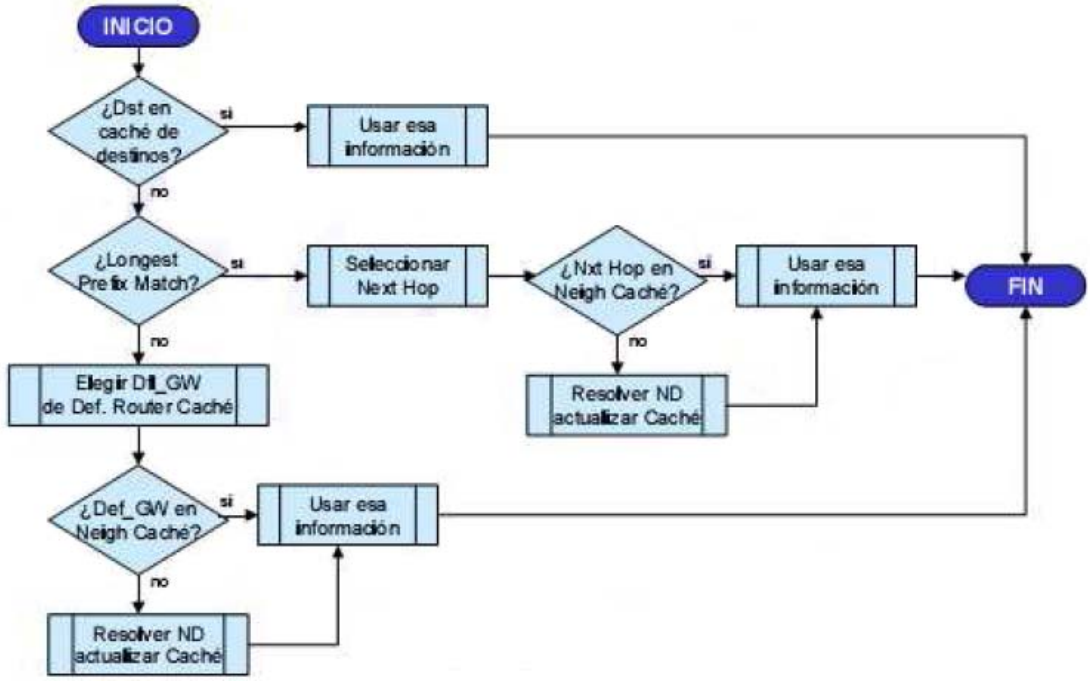


Figura 3.18: Diagrama de estados para cada intento de transmisión por parte de un host

3.7.4 Comparación con IPv4

El protocolo ND corresponde a una combinación de los protocolos de IPv4 ARP, ICMP(v4) Router Discovery (RDISC) e ICMP(v4) Redirect. De hecho, en IPv4 no existía un método estándar mediante el cual fijar mecanismos de detección de vecinos.

El protocolo ND provee multitud de mejoras con respecto al conjunto de protocolos utilizados para funciones parecidas en IPv4:

Router Discovery es parte del protocolo, por lo que no es necesario que los hosts tengan algún conocimiento de los protocolos de enrutamiento.

Los mensajes Router Advertisement contienen información acerca de sus direcciones de enlace, por lo que no son necesarios intercambios adicionales de paquetes para que el resto de nodos tengan conocimiento de estas.

La información sobre el prefijo del enlace que contienen estos mismos mensajes evita tener que implementar otros mecanismos para configurar las máscaras de la red.

Estos mensajes proporcionan también servicios de autoconfiguración de dirección.

Los routers pueden indicar la MTU a los hosts del enlace, asegurándose así de que todos los nodos usen el mismo valor en enlaces que no tengan una MTU bien definida.

Los mensajes Redirect contienen la dirección de enlace del nuevo Primer Salto, por lo que de nuevo no será necesario un posterior intercambio de paquetes para obtenerla.

Un mismo enlace puede ser asociado a múltiples prefijos. Por defecto, los hosts aprenden todos los prefijos del enlace al que están conectados a partir de los Router Advertisement. En algunos casos, los routers pueden estar configurados para omitir algunos de los prefijos (o todos) en sus avisos, de manera que los hosts asuman que destinos no se encuentran en su enlace y manden el tráfico a través de los routers, que serán los encargados de redireccionarlos apropiadamente.

El receptor de un paquete de Redirección asume que el nuevo Next-Hop pertenece al enlace. En IPv4, los hosts ignoraban los paquetes de redirección si consideraban que el siguiente salto no estaba en el enlace, basándose en su máscara. Esto era un problema en enlaces de medio compartido o en los que no se soportase broadcast (ATM, Frame Relay, AX.25...).

El algoritmo "Neighbor Unreachability Detection" es también parte del protocolo, lo que aumenta la robustez del reparto de paquetes frente a fallos de routers o cambios de direcciones de enlace por parte de los nodos. Esto permite, por ejemplo, que nodos móviles puedan cambiar de red (abandonando el vecindario) sin perder conectividad como ocurría con las cachés de ARP.

El uso de direcciones link-local para identificar unívocamente los routers hace posible que los hosts mantengan las asociaciones de los routers en el caso de que se establezca un nuevo prefijo global.

ND es inmune a los ataques por parte de usuarios no pertenecientes al enlace que envíen, accidental o intencionadamente, mensajes de ND con el campo Hop-Limit igual a 255 (debido a que los mensajes deberán proceder de direcciones de alcance local). En IPv4 estos eran capaces de enviar tanto mensajes ICMP de redirección como Avisos de Router.

Tabla I: Mensajes IPv4, componentes, funciones y sus equivalencias en IPv6

IPv4	*IPv6*
ARP Request message	Neighbor Solicitation message
ARP Reply message	Neighbor Advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router Solicitation message (optional)	Router Solicitation message (required)
Router Advertisement message (optional)	Router Advertisement message (required)
Redirect message	Redirect message

3.8 Autoconfiguración en IPv6

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que permite afirmar que IPv6 es “Plug & Play”.

El proceso incluye la creación de una dirección de enlace local, verificación de que no está duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (statefull o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración “stateless**”** (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de router,

el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración “stateful” (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración “sin intervención” se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan sólo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuánto tiempo está vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección

es “preferred” (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es “deprecated” (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras está en estado “desaprobado”, su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión **TCP**), debe usar una dirección “preferida”, siempre que sea posible.

Una dirección “desaprobada” debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las *direcciones* configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración está diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que “aprobar” el algoritmo de detección de *direcciones duplicadas*.

3.8.1 Autoconfiguración Stateless IPv6

El procedimiento de autoconfiguración stateless (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismo que permita a los host obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para sí misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha interfaz. El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.

Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor "stateful" o router, como requisito para comunicarse. Para obtener, en este caso, características "plug & play", empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local anteponiendo el prefijo de enlace local a su identificador de interfaz.

En el caso de redes o sitios grandes, con múltiples subredes y routers, tampoco se requiere la presencia de un servidor de configuración de direcciones "stateful", ya que los host han de determinar, para generar sus direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.

La configuración de direcciones debe de facilitar la re numeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios. La re numeración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe "en préstamo". El tiempo del "préstamo" es el mecanismo por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga. Al poder

disponer de varias direcciones simultáneamente, permite que la transición no sea "disruptora", permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.

Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que permite multicast.

Los administradores de sistemas necesitan la habilidad de especificar que mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.

Los pasos básicos para la autoconfiguración, una vez la interfaz ha sido activada, serían:

Se genera la dirección "tentativa" de enlace local, como se ha descrito antes.

Verificar que dicha dirección "tentativa" puede ser asignada (no está duplicada en el mismo enlace).

Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).

Si no está duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.

Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.

Si no hay routers, se invoca el procedimiento de autoconfiguración "stateful". Si hay routers, estos contestarán indicando fundamentalmente, como obtener las

direcciones si se ha de utilizar el mecanismo “stateful”, u otra información, como tiempos de vida, etc.

Hay algunos detractores de este mecanismo, ya que implica que cualquier nodo puede ser identificado en una determinada red si se conoce su identificador IEEE (dirección MAC).

3.8.2 Autoconfiguración Statefull IPv6 - DHCPv6

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración “stateless”. Como se ha indicado, ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.

Para lograr este objetivo, se centraliza la gestión de los recursos de la red, tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo.

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de “extensiones” que incorporan esta nueva información.

Los objetivos de DHCPv6 son:

DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.

DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración *"stateless"*.

DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.

DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.

DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.

Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.

Los clientes DHCP proporcionan la habilidad de re numerar la red.

Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.

DHCP incorpora los mecanismos apropiados de *control de tiempo* y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguración IPv6; son las siguientes:

La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección *IP* fuente para localizar un servidor o relé en su mismo enlace.

Los indicadores de compatibilidad BOOTP *y* broadcast han desaparecido.

El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.

La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la re numeración automática de direcciones y su gestión.

Se soportan múltiples direcciones por cada interfaz.

Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios.

De esta forma, se soportan las siguientes funciones nuevas:

Configuración de actualizaciones dinámicas de DNS.

Desaprobación de direcciones, para re numeración dinámica.

Relés pre configurados con direcciones de servidores, o mediante multicast.

Autenticación.

Los clientes pueden pedir múltiples direcciones IP.

Las direcciones pueden ser reclamadas mediante el mensaje de “iniciar reconfiguración”.

Integración entre autoconfiguración de direcciones *“*stateless*” y “*stateful”

Permitir relés para localizar servidores fuera del enlace.

CAPÍTULO IV

COMPARACION DE AMENAZAS PARA IPV4 E IPV6

En este capítulo se realizará un análisis de las amenazas a las que están expuestas las redes bajo IPv4 y las diferencias que se tiene al adoptar Ipv6, así como las amenazas que siguen afectando a una red sin importar la versión del protocolo.

4.1. Introducción

La seguridad de IPv6 es de muchas maneras la misma que la seguridad de IPv4, los mecanismos básicos para transportar paquetes a través de la red básicamente no han cambiado y los protocolos de las capas superiores que transportan los datos de

las aplicaciones actuales no han sido mayormente afectados. Sin embargo, debido a que IPv6 obliga la inclusión de IPsec a menudo se ha dicho que es más seguro. Aunque esto puede ser cierto en un entorno ideal, con aplicaciones bien codificadas, una infraestructura de identidad robusta y una eficiente administración de claves, en realidad los mismos problemas que afectaron el despliegue de IPsec con IPv4 afectarán a IPsec con IPv6, por lo tanto IPv6 es usualmente desplegado sin protecciones criptográficas de ningún tipo.

Adicionalmente, debido a que la mayoría de las infracciones suceden en el nivel de aplicación, aún un exitoso despliegue de IPsec con IPv6 no garantiza ninguna seguridad adicional más allá de la valiosa habilidad de determinar la fuente de esos ataques. Algunas diferencias significantes sin embargo existen más allá de la obligatoriedad de IPsec. Estas diferencias cambian los tipos de ataques que probablemente se verán en las redes IPv6, también es poco probable que la organización promedio migre por completo a IPv6 en un breve espacio de tiempo. Hasta la fecha, sin embargo, no ha habido un tratamiento exhaustivo de las amenazas a que este tipo de redes se enfrentan y las modificaciones de diseño necesarias para hacer frente a estas amenazas.

4.2. Ataques con nuevas consideraciones para IPv6

Los siguientes ataques tienen substanciales diferencias cuando se ha migrado a IPv6, en algunos casos los ataques son fáciles de ejecutar, en otros presentan más dificultad y en otros solo cambian los métodos.

- Reconocimiento
- Acceso no autorizado
- Manipulación de encabezados y fragmentación
- Spoofing en las capas 3 y 4
- Ataques a ARP y DHCP
- Ataques de amplificación de broadcast (Smurfing)
- Ataques de ruteo
- Virus y gusanos
- Transición, traslación y mecanismos de túnel

4.2.1. Reconocimiento

La primera categoría de ataques es el reconocimiento, el cual es generalmente el primer ataque ejecutado por un intruso, donde este trata de conocer todo lo que le sea posible de su objetivo de red.

Esto incluye tanto métodos de redes activas, tales como la exploración, así como pasivos como la minería de datos por ejemplo a través de motores de búsqueda o documentos públicos. Los métodos activos tienen el objetivo de dar la información

específica al intruso sobre los hosts y dispositivos de red que se utiliza, sus interconexiones con otros, y cualquier tipo de ataques que se puede teorizar sobre la base de la evaluación de los datos obtenidos.

4.2.1.1. Consideraciones en IPv4

En IPv4 los intrusos tienen algunos métodos bien establecidos de recolectar la información:

- Barrido con Ping: Mediante la determinación de las direcciones IPv4 en uso en una organización (a través de pruebas activas, consultas whois y conjeturas) un intruso de manera sistemática puede barrer una red con ICMP o mensajes ping de capa 4, que solicitan una respuesta, suponiendo que tanto las consultas así como las respuestas no se filtran en el borde de la red. Después de este análisis, el intruso utiliza los datos para formular algunas hipótesis sobre el diseño de la red de la víctima. Herramientas como traceroute y firewalk puede proporcionar datos adicionales para ayudar al intruso.

- Exploración de puertos: Después de identificar los sistemas accesibles, el intruso de manera sistemática puede probar estos sistemas en cualquier número de puertos de la capa de 4 para encontrar servicios activos y accesibles. Una vez descubiertos los hosts con servicios activos el intruso puede ir al siguiente paso.

- Aplicaciones y exploración de vulnerabilidades: El intruso puede entonces probar estos puertos activos por diversos medios para determinar el sistema

operativo y los números de versión de aplicaciones que se ejecutan en los hosts, e incluso detectar la presencia de ciertas conocidas vulnerabilidades.

Algunas herramientas como Nmap pueden llevar a cabo todos los elementos de este tipo de sondeos al mismo tiempo. Las técnicas de mitigación de ataques de reconocimiento generalmente se limitan a filtrar ciertos tipos de mensajes utilizados por un intruso para identificar los recursos de la red de la víctima y tratar de detectar la actividad de reconocimiento que se puede permitir y debido a la propia comunicación entre los dispositivos las actividades de reconocimiento no se pueden detener por completo.

4.1.1.2. Consideraciones en IPv6

A continuación se va a describir las diferencias en el ataque de reconocimiento cuando se traslada a IPv6. Debido a que los escaneos de puertos y vulnerabilidades de aplicaciones son idénticos después de que una dirección válida se identifica, ese será el punto central, primero se va a destacar las diferencias de tecnología independientemente de la actualmente disponible, y luego las capacidades actuales en esta área tanto para el intruso como para el defensor.

Tecnología y diferentes de amenazas

Con lo que respecta a la parte tecnológica, el reconocimiento con IPv6 es diferente al de IPv4 de dos maneras. La primera es que el barrido mediante ping o escaneo de puertos, cuando se utiliza para enumerar los hosts de una subred, son mucho

más difíciles de completar en una red IPv6. La segunda es que las nuevas direcciones multicast de IPv6 permiten al intruso encontrar un determinado conjunto de sistemas claves (routers, Network Time Protocol-NTP, servidores, etc) con más facilidad. Más allá de estas dos diferencias, las técnicas de reconocimiento en IPv6 son las mismas que en IPv4. Además, las redes IPv6 son aún más dependientes de ICMPv6 para funcionar correctamente. Un filtrado agresivo de ICMPv6 puede tener efectos negativos en las funciones de red.

- **Diferencias de tamaño de una subred IPv6**

  El tamaño por defecto de una subred en IPv6 es de 64 bits o 2^{64} versus el más común tamaño de una subred en IPv4 de 8 bits o 2^{8}. Esto incrementa el tamaño de la exploración para chequear cada host en una subred de $2^{64} – 2^{8}$ (aproximadamente 18 quintillones).

  Adicionalmente, la dirección de 64 bits es derivada de la versión EUI-64 de la dirección de la MAC del host o en el caso de las extensiones de privacidad de IPv6 (las cuales son habilitadas por defecto en Windows XP y disponible en numerosas plataformas), el número es seudo aleatorio y cambia regularmente. De ese modo una red que ordinariamente requería solo enviar 256 pruebas ahora requeriría más de 18 quintillones de pruebas para cubrir una subred entera. Aún si se asume que los principios de diseño de escuchar a la red se descuentan de estos cálculos y que la misma subred de 64 bits ahora contiene 10.000 host, que aún significa solo una en cada 1.8 cuadrillones de direcciones que están ocupadas (asumiendo una distribución aleatoria uniforme) e incluso a una velocidad de barrido de 1 millón de sondas por segundo (más de 400 Mbps de tráfico), se necesitarían más de 28 años de exploración constante para

encontrar el primer host activo, suponiendo que ocurre el primer éxito después de iterar el 50% de los primeros 1.8 cuadrillones de direcciones. Si se asume una típica subred con 100 host, ese número salta a más de 28 siglos de constante exploración de un millón de paquetes por segundo para encontrar el primer host y la primera subred de la red de la víctima.

Ahora hay que señalar que muchas variables pueden hacer que esta exploración sea más fácil para el intruso. En primer lugar, los servicios públicos en el borde de Internet tienen que ser alcanzables con DNS, dando al intruso por lo menos un pequeño número de hosts críticos dentro de la red para atacar a la víctima. En segundo lugar, la naturaleza del gran tamaño de las direcciones IPv6 y la falta de requerimientos estrictos para NAT (Network Address Translation) puede hacer que más redes adopten DNS dinámicos u otros mecanismos para garantizar que cada host tenga un nombre DNS válido (escribir FE80: CA01: 0:56:: ABCD: EF12: 3456 para hablar con el PC de un amigo no resulta una idea viable mucho menos para el usuario común).

Esto significa que los administradores pueden optar por direcciones de host fáciles de recordar para los sistemas de clave (:: 10:: 20:: F00D, y así sucesivamente) que podría ser introducido en una base de datos utilizada por una herramienta de análisis. Estos nombres fáciles de recordar podrían incluir simplemente un mapeo del último octeto decimal de IPv4 al último octeto de IPv6, porque la doble pila será la norma en los próximos años. En cuarto lugar, al centrarse en las designaciones populares IEEE OUI para los vendedores de NIC, un intruso podría reducir significativamente la cantidad de espacio 2^{64}. Y, por último, mediante la explotación de routers mal asegurados u otros dispositivos de puerta de enlace, un intruso puede ver la caché del descubrimiento de vecinos de IPv6 (el equivalente funcional de una caché ARP)

para encontrar hosts disponibles, o, simplemente, podría activar una captura de paquetes, con herramientas como tcpdump para encontrar las direcciones disponibles para escanear.

También, como en las redes IPv4, los hosts internos deben ser protegidos por un firewall que limita o impide por completo las conversaciones no iniciadas para alcanzar esos sistemas. Las implicaciones de estas subredes más grandes son significativas. Los sistemas actuales de gestión de red usadas por los administradores a menudo emplean barridos de ping como un método para enumerar una red. Nuevas técnicas deben ser adoptadas con este fin (tal vez comprobar la cache de vecinos en los routers). Con base en las pruebas iniciales, la caché de los vecinos contiene datos sólo cuando el dispositivo se comunica con el router (por ejemplo, el envío de mensajes off-net traffic).

Además, esto tiene potencialmente implicaciones de largo alcance por la manera en que los gusanos de Internet se propagan, ya sean basados en direcciones al azar o utilizar algún tipo de designaciones de dirección jerárquicas. Se supone que los gusanos tendrán un tiempo mucho más difícil de propagación de la misma manera como lo hicieron en IPv4.

- **Nuevas direcciones Multicast**

IPv6 admite las nuevas direcciones multicast que puede permitir a un intruso identificar los principales recursos en una red y luego atacarlos. Estas direcciones tienen un dominio específico para nodos, enlaces, o sitios de uso tal como se define en el RFC 2375. Por ejemplo, todos los enrutadores (FF05:: 2) y todos los servidores DHCP (FF05:: 3) tienen una dirección específica de sitio.

Aunque esta configuración claramente tiene un uso legítimo, es en efecto para el intruso una lista oficial de los sistemas a ser atacados. Por lo tanto, se vuelve crítico que estas direcciones de uso interno se filtren en el límite de la red y no sean accesibles desde el exterior.

Capacidades actuales de la tecnología

Hoy en día no existe una herramienta conocida de barrido de ping para IPv6. Nmap, que soporta barridos en Ipv4, optó por no soportarlo en IPv6. Por el lado de detección, algunos sistemas IDS (Instrusion Detection System) hoy (para host o red) no son compatibles con IPv6, por lo que la detección de la actividad de reconocimiento es difícil. Esto mejorará a medida que más proveedores aprovechen las capacidades IPv6. Las versiones actuales de la mayoría de los firewalls de las redes populares soportan IPv6, lo que significa que el filtrado de mensajes va a complicar los esfuerzos de reconocimiento de los intrusos.

4.2.1.3. Las mejores prácticas

Basado en los cambios en los ataques de reconocimiento en IPv6, las siguientes prácticas son sugeridas como las mejores:

- **Implementar las extensiones de privacidad cuidadosamente**: A pesar de que las extensiones de privacidad son un beneficio respecto a los ataques de escaneo, pueden también hacer que sea difícil rastrear los problemas y solucionarlos. Si una red tiene una gran cantidad de direcciones que presentan

dificultades usualmente además de que las direcciones de los host se cambian con regularidad, puede ser muy difícil rastrear el host exacto o incluso determinar si los problemas son de muchos. Una mejor opción es utilizar direcciones estáticas para la comunicación interna basadas en las direcciones MAC y pseudo aleatorias para el tráfico destinado a Internet. Además, se hace que las capacidades actuales de auditoría para realizar un seguimiento gusanos sea más difícil, porque cuando se realiza un seguimiento de una infección a una subred particular, la rotación de las direcciones propia de las extensiones de privacidad podría hacer que sea un verdadero reto identificar el host infectado.

- **Filtrado para uso interno de direcciones IPv6 en los routers de borde de la organización:** Los administradores pueden definir las direcciones de tipo site local para su organización, incluyendo las direcciones de multicast específicas como por ejemplo todos los routers con la dirección FF05:: 2. Estas direcciones locales de sitio (site-local) potencialmente puede conducir a nuevas vías de ataque, por lo que los administradores deben filtrar estas direcciones en los routers de borde de la organización.

- **Uso de direcciones estáticas estándar, pero no obvias para los sistemas críticos**: en lugar de la estandarización de las direcciones de host, tales como:: 10 o:: 20, intentar algo que es más difícil para los intrusos de adivinar, tales como: : DEF1 para la puerta de enlace predeterminada. Esto es ciertamente una técnica sencilla pero se consigue con poco esfuerzo adicional por parte del administrador, su uso no tiene inconvenientes. El objetivo aquí es hacer que sea difícil para el intruso adivinar las direcciones globales de los sistemas clave. La estandarización de un patrón corto, fijo para las interfaces que no deben ser

directamente accesible desde el exterior permite una corta lista de filtros en los enrutadores de borde.

- **Filtro de los servicios innecesarios en el firewall** Al igual que en IPv4, los sistemas públicos e internos no deben ser accesibles a los servicios que no necesitan alcanzarlos. Aunque algunos esperan que las herramientas tales como IPsec eliminen la necesidad de firewalls, esto tomará algún tiempo mientras se entienda completamente los filtros de las capas 3 y 4. Hasta que algunas cuestiones no técnicas (como el establecimiento de políticas internacionales de confianza) se resuelven, el despliegue a gran escala de IPsec será impracticable tanto para IPv4 como para IPv6.

- **Filtro selectivo de ICMP**: Debido a que la detección de vecinos utiliza ICMP y la fragmentación se realiza sólo en las estaciones finales (lo que requiere PMTUD - path maximum-transmission-unit discovery), es imperativo que algunos de los mensajes ICMP se permitirán en IPv6.

  Por tanto los mensajes ICMP no esenciales pueden ser filtrados por el firewall, como echo y echo reply, si esto no hace más compleja la administración. Se recomienda que particularmente para IPv6, los mensajes echo de ICMP sean habilitados en todas las direcciones para todos los host, excepto los que vienen de Internet hacia la red interna, esos deben estar denegados. Adicionalmente, IPv6 requiere los mensajes ICMPv6 neighbor discovery-neighbor solicitation (ND-NS) y neighbor discovery-neighbor advertisement (ND-NA) para funcionar, así como los mensajes router-advertisement (RA) si la autoconfiguración está siendo usada.

