



GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-495)

Seguridad en IPv6

JULIO 2016

Edita:



© Centro Criptológico Nacional, 2016

NIPO: 002-16-027-5

Fecha de edición: Julio 2016

El Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid ha participado en la elaboración del presente documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesaria para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e) y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

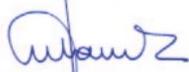
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156, apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que, a través de la serie CCN-STIC, el Centro Criptológico Nacional desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia, que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio 2016



Félix Sanz Roldán
Secretario de Estado

Director del Centro Criptológico Nacional

ÍNDICE

1. RESUMEN EJECUTIVO	1
1.1. EL ESTADO ACTUAL DE LA IMPLEMENTACIÓN DE IPV6	1
1.2. EL DESAFÍO DE IPV6	2
2. ACERCA DE IPV6	3
2.1. INTRODUCCIÓN	3
2.2. CAMBIOS DE SEGURIDAD RESPECTO A IPV4	3
2.3. MECANISMOS Y MIGRACIÓN DE IPV4 A IPV6	4
2.3.1. IMPLEMENTACIÓN RÁPIDA DE IPV6 EN INFRAESTRUCTURAS IPV4 (6RD).....	5
2.3.2. DNS64.....	5
2.3.3. DUAL STACK LITE.....	5
2.3.4. REQUISITOS DE MIGRACIÓN	6
3. PERSPECTIVA GENERAL DEL PROTOCOLO IPV6.....	6
3.1. CONVENCIONES DE DIRECCIONAMIENTO	6
3.2. CABECERA FIJA DEL PAQUETE	7
3.3. CONFIGURACIÓN AUTOMÁTICA SIN ESTADO	8
3.4. PROTOCOLO NEIGHBOUR DISCOVERY	8
3.5. MÓVIL E IPV6	9
3.5.1. MOBILE IP	9
3.5.2. REDES MÓVILES AD HOC	9
3.6. REDES DE SENSORES	9
4. DIRECTRICES GENERALES DE SEGURIDAD.....	10
4.1. VECTORES DE ATAQUE CONOCIDOS.....	10
4.2. CONFIGURACIONES DE DOBLE PILA	11
4.3. ENRUTAMIENTO Y PLANO DE CONTROL	11
4.3.1. OPEN SHORTEST PATH FIRST (OSPF)	12
4.3.2. PROTOCOLO DE SISTEMA INTERMEDIO A SISTEMA INTERMEDIO (IS-IS)	12
4.3.3. PROTOCOLO ENHANCED INTERIOR GATEWAY PROTOCOL.....	12
4.3.4. BORDER GATEWAY PROTOCOL (BGP).....	13
4.3.5. CONSIDERACIONES DE IMPLEMENTACIÓN DE PLANOS DE CONTROL.....	13
4.4. PROTECCIÓN DESPUÉS DE NAT	13
4.5. DIRECCIONAMIENTO MULTICAST E ICMP	13
4.6. CONTROL DE TRÁFICO DE ALGUNOS PREFIJOS	13
4.7. ACTUALIZACIÓN DE EQUIPOS DE SEGURIDAD Y PROTOCOLOS A IPV6.....	14
4.8. FINGERPRINTING	14
4.9. PROBLEMAS DE REVERSE DNS	14
4.10. SOPORTE PARA CARACTERÍSTICAS DE IPV6 EN DESUSO/INSEGURAS	15
4.11. PÉRDIDA DE SESIÓN DEBIDA A LA UNIÓN CON DIRECCIONES IP	15
5. VULNERABILIDADES Y CONFIGURACIÓN SEGURA.....	15
5.1. ESCANEOS DE DIRECCIONES DE LA RED.....	16
5.1.1. DESCRIPCIÓN	16
5.1.2. CONFIGURACIÓN SEGURA.....	16
5.2. ATAQUES SOBRE SLAAC.....	17
5.2.1. DESCRIPCIÓN	17
5.2.2. CONFIGURACIÓN SEGURA.....	17
5.3. DENEGACIÓN DE SERVICIO MEDIANTE DIRECCIÓN DESTINO MULTICAST (ATAQUE SMURF)	17

5.3.1. DESCRIPCIÓN	17
5.3.2. CONFIGURACIÓN SEGURA.....	17
5.4. DENEGACIÓN DE SERVICIO MEDIANTE DIRECCIÓN ORIGEN MULTICAST (ATAQUE SMURF)	18
5.4.1. DESCRIPCIÓN	18
5.4.2. CONFIGURACIÓN SEGURA.....	18
5.5. ATAQUES SOBRE NEIGHBOUR DISCOVERY	18
5.5.1. DESCRIPCIÓN	18
5.5.2. CONFIGURACIÓN SEGURA.....	18
5.6. AGOTAMIENTO DE LA TABLA DE NEIGHBOUR DISCOVERY POR INUNDACIÓN	19
5.6.1. DESCRIPCIÓN	19
5.6.2. CONFIGURACIÓN SEGURA.....	19
5.7. PAQUETES NEIGHBOUR DISCOVERY FALSOS.....	19
5.7.1. DESCRIPCIÓN	19
5.7.2. CONFIGURACIÓN SEGURA.....	20
5.8. PAQUETES ROUTER ADVERTISEMENT FALSOS.....	20
5.8.1. DESCRIPCIÓN	20
5.8.2. CONFIGURACIÓN SEGURA.....	20
5.9. PAQUETES ICMPV6 DE REDIRECCIONAMIENTO FALSOS	20
5.9.1. DESCRIPCIÓN	20
5.9.2. CONFIGURACIÓN SEGURA.....	20
5.10. ROGUE DHCPV6.....	21
5.10.1. DESCRIPCIÓN.....	21
5.10.2. CONFIGURACIÓN SEGURA.....	21
5.11. ATAQUES SOBRE LAS CABECERAS DE EXTENSIÓN.....	21
5.11.1. DESCRIPCIÓN.....	21
5.11.2. CONFIGURACIÓN SEGURA.....	21
5.12. FILTRADO DE PAQUETES ICMPV6.....	22
5.12.1. DESCRIPCIÓN.....	22
5.12.2. CONFIGURACIÓN SEGURA.....	22
5.13. FILTRADO DE TRÁFICO	22
5.13.1. DESCRIPCIÓN.....	22
5.13.2. CONFIGURACIÓN SEGURA.....	22
5.14. TÚNELES ENCUBIERTOS	22
5.14.1. DESCRIPCIÓN.....	22
5.14.2. CONFIGURACIÓN SEGURA.....	23
5.15. TÚNELES IPV6	23
5.15.1. DESCRIPCIÓN.....	23
5.15.2. CONFIGURACIÓN SEGURA.....	23
5.16. FALSIFICACIÓN DE RELAYS TEREDEO.....	23
5.16.1. DESCRIPCIÓN.....	23
5.16.2. CONFIGURACIÓN SEGURA.....	24
5.17. DESBORDAMIENTO DE LA MEMORIA EN TEREDEO	24
5.17.1. DESCRIPCIÓN.....	24
5.17.2. CONFIGURACIÓN SEGURA.....	24
5.18. FALSIFICACIÓN DE RELAYS 6TO4.....	24
5.18.1. DESCRIPCIÓN.....	24
5.18.2. CONFIGURACIÓN SEGURA.....	25

5.19.	DESBORDAMIENTO DE LA MEMORIA EN 6TO4	25
5.19.1.	DESCRIPCIÓN.....	25
5.19.2.	CONFIGURACIÓN SEGURA.....	25
5.20.	MAL REENSAMBLADO DE PAQUETES.....	25
5.20.1.	DESCRIPCIÓN.....	25
5.20.2.	CONFIGURACIÓN SEGURA.....	26
5.21.	SUPERPOSICIÓN DE FRAGMENTOS	26
5.21.1.	DESCRIPCIÓN.....	26
5.21.2.	CONFIGURACIÓN SEGURA.....	26
5.22.	PAQUETES CON CABECERAS DE EXTENSIÓN LIMITADA	27
5.22.1.	DESCRIPCIÓN.....	27
5.22.2.	CONFIGURACIÓN SEGURA.....	27
5.23.	INUNDACIÓN DE ROUTER ADVERTISEMENT	27
5.23.1.	DESCRIPCIÓN.....	27
5.23.2.	CONFIGURACIÓN SEGURA.....	27
5.24.	DENEGACIÓN DE SERVICIO CON BUCLES DE ENRUTAMIENTO MEDIANTE TÚNELES	27
5.24.1.	DESCRIPCIÓN.....	27
5.24.2.	CONFIGURACIÓN SEGURA.....	28
5.25.	ICMP SPOOFING PARA REDIRIGIR TRÁFICO Y DENEGACIÓN DE SERVICIO.....	28
5.25.1.	DESCRIPCIÓN.....	28
5.25.2.	CONFIGURACIÓN SEGURA.....	28
5.26.	UTILIZACIÓN DE DIRECCIONES ULA EN REDES EXTERIORES	28
5.26.1.	DESCRIPCIÓN.....	28
5.26.2.	CONFIGURACIÓN SEGURA.....	28
5.27.	AGOTAMIENTO DE LA TABLA CAM.....	29
5.27.1.	DESCRIPCIÓN.....	29
5.27.2.	CONFIGURACIÓN SEGURA.....	29
6.	CONFIGURACIÓN EN ENRUTADORES CISCO.....	29
6.1.	IMPLEMENTACIÓN DE CONECTIVIDAD BÁSICA IPV6.....	30
6.1.1.	CONECTIVIDAD IPV6	30
6.1.2.	CONFIGURAR UN LÍMITE DE CACHÉ PARA EL PROTOCOLO NEIGHBOUR DISCOVERY	30
6.1.3.	PERSONALIZAR PARÁMETROS DE NEIGHBOUR DISCOVERY	30
6.1.4.	CONFIGURAR PREFIJOS	31
6.1.4.1.	CONFIGURAR UN PREFIJO MANUAL	31
6.1.4.2.	DEFINIR UN PREFIJO CON DHCPV6	31
6.1.5.	CONFIGURAR UNA INTERFAZ PARA QUE SOPORTE IPV4 E IPV6.....	32
6.1.6.	PERSONALIZAR LA TASA LÍMITE DE ICMP	32
6.1.7.	CONFIGURAR LA EXTENSIÓN DRP PARA INGENIERÍA DE TRÁFICO.....	32
6.1.8.	HABILITAR UNICAST RPF.....	32
6.1.9.	VISUALIZACIÓN DE INFORMACIÓN DE IPV6	33
6.2.	IMPLEMENTACIÓN DE DHCP PARA IPV6	34
6.2.1.	DELEGACIÓN DE PREFIJO EN DHCPV6	34
6.2.1.1.	CLIENTE DHCP	34
6.2.1.2.	SERVIDOR DHCP	34
6.2.1.3.	RELAY DHCP	35
6.2.2.	CONFIGURACIÓN DE LA FUNCIÓN DE SERVIDOR DHCPV6	35

6.2.2.1. CONFIGURACIÓN DEL POOL DE DHCPV6.....	35
6.2.2.2. CONFIGURAR BASE DE DATOS DE VINCULACIÓN DE PREFIJOS ASIGNADOS	36
6.2.3. CONFIGURAR LA FUNCIÓN CLIENTE DE DHCPV6.....	36
6.2.4. CONFIGURAR LA FUNCIÓN RELAY DE DHCPV6	36
6.2.5. CONFIGURAR DHCPV6 PARA LA ASIGNACIÓN DE DIRECCIONES	37
6.2.6. CONFIGURAR LA FUNCIÓN STATELESS DE DHCPV6.....	38
6.2.7. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE DHCPV6	39
6.3. IMPLEMENTACIÓN DE MULTICAST PARA IPV6.....	39
6.3.1. PROTOCOLO MULTICAST LISTENER DISCOVERY (MLD)	40
6.3.2. HABILITAR MULTICAST EN IPV6	41
6.3.3. PERSONALIZAR MLD.....	41
6.4. IMPLEMENTACIÓN DE POLÍTICAS DE ENRUTAMIENTO EN IPV6.....	42
6.4.1. HABILITAR PBR EN UNA INTERFAZ	43
6.4.2. HABILITAR PBR LOCAL EN IPV6	44
6.4.3. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE PBR EN IPV6.....	44
6.5. IMPLEMENTACIÓN DE FILTROS DE TRÁFICO Y CORTAFUEGOS PARA SEGURIDAD EN IPV6	44
6.5.1. CONFIGURAR FILTROS DE TRÁFICO IPV6.....	45
6.5.1.1. CREAR Y CONFIGURAR UNA ACL PARA EL FILTRADO DE TRÁFICO	45
6.5.1.2. APLICAR UNA ACL IPV6 A UNA INTERFAZ ESPECÍFICA	46
6.5.2. CONFIGURAR EL CORTAFUEGOS PARA IPV6.....	46
6.5.3. VERIFICAR LA CONFIGURACIÓN DE SEGURIDAD DE IPV6.....	47
6.6. IMPLEMENTACIÓN DE RUTAS ESTÁTICAS PARA IPV6	47
6.6.1. CONFIGURAR UNA RUTA ESTÁTICA IPV6	48
6.6.2. CONFIGURACIÓN DE UNA RUTA ESTÁTICA RECURSIVA PARA EL USO POR DEFECTO	48
6.6.3. CONFIGURAR UNA RUTA ESTÁTICA FLOTANTE.....	48
6.6.4. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE LAS RUTAS ESTÁTICAS.....	49
6.7. IMPLEMENTACIÓN DE TÚNELES EN IPV6.....	49
6.7.1. CONFIGURAR TÚNELES MANUALES EN IPV6.....	49
6.7.2. CONFIGURAR TÚNELES IPV6 GRE	50
6.7.3. CONFIGURAR TÚNELES AUTOMÁTICOS 6TO4	51
6.7.4. CONFIGURAR TÚNELES COMPATIBLES IPV4 CON IPV6.....	52
6.7.5. CONFIGURAR TÚNELES ISATAP.....	52
6.7.6. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE TÚNELES IPV6.....	53
6.8. IMPLEMENTACIÓN DE RA GUARD Y SEND	53
6.8.1. CONFIGURACIÓN DE RA GUARD	53
6.8.2. CONFIGURACIÓN DE ND INSPECTION	54
6.8.3. CONFIGURACIÓN DE SECURE ND (SEND).....	54
6.8.4. CONFIGURACIÓN DEL SERVIDOR DE CERTIFICACIONES	56
6.8.5. CONFIGURACIÓN DEL MODO HOST	57
6.8.6. CONFIGURACIÓN DEL MODO ROUTER.....	57
6.8.7. CREACIÓN DE LA CLAVE RSA Y CGA PARA LA CLAVE.....	58
6.8.8. CONFIGURAR EL TRUSTPOINT DE SEND.....	59
6.8.9. CONFIGURAR TRUST ANCHORS (TERCERO) DE SEND EN UNA INTERFAZ... 60	
6.9. EJEMPLO DE CONFIGURACIÓN DE ENRUTADOR	61
6.9.1. CONECTIVIDAD BÁSICA.....	61

6.9.2. CONFIGURACIÓN DE DHCPV6.....	63
6.9.3. RUTAS ESTÁTICAS	64
6.9.4. CONFIGURACIÓN DE TÚNELES	64
6.9.5. CONSIDERACIONES ADICIONALES DE SEGURIDAD	66
6.10. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR.....	67
7. CONFIGURACIÓN DE SISTEMAS WINDOWS: WINDOWS 10.....	67
7.1. INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE IPV6 EN EL EQUIPO	67
7.1.1. INSTALACIÓN DE IPV6.....	68
7.1.2. OBTENCIÓN DE LA DIRECCIÓN IPV6.....	68
7.1.3. CONFIGURACIÓN DE IPV6.....	68
7.1.3.1. CONFIGURACIÓN ICMP	68
7.1.3.2. MULTICAST	70
7.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6	70
7.3. CONFIGURACIÓN DE TÚNELES EN IPV6	71
7.3.1. TEREDO.....	72
7.3.2. ISATAP.....	74
7.3.3. 6TO4	75
7.4. TRADUCCIÓN DE DIRECCIONES IPV6.....	77
7.5. DESHABILITAR IPV6 Y SUS COMPONENTES	78
7.5.1. DESHABILITAR IPV6	78
7.5.2. PREFERENCIA DE IPV4 SOBRE IPV6 EN LAS POLÍTICAS DE PREFIJOS	79
7.5.3. DESHABILITAR IPV6 EN TODAS LAS INTERFACES SIN TÚNELES	80
7.5.4. DESHABILITAR IPV6 EN TODAS LAS INTERFACES DE TÚNELES.....	80
7.5.5. DESHABILITAR IPV6 EN TODAS LAS INTERFACES EXCEPTO LA DE LOOPBACK.....	80
7.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR.....	80
8. CONFIGURACIÓN DE SISTEMAS MAC OS X	80
8.1. INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE IPV6 EN EL EQUIPO	81
8.1.1. INSTALACIÓN DE IPV6.....	81
8.1.2. OBTENCIÓN DE UNA DIRECCIÓN IPV6	81
8.1.3. CONFIGURACIÓN BÁSICA DE IPV6	81
8.1.3.1. ICMP	81
8.1.3.2. MULTICAST	82
8.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6	82
8.3. CONFIGURACIÓN DE TÚNELES EN IPV6	83
8.3.1. TEREDO.....	83
8.3.2. ISATAP.....	84
8.3.3. 6TO4	84
8.4. TRADUCCIÓN DE DIRECCIONES IPV6.....	84
8.5. DESHABILITAR IPV6 Y SUS COMPONENTES	85
8.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR.....	86
9. CONFIGURACIÓN DE SISTEMAS LINUX.....	86
9.1. INSTALACIÓN Y CONFIGURACIÓN DE IPV6 EN EL EQUIPO	86
9.1.1. INSTALACIÓN DE IPV6.....	86
9.1.2. OBTENCIÓN DE DIRECCIÓN IPV6	86
9.1.3. CONFIGURACIÓN DE IPV6.....	87
9.1.3.1. ICMP	87
9.1.3.2. MULTICAST	88
9.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6	89