- **Mantener host y aplicaciones con seguridad:** aunque a su tiempo los parches y el bloqueo de host fueron elementos críticos en IPv4, lo fueron más en los estadíos tempranos de IPv6 debido a que muchas de las protecciones de host (firewall, IDS, etc) no son aún ampliamente soportadas en IPv6. Adicionalmente es altamente probable que en la introducción de las redes a IPv6 resulte que algunos host no sean apropiadamente asegurados. Es necesario centrarse en el mantenimiento de la seguridad de todos los host para asegurarse de que los que no son de uso crítico no sean usados como plataforma para llenar a los host vitales.

4.2.2. Acceso no autorizado

Acceso no autorizado se refiere a la clase de ataques en los que el intruso trata de explotar la política de transporte abierto propia del protocolo IPv4. Nada en la pila de protocolos IP limita al conjunto de hosts para que se pueda establecer la conectividad con otra red IP. Los atacantes se basan en este hecho para establecer la conectividad hacia los protocolos y aplicaciones de las capas superiores y aplicaciones en los dispositivos de interconexión de redes y hosts finales.

4.2.2.1. Consideraciones IPv4

Las redes IPv4 se han concentrado en limitar el acceso no autorizado mediante la implementación de tecnologías de control de acceso dentro de los sistemas finales y

en los dispositivos de puerta de enlace entre los extremos de IPv4. Estos controles pueden ocurrir tanto en la capa 3 como en la capa 4.

Los métodos de control de acceso en IPv4 se vuelven más complejos a medida que asciende la pila de protocolos. En la capa IP, el defensor usa listas de control de acceso (ACL) para permitir que sólo los hosts autorizados envíen paquetes a un dispositivo.

Las ACL están destinadas a limitar el acceso a o por medio de un dispositivo basado en las políticas de seguridad y de esta manera, limitar las vías disponibles de ataque a servicios específicos disponibles en la red. En las redes IPv4, estos controles de acceso se aplican en dispositivos de red (firewalls) y en los dispositivos finales mismos (firewalls de host). Aunque los firewalls pueden implementar políticas de seguridad basadas en información solo de las cabeceras de IPv4, estas son mejor usadas cuando son combinadas con la inspección de información de las capas superiores de TCP/UDP y de la capa de aplicación.

4.2.2.2. Consideraciones de IPv6

La necesidad de tecnologías de control de acceso es la misma en IPv4 como en IPv6, aunque eventualmente el requerimiento de uso de IPsec puede hacer más fácil el control de acceso a los host. El defensor desea limitar la capacidad del intruso de ganar vías de ataque contra los servicios ofrecidos por un host final. La capacidad para hacer este control de acceso basados en IPv6 cambia no solo en la información que puede ser filtrada en la cabecera de la capa 3 sino también en el

modo de direccionamiento, ya que en IPv6 se incluye la capacidad de que una interfaz tenga múltiples direcciones.

Estas múltiples direcciones IPv6 tienen un significado en la comunicación en la subred local (link local - FE80::/10), dentro de la organización (site local – FC00::/16 or FD00::/16 dependiendo de la decisión del grupo de trabajo) o incluso en Internet. Cuando el uso de este rango de direcciones es combinada con el sistema de ruteo, el diseñador de la red puede limitar el acceso a los nodos finales IPv6 a través de las direcciones IPv6 y ruteo.

Por ejemplo, con IPv6 el diseñador de red puede asignar una dirección de tipo global unicast solo a dispositivos que necesiten comunicarse con Internet, mientras que puede asignar una dirección de tipo site-local a dispositivos que necesiten comunicaciones solo dentro de la organización. Igualmente, si un dispositivo necesita comunicarse solo un con una subred particular solo es necesario que se le asigne una dirección local o link-local. Adicionalmente el uso de las extensiones de privacidad de IPv6 puede limitar el tiempo que una dirección es accesible y está expuesta a amenazas de seguridad.

Tecnología y diferentes amenazas

En IPv6 las funciones básicas de mitigar el acceso a otros dispositivos Ip basado en políticas es aún implementado con firewall y ACL en los dispositivos finales y de red. Sin embargo numerosas y significativas diferencias entre las cabeceras IPv4 e IPv6 pueden cambiar la forma en que el administrador despliega estas tecnologías. Estas diferencias se mencionan a continuación.

- **IPsec**

Cuando se implementa IPsec en IPv4 e IPv6 se tiene un impacto similar en la capacidad del administrador de reforzar las políticas de seguridad con la información de la cabecera IP, por tanto lo que se discute a continuación se aplica en ambos casos. Si la encriptación de IPsec es implementada de extremo a extremo la tecnología actual de firewall es efectiva solo en aplicar políticas de privacidad basadas en información de la capa 3 debido a protección de la criptografía. Si IPv6 usa solo la cabecera de autenticación es concebible que los firewalls puedan inspeccionar los protocolos de las capas superiores dentro de la encapsulación de la cabecera de autenticación y permitir o denegar el acceso al paquete basados en esa información.

- **Cabeceras de extensión**

Las opciones de IPv4 son reemplazadas por las cabeceras de extensión de IPv6, con esta sustitución, las cabeceras de extensión se pueden utilizar en un intento de eludir la política de seguridad. Por ejemplo, todos los extremos de IPv6 están obligados a aceptar los paquetes IPv6 con una cabecera de enrutamiento. Es posible que además de aceptar los paquetes IPv6, los host también procesen los encabezados de enrutamiento y reenvíen el paquete. Con esta posibilidad, las cabeceras de enrutamiento pueden ser usadas para eludir las políticas de seguridad implementadas en dispositivos de filtrado como un firewall.

Para eliminar esta posibilidad el administrador de red debe designar un conjunto específico de nodos que actúen como agentes home de MIPv6 (típicamente el

router por defecto de la red). EL diseñador de la red debe también validar que sistemas operativos dentro de la red de la organización no van a enviar paquetes que incluyen las cabeceras de ruteo. Si los sistemas operativos que hacen envío de paquetes que incluyan las cabeceras de ruteo están en la red, entonces los diseñadores de la red deben configurarla para filtrar las cabeceras de routing sobre los dispositivos de control de acceso.

Si MIPv6 no es necesitado, los paquetes con las cabeceras de ruteo pueden fácilmente ser omitidos de los dispositivos de control de acceso si no se confía en la procedencia de los paquetes. Aunque es fácil comenzar con una política de no usar MIPv6, las aplicaciones que están emergiendo en dispositivos de mano con acceso a WiFi, harán esta postura difícil de mantener. Por esta razón es lo mejor asegurarse que las políticas de los sistemas finales estén correctamente implementadas como "no-forwarding".

- **ICMP**

ICMPV6 es una parte integral de las operaciones de IPv6 aún más que en IPv4. Las mejores prácticas de firewall para ICMP para IPv4 son algunas veces objeto de debate, pero es en general aceptada como la mejor práctica un estricto filtrado de ICMP. En algunos casos extremos todos los mensajes ICMP son filtrados. Este tipo de filtro prohibitivo no es posible en IPv6. Comparar y contrastar como se podrían trasladar las políticas genéricas de IPv4 a IPv6 es muy importante.

Los siguientes mensajes ICMPv4 son permitidos a través del firewall y todos los demás son denegados. Las reglas generales son para permitir estos mensajes entrantes ICMP desde el Internet a una DMZ (demilitarized zone) en un firewall

y denegar ICMP para el dispositivo. Estas reglas pueden ser más o menos exigentes, pero se incluyen como una demostración:

- ICMPv4 Type 0 - echo reply
- ICMPv4 Type 3 Code 0 - Destination unreachable net unreachable
- ICMPv4 Type 3 Code 4 – Fragmentation needed but don't-fragment (DF) bit set
- ICMPv4 Type 8 - Echo request
- ICMPv4 Type 11 - Time exceeded

En contraste, las políticas en un firewall ICMPv6 necesitan soportar mensajes adicionales no solo a través del dispositivo sino desde y hacia el dispositivo. Los mensajes ICMPv6 requeridos para soportar funciones equivalentes a las políticas de un firewall son:

- ICMPv6 Type 1 Code 0 – No route to destination
- ICMPv6 Type 3 - Time exceeded
- ICMPv6 Type 128 and Type 129 - Echo request and echo reply

Los nuevos mensajes IPv6 requeridos para potencialmente ser soportados a través de los dispositivos firewall son los siguientes

- ICMPv6 Type 2 - Packet too big— Esto es requerido para que la técnica PMTUD funcione correctamente porque a los nodos intermedios en una red IPv6 no se les permite la fragmentación de paquetes. Aunque permitir PMTUD para funcionar en IPv4 es muy usado en IPv6 los dispositivos

intermedios no pueden fragmentar, así que estos mensajes son críticos para el correcto funcionamiento de las operaciones de red.

- ICMPv6 Type 4 - Parameter problem—Esto es requerido como un mensajes informacional si un nodo IPv6 no puede completar el procesamiento de un paquete debido a que este tiene problemas identificando un campo en el encabezado de IPv6 o una cabecera de extensión. Se están realizando investigaciones sobre el potencial abuso de este tipo de mensaje.

Los mensajes ICMPv6 potencialmente requeridos para ser soportados desde y hacia un dispositivo firewall son los siguientes:

- ICMPv6 Type 2 – Packet too big: El dispositivo firewall debe ser capaz de generar estos mensajes para que tenga lugar el descubrimiento de MTU, porque estos dispositivos no pueden fragmentar paquetes IPv6.
- ICMP Type 130-132 - Multicast listener messages: En IPv4, IGMP podría necesitar ser permitido para que multicast funcione correctamente. En IPv6 un dispositivo de ruteo debe aceptar estos mensajes para participar en ruteo multicast.
- ICMPv6 Type 133/: Son necesarios por una variedad de razones, las más notables la autoconfiguración de los nodos finales.
- ICMPv6 Type 135/136: Estos mensajes son usados para la detección de direcciones duplicadas y la resolución de direcciones de capa 2 (Ethernet MAC) a IPv6.
- ICMPv6 Type 4 – Parameter problem

- **Multicast Inspection**

Actualmente la mayoría de los firewall IPv4 hacen una mínima inspección y filtrado de multicast. El uso local de multicast es integral para el funcionamiento de IPv6. Los dispositivos firewall mínimo necesitan permitir las direcciones de tipo multicast link-local para proveer el descubrimiento de vecinos. Los firewall en el modo de capa 3 no deberían nunca enviar multicast del tipo link-layer. Todo dispositivo que actúe como firewall debería inspeccionar todas las fuentes de direcciones IPv6 y filtrar cualquier paquete con una dirección fuente multicast.

- **Anycast Inspection**

Adicionalmente, aunque cualquier anycast está restringido, los sistemas operativos deben haber comenzado dando soporte anycast a sus kernels. Esto podría hacer el uso de anycast más frecuente para servicios como DNS y NTP.

Si esto sucede cualquier dispositivo con estado (firewall, network IDS, servidor de balanceo de carga) necesita hacer mejoras en las funciones de su código para ser capaz de designar cualquier dirección anycast para inspección y servidores de origen que escuchan y responden a direcciones anycast. Si esto se hace, entonces cuando un servidor que está dando servicio de respuesta anycast con su dirección real puede mapear el tráfico de retorno con la dirección anycast. Finalmente con el uso de IPsec e IKE las comunicaciones seguras anycast tienen limitaciones. Se está llevando a cabo investigaciones dentro de la IETF, pero este requisito puede potencialmente ser abordado con el uso del dominio de Grupo de Interpretación (GDOI).

- **Firewalls transpartentes**

Algunos firewall de capa 2 o transparentes en el mercado actúan como bridges mientras refuerzan las políticas de las capas de la 3 a la 7. En las redes actuales IPv4, estos dispositivos están especialmente programados para tratar con una variedad de interacciones de Ip y la capa de enlace de datos como inspecciones ARP y DHCPv4. En IPv6 este tipo de firewall necesita mejorar sus capacidades para inspeccionar apropiadamente los IPv6 ICMP y mensajes multicast. Como se dijo anteriormente ICMPv6 es integral para el funcionamiento apropiado de IPv6 y estos firewall transparentes deben ser capaces de tratar con los mensajes ICMPV6 como el descubrimiento de vecinos, detección de direcciones duplicadas, autoconfiguración, manejo de multicast, solo por nombrar unas pocas.

Capacidades actuales de la tecnología

Aunque muchos firewall que trabajen con IPv6 están ya disponibles, muchos otros están implementados como soluciones parciales por razones de comercialización. Por ejemplo algunos firewall IPv6 entienden solo un subconjunto de cabeceras de extensión y entonces eliminan el tráfico IPv6 que tienen otras cabeceras. Un ejemplo es un firewall que no tiene la lógica para procesar las cabeceras de ruteo, si el firewall recibe estos paquetes este los descarta. Este comportamiento tiene algunos beneficios de seguridad cuando un firewall está protegiendo a un host que podría desempacar y reenviar el paquete con una cabecera de ruteo. Sin embargo esto limitaría a este equipo para no ser usado en ambientes que requieran MIPv6.

4.2.2.3. Candidatas a las mejores prácticas

Basados en las diferencias en el encabezado IPv6 y sus cabeceras de extensión asociadas, se sugieren las siguientes como mejores prácticas:

- Determinar que cabeceras de extensión serán permitidas a través de los dispositivos de control: Los diseñadores de red deben poner a la par sus políticas de IPv4 e IPv6. Si alguna opción de IPv4 es denegada en dispositivos de control de acceso el dispositivo correspondiente para IPv6 también debe denegarla. Adicionalmente los administradores deben entender el comportamiento de los sistemas operativos de los host cuando tratan con cabeceras de extensión y dictar políticas de seguridad basadas en ese comportamiento.
- Determinar cuáles mensajes ICMPv6 son requeridos: es recomendable que los administradores hagan coincidir sus equivalente políticas de ICMPv4 con las siguientes adiciones:

    - ICMPv6 Type 2 - Packet too big
    - ICMPv6 Type 4 – Parameter problem
    - ICMPv6 Type 130-132 – Multicast listener
    - ICMPv6 Type 133/134 – Router solicitation and router advertisement
    - ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement

4.2.3 Manipulación de encabezados y fragmentación

Esta categoría de ataques ha sido principalmente usada para dos propósitos: El primero es para usar la fragmentación como un modo de evadir los dispositivos de seguridad, como NIDS (***Network Intrusion Detection System***) o firewall con estado. El segundo propósito del ataque es usar la fragmentación u otra manipulación de cabeceras para atacar directamente la infraestructura de red.

4.2.3.1 Consideraciones IPv4

En IPv4 la fragmentación es una técnica usada para ajustar el datagrama IPv4 dentro de un MTU más pequeño en el camino entre los host finales. Ha sido usada para sobrepasar los controles de acceso en dispositivos como los routers y firewalls. También ha sido usada para ofuscar y sobrepasar productos de monitoreo de red como NIDS. La mayoría de los firewalls y NIDS modernos hacen grandes esfuerzos para reensamblar los paquetes y hacerlos coincidir con las reglas de control de acceso o firmas de ataque. En general, grandes cantidades de fragmentación de tráfico han sido usadas como un indicador de un intento de intrusión porque la mayoría de las líneas base del tráfico de Internet indica que el porcentaje de fragmentación es bajo.

4.2.3.2 Consideraciones IPv6

Tecnología y diferencia de amenazas

La fragmentación en IPv6 por dispositivos intermedios es prohibitiva según el RFC 2460. Uno de los ataques más comunes de fragmentación usa la superposición de fragmentos para ofuscar a los dispositivos de seguridad de IPv4. En IPv6 la superposición de fragmentos no es un camino normal para manejar la fragmentación basada en las reglas, entonces estos fragmentos son vistos como posibles ataques y son eliminados.

Adicionalmente, si los paquetes superpuestos son permitidos sobrepasando la seguridad de los dispositivos de seguridad, algunos sistemas operativos de los host finales los eliminan en su pila IPv6. Sin embargo, si el sistema operativo acepta estos fragmentos no hay nada que detenga al intruso de usar estos paquetes fragmentados para sobrepasar las políticas de seguridad de los dispositivos para propósitos similares que en los ataques de fragmentación en IPv4.

Capacidades de la tecnología actual

Similar a IPv4 los firewalls actuales de IPv6 e IDS implementan el reensamblado de paquetes y otros chequeos de fragmentación para mitigar los ataques de fragmentación. Estos chequeos incluyen examinar los fragmentos fuera de secuencia y ponerlos en orden, así como examinar el número de fragmentos de una IP dado un único identificador para determinar ataques de denegación de servicio. IPv6 no tiene herramientas conocidas de ataques de fragmentación, pero eso no elimina la amenaza de que puedan ser creadas fácilmente. Los firewalls chequean estos ataques y tratarán de hacerlos coincidir con las subredes fuente para

descubrir el caso donde el intruso está usando el RFC 3041 para generar ráfagas de fragmentos apareciendo como si fueran mandados de distintas fuentes.

4.2.3.3 Candidatas como mejores prácticas

Como se dijo anteriormente, aunque la gestión de la fragmentación de IPv6 se especifica de manera muy diferente a IPv4, las amenazas a los dispositivos de seguridad sobrepasados siguen siendo los mismos. Las siguientes candidatas a mejores prácticas se deben considerar en las redes de IPv6 para limitar la eficacia de los ataques de fragmentación:

- Denegar fragmentos IPV6 destinadas a un dispositivo de inter red cuando sea posible: Esto limitará ciertos ataques a los dispositivos. Sin embargo este filtro podría ser probado antes de ser implementado para asegurar de que no cause problemas en cada red en particular.

- Asegurar una adecuada capacidad de filtrar fragmentos IPv6: La combinación de varias cabeceras de extensión y la fragmentación en IPv6 crea la posibilidad de que el nivel 4 del protocolo no se incluirá en el primer paquete de un conjunto de fragmentos. Los dispositivos de monitoreo de seguridad que esperan encontrar el protocolo de la capa 4 necesitan contar con esa posibilidad y reensamblar los fragmentos.

- Descartar todos los fragmentos de menos de 1280 octetos (excepto el último). Por esta razón los dispositivos de seguridad deben ser capaces de descartar cualquier fragmento de IPv6 menor a 1280 octetos.

4.2.4 Layer 3-Layer 4 Spoofing o suplantación de identidad

Un elemento clave que habilita numerosos tipos diferentes de ataques es la capacidad del intruso de modificar su propia dirección IP y los puertos de donde se están comunicando con lo cual parece que el tráfico se está iniciando en una localización diferente o desde otra aplicación. Este ataque llamado "spoofing" prevalece a pesar de la presencia de mejores prácticas para mitigar el uso de los ataques.

4.2.4.1 Consideraciones IPv4

Hoy en día los ataques en IPv4 (principalmente basados en la capa 3) ocurren cada día. Pueden hacer los ataques spam, gusanos o virus más difíciles de parar. El spoofing de capa 3 no es usualmente un tipo de ataque interactivo como retorno de rutas de tráfico para falsificar la localización, requieren que el intruso "adivine" lo que el tráfico de retorno contiene (no es una propuesta sencilla para los ataques basados en TCP porque TCP tiene números de 32 bits de secuencia).

El spoofing de capa 4 puede ser usado en ataques interactivos para hacer aparecer el tráfico viniendo de una localización de la que no viene. Desafortunadamente como los filtros no están ampliamente implementados y estos necesitan un amplio uso para tener un beneficio significativo, este tipo de ataque es muy común aún.

4.2.4.2 Consideraciones IPv6

Tecnología y diferentes amenazas

Uno de los más prometedores beneficios de IPv6 en la capa 3 con respecto a este tipo de ataque es la naturaleza misma de las direcciones IPv6. A diferencia de IPv4, las asignaciones IPv6 se configuran de tal manera que fácilmente se pueden resumir en diferentes puntos de la red. Esto permite poner un filtro por medio del proveedor de servicios para asegurar que sus clientes no están siendo atacados fuera de sus rangos de direcciones.

Desafortunadamente esto no es un comportamiento estándar y esto requiere una implementación a conciencia por parte de los operadores. Los ataques en la capa 4 no han cambiado de ningún modo, porque los protocolos de esta capa no han cambiado con respecto a la suplantación de identidad. Nótese que las subredes con mucho más grandes entonces un invasor puede hacer una suplantación de un enorme rango de direcciones.

Desde un punto de vista de la transición, los diferentes mecanismos de túneles ofrecen la posibilidad a un intruso con conectividad IPv4 o IPv6 enviar tráfico a la otra versión de IP ocultando la verdadera fuente.

Capacidades de la tecnología actual

Actualmente el spoofing de la capa 3 puede ser mitigado usando las mismas técnicas de IPv4 con ACL estándar, mientras que el de la capa 4 no ha cambiado. El

tráfico de suplantación de identidad puede ser detectado usando firewalls IPv6 o IDS. Actualmente no hay técnicas disponibles para mitigar el spoofing de 64 bits del espacio de direcciones de host disponibles en IPv6. Un método que sería útil en redes IPv6 e IPv4 sería uno que correlacione IP, Mac puertos de la capa 2. Estos datos podrían ser almacenados por un switch y enviados a una estación de administración, habilitando al operador para determinar rápidamente el puerto de switch físico en la cual una determinada dirección IP se está comunicando.

4.2.4.3 Candidatas a las mejores prácticas

Basados en los cambios de los ataques de spoofing de las capas 3 y 4 en IPv6, las siguientes serían práctica candidatas a ser aplicadas:

- Implementar el filtrado del RFC 2827 y fomentar que el ISP haga lo mismo: Por lo menos contener el tráfico falso en la porción del host de la dirección IPv6 proporciona un gran beneficio para al menos rastrear el ataque hacia el segmento de red de origen.

- Documentar los procedimientos para el rastreo del último salto: Con el gran rango de direcciones susceptibles a spoofing dentro una red IPv6, es crítico que cuando un ataque ha sido realizado se tenga mecanismos para determinar a ciencia cierta la fuente física de ese tráfico. Esto generalmente implica algunas combinaciones de información de las capas 2 y 3 obtenida de switches y routers.

- Uso de protecciones de criptografía donde sea crítico: Si una aplicación usa una protección alta de criptografía un ataque exitoso de spoof no tendría mayor sentido sin también poder revertir las funciones de criptografía del dispositivo.

4.2.5 Ataques ARP y DHCP

Los ataques de ARP y DHCP tratan de alterar el proceso de inicialización de un host o un dispositivo al que el host accede para poder enviar sus paquetes. Esto generalmente implica que se trate de alterar el proceso de arranque de las comunicaciones del host a través de un dispositivo corrupto o comprometido o del robo de identidad en las comunicaciones. Estos ataques tratan de lograr ser vistos como un host de la red para comunicarse con dispositivos no autorizados o comprometidos, o ser configurados con información como la puerta de enlace por defecto, la dirección IP der servidor DNS, etc.

4.2.5.1 Consideraciones IPv4

DHCP usa mensajes de broadcast desde el cliente cuando quiere iniciar la comunicación, permitiendo a un servidor DHCP falso responder a esta petición antes de que lo haga el auténtico. Esto permite al servidor falso poner información crítica de configuración como puerta de enlace por defecto y servidor DNS, entonces entablar un ataque de tipo man-in-the-middle (hombre en el medio). Adicionalmente a esto los mensajes de DHCP pueden ser víctimas de spoofing, permitiendo a un intruso consumir todos los mensajes DHCP disponibles en el servidor.

Los ataques ARP se centran en la información obtenida de hacer una suplantación de identidad para causar que se cambie la relación de una dirección IP y una MAC de un host particular de modo que la dirección IP sea válida pero la víctima se comunica con la dirección MAC del intruso. Estos es la mayoría de las veces hecho suplantando la identidad de la puerta de enlace por defecto.

Se ha desarrollado tecnología en IPv4 para algunos de los ataques de este tipo. Por ejemplo Cisco tiene una característica en sus switches Ethernet llamado DHCP snooping, lo cual permite a ciertos puertos designados como “confiables” participar en respuestas DHCP mientras la mayoría de los otros puertos están configurados para permitir enviar solo mensajes DHCP de clientes. Adicionalmente una característica llamada ARP inspection ejecuta una protección similar para ARP.

4.2.5.2 Consideraciones IPv6

Tecnología y diferentes amenazas

En IPv6 desafortunadamente ninguna seguridad inherente ha sido añadida al equivalente de DHCP o ARP. La autoconfiguración de tipo stateless puede proveer una alternativa viable a DHCP en muchos casos, servidores dedicados a DHCP no son comunes en IPv6 y aún no son ampliamente disponibles en los servicios de los sistemas operativo actuales.