9.3. CONFIGURACIÓN DE TÚNELES EN IPV6	90
9.3.1. TEREDO	90
9.3.2. CONFIGURACIÓN DE ISATAP	92
9.3.3. CONFIGURACIÓN DE 6TO4	92
9.4. TRADUCCIÓN DE DIRECCIONES IP	94
9.5. DESHABILITAR IPV6 Y SUS COMPONENTES	94
9.5.1. DESHABILITARLO DESDE SYSCTL	94
9.5.2. DESHABILITARLO DESDE EL FICHERO DE CONFIGURACIÓN GRUB	95
9.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR	96
10. CONFIGURACIÓN DE SISTEMAS MÓVILES (ANDROID Y IOS).....	96
10.1. CONECTIVIDAD BÁSICA IPV6 ANDROID	96
10.1.1. PROBLEMAS DE CONECTIVIDAD IPV6.....	96
10.1.2. CONEXIÓN MANUAL A IPV6 DESDE EL TERMINAL (SIN ROOTEAR).....	97
10.1.3. SOLUCIÓN DE PROBLEMAS DE CONECTIVIDAD.....	97
10.2. CONECTIVIDAD BÁSICA EN IOS.....	97
10.2.1. CONEXIÓN MANUAL A IPV6 DESDE EL TERMINAL (SIN ROOTEAR).....	98
11. REFERENCIAS.....	99

1. RESUMEN EJECUTIVO

1. La transición a redes capaces de encaminar, administrar, proteger y soportar el Protocolo de Internet versión 4 (IPv4) y el Protocolo de Internet versión 6 (IPv6) es un proceso de vital importancia en la actualidad. IPv6 supone un cambio tecnológico importante que modificará la forma en que las organizaciones configuran y protegen las redes.
2. Aunque la comunidad de Internet se ha centrado en los mecanismos para soportar la transición de IPv4 a IPv6, es probable que IPv4 e IPv6 coexistan en el futuro. Incluso cuando IPv6 se haya implantado completamente, no será fácil que IPv4 desaparezca, especialmente teniendo en cuenta la prevalencia de la traducción de direcciones de red (NAT) y el gran despliegue de la base IPv4.
3. Los ataques que se centran en comprometer redes lo hacen en tres áreas principales: el transporte (TCP/IP), el plano de control (principalmente protocolos de enrutamiento), y las aplicaciones que se ejecutan en hosts y servidores con conexiones de red. El despliegue de IPv6 incrementa la superficie de ataque en estas áreas mediante la inclusión de una nueva capa de transporte, nuevos planos de control (que aumenta la complejidad existente), añadiendo nuevos puertos abiertos y pilas de protocolos en los hosts y nuevos puntos de entrada en las aplicaciones. Como con cualquier tecnología o aplicación nueva, habrá desarrolladores y/o vendedores que no verifiquen la seguridad de sus aplicaciones de forma adecuada antes de sacarlas al mercado. Además, hay vulnerabilidades sin descubrir en productos ya existentes que los investigadores no han analizado todavía.
4. Algunos de estos ataques se transferirán directamente a IPv6 aunque también surgirán nuevos vectores de ataque que serán más difíciles de mitigar. Por ejemplo, las implementaciones de código dañino moderno siempre tienen ciertas capacidades de red para comunicarse con los servidores de mando y control (C&C) o para propagarse. Los autores de código dañino siempre han utilizado implementación de protocolos de red de sistemas operativos a través de llamadas API (Application Programming Interface) y estructuras de datos. No existen tendencias que indiquen que este comportamiento vaya a cambiar con la adaptación del protocolo IPv6.
5. En general, el antiguo modelo de seguridad de red no es de aplicación en este nuevo entorno, sobre todo cuando el despliegue de IPv6 se aúne con el uso de la computación en nube en los centros de datos, el enfoque BYOD (Bring Your Own Device) y la creciente complejidad de los datos que atraviesan redes.
6. Este informe, que no pretende ser un guía de seguridad técnica exhaustiva, se centra en las consideraciones de seguridad y los mecanismos de transición del protocolo IPv6, incluyendo algunas estrategias básicas de implementación que las organizaciones necesitan conocer en caso de que utilicen ambos protocolos (IPv4 e IPv6) en configuraciones duales de pila mientras realizan la migración total a IPv6, a la vez que se proponen medidas para prevenir ataques sobre la propia red IPv6.

1.1. EL ESTADO ACTUAL DE LA IMPLEMENTACIÓN DE IPV6

7. IPv4 ha sido capaz de alargar sus últimos años de vida. Una vez que las organizaciones se queden sin direcciones IPv4, no habrá más opción que utilizar IPv6, pero prolongar

tanto la migración es una garantía segura de fallos en la transición. Esta toma de conciencia ha cobrado impulso en los EE.UU. durante los últimos años, donde se ha producido una oleada de actividad IPv6.

8. Según el Registro Regional de Internet (RIR, organizaciones que se encargan de supervisar la asignación de direcciones IP) del Registro Americano para Números de Internet (ARIN) para Norteamérica, el número de asignaciones y peticiones IPv6 ha aumentado constantemente desde 2007.
9. Las principales industrias que promueven el despliegue de IPv6 se dividen en tres categorías: proveedores de sistemas operativos y aplicaciones software; fabricantes de equipos de red; y empresas relacionadas con Internet. Los principales proveedores de sistemas operativos (como Microsoft Corp., Linux Foundation, Apple Inc., IBM, Hewlett-Packard Development Company LP, etc.) llevan muchos años ofreciendo soporte IPv6 para sus sistemas operativos. En cuanto a los proveedores de aplicaciones de software, cada vez más aplicaciones nuevas ofrecen soporte IPv6 a medida que aumenta la demanda.

1.2. EL DESAFÍO DE IPV6

10. IPv6 se convertirá en el cambio TIC más importante de Internet hasta la fecha, con el que se espera ofrecer una solución válida al problema del crecimiento de Internet para los próximos 50 años. Actualmente, el problema con su implementación es que la industria no ha evaluado en profundidad la seguridad de esta tecnología, además del componente de incertidumbre añadido a su novedad.
11. Es recomendable que las organizaciones inicien primero la supervisión del tráfico IPv6 en sus redes y después desarrollen un proyecto IPv6 piloto en un único segmento de la red utilizando tecnologías de transición. Una vez aplicado el proyecto piloto con éxito, el siguiente paso es desarrollar un plan de transición y después comenzar con la implementación de IPv6, mientras siguen vigilando el tráfico IPv6 y construyendo escenarios de referencia. Una vez que las organizaciones hayan hecho la planificación necesaria para el éxito de la transición, deberían aplicar el plan de transición a toda la organización, de esta forma se limitan los riesgos de utilizar ambos protocolos en redes paralelas.
12. El intercambio de información es un componente crítico para la comprensión del impacto de estos cambios tecnológicos, sobre todo la respuesta de los administradores que gestionan infraestructuras críticas y el encaminamiento del tráfico de Internet. Con respecto a los protocolos de la próxima generación, como IPv6 y las extensiones de Seguridad para el Sistema de Nombre de Dominios (DNSSEC), cada tecnología se encuentra en una etapa de implementación diferente y la adopción de estas tecnologías ya ha demostrado que alterarán de manera significativa las infraestructuras de las redes.
13. El impacto de IPv6, junto con DNSSEC y el Protocolo Internet seguro (IPsec) puede introducir un nivel de complejidad en la gestión de la red que provocará una sobrecarga de trabajo, por lo que se requerirá la supervisión adicional de los proveedores e integradores de seguridad.
14. En este sentido, mientras las organizaciones gestionan la transición a IPv6, la comunidad DNS está implementando la tecnología DNSSEC para la protección de la autenticidad de la información de resolución de nombres. DNSSEC sirve para garantizar que los datos en tránsito de un registro DNS a un usuario final no han sido modificados.