Servidores dedicados DHCPv6 pueden aparecer para ofrecer parámetros de configuraciones adicionales como servidores DNS, de telefonía Ip, etc, por tanto la protección a nivel de DHCP es aún requerida. Desafortunadamente los mensajes de autoconfiguración stateless pueden ser víctimas de spoofing pudiendo usarlo para

denegar el acceso a los dispositivos. Para mitigar esto, el concepto de puerto confiable debe ser usado en conjunto con los mensajes router-advertised.

En IPv6 en lugar de continuar con una versión única de ARP para cada tipo de medio, es reemplazado con elementos de ICMPv6 llamados neighbor discovery (descubrimiento de vecinos) teniendo las mismas inherencias de seguridad que ARP en IPv4. Aunque la posibilidad de que se tenga más seguridad usando IPsec existe, esto está lejos de estandarizarse e implica consideraciones de implementación únicas debido a esta seguridad añadida. Existen grupos dentro de la IETF específicos trabajando para solucionar estos inconvenientes, pero los problemas de seguridad son los mismos que con ARP en IPv4.

Capacidades de la tecnología actual

No existen herramientas disponibles hoy en día para detectar o parar el abuso de la autoconfiguración o el descubrimiento de vecinos de DHCPv6. Estos mensajes pueden ser filtrados en un router o firewall como los mensajes ICMP, pero debido a que la mayoría de estos ataques son significativos solo localmente este sería un beneficio mínimo. Los ataques al descubrimiento de vecinos no han sido implementados en ningún código de prueba público para IPv6, por lo que algunas consideraciones específicas pueden aparecer después de que este código sea lanzado y probado. Obtener la capacidad de inspección equivalentes que se encuentra actualmente en IPv4 podría ayudar a mitigar esta amenaza.

4.2.5.3 Candidatas a las mejores prácticas

Sin la capacidad de detector el buen uso de los mensajes de descubrimiento de vecinos o asegurar su transporte la mejor práctica se limita a la siguiente:

- Usar entradas estáticas de vecinos para los sistemas críticos: en entornos altamente sensibles se puede especificar que un sistema tenga una entrada estática a su router por defecto y eliminar muchas de los ataques del descubrimiento de vecinos. Esta es una práctica muy pesada administrativamente y no debe tomarse a la ligera

4.2.6 Ataques de amplificación de Broadcast (smurf)

Los ataques de amplificación de broadcast comúnmente referidos como “smurf” son del tipo DoS (Denial of Service- denegación de servicios) que toman ventaja del envío de mensajes de tipo echo-request con una dirección destino de una subred broadcast y suplanta la dirección fuente, usando la dirección IP de la víctima. Todos los host de la subred responden a la dirección de la fuente suplantada e inundan a la víctima con mensajes de tipo echo-reply.

4.2.6.1 Consideraciones en IPv4

Este tipo común de ataque tiene un método simple de mitigarlo en redes IPv4. Si IPv4-directed broadcasts está deshabilitado en un router cuando un intruso envía un mensaje de echo-request a la dirección de broadcast de la subred IP dejan de enviar mensajes de respuesta de eco a la víctima, a diferencia de las respuestas de todos los dispositivos de la red. De acuerdo a la mejor práctica actual, el comportamiento por defecto para routers IP es poner en estado de apagado (off) a

IP-directed broadcasts. El comando no IP-directed broadcasts es el comando por defecto en los routers cisco desde la versión 12. Este ataque específico está siendo cada vez menos común, pero aún es usado para crear ataques DoS.

4.2.6.2 Consideraciones IPv6

Tecnología y diferentes amenazas

En IPv6 el concepto de IP-directed broadcasts es removido desde el protocolo y se añade un lenguaje específico para mitigar este tipo de ataques. Específicamente con respecto a los ataques smurf el RFC 2463 establece que un mensaje ICMPv6 no podrá ser generado como una respuesta a un paquete con una dirección destino multicast ni link-layer multicast, o a link-layer broadcast. Si los nodos finales acatan el RFC este no debería ser un problema en las redes IPv6.

Capacidades de la tecnología actual

En pruebas realizadas a los sistemas operativos más populares que cumplen con el RFC se ha observado que no se responde a peticiones echo-request, existen algunas ambigüedades en el estándar acerca de si los nodos finales deberían responder a mensajes ICMP con direcciones multicast globales como direcciones fuente. Si los nodos finales responden entonces un intruso podría hacer un ataque amplificado en la infraestructura de multicast que puede causar un DoS debido al consumo de recursos en sus dispositivos de red.

4.2.5.3 Candidatas a la mejor práctica

- Implementar un filtro de ingreso de paquetes con direcciones IPv6 multicast fuente: No hay una razón válida para que una dirección fuente sea multicast, así que el administrador podría descartar cualquier paquete con esta característica en el borde mismo de la red.

4.2.7 Ataques de ruteo

Los ataques de ruteo se enfocan en interrumpir o redirigir el flujo de tráfico en la red. Esto puede ser hecho de una variedad de formas que van desde ataques de flooding (inundación), anuncio y eliminación rápida de las rutas, y el anuncio falso de las rutas. Las particularidades de los ataques varían dependiendo del protocolo que se esté usando

4.2.7.1 Consideraciones en IPv4

En IPv4 los protocolos de ruteo son comúnmente protegidos usando autenticación encriptada para un anuncio seguro entre pares. La implementación más común es el algoritmo de autenticación MD5 (Message Digest Algorithm) con una clave pre compartida entre los participantes.

4.2.7.2 Consideraciones en IPv6

Tecnología y diferentes amenazas

Algunos protocolos no cambian sus mecanismos de seguridad cuando pasan de IPv4 a IPv6.

El multiprotocolo BGP (Border Gateway Protocol) fue llevado a IPv6 en el RFC 2545, y sigue usando el algoritmo TCP MD5 para autenticación.

El protocol IS-IS (Intermediate System-to-Intermediate System) fue extendido en una especificación en borrador para soportar IPv6, pero dicha extensión no cambia la autenticación fundamental de IS-IS. Originalmente proveía autenticación para paquetes link-state (LSP) a través de la inlcusión de la información como parte del LSP. Sin embargo una simple autenticación del password no fue encriptada. El RFC3567 añade una autenticación encriptada a IS-IS, y seguirá siendo usada para proteger el tráfico IS-IS en IPv6.

En el protocol OSPFv3 (Open Shortest Path First Version 3), los campos de autenticación de la cabecera fueron removidos. RIPng (Routing Information Protocol Next-Generation) también removió la autenticación de sus especificaciones de protocolo. OSPF y RIPng confían en las cabeceras de IPsec AH y ESP para proveer integridad, autenticación, confidencialidad y protección anti repetición en el intercambio de información.

Capacidades actuales de la tecnología

Los mecanismos de seguridad para los protocolos que han cambiado con IPv6 se han implementado de manera inconsistente a través de los proveedores de red.

4.2.7.3 Candidatas a mejores prácticas

- Uso tradicional de mecanismos de autenticación en BGP y IS-IS.

- Uso de IPsec para asegurar protocolos como OSPFv3 y RIPng: Esto depende del funcionamiento de las diferentes implementaciones de los proveedores de equipos.

4.2.8 Virus y Gusanos

Los virus y los gusanos siguen siendo uno de los problemas más importantes en las redes IP, casi todos los ataques públicos más dañinos en los últimos años han tenido que ver con un virus o un gusano.

4.2.8.1 Consideraciones IPv4

En IPv4, los virus y los gusanos no solo dañan a los host infectados también afectan el transporte de las redes ya que incrementar la carga a los routers y a los servidores de correo en el Internet. SQL slammer por ejemplo causa una inundación masiva de la red debido en parte a la velocidad con la que la escanea (cada paquete de ataque es un mensaje UDP único).

Parches, antivirus en los host y la detección temprana seguida por el bloqueo de perímetro han sido las tres técnicas que se utilizan en IPv4. La detección temprana se realiza más fácilmente con los sistemas de detección de anomalías tales como los disponibles de Arbor Networks.

Adicionalmente, nuevos productos basados en IDS pueden interceptar ciertas llamadas a los sistemas que podrían causar que se vean comprometidas.

4.2.8.2 Consideraciones IPv6

Tecnología y diferentes amenazas

Un virus tradicional no cambia con IPv6. Los virus basados en e-mail o los que afectan las unidades removibles siguen siendo lo que eran. Sin embargo, los gusanos o virus que usan alguna forma de escanear la red para encontrar host vulnerables pueden experimentar significantes barreras de propagación en IPv6 como se mencionó anteriormente. Se necesita más investigación para identificar cuán significativo es el cambio que tendría que hacer el programador de estos gusanos para mejorar su eficiencia de propagación.

Parecería que SQL Slammer sería mucho menos eficaz en un entorno IPv6, debido a su incapacidad para encontrar hosts para infectar y por lo tanto su incapacidad para lograr las inundaciones resultantes.

Capacidades de la tecnología actual

Las tres técnicas de mitigación que actualmente se utilizan en IPv4 están todavía disponibles en IPv6. No hay, sin embargo, un amplio apoyo de IPv6 en los productos IDS de host disponibles en la actualidad. Además, la información proporcionada por los routers para ayudar en la detección de anomalías no es tan extensa en IPv6 actualmente.

4.2.8.3 Candidatas a las mejores prácticas

Además de establecer técnicas para hacer más fácil el rastreo ataque local, no hay cambios significativos en las prácticas para contrarrestar los ataques de virus y

gusanos. Todos los mecanismos de IPv4 (cuando los productos son compatibles con IPv6) funcionan correctamente.

4.2.9 Traslación, transición y mecanismos de túnel

Se ha puesto mucha atención en cómo las redes IPv4 serán trasladadas a redes IPv6. Adicionalmente se han comenzado a hacer las evaluaciones de las implicaciones de seguridad de las técnicas de migración de IPv4 e IPv6. A continuación se va a resumir los esfuerzos de investigación en ese sentido y se harán ciertas observaciones.

Existen varios enfoques para realizar la transición de IPv4 a IPv6, los cuales caen dentro de las siguientes categorías:

- Doble pila (Dual stack)
- Túneles
- Translation

La existencia de muchas tecnologías de transición crea una situación en la cual los diseñadores de red necesitan entender las implicaciones de seguridad de las tecnologías de transición y seleccionar la más apropiada para su red en particular.

4.2.9.1 Problemas y observaciones

- Con respecto a las tecnologías IPv6 de túnel y los firewalls, si el diseñador de la red no considera un túnel IPv6 en las definiciones de las políticas de seguridad,

el tráfico no autorizado podría atravesar el firewall en los túneles. Esto es similar al problema de mensajería instantánea (IM) y aplicaciones para compartir archivos usando el puerto TCP 80 de las organizaciones que se tiene con IPv4.

- En diferentes estudios de transición realizados se ha notado que los mecanismos de túnel automático son susceptibles a ataques como falsificación de paquetes y de tipo de denegación de servicios. Estos riesgos son los mismos que en IPv4 pero se incrementa el número de caminos para ser explorados por los atacantes.

- Superposición de túneles son consideradas redes de tipo multiacceso no broadcast para IPv6 y requiere que el diseñador de la red considere ese hecho en el diseño de la seguridad de la red en especial cuando implementa un túnel estático o automático.

- Tecnologías de traslación introducen túneles automáticos con terceras partes y vectores DoS, este riesgo no cambia desde IPv4 pero se abren nuevo campos para la explotación que pueden ser limitados restringiendo los anuncios de routing tanto para clientes internos como externos.

- Se prefiere los túneles estáticos para Ipv6 e Ipv4 porque explícitamente son permitidos o desautorizados en las políticas de los dispositivos de borde.

- Las técnicas delineadas en IPv6 han sido analizadas y muestran que sufren problemas similares en ataques de soopfing y DoS tanto como en redes solo Ipv4.

- La traslación de Ipv6 a Ipv4 y sus técnicas de retransmisión pueden vencer los esfuerzos de defensa porque esconden el origen del ataque.

- Cuando se enfoca en la seguridad de un host en un dispositivo con doble pila se debe ser cuidadoso de que las aplicaciones pueden estar sujetas a ataques tanto de IPv4 como de Ipv6. Por lo tanto cuando se hacen controles estos deberían bloquear el tráfico de ambas versiones de ser necesario.

4.2.9.2 Candidatas a la mejor práctica

Las recomendaciones generales para redes cuando se considera una técnica de transición de IPv4 a Ipv6 incluyen lo siguiente:

- Uso de doble pila como elección de técnica de migración: Usar el acceso a los servicios nativos de cada uno pero no la traslación debido a que los problemas de seguridad serán mejor entendidos y las políticas de seguridad simplificadas.

- Uso de túneles estáticos en lugar de dinámicos: Esto permite al administrador establecer una relación confiable entre los extremos de los túneles y continuar con la implementación se las políticas de seguridad de entrada y salida.

- Implementar filtrado de salida en el firewall para permitir solo túneles autorizados.

4.3 Ataques en IPv4 e IPv6 con Fuertes similitudes

Los ataques mencionados a continuación fundamentalmente no se han visto alterados cuando se trabaja en un entorno IPv6.

- Sniffing (husmear)
- Ataques en la capa de aplicación
- Dispositivos falsos
- Ataques Man-in-the-middle (hombre en el medio)
- Flooding (Inundación)

4.3.1 Sniffing

El sniffing o husmeo se refiere a la clase de ataque donde la información que se transmite a través de la red es capturada. El ejemplo más común de este ataque es el uso de Tcpdump, el cual es incluido en la mayoría de sistemas operativos basados en Linux. Un intruso que ejecuta un sniff puede algunas veces determinar las credenciales de inicio de sesión o ver información sensible en texto plano. Aunque IPv6 provee tecnología fundamental para prevenir el husmeo por medio de IPsec esto no provee ninguna simplificación para los problemas de manejo de claves que han demostrado ser un gran reto. Antes de que los problemas de administración de claves (entre otros) sean resueltos, la implementación de IPsec quedará estancada y los ataques de sniffing continuarán siendo posibles.

4.3.2 Ataques en la capa de aplicación

Se refiere a todos los ataques ejecutados sobre la capa 7 del modelo OSI, estos representan la mayoría de los ataques en Internet hoy en día y las vulnerabilidades que habilitan estos ataques representan la fuente de la mayoría de los problemas de inseguridad que tienen todas las redes actualmente. Ataques típicos como el desbordamiento del buffer, ataques a aplicaciones Web, virus y gusanos caen dentro de esta categoría.

Tanto Ipv4 como IPv6 son la mayoría de las veces partes neutrales en los ataques a la capa de aplicación. Ciertamente si el protocolo ha sido adoptado más estrictamente la autenticación de la dirección IP en algunos de estos ataques podrían ser más fácilmente rastreados, pero la mayoría de ataques se generan en esta misma capa no en la capa subyacente de transporte.

Aun suponiendo la aplicación mundial de IPsec, los ataques de la capa de aplicación cambian muy poco con la adopción de IPv6. Aunque una conexión puede estar protegida por encriptamiento, no hay nada que pueda parar los ataques en la capa de aplicación cuando se atraviesa esa seguridad, causando el mismo daño que si no estuviera encriptada. La única diferencia es que el rastreo es más fácil debido a la autenticación que caso contrario podría ser falsa.

Sin embargo si IPsec es ampliamente implementado de extremo a extremo sin algún mecanismo para las claves, todas las protecciones de seguridad caerán sobre el host y debido a que los firewalls e IDS ven el tráfico encriptado estos no pueden tomar ninguna decisión basada en los datos.

4.3.3 Dispositivos falsos

Los dispositivos falsos son equipos introducidos en la red sin ser autorizados. Aunque podría ser una laptop simplemente, sería más interesante para un atacante introducir un punto de acceso inalámbrico, o servidores DNS o DHCP, switchs o routers. Estos ataques son muy comunes en redes IPv4 y substancialmente no han cambiado para IPv6. Si IPsec fuera usado ampliamente con IPv6 la autenticación podría mitigar en algo este tipo de ataques. El estándar 802.1x podría ser de ayuda potencial en este caso, aunque un dispositivo no detectado podría canalizar la secuencia de autenticación y comprometer el nodo actuando como un ser servidor mientras captura credenciales válidas.

4.3.4 Ataques Man-in-the-Middle

Debido a que las cabeceras de IPv4 e IPv6 no tienen mecanismo de seguridad por si mismos cada protocolo depende de la suite de protocolos de IPsec para protegerse. De esta manera IPv6 cae presa de los riesgos de seguridad planteados por man in the middle atacando al conjunto de protocolos IPsec, específicamente IKE. Ya han sido documentadas herramientas que atacan de modo agresivo el modo de negociación de IKE y rompen una clave compartida, con esto en mente es recomendable usar IKE en modo main cuando se usa claves compartidas. Se espera que IKEv2 mitigue estos problemas en el futuro.

4.3.5 Inundación

Aunque ciertamente el incremento del número de direcciones IP que pueden ser falsificadas hacen el ataque de inundación más difícil de rastrear, los principios de los ataques de inundación o flooding siguen siendo los mismos para IPv6. Si un ataque ya sea local o distribuido inunda el dispositivo de red o un host con más tráfico del que puede proceder o transmitir el dispositivo fácilmente sale de servicio. Las mismas técnicas usadas para localizar y rastrear un ataque de DoS en IPv4 pueden ser usadas en IPv6 aunque nuevas técnicas están siendo desarrolladas.

4.4 Análisis global

Tabla I: Comparación de amenazas para IPv4 e IPv6

Tipo de ataque	IPv4	IPv6
Reconocimiento	El intruso se vale de estrategias como: • Barrido con Ping • Exploración de puertos • Aplicaciones y exploración de vulnerabilidades	Las técnicas de ataque son las mismas pero se tiene otras características en IPv6: • Barrido mediante ping y exploración de puertos son mucho más difíciles de completar en una red IPv6 por la cantidad de direcciones. • Direcciones multicast de IPv6 permiten encontrar sistemas claves con más facilidad
Acceso no autorizado	• Los controles de acceso se aplican en dispositivos de red (firewalls) y en los dispositivos finales mismos (firewalls de host). • Se controla a través de ACL	Aún se implementa controles con firewall y ACL en los dispositivos finales y de red, pero las numerosas y significativas diferencias entre las cabeceras pueden cambiar la forma en que el administrador despliega las tecnologías.
Manipulación de encabezados y fragmentación	En IPv4 la fragmentación es usada para ajustar el datagrama IPv4 dentro de un MTU más pequeño en el camino entre los host finales para así sobrepasar los controles de acceso en dispositivos como los routers y firewalls	La fragmentación en IPv6 por dispositivos intermedios es prohibitiva

Tabla I: Comparación de amenazas para IPv4 e IPv6 (Continuación)

Spoofing en las capas 3 y 4	Los filtros no están ampliamente implementados y estos necesitan un amplio uso para tener un beneficio significativo, este tipo de ataque es muy común aún.	Las asignaciones IPv6 se configuran de tal manera que fácilmente se pueden resumir en diferentes puntos de la red. Esto permite poner un filtro por medio del proveedor de servicios para asegurar que sus clientes no están siendo atacados fuera de sus rangos de direcciones.
Ataques a ARP y DHCP	Los ataques de ARP y DHCP tratan de alterar el proceso de inicialización de un host o un dispositivo al que el host accede para poder enviar sus paquetes.	No existe ninguna seguridad inherente al equivalente de DHCP o ARP. Aunque la posibilidad de que se tenga más seguridad usando IPsec existe, esto está lejos de estandarizarse.
Ataques de amplificación de broadcast	El modo de mitigar estos ataques en IPv4 es deshabilitar IPv4-directed broadcasts entonces cuando un intruso envía un mensaje de echo-request a la dirección de broadcast de la subred IP se dejan de enviar mensajes de respuesta de eco a la víctima	Específicamente con respecto a los ataques smurf el RFC 2463 establece que un mensaje ICMPv6 no podrá ser generado como una respuesta a un paquete con una dirección destino multicast ni link-layer multicast, o a link-layer broadcast.
Ataques de ruteo	Los protocolos de ruteo son comúnmente protegidos usando autenticación encriptada. La implementación más común es el algoritmo MD5.	OSPF y RIPng confían en las cabeceras de IPsec AH y ESP mientras que BGP e IS-IS conservan sus mecanismos de autenticación.
Virus y gusanos	Parches, antivirus en los host y la detección temprana seguida por el bloqueo de perímetro han sido las tres técnicas que se utilizan.	Las tres técnicas de mitigación que actualmente se utilizan en IPv4 están todavía disponibles en IPv6. No hay, sin embargo, un amplio apoyo de IPv6 en los productos IDS de host disponibles en la actualidad

Tabla I: Comparación de amenazas para IPv4 e IPv6 (Continuación)

Sniffing	La información que se transmite a través de la red es capturada.	Aunque IPv6 provee tecnología fundamental para prevenir el husmeo por medio de IPsec esto no provee ninguna simplificación para los problemas de manejo de claves y mientras eso no sea resuelto, la implementación de IPsec quedará estancada y los ataques de sniffing continuarán siendo posibles.
Ataques en la capa de aplicación	Se refiere a todos los ataques ejecutados sobre la capa 7 del modelo OSI, estos representan la mayoría de los ataques en Internet hoy en día y las vulnerabilidades que habilitan estos ataques representan la fuente de la mayoría de los problemas de inseguridad que tienen todas las redes actualmente.	Aun suponiendo la aplicación mundial de IPsec, los ataques de la capa de aplicación cambian muy poco con la adopción de IPv6.
Dispositivos falsos	Los dispositivos falsos son equipos introducidos en la red sin ser autorizados.	Si IPsec fuera usado ampliamente con IPv6 la autenticación podría mitigar en algo este tipo de ataques. El estándar 802.1x podría ser de ayuda potencial en este caso, aunque un dispositivo no detectado podría canalizar la secuencia de autenticación y comprometer el nodo actuando como un ser servidor mientras captura credenciales válidas.
Ataques Man-in-the-middle (hombre en el medio)	La cabecera de IPv4 no tiene un mecanismo de seguridad por si misma cada protocolo depende de la suite de protocolos de IPsec para protegerse	La cabecera de IPv6 no tiene un mecanismo de seguridad por si misma cada protocolo depende de la suite de protocolos de IPsec para protegerse

Tabla I: Comparación de amenazas para IPv4 e IPv6 (Continuación)

Flooding (Inundación)	Si un ataque ya sea local o distribuido inunda el dispositivo de red o un host con más tráfico del que puede proceder o transmitir el dispositivo fácilmente sale de servicio.	Los principios de este ataque siguen siendo los mismos por lo que mismas técnicas usadas para localizar y rastrear un ataque de DoS en IPv4 pueden ser usadas en IPv6 aunque nuevas técnicas están siendo desarrolladas.

CAPITULO V

FASE DE PRUEBAS

Dentro de este capítulo se realizarán pruebas sobre la red propuesta en el anteproyecto de tesis para verificar las seguridades que se tienen tanto en IPv4 como en IPv6, ante ataque realizados.