15. Con IPv6 casi todo lo manejable en el mundo físico (desde las bombillas de la nevera hasta los subsistemas de automóviles) tendrá una dirección IP, es decir, estaremos en el Internet de las Cosas. El uso creciente del espacio de direcciones IPv6 prepara el escenario para la incorporación de miles de millones de dispositivos embebidos de bajo coste que las compañías desplegarán a través de empresas proveedores de servicios públicos.

2. ACERCA DE IPV6

16. IPv6 es la nueva versión de Internet Protocol. Para que los usuarios de Internet sigan creciendo y muchos más dispositivos se puedan conectar para evolucionar en cuanto a conectividad y servicios se ha rediseñado el protocolo IP, que es la base sobre la que se sustenta ahora mismo Internet.

2.1. INTRODUCCIÓN

17. La nueva versión está diseñada para resolver algunos de los problemas críticos que tenía IPv4. IPv6, entre otras ventajas, soluciona la escasez de direcciones IP, añade nuevas funcionalidades de seguridad para el cifrado y autenticación en las comunicaciones del protocolo extremo a extremo, y permite la realización de nuevos servicios.
18. Puesto que las direcciones IP actuales (IPv4) son solo de 32 bits, esto permite solo tener algo más de 4000 millones de direcciones para conectar equipos. Aunque Internet no ha llegado aún a todos los rincones del planeta, la gran cantidad de dispositivos que actualmente se tienen que conectar a internet para aprovechar al cien por cien sus funcionalidades es cada vez mayor. Debido a esto, el número de direcciones disponibles de IPv4 se está agotando, ya que todos los equipos de red necesitan una. Aunque estos problemas se han ido solventando mediante soluciones como NAT (con cualquiera de sus posibles usos), estas medidas no resuelven el problema.
19. Para solucionar este y otros problemas se ha creado una nueva versión del protocolo llamada IPv6 que utiliza como dirección IP un número de 128 bits, en vez de los 32 bits que usaba IPv4 en sus direcciones. Con este cambio, se solventa el problema de la escasez de direcciones IP, dado que hay 96 bits más para direcciones que en IPv4.
20. Este aumento en el número de direcciones IP disponibles hará posible que un número muy alto de dispositivos se puedan conectar para ofrecer nuevos servicios. Además se han introducido mejoras y nuevas funcionalidades en el protocolo IP, como la posibilidad de configurar la red automáticamente.
21. Sin embargo, se espera que los dispositivos y direcciones IPv4 coexistan durante un tiempo con los dispositivos y direcciones IPv6 mediante algunos mecanismos para facilitar la transición desde una versión a otra (ya que hay dispositivos y redes que no son compatibles con el nuevo protocolo), implementando ambos protocolos simultáneamente o mediante túneles sobre IPv4.

2.2. CAMBIOS DE SEGURIDAD RESPECTO A IPV4

22. La seguridad en IPv6 ha sido mejorada de forma notable con varios cambios (1), pero el principal ha sido IPsec. IPsec (Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos, a la vez que incluye

protocolos para el establecimiento de claves de cifrado entre los extremos de la comunicación. Tiene como fin proporcionar seguridad en las comunicaciones de la capa de red del modelo OSI (a la que pertenece el protocolo IPv6), y de ese modo, a todos los protocolos de capas superiores.

23. Aunque en IPv4 se puede hacer uso de IPSec, su implementación se define en una especificación diferente a la del propio protocolo IPv4, por lo que la inclusión del protocolo se hace con mecanismos definidos fuera del mismo, mientras que en IPv6 la propia arquitectura "extensible" del protocolo permite implementar IPsec de forma natural. Hay dos modos o tipos de transferencia: el modo transporte y el modo túnel.
24. En el modo transporte se cifra y/o autentica la carga útil del paquete, es decir, la información a transmitir, pero las cabeceras no. Por consiguiente, la información de las cabeceras, como la dirección IP de origen y destino, es visible, aunque tiene como principal ventaja que se puede utilizar de extremo a extremo. Por otro lado, en el modo túnel se encapsula el paquete original en otro paquete. Con ello se cifra y/o autentica el paquete original completo, pero se necesita que algún tipo de plataforma realice este túnel.
25. En cuanto a tipos o niveles de seguridad, IPSec implementa dos opciones, que a su vez pueden funcionar en modo transporte o en modo túnel: AH (Authentication Header), que proporciona autenticación, integridad y servicio de anti-repetición, mientras que el otro modo, ESP (Encapsulating Security Payload), añade confidencialidad a todas las características anteriores.
26. Otras mejoras en cuanto a seguridad es la mayor fortaleza de la red, debido, por ejemplo, a no tener que fragmentar los paquetes en nodos intermedios o el uso de cabeceras simplificadas. Además, el escaneo de direcciones se vuelve mucho más complicado debido al alto número de direcciones IPv6 que se pueden encontrar, que imposibilita realizar un ataque de fuerza bruta. También se puede prescindir del uso de NAT, debido también al gran espacio de direcciones disponible. Por último, se elimina la opción de realizar ataques de tipo broadcast al desaparecer este tipo de direccionamiento.

2.3. MECANISMOS Y MIGRACIÓN DE IPV4 A IPV6

27. Existen múltiples técnicas y tecnologías a disposición para gestionar la transición a IPv6. Algunas de estas técnicas son tan especializadas que solo funcionan con determinados entornos.
28. Uno de los mayores retos para la adopción de IPv6 es la necesidad de aplicar una política de seguridad en cualquier red que soporte dos tecnologías diferentes. Los administradores aplican listas de control de acceso (ACL) y reglas en el cortafuegos para ambos protocolos con una comprensión clara de que dichas ACL y reglas del cortafuegos cumplen con una política de seguridad de la red.
29. Identificar el tráfico es importante también. Para hacerlo y tomar las acciones adecuadas, se tiene que invertir en software y hardware capaz de gestionar IPv4, IPv6 y todo lo que este proceso implica. Diferentes componentes de red han madurado a diferentes niveles durante el proceso de migración a IPv6. Los nodos finales con sistemas operativos son los más consolidados, con software de detección de intrusiones (IDS) y software de prevención de intrusiones (IPS) avanzados. Independientemente del nivel de madurez de los diferentes componentes, todos son necesarios para ejecutar una

red segura y eficaz. Por tanto, la elección de tecnologías y la planificación son aspectos clave para la seguridad.

30. Aunque se ha trabajado para facilitar la migración durante la última década, la realidad es muy diferente a lo que la industria había planeado. Existen varias razones para esta realidad, como la existencia de dispositivos de red incompatibles, proveedores ISP que no soportan IPv6, o los costes de migración de una tecnología que no parece inmediatamente necesaria. El resultado de esto es que se utiliza IPv6 en islas que se comunican a través de IPv4. A continuación se describen algunos mecanismos para llevar a cabo esta transición.

2.3.1. IMPLEMENTACIÓN RÁPIDA DE IPV6 EN INFRAESTRUCTURAS IPV4 (6RD)

31. Las redes de tránsito exclusivo IPv4 presentan una serie de problemas. Por tanto, se debe implementar IPv6 en todas las partes de la red al mismo tiempo que proporcionen servicios. 6rd aborda estas implementaciones asignando direcciones de destino IPv6 a direcciones IPv4 next hop (de próximo salto) en el extremo de la red y túneles de autoconfiguración entre la entrada de red y los puntos de salida para conducir el tráfico IPv6. Los administradores pueden utilizar este mecanismo de transición en cualquier lugar donde puedan ubicar destinos IPv6 en islas claramente definidas en los extremos de una red.

2.3.2. DNS64

32. Proporciona conectividad para hosts IPv6 que intentan alcanzar servicios en dispositivos IPv4. Un host que solo soporta IPv6 solicita una resolución a algún dominio desde un servidor DNS. EL servidor DNS examina sus tablas y descubre que la única dirección resoluble para este nombre es una dirección IPv4 (un registro) en vez de una dirección IPv6. Dado que la petición original era para un registro AAAA, el servidor DNS crea una respuesta AAAA desde el registro A tomando la parte superior de la dirección de un relay 6-a-4 y combinándolo con la dirección IPv4 de 32 bits. El host solicitante conecta con la dirección IPv6 retornada, que es un relay 6to4, que convierte los paquetes IPv6 a IPv4 y envía los paquetes IPv4 resultantes al host o servidor de destino.

2.3.3. DUAL STACK LITE

33. Dual Stack Lite (DS-Lite) no es una especificación nueva, sino una combinación de otras especificaciones existentes y la traducción de direcciones de red (NAT) Ipv6 a IPv4 en dispositivos de red NAT CGN (carrier-grade NAT).
34. En funcionamiento, un host que solo tiene una dirección IPv6 transmite un paquete hacia un destino IPv4. Para ello, utiliza un router local en la ubicación física de un cliente para traducir una dirección de destino IPv6 a una dirección IPv4, en vez de utilizar paquetes de túneles NAT a un CGN gestionado por un proveedor de servicio. EL CGN traduce paquetes IPv6 a paquetes IPv4 y transmite el paquete IPv4 resultante hacia su destino. DS-Lite funciona con hosts IPv4 que intentan alcanzar los destinos IPv6 y también con un proveedor de servicios IPv6.

2.3.4. REQUISITOS DE MIGRACIÓN

35. Claves para el plan de migración a IPv6:
- Informarse acerca de si los proveedores de equipos tienen planes de transición a IPv6 y sus capacidades actuales y futuras para dar soporte a IPv6.
 - Informarse acerca de los planes de los ISP y proveedores WAN para conocer sus mecanismos de encapsulamiento y qué clase de túneles IPv6 soportan, a la vez que averiguar si los ISP priorizarán el tráfico de IPv6.
 - Hacer inventario de las aplicaciones utilizadas, para comprobar la funcionalidad y compatibilidad con el protocolo IPv6.
 - Asegurarse de no confundir el tráfico encapsulado con el tráfico no encapsulado.
 - La gestión de direcciones IP (IPAM) es una parte importante de la gestión de una red, ya que permite a los administradores de red automatizar la asignación y gestión de direcciones IP, a la vez que ayuda a la monitorización del tráfico presente en la red. Hay herramientas como Bluecat, Infobox e IPControl para IPAM y Nagios, Zenoss y ntop (herramientas de código abierto) para la monitorización de la red, que soportan IPv6.

3. PERSPECTIVA GENERAL DEL PROTOCOLO IPV6

36. IPv6 es una versión mejorada de la especificación IP que Internet Engineering Task Force (IETF) diseñó para resolver muchos problemas de IPv4, como el agotamiento de las direcciones, el rendimiento (mediante la eliminación de la fragmentación en la capa de red), la complejidad de cabecera (confinando todas las cabeceras en un formato común), la autoconfiguración (permitiendo la configuración sin estados), la movilidad y la seguridad (exigiendo soporte IPsec). RFC 2460 establece las especificaciones para IPv6.

3.1. CONVENCIONES DE DIRECCIONAMIENTO

37. El cambio más visible en IPv6 es el formato de la dirección (2). Mientras que las direcciones IPv4 tienen cuatro octetos de longitud (un total de 32 bits), las direcciones IPv6 tienen 16 octetos de longitud (128 bits). Las configuraciones expresan las direcciones IPv6 en ocho palabras de 16 bits en formato hexadecimal, con dos puntos que separan las palabras de 16 bits (por ejemplo, 2001:0db8:85a3:0000:0000:8a2E:0370:7334).
38. Las direcciones IPv6 resultan mucho más difíciles de leer y recordar que las direcciones IPv4 y, por tanto, la dependencia del DNS será más común en las implementaciones IPv6.
39. La Autoridad para la Asignación de Números de Internet (IANA) es responsable de gestionar y asignar el espacio de direcciones IPv6 a nivel mundial. IANA define rangos de direcciones IPv6 especiales y asigna gran parte del espacio de direcciones global a los RIR, como ARIN, que cubre Norteamérica y parte del Caribe; el Centro de Coordinación de Red (RIPE NCC) Réseaux IP Européens (RIPE) que abarca Europa, Oriente Medio y Asia Central; el Centro de Información de Redes de Asia y el Pacífico (APNIC), que abarca Asia y el Pacífico; el Registro de direcciones de Internet de

- América Latina y el Caribe (LACNIC), que abarca Latinoamérica y parte de la región del Caribe; y el Centro de Información de Redes de África (AfriNIC), que cubre África.
40. En IPv6, las direcciones se clasifican en tres categorías: Unicast (identifica un único interfaz de red), Multicast (identifica un grupo de interfaces, por lo que cualquier paquete enviado a la dirección será entregado a todas esas interfaces) y Anycast (también identifica un grupo de interfaces, pero el paquete solo será enviado al de menor coste según la métrica que tiene).
 41. Además, existen diferentes tipos de direcciones. Las del tipo Link Local Unicast están pensadas para enlaces locales y suelen usarse para los mecanismos de autoconfiguración de direcciones o para el protocolo Neighbour Discovery, entre otros. Por otro lado, tenemos las direcciones Unique Local Unicast, también de ámbito local como su nombre indica y solo enrutables dentro de un ámbito corporativo. Sin embargo, estas direcciones son únicas a nivel global.
 42. Hay algunas direcciones Unicast que son especiales debido a sus características y usos. Una de ellas es la dirección no especificada (0:0:0:0:0:0:0:0), la dirección de loopback (0:0:0:0:0:0:0:1), que se utiliza para enviar un paquete sin que salga a la red, únicamente atraviesa la pila del sistema u otro tipo de direcciones usadas para realizar túneles para poder utilizar la red IPv6 con la red IPv4, con mecanismos como 6to4 o Teredo.
 43. Para que un equipo pueda funcionar con IPv6, necesita tener configuradas las siguientes direcciones IPv6 para identificarse:
 - Dirección Link Local en cada interfaz
 - Dirección de Loopback
 - Dirección Multicast del grupo al que pertenece la interfaz
 - Alguna dirección de tipo Unicast o Anycast asignada
 44. En la siguiente lista se muestra la distribución actual del espacio de direcciones IPv6. Incluye el espacio de direcciones reservado para redes enrutables a nivel mundial, además de los bloques de direcciones que la IETF ha reservado para fines específicos de protocolos.
 - 2000::/3 -> Global Unicast
 - FC00::/7 -> Unique Local Unicast
 - FE80::/10 -> Link Local Unicast
 - FF00::/8 -> Multicast
 - Resto -> Reservado

3.2. CABECERA FIJA DEL PAQUETE

45. IPv6 especifica dos cabeceras: una cabecera fija de 40 octetos que el emisor debe incluir en todos los paquetes y cabeceras de extensión de longitud variable que el remitente podría incluir si fuera necesario en un paquete o flujo concreto. Cada cabecera de extensión sólo puede aparecer una vez en un paquete IPv6 y debe aparecer en un orden determinado. Dado que la longitud de la cabecera es una constante, en IPv6 se elimina el campo "Internet Header Length" (longitud de la cabecera de Internet) de la estructura

del datagrama. Por lo tanto, el datagrama general de IPv6 consiste en una “cabecera principal”, cabeceras de extensión y un área de datos.

46. Restringir el tamaño de la cabecera principal a 40 bytes y permitir el encadenamiento ilimitado de las cabeceras de extensión permite una alta flexibilidad y ofrece un espacio ilimitado para la modificación y expansión.

3.3. CONFIGURACIÓN AUTOMÁTICA SIN ESTADO

47. La configuración automática de direcciones sin estado (SLAAC, Stateless Address Auto Configuration), definida por la RFC 2462, permite que un dispositivo de red IPv6 genere automáticamente una dirección IP sin necesidad de comunicarse con un servidor DHCP.
48. Cuando un host IPv6 que utiliza SLAAC para la configuración automática de direcciones se conecta por primera vez a una red, genera una dirección de enlace local mediante la combinación de una dirección local MAC con el prefijo de enlace local FE80::0 comentado anteriormente. El dispositivo realiza una consulta a la subred local para determinar si otro host está utilizando la misma dirección. Si no, el dispositivo consulta a un enrutador local para localizar el prefijo real del enlace local y utiliza este prefijo para crear una dirección única a nivel mundial. Una dirección de host local única combinada con un prefijo único a nivel mundial se traducirá en una dirección única a nivel mundial. Estas son las ventajas de SLAAC:
 - No se requiere infraestructura DHCP para utilizar IPv6.
 - Los nuevos dispositivos no requieren ninguna configuración manual inicial.
49. Por otro lado, tenemos el protocolo DHCP (Dynamic Host Configuration Protocol). Este protocolo se utiliza para la configuración de direcciones de red en IPv4. Con el mecanismo de autoconfiguración aparecido en IPv6, no hay necesidad de ello. Sin embargo, en algunas ocasiones sí que es necesario usarlo. En IPv6 se implementa una versión de DHCP, DHCPv6. La configuración de equipos mediante este protocolo se llama Stateful Configuration y puede ser útil para la asignación dinámica de servidores DNS, configurar una dirección IPv6 que no provenga de la dirección MAC o para la utilización de un esquema específico de direcciones IPv6.