5.1 Escenario de pruebas para IPv4

5.1.1 Esquema de la red

De acuerdo al esquema propuesto dentro del anteproyecto de tesis se ha diseñado un esquema que servirá para realizar las pruebas con IPv4 e IPv6:

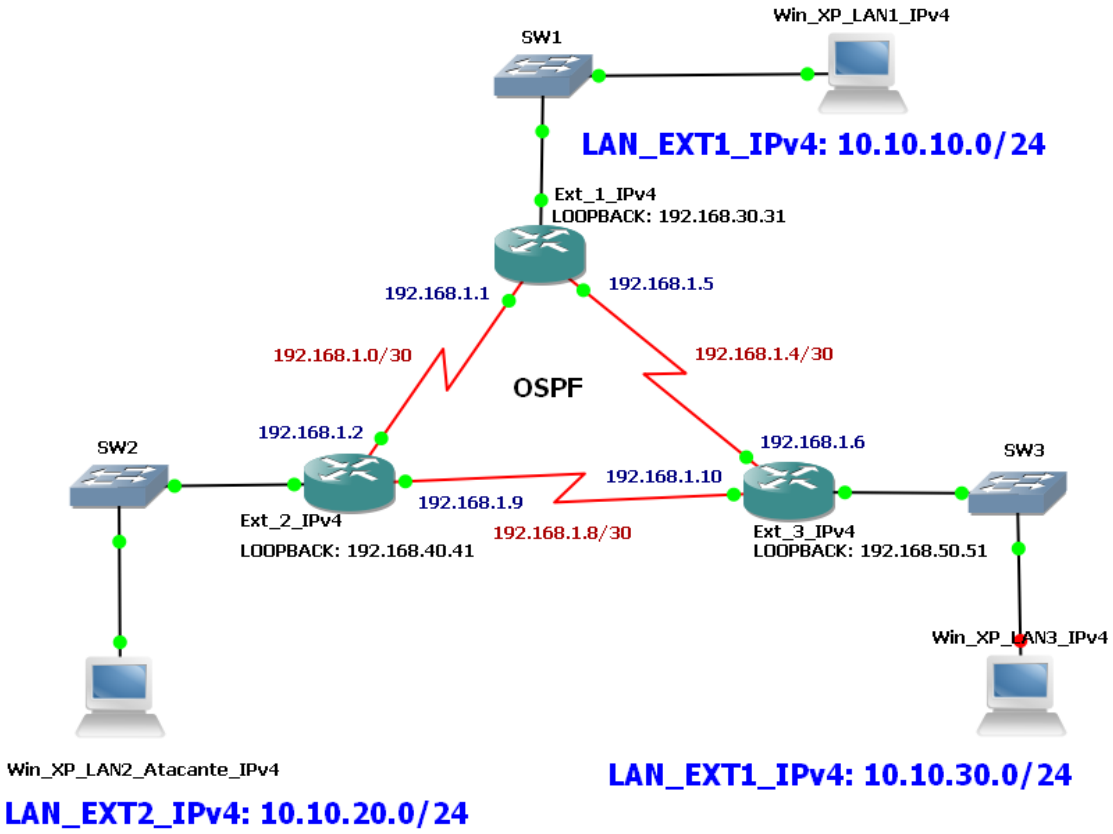


Figura 5.1: Esquema de red con IPv4

5.1.2 Verificando conectividad en la red

A continuación se puede observar las diferentes pantallas donde se comprueba que existe conectividad dentro de la red:

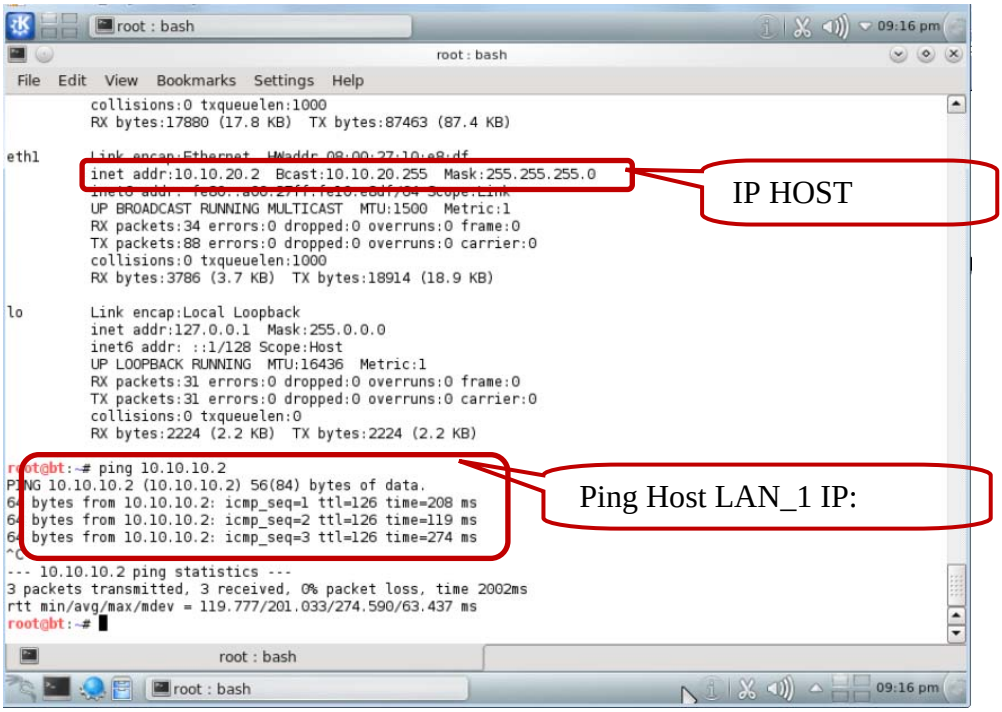


Figura 5.2: Ping de máquina BACKTRACK (IP: 10.10.20.2) máquina Win LAN1 (IP: 10.10.10.2)

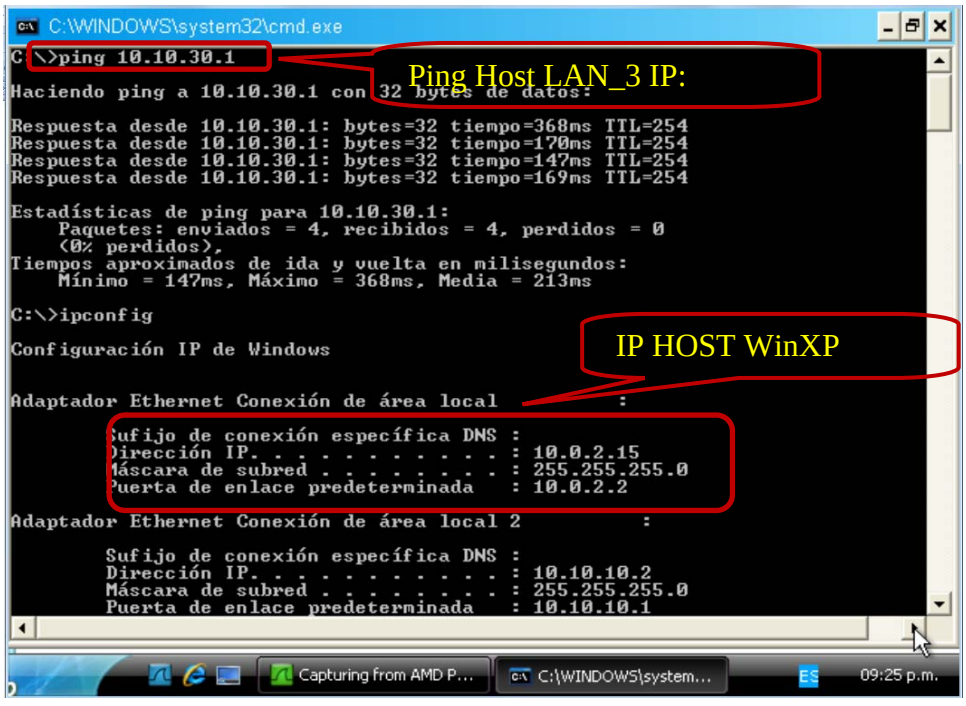


Figura 5.3: Ping desde PC Windos XP LAN1 (IP: 10.10.10.2) a GW de LAN3 (IP: 10.10.30.1)

5.1.3 Insertando tráfico ICMP a la red

Se puede apreciar que desde la PC Con BackTrack 5R1 se está ejecutando un PING continuo a la maquina Win_XP_LAN_1_IPv4 con la IP: 10.10.10.2

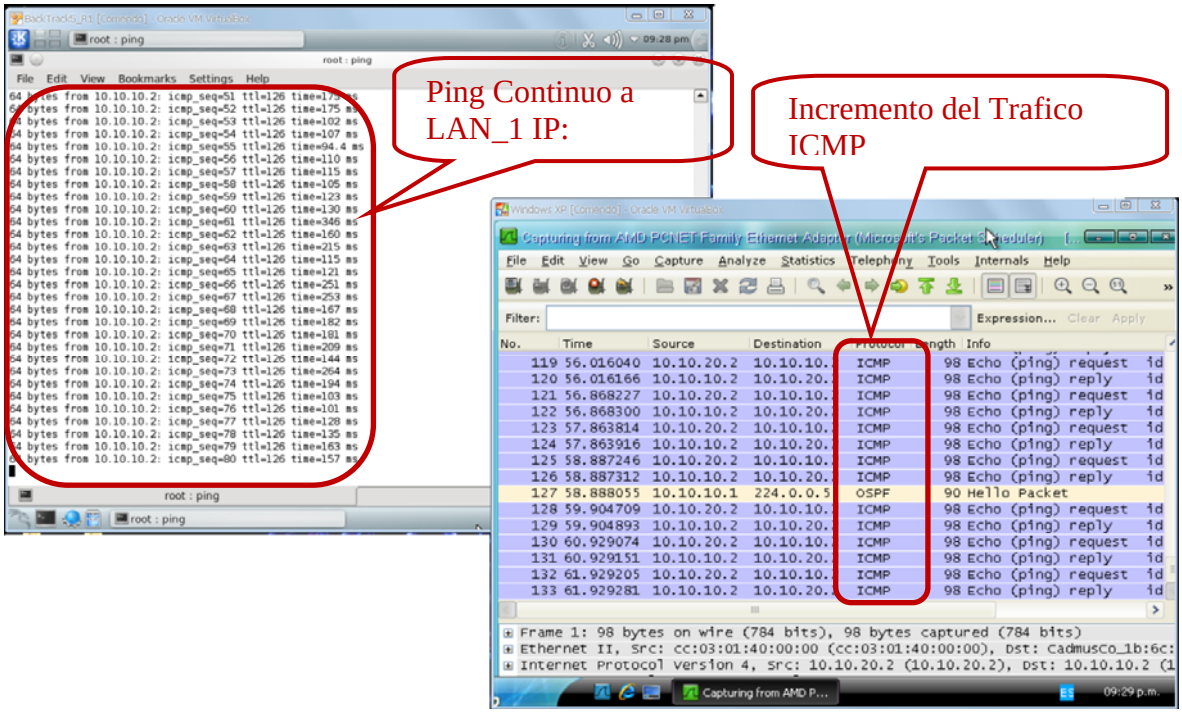


Figura 5.4: Insertando tráfico ICMP

Dado que en la red no se encuentra implementado ningún servicio como Servidores DNS, FTP, WEB, etc., la actividad en la red es mínima puesto que a mas de los paquetes presentados por el ping activo (paquetes ICMP) desde la máquina atacante a la máquina de la víctima, solo se ven unos muy pocos paquetes OSPF -> HELLO.

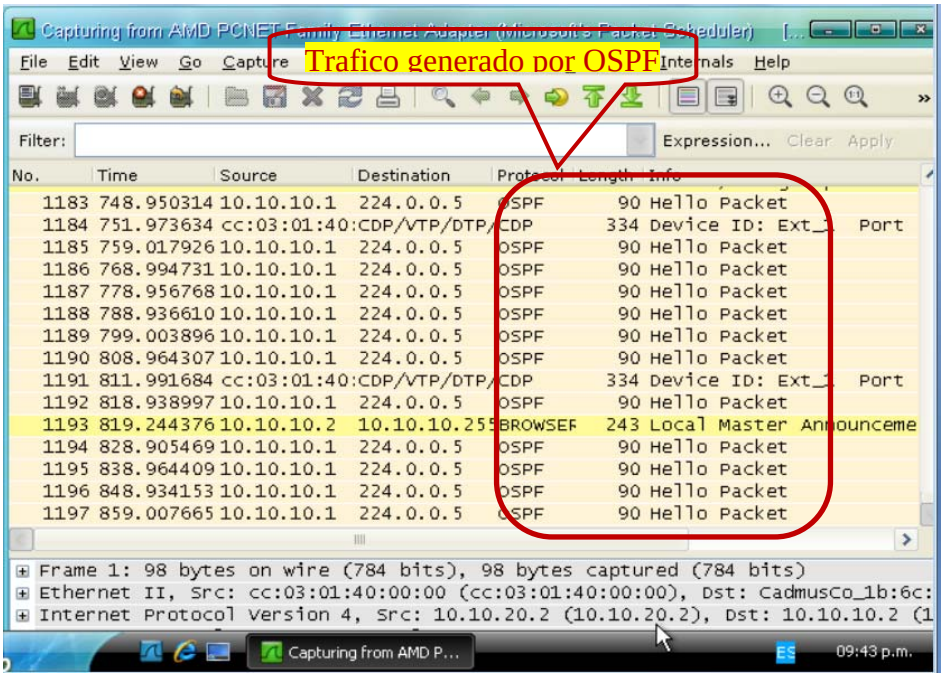


Figura 5.5: Captura de tráfico generado por OSPF

5.2 Detección de vulnerabilidades de la red con las Herramientas de BackTrack5R1

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX. WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión

de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless.

5.2.1 OpenVas:

OpenVAS, una herramienta que permite identificar las vulnerabilidades de un equipo o servidor desde otra PC remota, es decir, nos dice cuales son las posibles vulnerabilidades a las que puede estar expuesto el equipo analizado durante un ataque remoto, la gravedad de esas vulnerabilidades y unas recomendaciones para su solución.

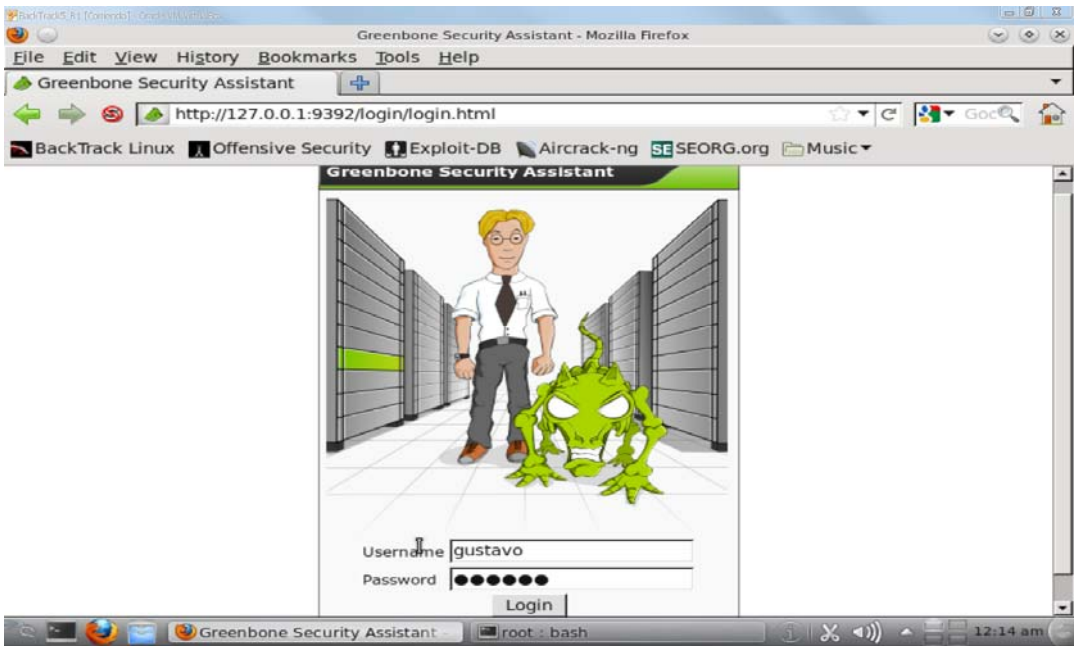


Figura 5.6: Pantalla de ingreso a OpenVas

5.2.1.1 Creando objetivos (Targets)

Se debe seleccionar la ubicación *Configuration – Targets*, del lado izquierdo de la pantalla, luego es necesario especificar el nombre del Dispositivo (*Name*), su dirección IP (*Hosts*), y de ser necesario un comentario adicional (*Comment – optional*), para de esta forma determinar cuál será el dispositivo a ser analizado, luego de introducir estos datos damos un click en Create Target y aparecerá este en la parte inferior de la pantalla junto a los otros dispositivos que se hayan creado o se vayan a crear.

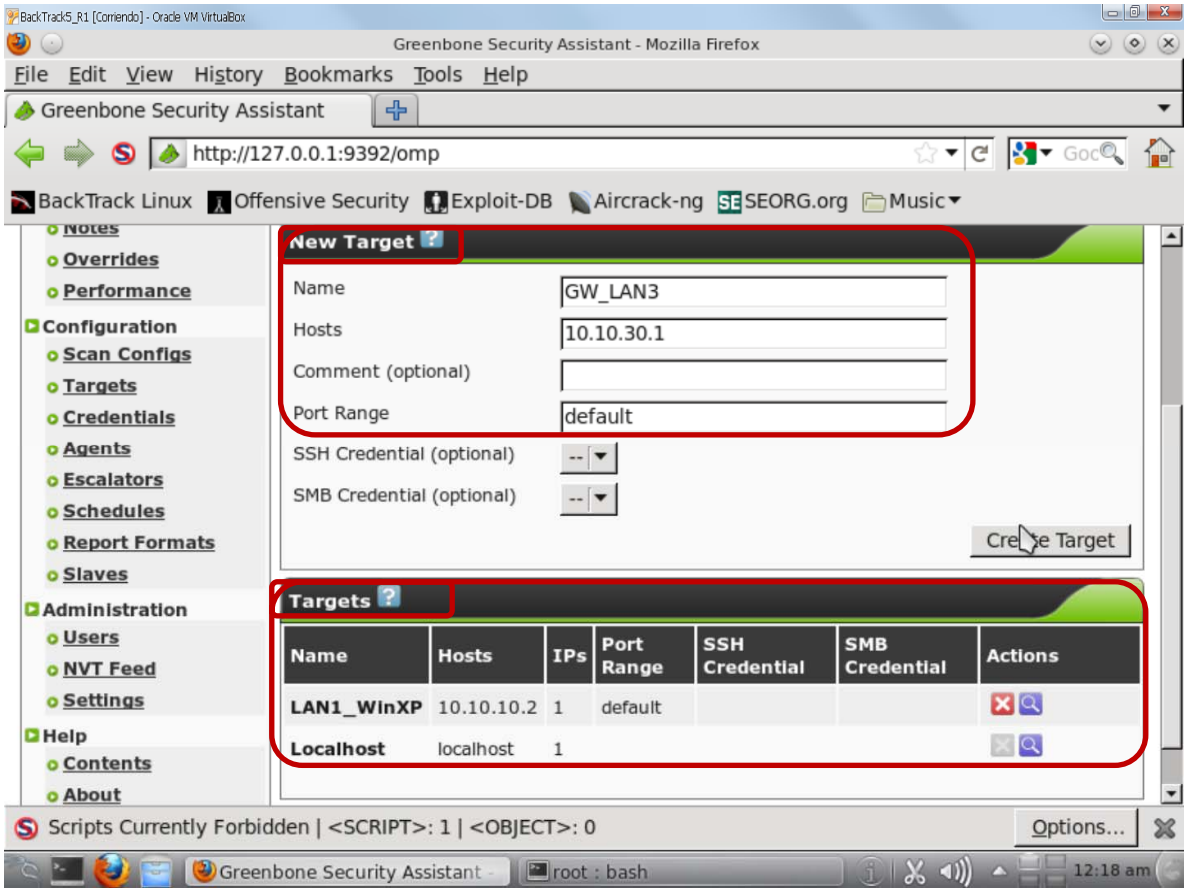


Figura 5.7: Crear targets

5.2.1.2 Nueva tarea (New task)

Una vez que se han definido los objetivos (targets) se puede definir qué tipo de tarea se puede ejecutar sobre cada uno de estos objetivos, para esto se selecciona *Scan Management – New Task*, aquí se puede escoger el Nombre del Objetivo (*Name*), configurar el nivel de escaneo que se realizará sobre el objetivo como se muestra en la figura siguiente, los demás campos son opcionales o se puede mantener la configuración por defecto.

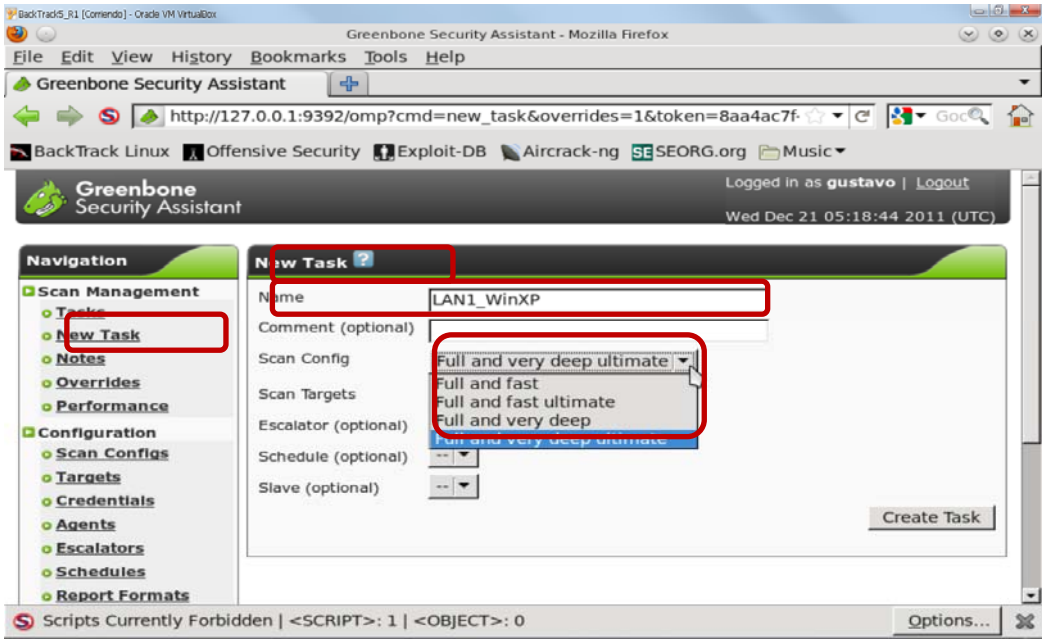


Figura 5.8: Crear nuevas tareas

Una vez definida la tarea a realizar sobre un determinado Objetivo, se dará un click en el botón *Create Task*, luego se debe seleccionar la pestaña del lado izquierdo de la pantalla la opción *Scan Management – Tasks* y se puede verificar su correcta creación como indica la figura siguiente:

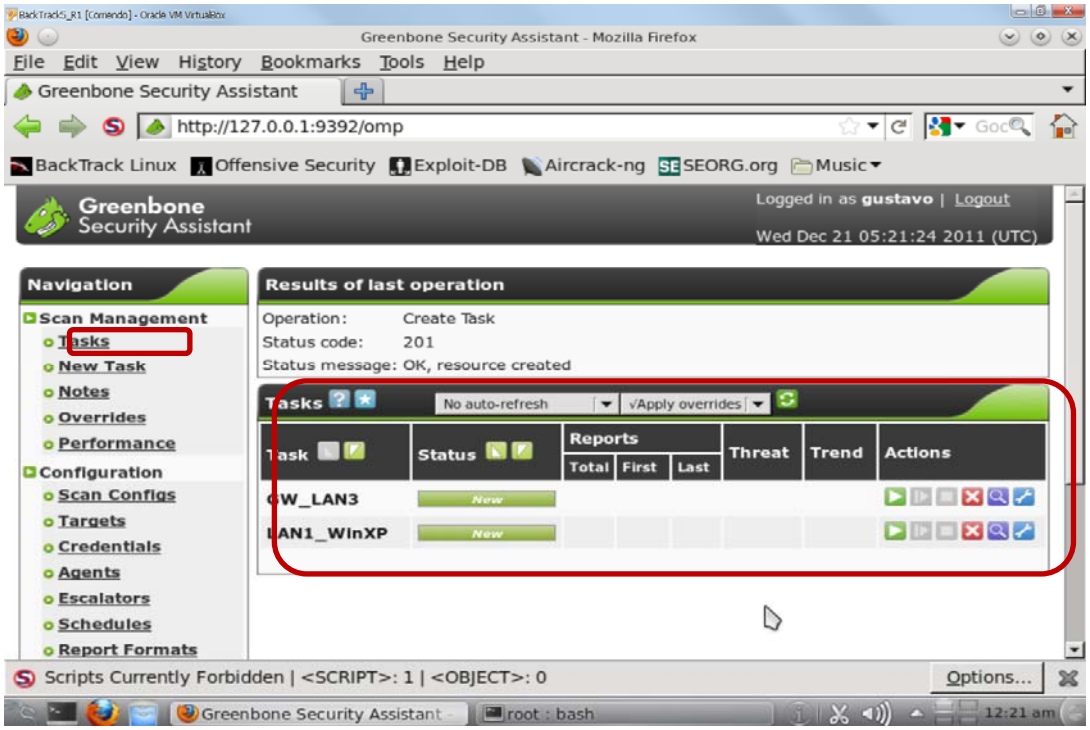


Figura 5.9: Visualización de tareas creadas

5.2.1.3 Iniciar tarea (Start task)

En la opción *Scan Management -Tasks* se debe dar click en el ícono resaltado en el recuadro rojo de la figura que se encuentra a continuación e iniciará el escaneo que tendrá un respuesta más o menos larga de acuerdo al nivel de escaneo seleccionado y a la complejidad de la configuración y/o servicios que se encuentre en el dispositivo objetivo:

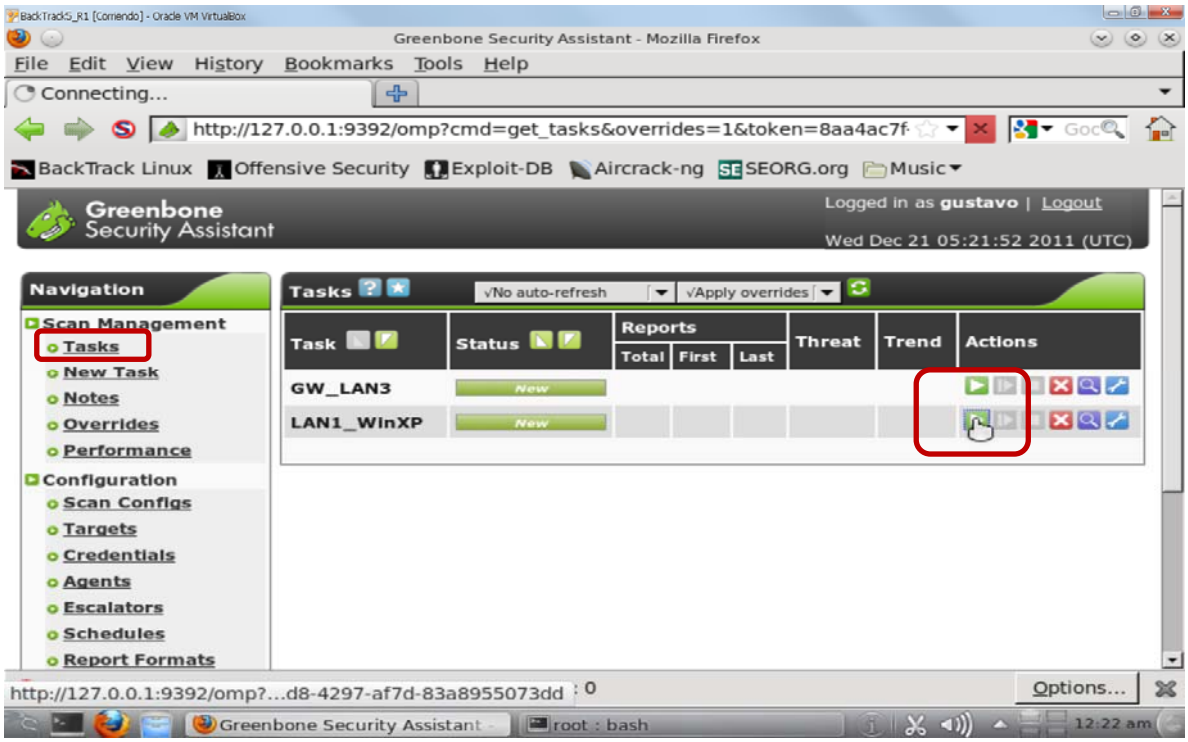


Figura 5.10: Inicio de tareas

A continuación se verificara el inicio del escaneo del dispositivo con un **Requested** como se muestra en la figura siguiente:

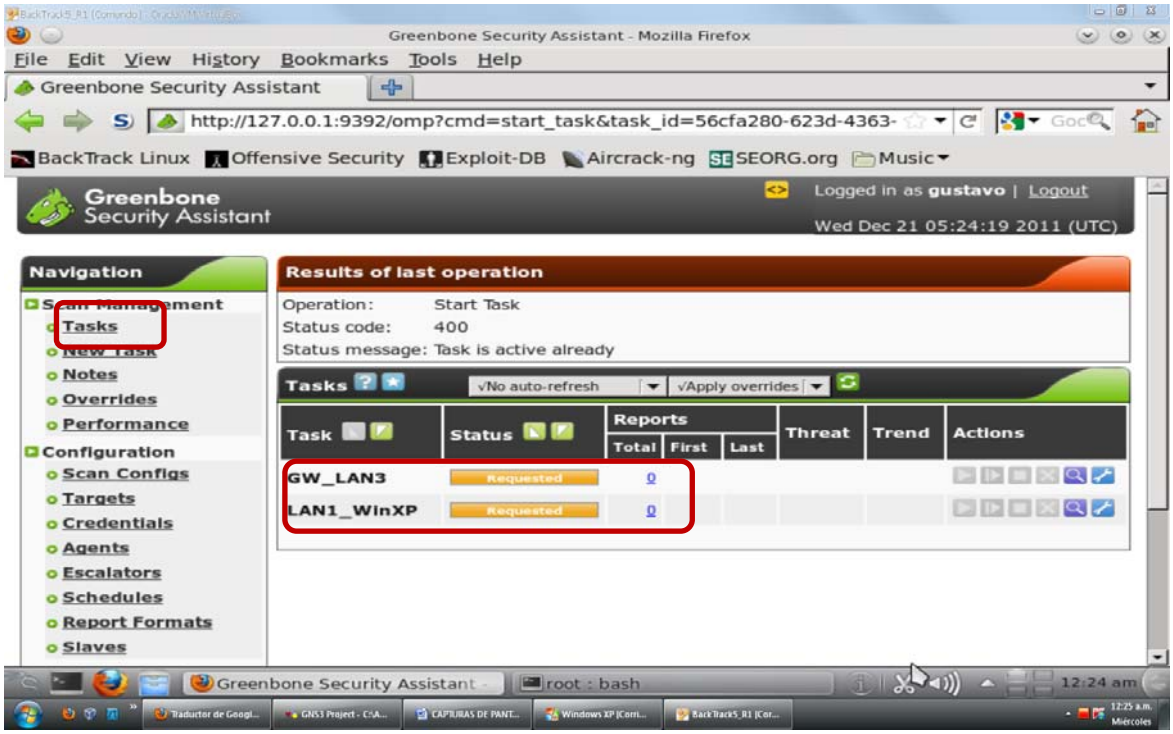


Figura 5.11: Estado REQUESTED de una tarea

Se puede verificar el avance del escaneo, mismo que se muestra en datos porcentuales como se indica a continuación:

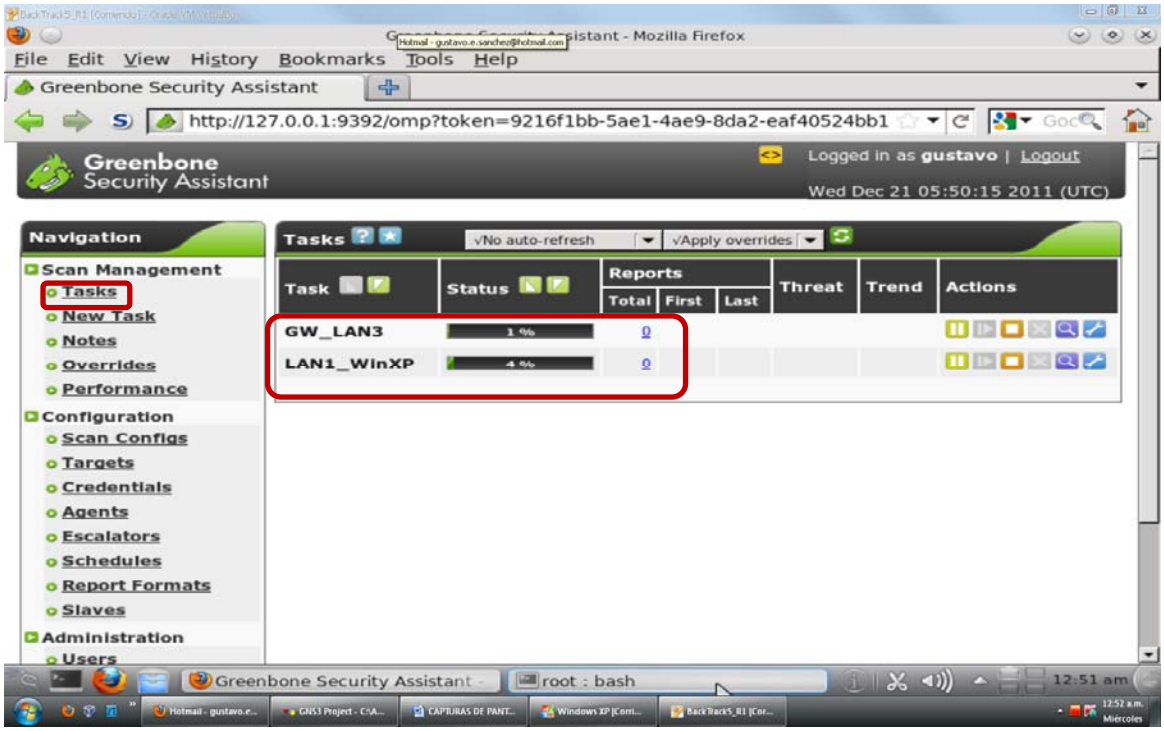


Figura 5.12: Progreso de escaneo a objetivos

Una vez finalizado el escaneo se presentara el mensaje *Done* en los *Tasks* ya finalizados, como se muestra en la figura siguiente:

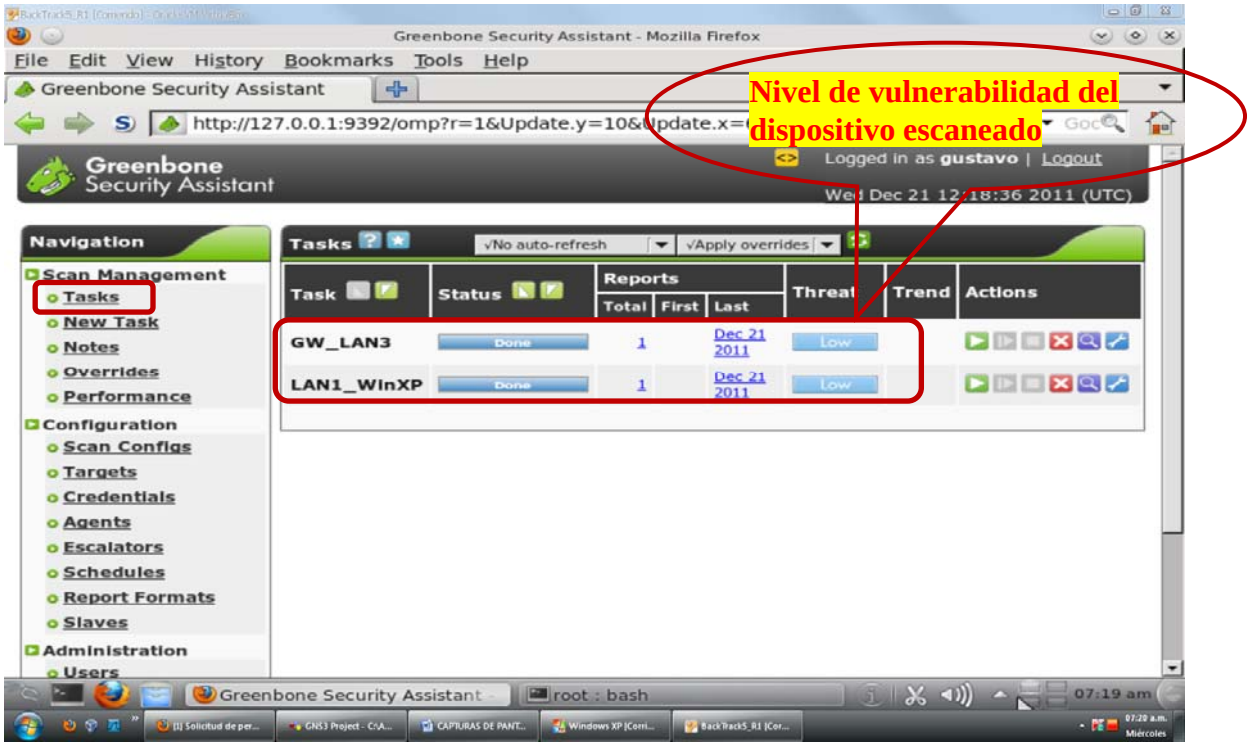


Figura 5.13: Finalización de escaneo a objetivos

5.2.1.4 Actividad en el Host Escaneado

El Host escaneado como se muestra en la Figuras 5.14, 5.15 y 5.16 muestra un incrementa en la actividad de su puerto Ethernet con presencia de actividad de los protocolos TCP, SMB, Ripv1, Ripv2, SNMP, XDCMP, UDP, TFTP, etc, cada uno de estos protocolos muestran a su vez actividad en distintos puertos lo que evidentemente muestra que externamente se está generando este tráfico para de esta manera tratar de obtener información sensible del Host:

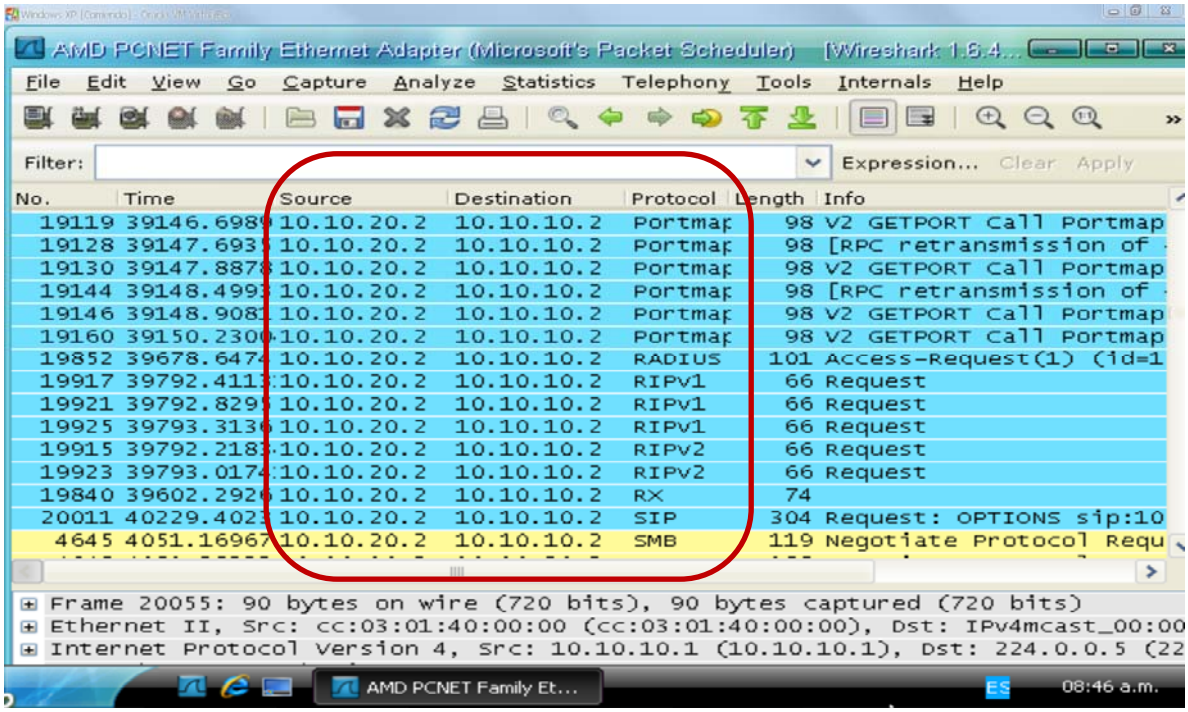


Figura 5.14: Actividad en el host escaneado

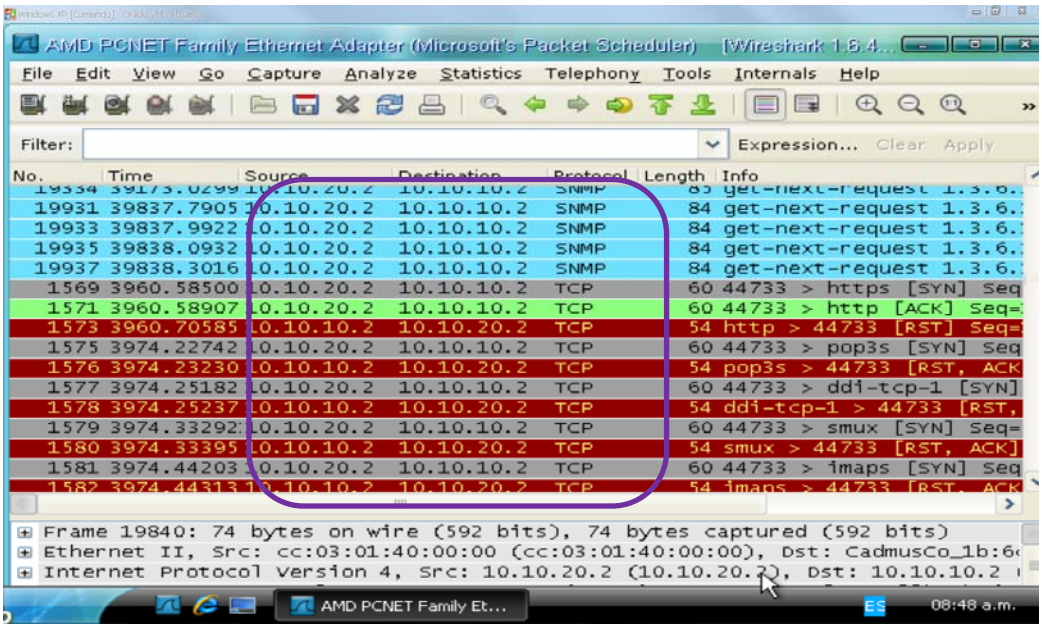


Figura 5.15: Actividad en el host escaneado

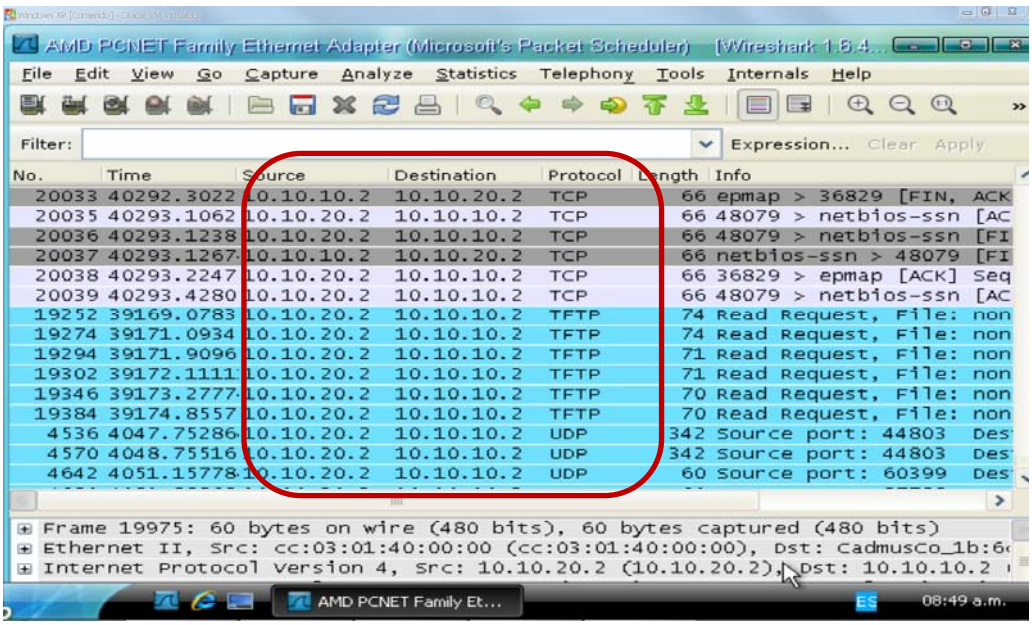


Figura 5.16: Actividad en el host escaneado

En el **Anexo 2** se adjunta un reporte realizado a una dirección IP, correspondiente a una dirección IP de un Servidor DNS (200.107.10.52) de un ISP REAL, OpenVas genera un reporte bastante detallado de los niveles de vulnerabilidad detectados en los diversos puertos o servicios del HOST, pudiendo definirlos como niveles BAJO, MEDIO o ALTO. OpenVas también está en capacidad de detectar el tipo de servicio, versión, vulnerabilidad del mismo, y así como puede emitir un consejo para solventar las fallas de seguridad en caso de ser detectadas.

5.3 ZENMAP – NMAP gráfico

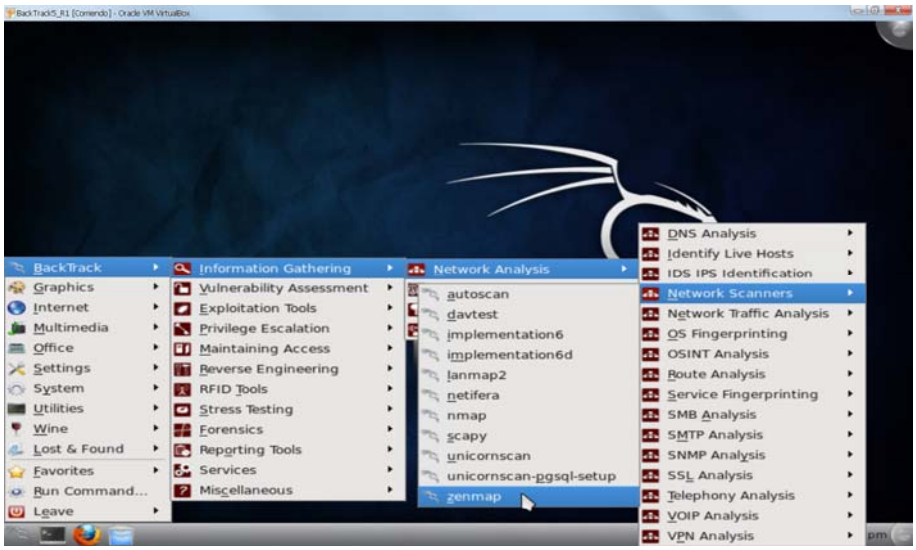


Figura 5.17. : Ubicación dentro de BackTrack

ZENMAP es una herramienta de escaneo de red, que necesita que se ingrese una dirección IP conocida de una posible víctima para seleccionar el tipo de escaneo, por cada tipo de escaneo se nos presenta el comando que se ejecutara para este fin, ZENMAP es una herramienta gráfica que se basa en NMAP.

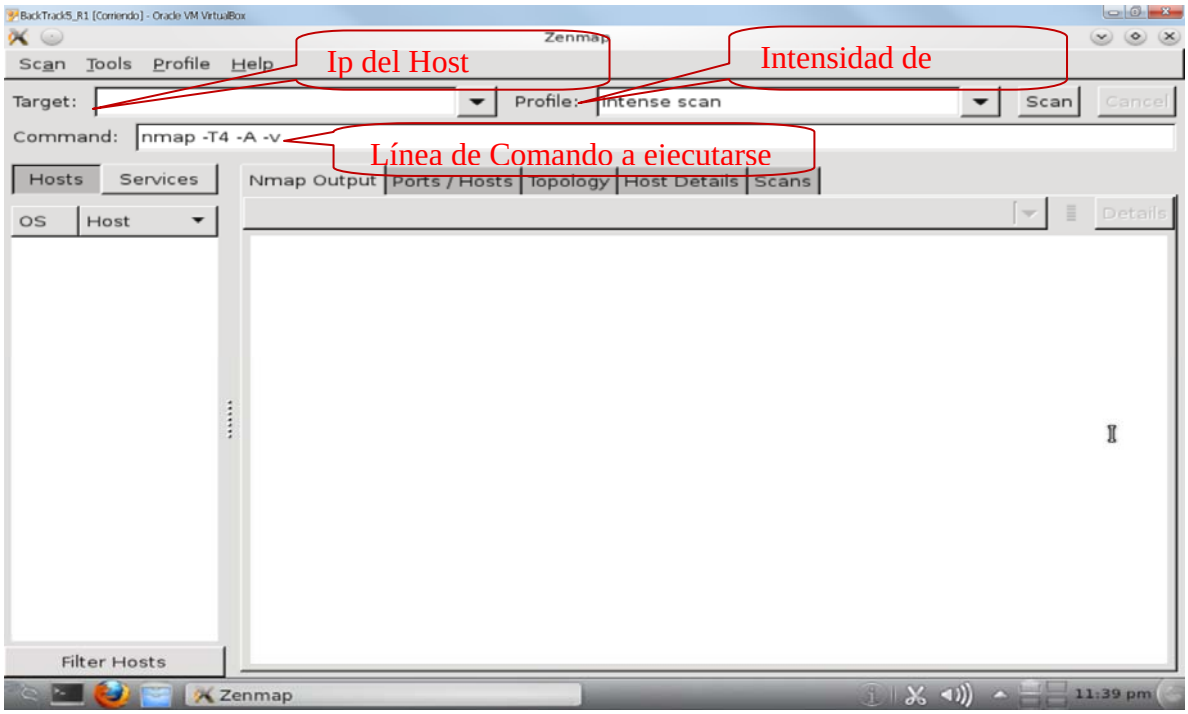


Figura 5.18 : Ingreso de parámetros en ZENMAP

Se puede notar que al ejecutar el escaneo a la dirección IP de la máquina de la LAN1 IP: 10.10.10.2, se incrementa notablemente el trafico TCP de la red como muestra la herramienta WIRESHARK.

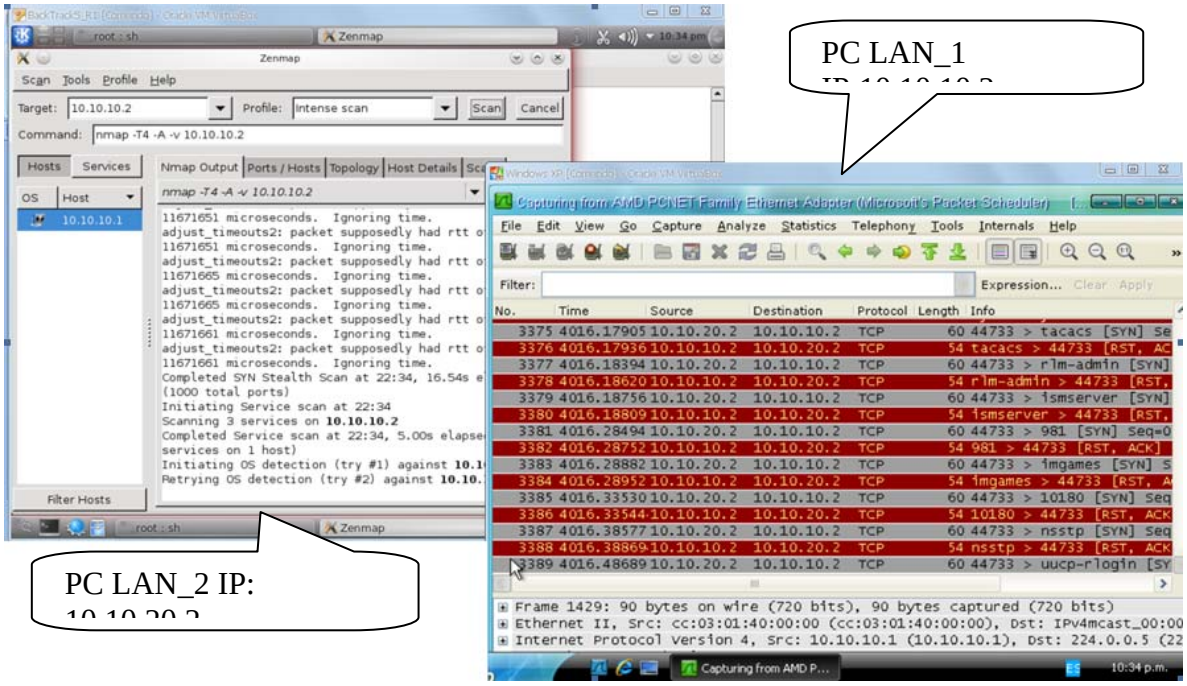


Figura: 5.19: Incremento de tráfico al ejecutar un escaneo de la red

Al final se ha escaneado las siguientes direcciones:

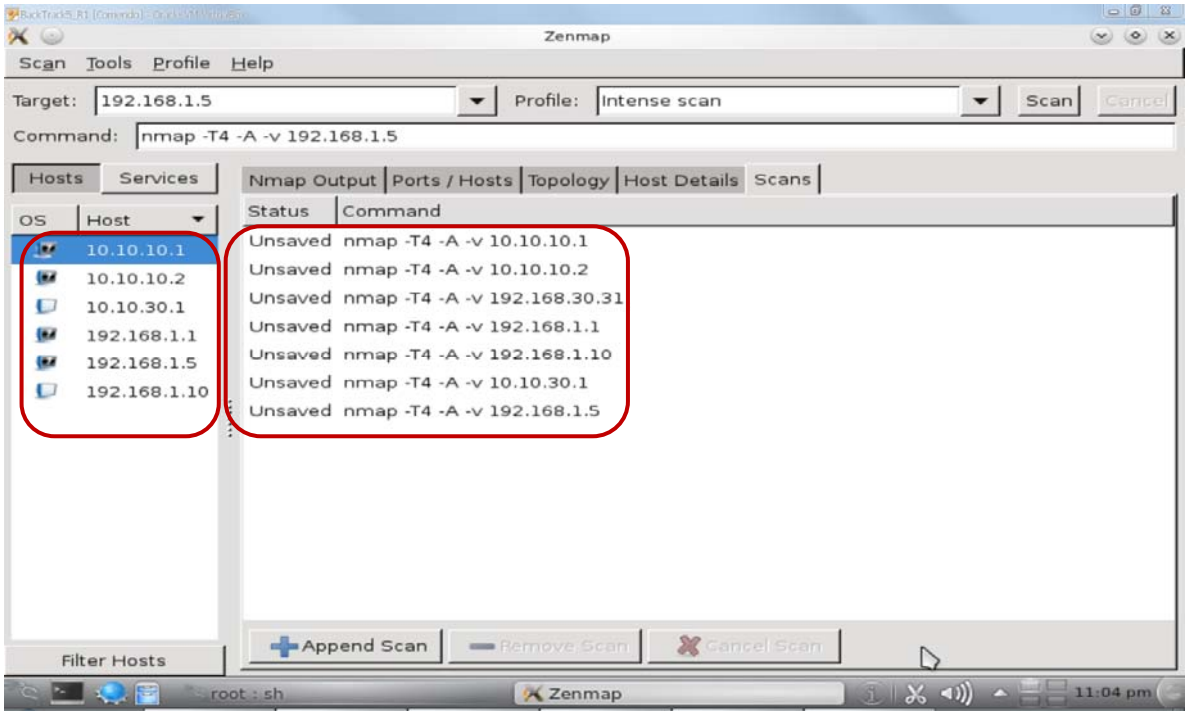


Figura 5.20 : Lista de direcciones IP escaneadas.

5.3.1 Detalles del HOST (10.10.30.1)

Al final del escaneo se puede identificar una cantidad interesante de información entre las cuales tenemos si el Host analizado esta encendido o no, el número de puertos que tiene abiertos, dirección IP del Host, Sistema Opertativo y versión del mismo.

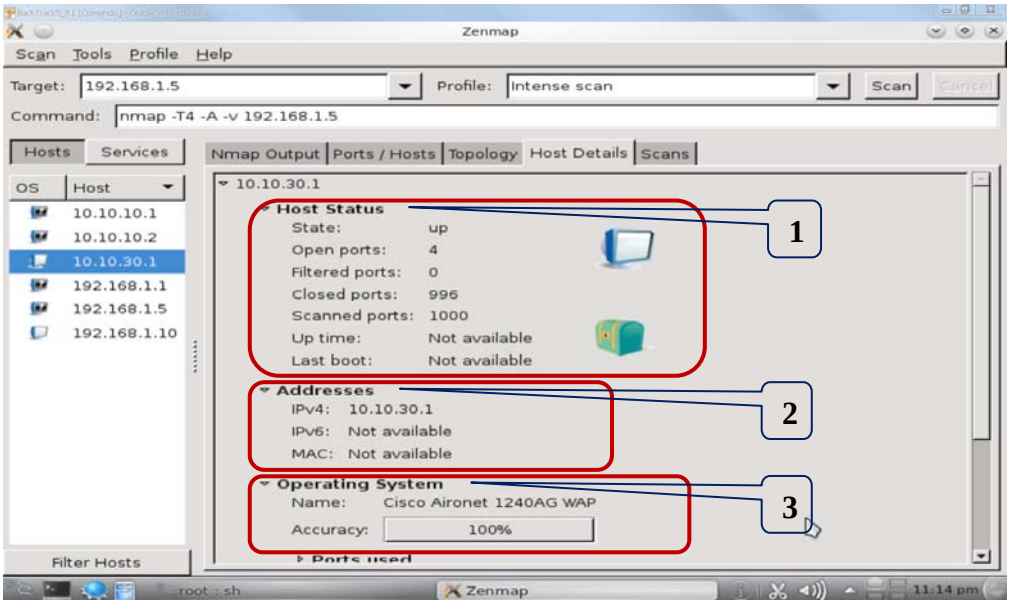


Figura 5.21: Resultados de escaneo de ZENMAP 1

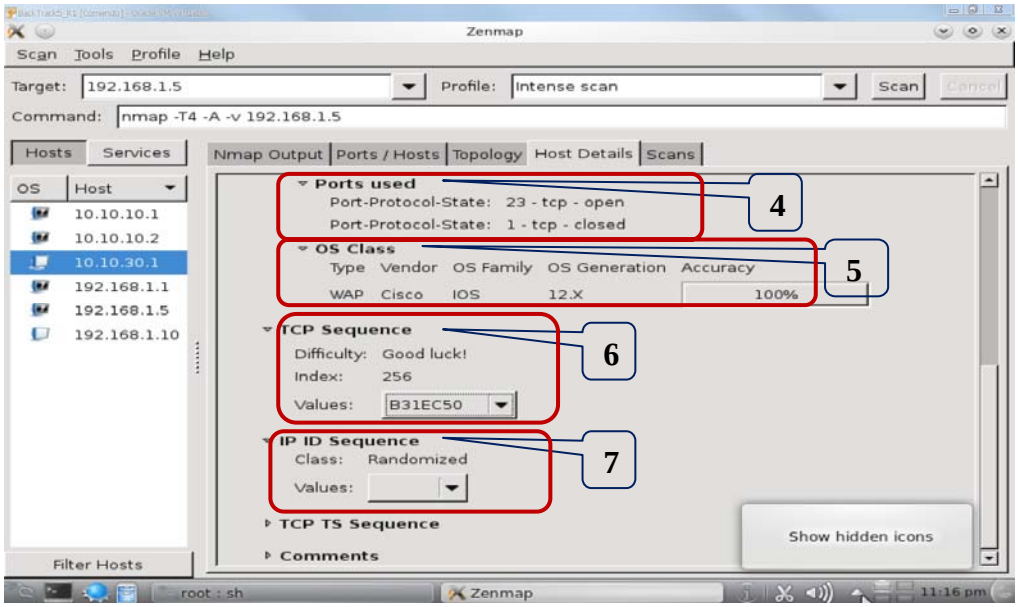


Figura 5.21: Resultados de escaneo de ZENMAP 2

5.3.2 Descubrimiento de topología

Se puede visualizar la gráfica de la topología que se auto genera a media que se va realizando el escaneo en diferentes direcciones IP.

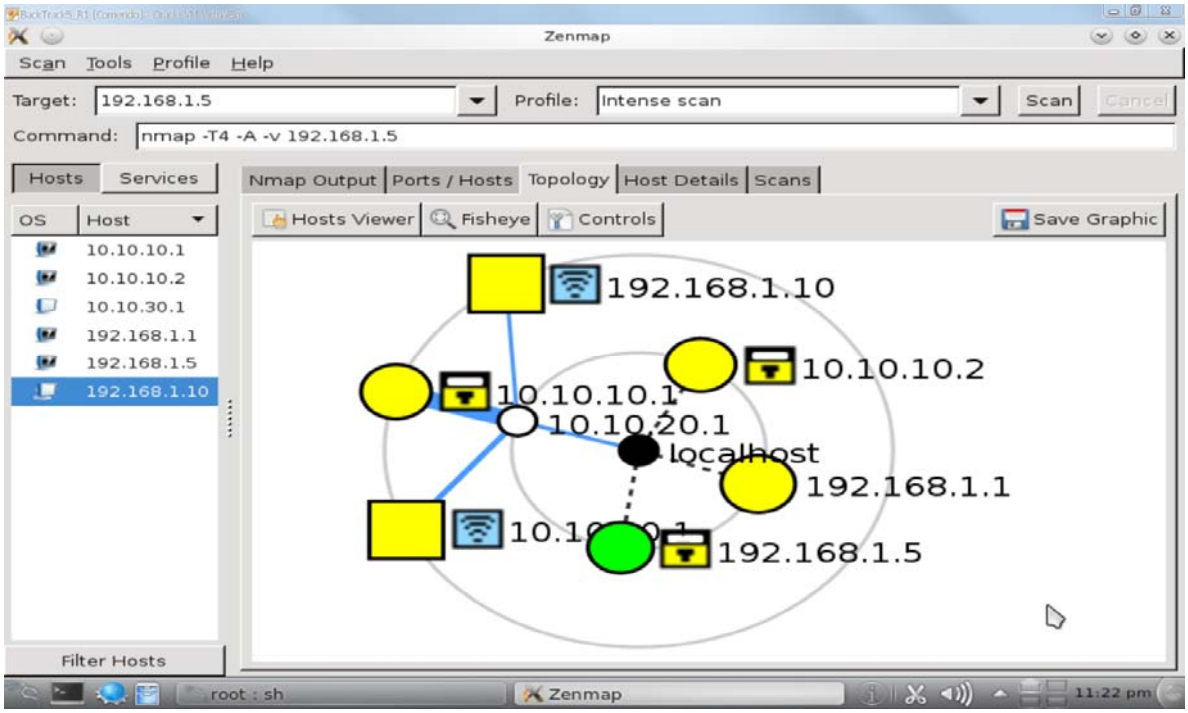


Figura 5.22: Descubrimiento de la topología de red mediante ZENMAP

5.3.3 NMAP OutPut

Permite determinar puertos, estado, servicio utilizado por cada uno de los puertos detectados, y finalmente versión.

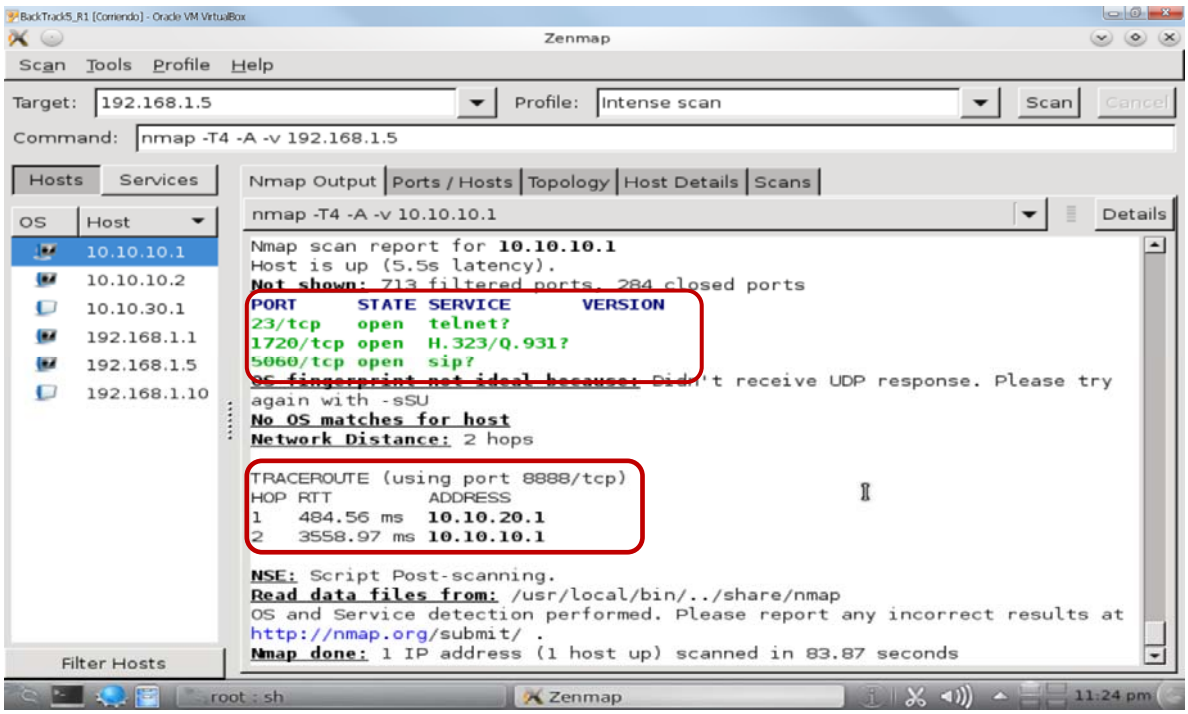


Figura 5.23: Salida de NMAP

Las pruebas realizadas son relativamente sencillas de hacer, se han realizado en un entorno IPv4 sin configurar IPsec, donde representaría una dificultad en primer término conocer las direcciones IP de las máquinas a las que se pretende analizar y luego realizar un ataque con la información que la herramienta nos proporciona.

ZENMAP brinda un reporte detallado de los puertos abiertos y las aplicaciones que se ejecutan sobre los mismos, las características de la máquina escaneada incluyendo marca, tipo de SO, versión, e incluso llega a indicar si el dispositivo escaneado tiene algún tipo de servicio activo, sus secuencias, si los datos son randomicos o no, en fin esto es una herramienta que permite sin duda obtener valiosa información que le daría a un atacante las pautas necesarias para penetrar a la red por sus puntos más vulnerables. Es además interesante la capacidad de obtener un mapa gráfico de la topología de la red, lo que aportaría a tener una mejor idea bastante precisa de cómo está estructurada la misma.

Un factor determinante también es el hecho que entrega los saltos exactos con sus respectivas IP lo que sin duda es una herramienta valiosa para quien quiere incursionarse en la red y realizar posibles ataques.

5.4 Escenario de pruebas para IPv6

5.4.1 Esquema de la red

De acuerdo al esquema propuesto dentro del anteproyecto de tesis se ha diseñado un esquema que servirá para realizar las pruebas con IPv4 e IPv6:

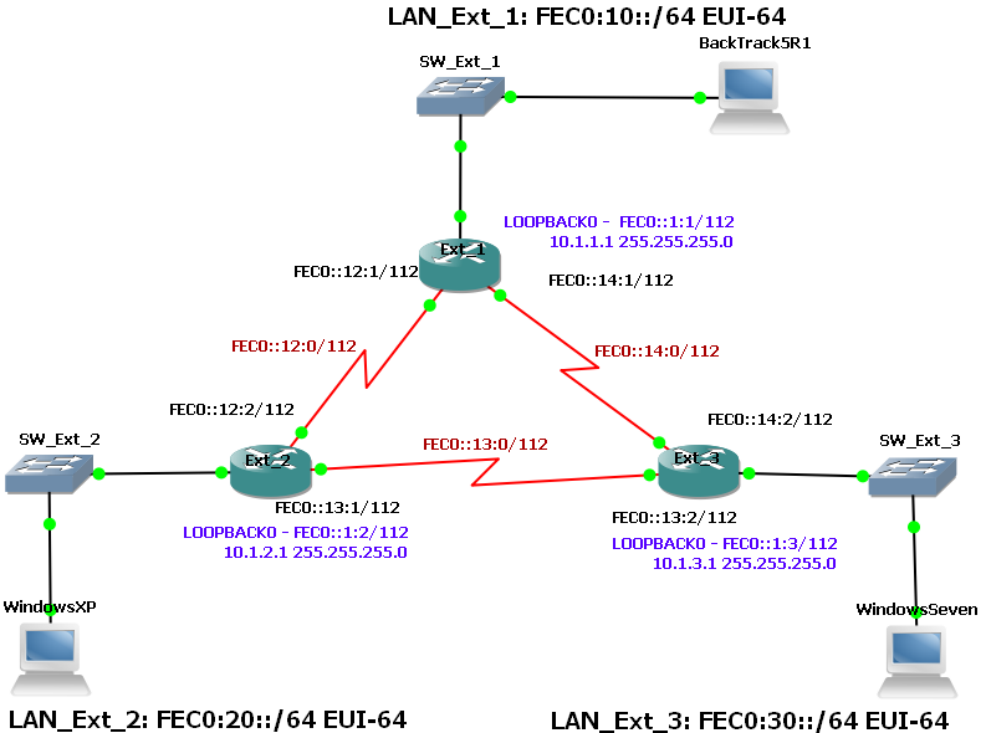


Figura 5.24: Esquema de red con IPv6

5.4.2 Verificando conectividad en la red

A continuación se puede observar las diferentes pantallas donde se comprueba que existe conectividad dentro de la red:

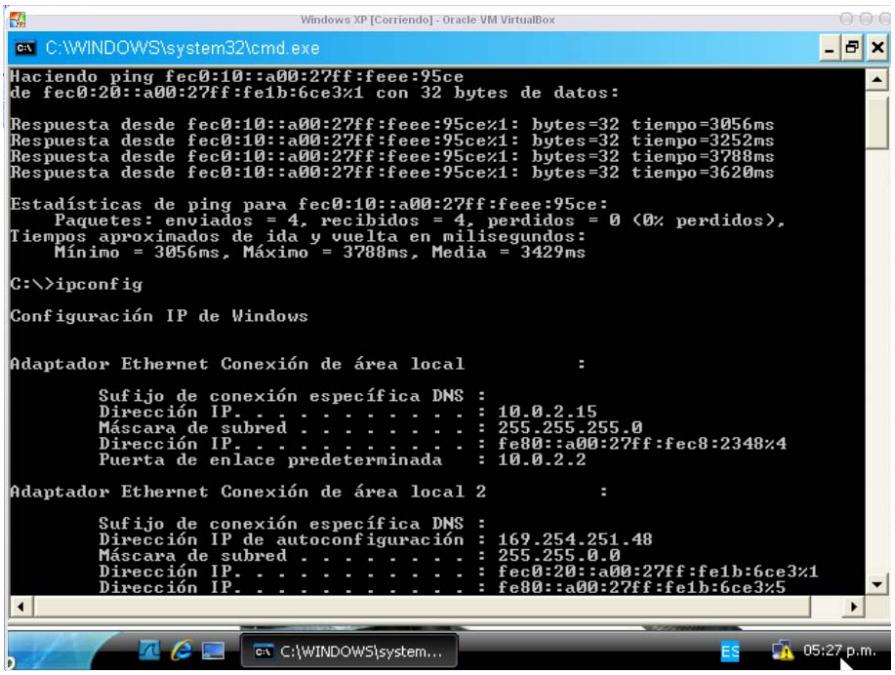


Figura 5.25: Ping desde Host Windows XP (FEC0:20::A00:27FF:FE1B:6CE3) hasta Host Backtrack5R1 (FEC0:10::A00:27FF:FEEE:95CE)

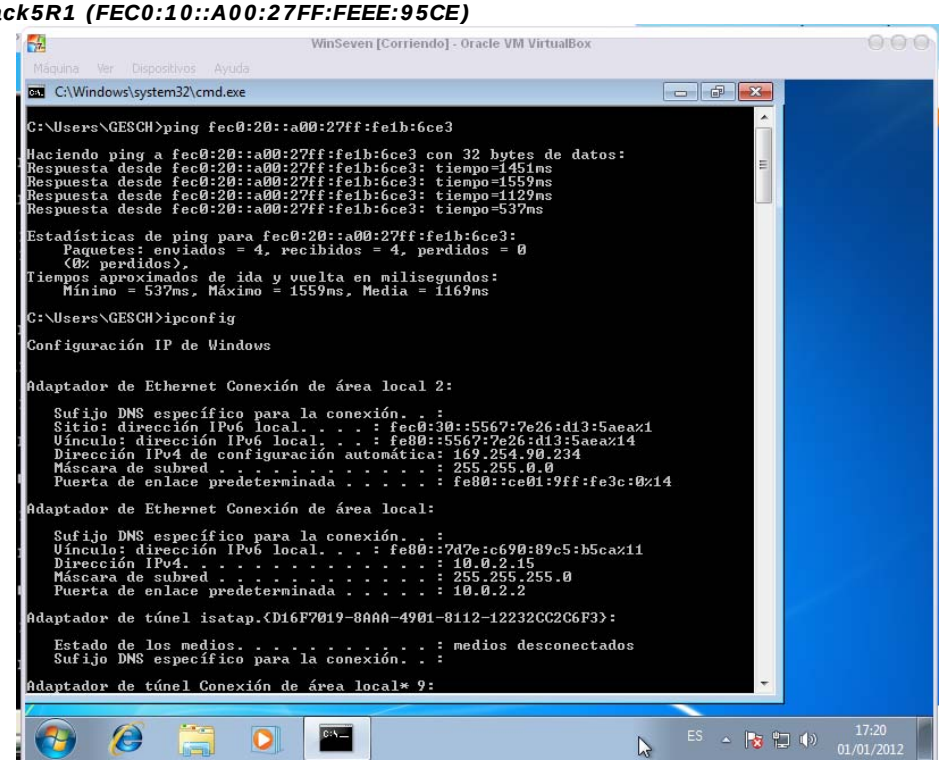


Figura 5.26: Ping desde Host Windows Seven (FEC0:30::5567:7E26:D13:5AEA) hasta Host Windows XP (FEC0:20::A00:27FF:FE1B:6CE3)