3.4. PROTOCOLO NEIGHBOUR DISCOVERY

50. El protocolo Neighbour Discovery es una mejora de IPv6. Su funcionalidad viene dada por el protocolo ICMPv6, una versión del protocolo ICMP presente en IPv4. Tiene muchas funciones, como descubrimiento de routers, determinación de prefijos de red, protocolo SLAAC o detección de direcciones duplicadas, entre otros.
51. Por un lado tenemos los mensajes del tipo Router Solicitation y Router Advertisement. El primero de ellos es generado por los equipos para pedir a los routers el envío de los segundos, aunque los routers también mandan los mensajes de Router Advertisement de forma periódica. Estos mensajes se utilizan para que los equipos puedan conocer los routers de la red.
52. Por otro lado, tenemos los mensajes del tipo Neighbour Solicitation y Neighbor Advertisement. En este caso, un nodo envía un mensaje Neighbour Solicitation para preguntar a otro nodo por su dirección del nivel de enlace, mientras que anuncia también su dirección del nivel de enlace. También se utiliza para el mecanismo de

direcciones duplicadas. La dirección de destino será de tipo multicast cuando el nodo trate de averiguar las direcciones de otros nodos o del tipo unicast cuando intente verificar si un nodo es alcanzable. Mediante estos mensajes se realiza el proceso de resolución a nivel de enlace, que antes en IPv4 se llevaba a cabo mediante el protocolo ARP y que no es usado en IPv6.

53. Y para terminar, se encuentran los mensajes de tipo Redirect, que son enviados por los routers hacia los equipos para informar de una mejor ruta hacia un destino.

3.5. MÓVIL E IPV6

54. Con el rápido aumento de las ventas de dispositivos móviles la movilidad se ha convertido en un requisito importante para los usuarios. IPv6 ya es compatible con muchas aplicaciones móviles actuales, IETF y otros profesionales están trabajando actualmente para aumentar la aplicación de IPv6 en entornos de alta movilidad.

3.5.1. MOBILE IP

55. RFC 5213 estandariza PMIPv6, la versión más actual de Mobile IP para IPv6. El trabajo actual sobre PMIPv6 incluye soporte para calidad de servicio, autenticación WiFi y la especificación de flujo IP.
56. La industria soporta Mobile IPv6 para una amplia gama de proveedores y en una amplia variedad de plataformas. Por ejemplo, existen distribuciones estándar de Linux, sistemas operativos de Microsoft y de Apple que soportan Mobile IPv6 y PMIPv6. Entre los proveedores de equipos de red, Cisco Systems Inc., Juniper Networks Inc., y muchos otros soportan Mobile IPv6. Sin embargo, actualmente, el uso de Mobile IPv6 y PMIPv6 no está muy extendido en el entorno empresarial.

3.5.2. REDES MÓVILES AD HOC

57. Una aplicación de movilidad menos conocida es IPv6 en los entornos de redes móviles ad hoc (MANET). Los entornos MANET son muy utilizados en entornos militares. Existen tres borradores experimentales (RFC 5449, RFC 5613 y RFC 5614) dentro del grupo de trabajo Open Shortest Path First (OSPF) de IETF que describen las diferentes adaptaciones de OSPFv3 a los cambiantes entornos móviles.
58. El grupo de trabajo MANET, de IETF, también dispone de una serie de borradores que describen los protocolos de enrutamiento experimentales que soportan IPv6 en entornos de alta movilidad y en entornos muy cambiantes.

3.6. REDES DE SENSORES

59. Dos grupos de trabajo del IETF, Routing Over Low power and Lossy networks (ROLL) y IPv6 Over Low Power WPAN (6LOWPAN), están trabajando actualmente en el área de las redes de sensores. Ambos grupos trabajan para la implementación de miles de sensores y dispositivos compatibles con IPv6 en hogares, edificios y espacios públicos.
60. Los fabricantes no pueden equipar los refrigeradores, contadores de agua, medidores eléctricos, interruptores de luz y otra multitud de dispositivos con las capacidades eléctricas o de procesamiento necesarias para participar plenamente en la red IPv6. Estos grupos IETF están trabajando para instalar IPv6 en estos dispositivos y

proporcionar una conectividad de red confiable, de bajo coste y escalable para diversas actividades.

4. DIRECTRICES GENERALES DE SEGURIDAD

61. Dado que el proceso de transición de IPv4 a IPv6 es lento y los dos protocolos van a coexistir, es importante identificar los posibles riesgos de esta situación, a la vez que vigilar los cambios que se llevan a cabo entre un protocolo y otro.
62. Existen tres superficies principales de ataque en una red IP: las capas de red y transporte (IPv4, IPv6, TCP, Protocolo de transmisión para el control de flujo [SCTP] y otros protocolos que manejan la transmisión de los datos); el plano de control (protocolos de enrutamiento y otros que proporcionan los metadatos necesarios para el correcto funcionamiento de la red); y aplicaciones que se ejecutan en hosts y servidores conectados a la propia red. Aunque los atacantes sin acceso a la capa de transporte pueden ejecutar determinados ataques contra las aplicaciones, un gran número de ataques se centran en IP. Esto implica que IPv6 aumenta la superficie de ataque en todas las redes.

4.1. VECTORES DE ATAQUE CONOCIDOS

63. Los vectores de ataque conocidos son aquellos que utilizan parámetros reconocibles gracias al análisis de los patrones de ataque actuales. Normalmente, los primeros ataques ejecutados en la red de una víctima tienen el objetivo de obtener la mayor cantidad de información posible sobre los dispositivos, la conectividad y servicios de la red. Los atacantes son muy conscientes de las herramientas y técnicas que necesitan para realizar escaneo de puertos, de vulnerabilidades y de aplicaciones en IPv4.
64. Como ya se ha dicho, el escaneo de direcciones en una red IPv6 es más difícil debido al aumento de direcciones (se pasa de 32 bits a 128 bits), por lo que se necesita más tiempo. Sin embargo, hay algunos factores que pueden reducirlo drásticamente, como la tendencia de los administradores de red a elegir un esquema de dirección común para todos los equipos con una función específica o elegir preferentemente direcciones bajas dentro del rango de direcciones.
65. Estos factores, combinados con técnicas de búsqueda avanzada, hacen que el análisis de una subred IPv6 sea factible con (casi) la misma dificultad que las subredes IPv4. Por otro lado, el análisis de ataques en redes IPv6 será más fácil debido a la información adicional contenida en las cabeceras IPv6, el descubrimiento de vecinos IPv6 y el descubrimiento de routers IPv6.
66. La habilitación de IPv6 en un sistema hace que un gran número de servicios que antes sólo eran accesibles a través de IPv4 también se encuentren disponibles a través de IPv6. Los servicios de conexión a hosts, tales como Telnet y HTTP, son conocidos puntos de entrada para los atacantes, por lo que los administradores deben inhabilitar o restringir el acceso a los mismos en infraestructuras y dispositivos protegidos. Los servicios de gestión, como el protocolo de gestión de red simple (SNMPv3), también son puntos vulnerables muy conocidos. Al igual que con IPv4, los administradores necesitan conocer y administrar la lista de servicios que se ejecutan en los puntos de entrada de red y dispositivos.

67. Los ataques de falsificación, que modifican la dirección IP de origen para que parezca que el tráfico dañino procede de una fuente confiable, siguen siendo posibles con IPv6. La falsificación en la capa de red permite al atacante sortear los filtros de seguridad, adquirir la apariencia de un dispositivo confiable y ocultar el origen real del ataque. Otros ataques pueden ser los de denegación de servicio, inyección falsa de información de enrutado o ataques del tipo Man in the Middle.
68. Además, hay que destacar que se suele pensar que IPv6 es otra aplicación de la red, pero en realidad es un sistema de transporte. Esto hace que la monitorización que a veces se lleva a cabo como protección no surta efecto porque no está pensada para IPv6. Y hay que tener en cuenta el encapsulamiento que se tiene que producir para conectar dos islas IPv6 mediante una red IPv4. Esto hace que el tráfico se pueda enmascarar y no se tenga control sobre él. Por otro lado, también se puede atacar sobre la cabecera de IPv6, que ha sido modificada en este protocolo, por ejemplo para dar las opciones de mandar un paquete por una cierta ruta, pudiendo hacer un ataque para que intente pasar por una ruta sin la pertinente seguridad.