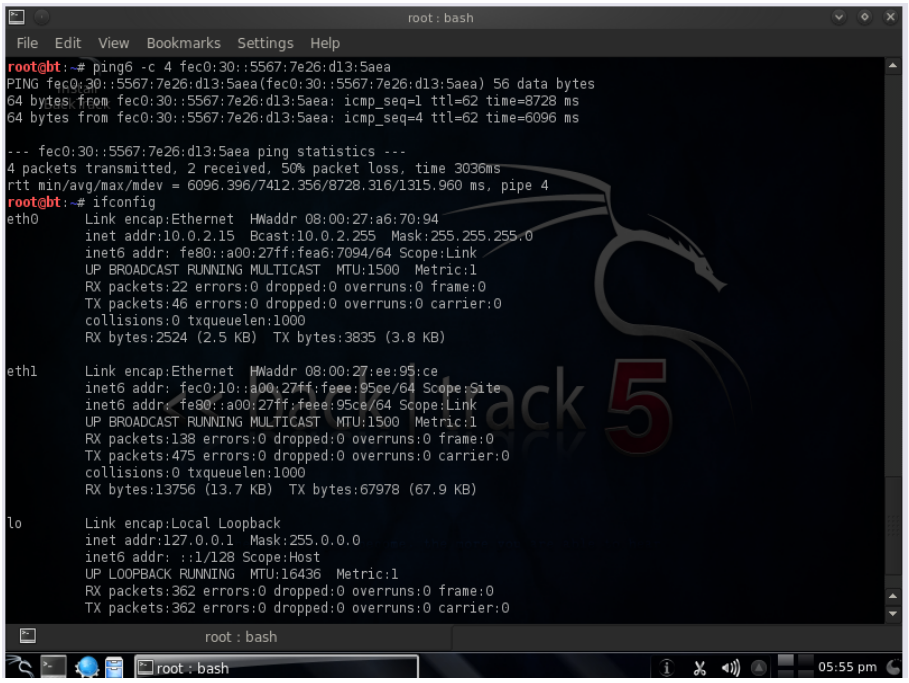


Figura 5.27: Ping desde Host BackTrack5R1 (FEC0:10::A00:27FF:FEEE:95CE) hasta Host Windows Seven (FEC0:30::5567:7E26:D13:5AEA)

5.4.3 Escaneo de Vulnerabilidades con NMAP en IPv6

Aún antes de iniciar el escaneo se puede observar la actividad de la red en LAN_Ext_3: Pc Windows Seven IPv6: FEC0:*30*::5567:7E26:D13:5AEA, mostrando datos interesantes como direcciones, protocolos que se están manejando:

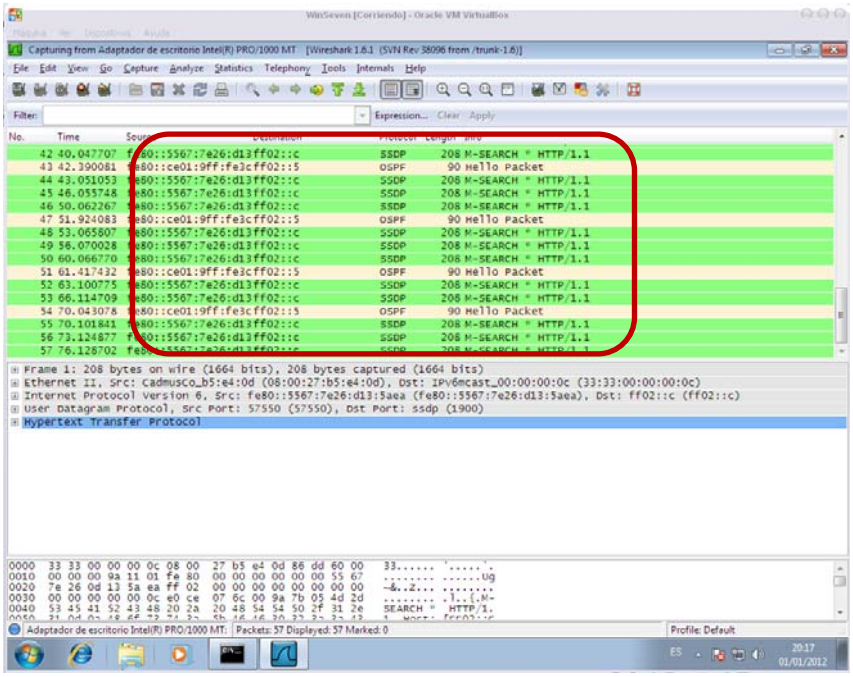


Figura 5.28: Actividad de la red antes de iniciar escaneo1

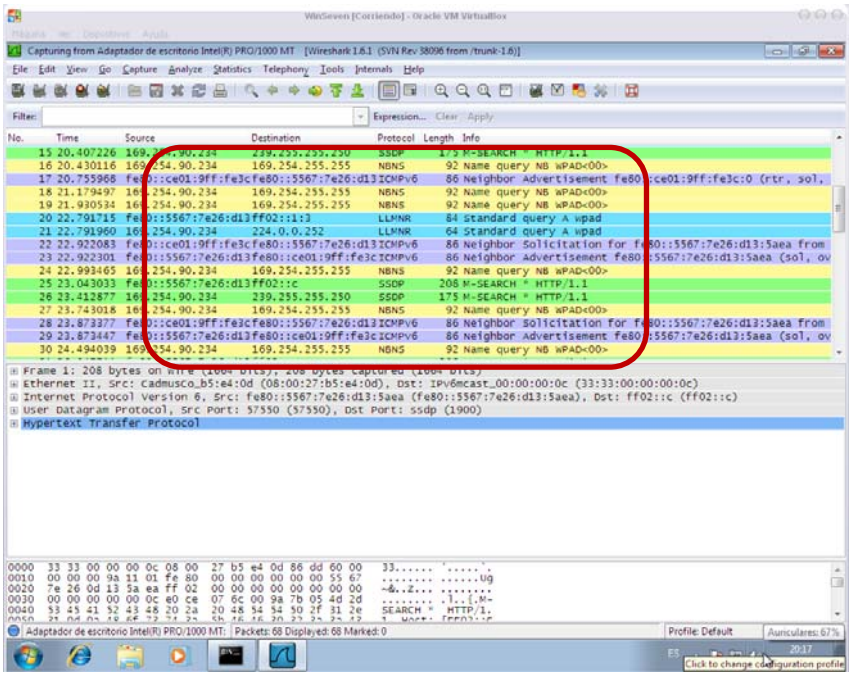


Figura 5.29: Actividad de la red antes de iniciar escaneo 2

En las dos imágenes se puede apreciar claramente que la actividad es mínima presentándose únicamente paquetes OSPF Hello Packet así como paquetes SSDP, NBNS, LLMNR, SSDP, ICMPv6 que son propios del protocolo IPv6 y de la forma en la que este mantiene la comunicación entre dispositivos.

Al contrario de lo que se tenía en IPv4 esta herramienta no cuenta aún con un entorno gráfico, lo que no limita de todos modos al atacante de realizar el escaneo y obtener los resultados buscados:

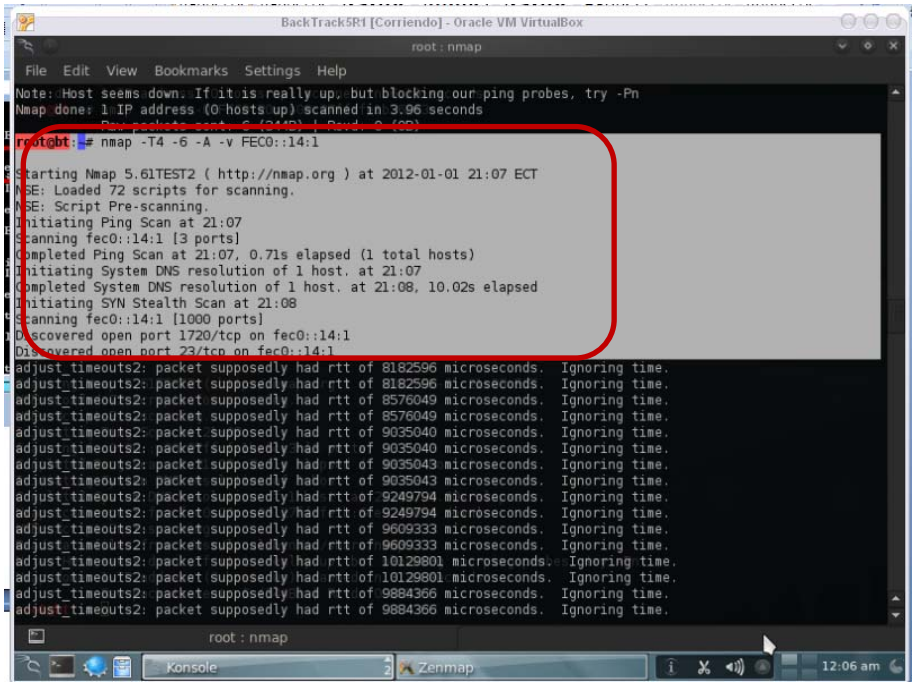
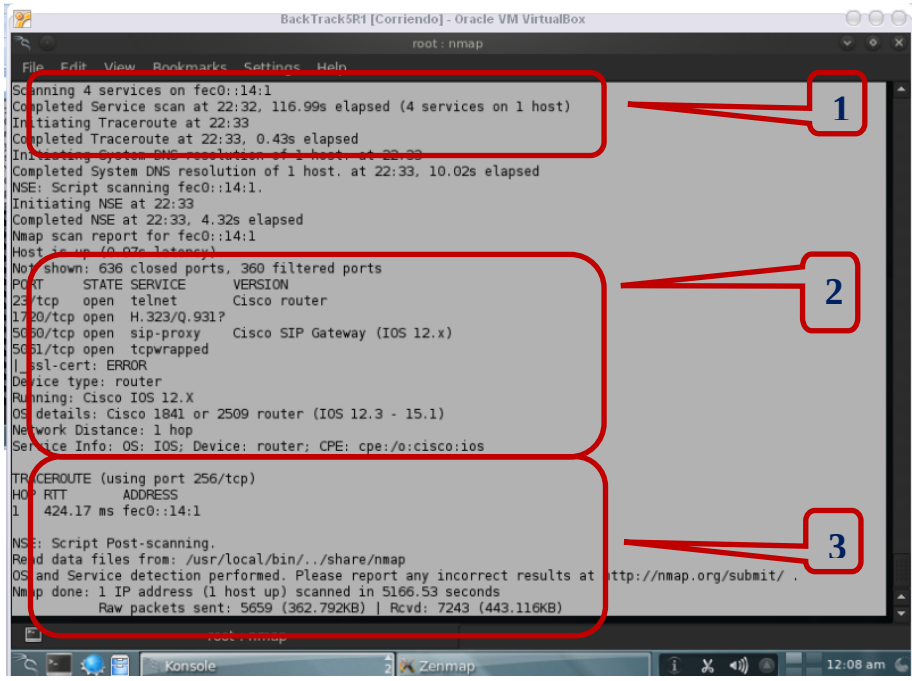


Figura 5.30: Escaneo desde Host BackTrack5R1 (FEC0:10::A00:27FF:FEEE:95CE) hasta el Puerto Serial 1/1 (FEC0::14:1) del Router Ext_1



5.31: Resultado del escaneo con NMAP

Se puede sacar las siguientes conclusiones:

En el recuadro 1.- se puede apreciar que se está realizando el escaneo sobre la Ipv6: FEC0::14:1, y se encontró cuatro servicios en este dispositivo.

El recuadro 2.- muestra la lista de puertos que se encontraron abiertos, los servicios a los que están relacionados y la versión de los mismos, así como detalles específicos del Sistema Operativo del Dispositivo.

Finalmente el recuadro numero 3.- Muestra los saltos detectados por el comando TRACEROUTE hasta llegar al destino, se determina también el tiempo en mili segundos que transcurrió para concluir con el escaneo, así como el numero de paquetes enviados y recibidos.

De las pruebas realizadas podemos concluir que el solo hecho de usar IPv6 no representa ninguna ventaja de seguridad en la red, ya que se ha obtenido el mismo tipo de información que con IPv4 en ataques en este caso de reconocimiento, man in the middle, sniffer.

CONCLUSIONES

1. La implementación de IPv6 ya no es una opción con el agotamiento de las direcciones IPv4, la transición es un proceso, largo, complejo y costoso pero inevitable.

2. La cabecera IPv6 elimina o hace opcionales varios campos de la cabecera de IPv4, consiguiendo una cabecera de tamaño fijo y más simple, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el costo en ancho de banda de la cabecera de IPv6.

3. Protocolos como OSPF y RIPgn confían en las cabeceras de IPsec AH y ESP para proveer integridad, autenticación, confidencialidad y protección anti repetición en el intercambio de información, mientras que OSPF e IS-IS siguen usando sus mecanismos propios al ser extendidos a IPv6.

4. IPv6 no pretende ser la solución a los problemas de seguridad en los diversos tipos de redes, por lo que se debe evitar el caer en una falsa sensación de seguridad al pensar que con tan solo implementar IPv6 se solucionaran gran parte de los problemas de seguridad de la red, mas sin embargo características como las de poder interactuar con protocolos como OSPFv3 permite garantizar un mejor nivel de seguridad tanto a nivel de área como a nivel de interface (Autenticacion y/o Encriptacion).

5. La misma arquitectura de IPv6 hace más dificultosa la propagación de ciertos tipos de ataques más no se observa una mejora substancial en su seguridad al

referirse a ataques internos, mientras que depende de las políticas utilizadas para determinar un nivel de seguridad optimo en ataques remotos.

6. Es importante señalar que el número extremadamente grande de posibles direcciones que se puede encontrar aun en una red del tamaño de un campus universitario o empresarial, hace que resulte muy difícil para un atacante realizar un escaneo en busca de direcciones activas, y de todas estas definir cuál de estas es más vulnerable y así poder iniciar una incursión en la red.

7. La aplicación de Seguridad es indispensable en las redes públicas. IPSec tiene un enfoque diferente a otros protocolos de seguridad más populares como SSH y SSL, que funcionan en la capa de transporte y están ligados con una aplicación particular. Con IPSec pueden establecerse comunicaciones seguras extremo a extremo, de forma flexible y bajo diversas configuraciones, sin importar la aplicación del nivel de usuario.

8. Para los diversos tipos de redes, es importante encontrar en IPv6 la posibilidad de recuperar o incorporar cualquiera sea el caso, la opción de una verdadera conexión extremo a extremo, gracias a que en IPv6 ya no se deberá depender del NAT, que trae como consecuencia el que solo funcionen correctamente las aplicaciones cliente-servidor, razón por la que Internet se ha convertido en una red mucho más compleja, cara y difícil de gestionar, haciendo de esto una oportunidad para IPv6 de reducir la complejidad de la red.

9. Es muy importante sacar a relucir que más allá de la complejidad del protocolo IPv6, para el usuario final resultara un cambio absolutamente transparente gracias a la capacidad de autoconfiguración de los dispositivos de red, que en la actualidad es soportada por si la totalidad de fabricantes.

RECOMENDACIONES

1. La migración a IPv6 en inminente por lo que se debería tender desde ya a hacer planes de migración para que esto se dé como un proceso planificado y no deje brechas que afecten la seguridad de las redes.
2. IPsec es una potente herramienta para la seguridad de las redes pero se necesita un alto grado de capacitación para explotarla.
3. El uso apropiado de las políticas que ofrece IPsec, representa una forma relativamente sencilla y a un bajo costo de brindar confidencialidad y seguridad en el envió o intercambio de información en una red Extremo a Extremo, y en el caso de las redes corporativas que suelen requerir del uso de VPN's las aplicaciones y ventajas que ofrece IPsec tunneling son indudables y por mucho, mejor a las que se puede encontrar en IPv4.
4. La mayoría de los ataques siguen teniendo el mismo modo de funcionamiento por lo que se debe basar en la experiencia de cómo mitigarlos en IPv4 para poder reaccionar eficientemente ante las amenazas conocidas y aplicar las mismas políticas de seguridad de IPv4 para evitar ser víctima de estos ataques o amenazas.
5. IPSec es obligatorio para IPV6 pero también se puede implementar en IPV4, éste sería un buen inicio para las empresas que no planean implementar IPV6 a corto plazo, mas es importante recalcar que en la actualidad sería muy interesante implementar una red hibrida con IPv4 e IPv6, pues esto implicaría mayor complejidad de escaneo, o monitoreo de red, y por ende seria una red con un nivel de vulnerabilidad mayor en cuanto a ataques remotos se refiere.
6. La implantación de cualquier tecnología debe apoyarse en una robusta política de seguridad y su estricta aplicación, porque muchas de las fallas de seguridad

se dan precisamente por la falta de elaboración y puesta en marcha de las mismas.

RESUMEN

El objetivo de esta tesis fue realizar realizar un estudio de seguridades en una red extremo a extremo, basada en protocolo IPV6 para la Escuela de Ingeniera Electrónica de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo.

Para poder realizar este estudio se aplicaron métodos analíticos, técnicas de observación y se hizo una exploración del funcionamiento de IPsec indiferentemente de la versión del protocolo IP, además de que se implementó un escenario para determinar las vulnerabilidades en las dos versiones del protocolo usando herramientas de auditoría informática, con ataques de reconocimiento, sniffing, y hombre en el medio, mediante el uso de Nmap y Zenmap.

Como resultado de este estudio se pudo conocer aspectos importantes como la aplicación de políticas de seguridad, herramientas de auditoría informática, complejidad, información disponible, tendencias, facilidades, limitaciones entre otros, los cuales son indispensables a la hora de decidir si migrar una red a IPv6.

Se concluyó que la implementación de IPv6 en sí no representa una mejora en la seguridad de las redes, si bien IPsec es una herramienta poderosa a la hora de proteger los datos sensibles sin la elaboración y aplicación de políticas de seguridad robustas no se lograra aprovechar se potenciabilidad, además se recomienda apoyarse en la experiencia en el manejo de redes basadas en IPv4 ya que las amenazas siguen siendo prácticamente las mismas.

SUMMARY

This thesis was conducted in order to perform a safety study in end to end network based on IPv6 protocol, which could determine the improvements in that sense with respect to IPv4 and the importance of implementing policies of security.

To perform this study was an exploration of how IPsec regardless of the IP protocol version, plus a scenario that was implemented to identify vulnerabilities in the two versions of the protocol using computer audit tools with reconnaissance attacks, sniffing , and man in the middle.

As a result of this study were able to learn important aspects such as security policies, computer audit tools, complexity, information available, trends, facilities, among other limitations, which are essential to deciding whether to migrate a network to IPv6.

It was concluded that the implementation of IPv6 itself does not represent an improvement in network security, although IPsec is a powerful tool in protecting sensitive data that must be supported by the development of robust security policies and their application as to ensure security within the network.

GLOSARIO

ANEXOS

ANEXO 1

Propuesta Metodológica Para Implementar Ipv6 Y Seguridades

Índice de Contenido

Implementando direccionamiento IPv6 y su conectividad básica

a. Configurando direccionamiento IPv6 y estableciendo ruteo IPv6

b. Definiendo y usando prefijos IPv6

c. Configurando una interfaz para soportar IPv4 e IPv6

d. Configurando IPv6 ICMP Rate Limiting

e. Mapeando nombres de host a direcciones IPv6

a. Configurando direccionamiento IPv6 y estableciendo ruteo IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar el password si este ha sido configurado
3. Ingresar al modo de configuración global con el comando **configure terminal**
4. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
5. Ingresar la red IPv6 asignada al interface y habilitar el proceso de IPv6 en el interfaz, con las siguientes opciones de comandos:

   - **ipv6 address** *ipv6-prefix* **/** *prefix-length* **eui-64**
   - **ipv6 address** *ipv6-address* **/** *prefix-length***link-local**
   - **ipv6 address** *ipv6-prefix* **/** *prefix-length* **anycast**
   - **ipv6 enable**

   Especificando el comando **ipv6 address eui-64** se configura una dirección global IPv6 con un identificador de interface con los primeros 64 bits

especificados porque los 64 restantes serán automáticamente calculados desde el ID del interface.

Cuando se especifica el comando **ipv6 address link-local** se configura una dirección de tipo link-local en el interfaz que es usada en lugar de la que es automáticamente configurada cuando IPV6 es habilitado en el interface.