4.2. CONFIGURACIONES DE DOBLE PILA

69. En las configuraciones de doble pila, un dispositivo admite a la vez IPv4 e IPv6. Esto aumenta el riesgo, debido a que el modo de conexión a un equipo se puede hacer mediante cualquiera de los protocolos. Esto hace que las reglas aplicadas por los cortafuegos a las conexiones de IPv4, para IPv6 en la mayoría de los casos dejen de servir. Sin estos controles, estas conexiones y equipos quedan desprotegidos.
70. Una buena práctica de seguridad es desactivar el protocolo IPv6. En muchos equipos, esta opción suele venir activada por defecto, haciendo posible la comunicación mediante este protocolo aún sin quererlo. Por todo ello, se recomienda deshabilitar IPv6 en los dispositivos en los que su uso no sea necesario, además de bloquear el tráfico de IPv6 en las redes en las que no sea necesario.

4.3. ENRUTAMIENTO Y PLANO DE CONTROL

71. Al realizar la transición a IPv6, los diseñadores de red suelen examinar atentamente el plano de datos y aplicaciones, pero a menudo descuidan las capas intermedias. Cómo el plano de control, en concreto los protocolos de enrutamiento, van a proporcionar la información para que IPv4 e IPv6 coexistan en un futuro próximo es un factor a tener en cuenta. También lo es qué complejidad añade IPv6 a la red, y cómo los administradores harán frente a estas dificultades adicionales.
72. Los protocolos de enrutamiento IP han adoptado tres enfoques diferentes para el soporte IPv6:
 - Especificar un nuevo protocolo que soporte IPv6 al margen de IPv4.
 - Especificar los mecanismos de protocolo adicionales que permiten que el mismo proceso proporcione accesibilidad para IPv6 e IPv4.
 - Especificar los mecanismos de protocolo adicionales que permiten que el mismo proceso proporcione accesibilidad, pero solo en el contexto de múltiples procesos de enrutamiento.

4.3.1. OPEN SHORTEST PATH FIRST (OSPF)

73. OSPF es un protocolo interior de pasarela ampliamente utilizado, estandarizado por IETF. El grupo de trabajo OSPF, por razones técnicas, optó por construir un nuevo protocolo para soportar IPv6. Al igual que IPv4 e IPv6 son protocolos independientes, OSPFv2 soporta enrutamiento IPv4 mientras que OSPFv3 soporta enrutamiento IPv6.
74. Para soportar IPv6, las organizaciones que deciden implementar en sus redes OSPF exclusivamente tendrán que implementar dos protocolos de enrutamiento diferentes. Esta implementación duplica las necesidades de gestión de red. La interacción entre múltiples dominios de enrutamiento puede ser compleja, ya que cada protocolo puede ser diseñado con diferentes límites de dominio de inundación, diferentes esquemas de agregación de direcciones y diferentes características de convergencia. Un solo servicio accesible a través de los protocolos puede actuar de maneras completamente diferentes, según el protocolo de transporte que los usuarios individuales utilizan para acceder al servicio.
75. La implementación de IPv6 junto a IPv4 no sólo aumenta el número de puertos abiertos en los que los atacantes pueden centrarse, sino que también aumenta la superficie de ataque del plano de control. Dado que el soporte IPv6 está disponible sólo dentro de un nuevo protocolo en el entorno OSPF, es importante que los administradores de red se aseguren de que aplican los procesos de medición y monitorización adecuados en este segundo protocolo y que han gestionado adecuadamente la gestión de cambios, y los problemas de seguridad y de arquitectura de red.
76. El grupo de trabajo OSPF está trabajando en conseguir soporte para IPv4 e IPv6 en OSPFv3, lo que permitiría a una organización ejecutar un único protocolo de enrutamiento en configuraciones de doble pila.

4.3.2. PROTOCOLO DE SISTEMA INTERMEDIO A SISTEMA INTERMEDIO (IS-IS)

77. El sistema intermedio a sistema intermedio (IS-IS) es un protocolo de pasarela interior de estado-enlace estandarizado por IETF y la Unión Internacional de Telecomunicaciones (UIT). Una gran parte de los proveedores de servicios lo utilizan globalmente. El grupo de trabajo IS-IS aprovechó la flexibilidad del protocolo y decidió ampliarlo para soportar IPv6 en lugar de crear un nuevo protocolo.
78. Las organizaciones que utilizan IS-IS pueden utilizar un protocolo único en un proceso único para el enrutamiento IPv4 e IPv6. Aunque esto puede simplificar enormemente la implementación IPv6, concretamente en el área de herramientas de gestión de red, también puede aumentar los retos en términos de diseño y arquitectura de red.

4.3.3. PROTOCOLO ENHANCED INTERIOR GATEWAY PROTOCOL

79. Enhanced interior gateway protocol (EIGRP) es un protocolo propietario de vector de distancia mantenido por Cisco. EIGRP también es compatible con IPv6, pero debido a restricciones técnicas, el enrutamiento de IPv4 e IPv6 se realiza a través de dos procesos independientes.
80. Las organizaciones que utilizan EIGRP por lo tanto pueden utilizar el mismo protocolo, pero deben ejecutar dos procesos diferentes: uno para IPv4 y otro para IPv6. Esta situación es similar a la de OSPFv3, en el sentido de que los administradores de la red deben implementar un nuevo proceso en cada router de la red, y al mismo tiempo es

similar a IS-IS en el sentido de que esta nueva implementación puede utilizar sistemas de gestión de redes existentes. EIGRP, al ser un protocolo de vector de distancia, permite una mayor flexibilidad en el diseño de la implementación. Los diseñadores planean soportar un proceso único para IPv4 e IPv6 con EIGRP.

4.3.4. BORDER GATEWAY PROTOCOL (BGP)

81. Border Gateway Protocol (BGP) es un protocolo de vector de ruta estandarizado por IETF y utilizado por casi todas las organizaciones grandes del mundo para crear interconexiones desde redes independientes. BGP es compatible con IPv4 e IPv6 dentro de las familias de direcciones. Ambos protocolos soportan un solo proceso BGP en cualquier dispositivo determinado.

4.3.5. CONSIDERACIONES DE IMPLEMENTACIÓN DE PLANOS DE CONTROL

82. En situaciones en las que dos protocolos o dos procesos son necesarios para proporcionar accesibilidad IPv4 e IPv6, los operadores de red pueden optar por implementar dos protocolos diferentes de enrutamiento de pasarela interior. Por ejemplo, los operadores podrán seguir utilizando OSPFv3 e EIGRP para la accesibilidad IPv4 mientras implementan IS-IS en paralelo con el protocolo de enrutamiento IPv4 para IPv6. La implementación de dos protocolos diferentes puede proporcionar una barrera entre IPv4 e IPv6, así que aunque esto puede añadir complejidad en términos reales, también puede reducir el tiempo necesario para reparaciones en el caso de que se produzcan problemas al separar por completo las dos implementaciones.
83. Cuando las organizaciones eligen una instalación de doble pila como mecanismo de coexistencia, el administrador de la red debe asegurar la accesibilidad de IPv4 e IPv6 a través de la red. Configurar y gestionar un plano de control que proporcione accesibilidad extremo a extremo entre estas islas IPv6 es una tarea compleja.

4.4. **PROTECCIÓN DESPUÉS DE NAT**

84. NAT es un mecanismo muy utilizado en IPv4 debido al problema del escaso número de direcciones en este protocolo. Dado que IPv6 elimina la necesidad de uso de este mecanismo, se deberán cambiar las restricciones de los cortafuegos para proteger los dispositivos internos de red, ya que estos tendrán su dirección asignada y podrán realizarse conexiones hacia estos equipos.

4.5. **DIRECCIONAMIENTO MULTICAST E ICMP**

85. Aunque en muchas situaciones se recomienda bloquear las comunicaciones multicast y el uso de ICMP debido a que se pueden realizar ataques basados en este protocolo, en IPv6 tanto multicast como ICMP son necesarios para algunos sistemas, como el PMTU (Path MTU). Muchos cortafuegos bloquean estos protocolos por lo que se deberán modificar las restricciones de los cortafuegos para permitir determinadas comunicaciones multicast e ICMP.

4.6. **CONTROL DE TRÁFICO DE ALGUNOS PREFIJOS**

86. Como norma general a seguir, se recomienda filtrar el tráfico recibido que no provenga de prefijos que no hayan sido asignados por IANA o los RIRs. Las direcciones de tipo

Unique Local Address no deben salir tampoco fuera de la red ni entrar en ella, a la vez que se deberían filtrar las direcciones correspondientes a la red de pruebas 6Bone y las direcciones IP de documentación (prefijo 2001:0DB8::/32).