Especificar el comando **ipv6 address anycast** añade una dirección de tipo anycast al interfaz

6. Ingresar el comando **exit** que permitirá dejar el modo de configuración de interfaz para volver al modo de configuración global del router.
7. Digitar **ipv6 unicast-routing** que habilita el envío de paquetes unicast de IPv6

Configurando el límite de la cache para Neighbor Discovery

Se debe ejecutar las siguientes tareas para configurar el límite de la caché de ND por interfaz o globalmente:

- Configurar el límite de la caché en una interfaz específica del router
- Configurar el límite de la cahé en todas las interfaces del router

Configurar el límite de la caché para Neighbor Discovery en una interfaz específica del router

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**

3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Configurar el límite de la caché para Neighbor Discovery en una interfaz específica del router:

   ipv6 nd cache interface-limit *size* [**log** *rate*]

Configurar el límite de la cahé en todas las interfaces del router

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Configurar el límite de la cahé en todas las interfaces del router:

   ipv6 nd cache interface-limit *size* [**log** *rate*]

b. Definiendo y usando Prefijos generales de IPv6

Los prefijos generales pueden ser definidos de algunos modos:

- Manualmente
- Basado en la interfaz 6to4
- Dinámicamente desde prefijos recibidos por DHCP para IPv6

Definiendo prefijos generales manualmente

1. Digitar el comando **enable** para habilitar el modo privilegiado

2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Definir prefijos generales manualmente:

   ipv6 general-prefix *prefix-name* [*ipv6-prefix* **/** *prefix-length*] [**6to4** *interface-type interface-number*]

Definiendo prefijos generales basados interfaces 6to4

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Definir prefijos generales para una dirección IPv6:

   ipv6 general-prefix *prefix-name* [*ipv6-prefix* **/** *prefix-length*] [**6to4** *interface-type interface-number*]

Definiendo prefijos generales con la función de delegación de prefijos de clientes de DHCP

Se debe ejecutar esta tarea para configurar la función del cliente DHCPv6 sobre el interfaz y habilitar la delegación de prefijos, la cual es almacenada en los prefijos generales:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar el tipo de interface y su número y poner el router en modo de configuración de interfaz:

interface *type number*

4. Habilitar el proceso del cliente DHCPv6 y habilitar la búsqueda de delegación del prefijo a través de la interfaz especificada:

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

Usando prefijos generales en IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar el tipo de interface y su número y poner el router en modo de configuración de interfaz:

interface *type number*

4. Configurar un nombre de prefijo para la dirección IPv6 y habilitar el procesamiento de IPv6 en el interfaz

ipv6 address {*ipv6-address***/***prefix-length* | *prefix-name sub-bits***/***prefix-length*}

c. Configurar un interface para soportar IPv4 e IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Habilitar el envío de paquetes unicast IPv6

ipv6 unicast-routing

4. Especificar el tipo de interface y su número y poner el router en modo de configuración de interfaz:

   interface *type number*

5. Especificar una dirección IPv4 primaria o secundaria para el interfaz

   ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

6. Especificar la red IPv6 asignada a la interfaz y habilitar el procesamiento IPv6 en la misma:

   ipv6 address {*ipv6-address***/***prefix-length* | *prefix-name sub-bits***/***prefix-length*}

d. Configurando IPv6 ICMP Rate Limiting

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Configurar el intervalo y el bucketsize para los mensajes de error de ICMP de IPv6:

   ipv6 icmp error-interval *milliseconds* [*bucketsize*]

DETAILED STEPS

	Command or Action	Purpose

Step 3	**ipv6 icmp error-interval** *milliseconds* [*bucketsize*] Example: Router(config)# ipv6 icmp error-interval 50 20	Configures the interval and bucket size for IPv6 ICMP error messages. • The *milliseconds* argument specifies the interval between tokens being added to the bucket. • The optional *bucketsize* argument defines the maximum number of tokens stored in the bucket.

e. Mapeando nombres de host a direcciones IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Definir un mapeo estático de nombre de host a dirección en el caché del host

   ipv6 host *name* [*port*] *ipv6-address1* [*ipv6-addnameress2...ipv6-address4*]

4. Define un nombre de dominio por defecto que el software IOS de Cisco usará para completar nombres no calificados de host:

   ip domain name [**vrf** *vrf-name*] *name*

5. Especificar uno o más host que suplirán información del nombre:

   ip name-server [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]

6. Habilitar la transalación de direcciones basada en DNS:

   ip domain-lookup

Configuración de DHCP para IPv6

Para configurar DHCP para IPV6 se deben realizar las siguientes tareas:

1. Configurar la función del servidor DHCPv6
2. Configurar las funciones del cliente DHCPv6
3. Configurar el DHCPv6 Relay Agent
4. Configurar DHCP para asignación de direcciones IPv6
5. Configurar la función de DHCPv6 Stateless
6. Configurar las opciones del servidor DHCPv6
7. Definir prefijos generales con la delegación de prefijos de DHCPv6

1. Configurar la función de servidor DHCPv6

Para esto se debe crear y configurar un pool de direcciones IPv6, asociarlo con un servidor en una interfaz y configurar binding database agent:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Configura la información del pool (su nombre) e ingresar a modo de configuración mediante el comando:

ipv6 dhcp pool *poolname*

4. Configurar un nombre de dominio para un cliente DHCPv6 mediante el comando:

domain-name *domain*

5. Especificar el servidor DNS de IPv6 disponible para un cliente DHCPv6 mediante el comando:

dns-server *ipv6-address*

6. Especificar un prefijo numérico configurado manualmente para ser delegado a un cliente IAPD específico, mediante el comando:

prefix-delegation *ipv6-prefix* **/** *prefix-length client-duid* [**iaid** *iaid*] [*lifetime*]

7. Especificar un nombre para el pool de prefijos local desde el cual los prefijos son delegados a los clients DHCP, mediante el commando

prefix-delegation pool *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]

8. Salir del modo de configuración del pool y regresar al modo de configuración global del router, mediante el comando **exit**

9. Especificar un tipo deinterfaz y su número y poner el router en modo de configuración de interface con el comando:

interface *type number*

10. Habilitar DHCPV6 en la interfaz, con el comando:

    ipv6 dhcp server *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]

11. Salir al modo de configuración global para especificar los parámetros de binding database agent con el siguiente comando:

    ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds]*

2. Configurar la función del cliente de DHCPv6

Los prefijos generales pueden ser definidos dinámicamente desde un prefijo recibido por una delegación de prefijos del cliente de DHCPv6. Esta tarea se realiza para configurar la función de cliente DHCPv6 en una interfaz y habilitar la delegación de prefijo en una interfaz. El prefijo delegado se almacena en un prefijo general. Para esto se realizan los siguientes pasos:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Habilitar el proceso del cliente DHCPv6 y la solicitud para la delegación de prefijo a través de la interfaz especificada, mediante el siguiente comando:

   ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

3. Configurando el DHCPv6 Relay Agent

Se deben seguir los siguientes pasos para configurar el Relay Agent:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Especificar una dirección de destino a la cual los paquetes del cliente serán enviadas y habilita el servicio en esa interface:

   ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*]

Configurando DHCPv6 Relay Source en una interfaz

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Configurar una interfaz para usar como la fuente cuando se reciben mensajes del tipo relaying:

   dhcp relay source-interface *interface-type interface-number*

4. Configuración de DHCP para asignación de direcciones IPv6

Para ejecutar la configuración de la asignación de direcciones con DHCPv6 se deben completar dos tareas:

- Habilitar las funciones de servidor en el interfaz
- Habilitar las funciones de cliente en el interfaz

Habilitar las funciones de servidor en el interfaz

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Digitar **exit** para regresar al modo de configuración global

5. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
6. Habilitar la function del servidor DHCPv6 en el interface:

   ipv6 dhcp server [*poolname* | **automatic**] [**rapid-commit**] [**preference value**] [**allow-hint**]

7. Ingresar el comando **end para retornar** al modo privilegiado EXEC
8. Verificar las configuraciones:

   show ipv6 dhcp pool

   show ipv6 dhcp interface

9. Guardar las configuracione

    copy running-config startup-config

Habilitar la función de cliente de DHCPv6 en el interface

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Habilitar al interface para adquirir una dirección IPv6 desde el servidor DHCPv6:

    ipv6 address dhcp [**rapid-commit**]

5. Configurando la función Stateless de DHCPv6

Para ejecutar esta función se deben realizar las siguientes configuraciones:

- Configurar el servidor Stateless
- Configurar el cliente Stateless
- Habilitar el procesamiento de paquetes con opciones de Source Routing Header

Configurar el servidor Stateless DHCPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Especificar el servidor DNS IPv6 disponible para el cliente DHCPv6:

   dns-server *ipv6-address*

5. Configurar el nombre de dominio para el cliente DHCPv6:

   domain-name *domain*

6. Salir del modo de configuración del pool DHCPv6 y regresar al modo de configuración global del router: **exit**
7. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
8. Habilitar DHCPv6 en el interfaz seleccionado:

   ipv6 dhcp server *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]

9. Poner la bandera de “other stateful config”:

   ipv6 nd other-config-flag

Configurando el cliente Stateless DHCPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**

3. Especificar un tipo de interface, su número para poner el router en modo de configuración de interface, con el comando **interface *type number***
4. Habilitar la configuración automática de direcciones IPv6 usando la autoconfiguración en un interface y habilitando el procesamiento deIPv6 sobre la misma:

   ipv6 address autoconfig [**default**]

Habilitando el procesamiento de paquetes con opciones de Source Routing Header

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Hablitar el procesamiento de encabezados de ruteo IPv6 de tipo 0

   ipv6 source-route

6. Configuración de las opciones del servidor de DHCPv6

Se debe ejecutar las siguientes tareas para configurar las opciones stateless del servidor e importarlas hacia el cliente:

- Configurar las opciones de actualización del servidor
- Importar la información de actualización del servidor
- Configurar las opciones NIS y NISP-Related
- Importar las opciones SIP der servidor
- Configurar las opciones SNTP

- Importar las opciones SNTP
- Importar las opciones del servidor stateless de DHCPv6

Configurar las opciones de actualización del servidor

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

Especificar la información de actualización a ser enviada al cliente:

information refresh {*days* [*hours minutes*] | **infinity**}

Importar la información de actualización del servidor

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Importar la información de actualización al cliente DHCPv6:

   import information refresh

Configurar las opciones del servidor NIS y NIS-related

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Especifica la dirección NIS de un servidor IPv6 a ser enviada a un cliente:

   nis address *ipv6-address*

5. Habilitar al servidor para transmitirle al cliente su nombre de dominio NIS:

   nis domain-name *domain-name*

6. Especificar NIS más dirección del servidor IPv6 a ser enviado al cliente DHCPv6:

   nisp address *ipv6-address*

7. Habilitar al servidor para transmitirle al cliente DHCPv6 su información NIS más dominio:

   nisp domain-name *domain-name*

Importar las opciones del servidor NIS- and NIS+-Related

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Importar las opciones del servidor NIS al cliente DHCPv6:

import nis address

5. Importar el nombre de domio NIS al cliente DHCP:

   import nis domain-name

6. Importar la opción de dirección NISP al cliente DHCPv6

   import nisp address

7. Importar el nombre de dominio NISP al cliente DHCPv6:

   import nisp domain-name

Importando las opciones del servidor SIP

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Importar las listas de direcciones IPv6 SIP:

   import sip address

5. Importar la lista de nombres del servidor de dominio SIP:

   import sip domain-name

Configurando las opciones del servidor SNTP

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Especificar la lista SNTP a ser enviada al cliente:

   sntp address *ipv6-address*

Importando las opciones del servidor SNTP

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

   ipv6 dhcp pool *poolname*

4. Importar las opciones del servidor SNTP al cliente DHCPv6:

   import sntp address *ipv6-address*

Importar las opciones del servidor Stateless DHCPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Ingresar al modo de configuración de DHCP pool y definir el nombre del pool:

ipv6 dhcp pool *poolname*

4. Importar el nombre del servidor al cliente DHCPv6:

import dns-server

5. Importar la opción de búsqueda de dominio al cliente DHCPv6:

import domain-name

7. Definiendo un prefijo general con la función del cliente DHCPv6 Prefix Delegation

Se debe ejecutar esta tarea para configurar la función del cliente DHCPv6 sobre el interfaz y habilitar la delegación de prefijos, la cual es almacenada en los prefijos generales:

5. Digitar el comando **enable** para habilitar el modo privilegiado
6. Ingresar al modo de configuración global con el comando **configure terminal**
7. Especificar el tipo de interface y su número y poner el router en modo de configuración de interfaz:

interface *type number*

8. Habilitar el proceso del cliente DHCPv6 y habilitar la búsqueda de delegación del prefijo a través de la interfaz especificada:

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

Configurando IPsec para IPv6 Security

Para configurar IPsec para IPv6 Security se debe configurar una protección para una interfaz virtual de túnel (virtual tunnel interface -VTI) Site-to-site para tráfico unicast y multicast, lo cual permite usar la encapsulación IPsec para proteger el tráfico IPv6, para lo cual se deben ejecutar las siguientes tareas:

a. Crear políticas IKE y de clave pre-compartida en IPv6
b. Configurar ISAKMP en modo agresivo
c. Configurar IPsec TRansform y poner un perfil IPsec
d. Configurar un perfil ISAKMP en IPv6
e. Configurar un VTI en IPsec de IPv6

a. Crear políticas IKE y de clave pre-compartida en IPv6

Debido a que las negociaciones deben estar protegidas, cada negociación IKE comienzan agregando a ambas partes a una política IKE compartida. Esta política establece cuál parámetros serán usados para proteger las subsecuentes negociaciones IKE y obliga a cómo las partes serán autenticadas.

Después de que las dos partes se han agregado a la política, los parámetros de seguridad son identificados por una SA establecida en cada par y estas SA se aplicarán a todo el subsecuente tráfico durante la negociación.

Se puede configurar múltiples y priorizadas políticas para cada par –cada cual con una combinación diferente valores en sus parámetros. Sin embargo, por lo menos una de estas políticas deben contener exactamente la misma encriptación, hash, autenticación y parámetros Diffie-Hellman que su par remoto. Por cada política que se crea, se debe asignar una prioridad única (del 1 al 10,000, comenzando con 1 como la más alta prioridad).

Si se está interoperando con dispositivos que soportan solo un valor de sus parámetros, la elección es limitada al valor soportado en ambos dispositivos. Aparte de esta limitación hay a menudo hay un equilibrio entre seguridad y rendimiento y muchos de estos parámetros representan una compensación. Se debe evaluar el riesgo del nivel de seguridad de la red y la tolerancia para los mismos.

Cuando la negociación IKE comienza, IKE busca una política igual para ambas partes. El par que inica la negociación enviará todas sus políticas a su par remoto el cual tratará de encontrar emparejarlo. El par remoto busca esta pareja comparando sus propias políticas con altas prioridades sin importar las políticas recibidas por el otro par.

El emparejamiento se hace cuando ambas políticas contienen la misma encriptación, hash, autenticación y Diffie-Hellman en los valores de sus parámetros, y cuando el par remoto especifica que su tiempo de vida es igual o menor al tiempo de vida que su par. (Si el tiempo de vida no es idéntico, el más corto será usado)

Si la coincidencia es encontrada IKE completará la negociación y las asociaciones de seguridad de IPsec serán creadas, si una coincidencia aceptable no es enocntrada IKE rechaza la negociación e IPsec no será establecido.
Cuando dos pares usan IKE para establecer una asociación de seguridad , cada par envía su identidad a su par remoto, envían su hostname o su dirección IPv6 dependiendo de cómo se haya puesto la identidad ISAKMP en el router.

Por defecto la identidad de un par ISAKMP es la dirección IPv6 del par, si se considera apropiad se puede cambiar esta por el nombre del host. Una regla general pone las identidades de todos los pares del mismo modo, porque de otro modo las negociaciones podrían fallar.

A continuación se detallan los pasos:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Definir la política IKE e ingresar la política ISAKMP en modo de configuración:

   crypto isakmp policy *priority*

4. Especificar el método de autenticación dentro de la política de seguridad IKE:

authentication {**rsa-sig** | **rsa-encr** | **pre-share**}

5. Especifica el algoritmo hash dentro de la política IKE:

   hash {**sha** | **md5**}

6. Especifica el identificador de grupo Diffie-Hellman dentro de las políticas de seguridad IKE:

   group {**1** | **2** | **5**}

7. Especifica el algortimo de encriptación dentro la política IKE:

   encryption {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

8. Especifica el tiempo de vida de las asociaciones de seguridad de IKE, este valor es opcional:

   lifetime *seconds*

9. Salir del modod de configuración de políticas al modo de configuración global: **exit**

10. Configura una clave de autenticación pre establecida:

    crypto isakmp key *password-type keystring* {**address** *peer-address* [*mask*] | **ipv6**
    {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]

11. Define una cripto keyring a ser usado durante la autenticación de IKE:

    crypto keyring *keyring-name* [**vrf** *fvrf-name*]

12. Define la clave pre establecida a ser usada por la autenticación IKE

    pre-shared-key {**address** *address* [*mask*] | **hostname** *hostname* | **ipv6** {*ipv6-address* | *ipv6-prefix*}} **key** *key*

b. Configurar ISAKMP en modo agresivo

Probablemente no se necesite configurar el modo agresivo ya que generalmente el modo por defecto es usado:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Habilita un par para una consulta IKE de IPsec para los atributos de túnel:

    crypto isakmp peer {**address** {*ipv4-address* | **ipv6** *ipv6-address ipv6-prefix-length*} | **hostname** *fqdnhostname*}

4. Define la dirección IPv6 del par remote, la cual será usada para la negociación en modo agresivo. La dirección del par remoto es usualmente la dirección del cliente del otro extremo:

    set aggressive-mode client-endpoint *client-endpoint* | **ipv6** *ipv6-address*

c. Configurar IPsec Transform y poner un perfil IPsec

Una transformación es una combinación de protocolos de seguridad y algoritmos que son aceptados en los routers IPsec:

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Define un conjunto de transformación y pone el router en modo de configuración de encriptación:

   crypto ipsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]

4. Define los parámetros de IPsec que serán usados para encriptación de IPsec entre dos routers:

   crypto ipsec profile *name*

5. Especifica que conjunto de transformación será usado:

   set transform-set *transform-set-name* [*transform-set-name2...transform-set-name6*

d. Configurar un perfil ISAKMP en IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**
3. Define un perfil ISAKMP y audita la sesión de usuario de IPsec

   crypto isakmp profile *profile-name* [**accounting** *aaalist*

4. Define la identidad que usa el IKE local para identificarse a si mismo con su par remoto:

   self-identity {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}

5. Empareja una identidad desde el par remote en un perfil ISAKMP

   match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **ipv6** *ipv6-address*} | **host** *hostname* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*

e. Configurar un VTI en IPsec de IPv6

1. Digitar el comando **enable** para habilitar el modo privilegiado
2. Ingresar al modo de configuración global con el comando **configure terminal**

3. Habilita el ruteo unicast de IPv6. Esto se hace una sola vez si importar cuantas interfaces se necesite configurar:

   ipv6 unicast-routing

4. Especifica una interfaz de túnel y un número e ingresa al modo de configuración de interface

   interface tunnel *tunnel-number*

5. Provee una dirección IPv6 para esa interfaz de túnel para que el tráfico pueda ser ruteado a través de él:

   ipv6 address *ipv6-address/prefix*

6. Habilita IPv6 sobre la interfaz del túnel:

   ipv6 enable

7. Pone la dirección fuente para la interfaz de túnel:

   tunnel source {*ip-address* | *ipv6-address* | *interface-type interface-number*

8. Especifica el destino para el interfaz de túnel:

   tunnel destination {*host-name* | *ip-address* | *ipv6-address*

9. Pone el modo de encapsulación para el interfaz del túnel

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | i**pv6** | **ipsec ipv6** | **mpls** | **nos** | **r bscp**

10. Asocia un interfaz de túnel con un perfil IPsec.

tunnel protection ipsec profile *name* [**shared**]

ANEXO 2

Resultado de escaneo con OPENVAS a un Servidor DNS

1. Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found. It only lists hosts that produced issues. Issues with the threat level "Debug" are not shown.

This report contains all 18 results selected by the filtering described above. Before filtering there were 18 results.

Scan started: Sun Dec 11 20:13:32 2011
Scan ended: Sun Dec 11 21:00:39 2011

Host Summary

Host	High	Medium	Low	Log	False Positive
200.107.10.52	0	1	7	10	0
Total: 1	0	1	7	10	0

2. Results per Host

Host 200.107.10.52

Scanning of this host started at: Sun Dec 11 20:13:43 2011

Number of results: 18

Port Summary for Host 200.107.10.52

Service (Port)	Threat Level
domain (53/udp)	Medium
domain (53/tcp)	Low
general/tcp	Low
general/CPE	Log
general/HOST-T	Log

ssh (22/tcp) Log

Security Issues for Host 200.107.10.52

domain (53/udp)

Medium (CVSS: 4.3)
NVT: ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100251)

```
Overview:
ISC BIND is prone to a remote denial-of-service vulnerability because
the application fails to properly handle specially crafted dynamic
update requests.
Successfully exploiting this issue allows remote attackers to crash
affected DNS servers, denying further service to legitimate users.
Versions prior to BIND 9.4.3-P3, 9.5.1-P3, and 9.6.1-P1 are
vulnerable.
Solution:
The vendor released an advisory and fixes to address this issue.
Please see the references for more information.
References:
http://www.securityfocus.com/bid/35848
https://bugzilla.redhat.com/show_bug.cgi?id=514292
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=538975
http://www.isc.org/products/BIND/
https://www.isc.org/node/474
http://www.kb.cert.org/vuls/id/725188
** It seems that OpenVAS was not able to crash the remote Bind.
According to its version number the remote version of BIND is
anyway vulnerable.
Please check its status right now.
CVE : CVE-2009-0696
BID : 35848
```

domain (53/tcp)

Low
NVT: DNS Server Detection (OID: 1.3.6.1.4.1.25623.1.0.100069)

```
 Overview:
  A DNS Server is running at this Host.
  A Name Server translates domain names into IP addresses. This makes
it
  possible for a user to access a website by typing in the domain name
instead of
  the website's actual IP address.
```

domain (53/tcp)

Low
NVT: Determine which version of BIND name daemon is running (OID: 1.3.6.1.4.1.25623.1.0.10028)

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information.  The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.3.6-P1-RedHat-9.3.6-16.P1.el5
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

domain (53/udp)

Low

NVT: DNS Server Detection (OID: 1.3.6.1.4.1.25623.1.0.100069)

```
 Overview:
  A DNS Server is running at this Host.
  A Name Server translates domain names into IP addresses. This makes
it
  possible for a user to access a website by typing in the domain name
instead of
  the website's actual IP address.
```

general/tcp

Low

NVT: OS fingerprinting (OID: 1.3.6.1.4.1.25623.1.0.102002)

```
ICMP based OS fingerprint results: (0% confidence)
Unknown
```

general/tcp

Low

NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

```
Synopsis :
The remote service implements TCP timestamps.
Description :
The remote host implements TCP timestamps, as defined by RFC1323.
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.
See also :
http://www.ietf.org/rfc/rfc1323.txt
```

general/tcp

Low

NVT: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

```
Here is the route from 192.168.1.6 to 200.107.10.52
192.168.1.6
192.168.1.1
190.152.128.1
200.107.34.217
186.46.4.41
186.46.4.50
186.46.72.22
200.107.10.52
```

general/tcp

Low

NVT: Checks for open tcp ports (OID: 1.3.6.1.4.1.25623.1.0.900239)

```
Open TCP ports are 53
```

domain (53/tcp)

Log

NVT: (OID: 0)

```
Open port.
```

general/CPE

Log (CVSS: 0.0)

NVT: CPE Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

```
No CPE identities could be determined.
```

general/HOST-T

Log (CVSS: 0.0)

NVT: Host Summary (OID: 1.3.6.1.4.1.25623.1.0.810003)

traceroute:192.168.1.6,192.168.1.1,190.152.128.1,200.107.34.217,186.46
.4.41,186.46.4.50,18↵
6.46.72.22,200.107.10.52
ports:53

general/tcp

Log (CVSS: 0.0)
NVT: SSH Authorization (OID: 1.3.6.1.4.1.25623.1.0.90022)

No port for an ssh connect was found open.
Hence local security checks might not work.

general/tcp

Log
NVT: arachni (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.110001)

Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.

general/tcp

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.14260)

Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you
requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is
available in the PATH variable defined for your environment.

general/tcp

Log
NVT: DIRB (NASL wrapper) (OID: 1.3.6.1.4.1.25623.1.0.103079)

DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.

general/tcp

Log
NVT: 3com switch2hub (OID: 1.3.6.1.4.1.25623.1.0.80103)

Fake IP address not specified. Skipping this check.

general/tcp

Log (CVSS: 0.0)
NVT: Information about the scan (OID: 1.3.6.1.4.1.25623.1.0.19506)

Information about this scan :
OpenVAS version : 4.0.5
Plugin feed version : 201112091308
Type of plugin feed : OpenVAS NVT Feed
Scanner IP : 192.168.1.6
Port scanner(s) : nmap
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : no
Max hosts : 20
Max checks : 4
Scan Start Date : 2011/12/11 20:13

Scan duration : 2801 sec

ssh (22/tcp)

Log

NVT: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

An ssh server was discovered or assumed to be running on 22, but the port seems to be clos↵
ed now.

This file was automatically generated.

BIBLIOGRAFIA

PETE LOSHIN. IPv6 Theory, protocol and practice. 2da. edición. Estados Unidos de América: Morgan Kauffman Publisers. Pp. 89-120

HUGO ADRIAN FRANCISCONI. IPsec en Ambientes IPv4 e IPv6. 1era. Edición. Argentina: Hugo Adrian Francisconi. Pp.25-65

DIRECCIONES DE INTERNET

AGOTAMIENTO DE DIRECCIONES IPV4

http://www.slideshare.net/normyser/direcciones-ipv4-e-ipv6
http://es.wikipedia.org/wiki/IPv4
http://es.wikipedia.org/wiki/IPv6
http://es.wikipedia.org/wiki/Agotamiento_de_las_direcciones_IPv4

ARQUITECTURA IPV6

http://es.scribd.com/doc/55766034/ipv6p
http://www.monografias.com/trabajos-pdf/redes-banda-ancha/redes-banda-ancha.shtml
http://www.monografias.com/trabajos/ppp/ppp.shtml
http://es.scribd.com/doc/14971903/2/ARQUITECTURA-INICIAL-DE-ASIGNACION-IPV6

SEGURIDADES EN IPV6

http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm
http://www.ipsec-howto.org/spanish/x161.html
http://technet.microsoft.com/en-us/library/bb726956.aspx

AMENAZAS PARA IPV4 E IPV6

http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf
http://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/
AUDITORIA INFORMATICA
http://www.vtc.com/products/Ethical-Hacking-and-Penetration-Testing-tutorials.htm

CONFIGURACIONES

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec.html

TESIS

- **ERICK FERNANDO, LUJÁN MONTES.** Seguridad en IP con el protocolo IPsec para IPv6. Tesis. Ingeniro en Ciencias y Sistemas. Guatemala. **Universidad de San Carlos de Guatemala. Facultad de Ingeniería.** 2005. pp. 58-61.