4.7. ACTUALIZACIÓN DE EQUIPOS DE SEGURIDAD Y PROTOCOLOS A IPV6

87. Es normal que hasta que IPv6 se use masivamente, se soporten ambas versiones del protocolo, lo que provocará que haya mayores posibilidades de existencia de vulnerabilidades. Un sistema podrá ser atacado utilizando IPv4, IPv6 o una combinación de ambos, por ejemplo, utilizando IPv4 para detectar el equipo e IPv6 como canal oculto de comunicaciones. Para evitarlo, hay que asegurar los dos protocolos.
88. En general, es posible que los equipos de seguridad usados, como por ejemplo los cortafuegos u otras herramientas de red no sean capaces o no estén bien configurados para analizar datos del protocolo IPv6. Por lo tanto, hay que revisar IPv6, ya que muchos Sistemas Operativos lo tienen habilitado por defecto.
89. Además puede haber túneles IPv6. Los dispositivos de seguridad perimetral puede que no estén preparados o configurados para analizar estos flujos de datos, que pueden ser utilizados para comunicaciones no permitidas. Además, la posibilidad de crear túneles IPv6 se encuentra presente en todos los sistemas operativos.

4.8. FINGERPRINTING

90. Normalmente se basa en las respuestas específicas del sistema en base al protocolo TCP/IP. La mayoría de éstas se basan en elementos TCP, que siguen siendo iguales entre IPv4 e IPv6. Uno de los métodos utilizados en IPv4 es el valor por defecto de TTL. En este caso, en IPv6 el número de saltos funciona justo al contrario, por lo que no puede utilizarse este método.
91. Por otro lado, IPv6 da la posibilidad de utilizar un gran número de opciones nuevas en lugar de la anterior mencionada, algunas en la cabecera IP (como la flow label), y otras muchas en las cabeceras de extensión. También los protocolos relacionados, como ICMPv6 (e.j.: descubrimiento de un vecino) o DHCPv6. Se puede utilizar también varios valores de la capa de aplicación (como la cadena de agente de usuario en HTTP).
92. Alguna información puede ocultarse, como las páginas de cabecera o la información de versión apache. Esto normalmente es específico de la aplicación.
93. El comportamiento de IPv6 específicamente para el sistema operativo, por ejemplo la respuesta con paquetes ICMPv6 a una dirección de broadcast, puede configurarse manualmente.

4.9. PROBLEMAS DE REVERSE DNS

94. Este es un método que se utiliza para traducir una dirección IP a un hostname. Mientras la mayoría de las búsquedas de DNS son traducir un hostname a una dirección IP, las búsquedas invertidas siguen jugando un papel en el correcto funcionamiento de internet. Varios ejemplos de esto son:
 - Hacer logging de IP y hostname (para inicios de sesión u otros eventos).
 - Mostrar información extra (ping, traceroute, tcpdump).

- Reglas de filtrado coincidentes basadas en hostnames.
 - Verificando la identidad del servidor de correo (los correos que provienen de un servidor que no tiene registro PTR, normalmente se marca como spam).
95. Con IPv4, asignar registros PTR a direcciones IP es manejable, ya que el número de direcciones IP asignadas al cliente es limitado. En IPv6 esto no es igual, ya que los clientes normalmente obtienen un rango entero de direcciones IP. Utilizar comodines en ip6.arpa no es una solución válida. Las zonas enumeradas automáticamente no son una respuesta por el tamaño resultante de la zona y los problemas de rendimiento que acarrea. Para el propósito de verificación, las dos entradas (ida y vuelta) del DNS deben coincidir. Las direcciones IP generadas dinámicamente aumentan la complejidad aún más.

4.10. SOPORTE PARA CARACTERÍSTICAS DE IPV6 EN DESUSO/INSEGURAS

96. A lo largo del desarrollo de IPv6 ha habido diversos cambios en lo referido a sus características, ya sea en el protocolo como en su implementación (se han añadido cosas, eliminado y/o cambiado). Aunque algunas de estas características se encuentren en desuso, pueden seguir presentes en algunas implementaciones. Esto hace que puedan crear problemas de seguridad en la red.
97. Se deben realizar los siguientes procedimientos:
- Eliminar las características de IPv6 en desuso de las implementaciones.
 - Inhabilitar las características en desuso de las configuraciones.
 - Filtrar hacia fuera, donde sea posible, en los cortafuegos y los switches.
 - Eliminar o bloquear la funcionalidad en los sistemas afectados.
 - Filtrar la funcionalidad en los sistemas intermedios.

4.11. PÉRDIDA DE SESIÓN DEBIDA A LA UNIÓN CON DIRECCIONES IP

98. Es una práctica común el unir las sesiones del usuario con la dirección IP del mismo. Sin embargo, con IPv6 el usuario no tendrá una dirección IP fija en relación con la sesión, por ejemplo, por las extensiones de privacidad (RFC 4941), Mobile IPv6 (RFC 6275), o el protocolo "happy eyeballs" (RFC 6555). Si una sesión se une a la dirección IP de la fuente, el cambiar la dirección IP provocaría la pérdida de la sesión.
99. La forma segura de evitar esto es evitar el uso de direcciones IP basadas en identificadores de sesión.

5. VULNERABILIDADES Y CONFIGURACIÓN SEGURA

100. A continuación se van a describir una serie de vulnerabilidades (3) (4) que tiene IPv6, y cómo se pueden evitar. Todas las vulnerabilidades expuestas seguirán el mismo patrón, primero se realizará una breve descripción del problema y el escenario donde se puede desarrollar, para después exponer una serie de medidas a nivel de configuración para poder evitarlas o que su impacto sea mínimo.
101. El uso de IPSec hace mucho más difícil que algunas de estas vulnerabilidades se puedan llevar a cabo, por lo que su utilización es muy importante para evitarlas. Sin embargo,

algunas de ellas necesitan de configuración adicional para poder evitarse, por lo que a continuación se van a tratar esta serie de medidas adicionales para mitigar los ataques.

5.1. ESCANEEO DE DIRECCIONES DE LA RED

5.1.1. DESCRIPCIÓN

102. En IPv4 es común la utilización de direcciones IP para encontrar dispositivos en la red, mandando un paquete a cada dirección IP dentro del rango de direcciones. Esto es una manera “bruta” de buscar sistemas activos. La razón por la que esto puede llevarse a cabo es porque el espacio de direcciones es relativamente pequeño, normalmente no tienen que probarse más de 65.536 direcciones IPv4 en una subred /16. Este proceso se puede llevar a cabo en minutos.
103. Sin embargo, en IPv6 el espacio de direcciones IP es bastante más grande (2^{64} direcciones en una red /64), lo que hace que sea inviable hacer un descubrimiento por fuerza bruta de todas las direcciones IPv6. Por otro lado, también ocurre que IPv6 utiliza anycasting, lo que resulta en la compartición de la misma dirección IP por distintos sistemas, y el escaneo de la red sólo encontraría uno de ellos en dicho caso.
104. Con IPv6 es más difícil emplear esta técnica debido a que el espacio de direcciones aumenta, pero aun así se realizan, debido a configuraciones inseguras.

5.1.2. CONFIGURACIÓN SEGURA

105. No asignar direcciones secuencialmente: hace que se reduzca el espacio efectivo de direcciones y, por tanto, facilita el escaneo de la red.
106. No utilizar reglas de ningún tipo para asignar direcciones IPv6: una vez averiguada la regla, se puede conocer la topología de forma sencilla. Por ejemplo, dado que conviven IPv4 e IPv6, una práctica utilizada es tomar los últimos 8 bits de la dirección de IPv4 para IPv6.
107. No asignar direcciones a partir de las direcciones link-local: estas direcciones están pensadas en IPv6 para utilizarse de forma local y a modo de configuración. Si se asignan las direcciones IPv6 de esta manera, el espacio de direcciones se reduce. Es más, si se conoce el fabricante del equipo, se reduce aún más (hasta los 24 bits) debido a que la mac va incluida en la dirección y cada fabricante tiene unos bits característicos. Por tanto, lo mejor es no hacer uso de esta opción, salvo para la configuración inicial.
108. No responder a peticiones multicast: IPv6 tiene la opción de enviar paquetes a dirección multicast, de forma que se puede mandar un ping a todos los nodos de la red si se envía a la dirección FF02::1. Para llevar esto a cabo hace falta estar en la red local y sería un ataque interno.
109. Por tanto, la configuración segura es utilizar asignación de direcciones mediante DHCPv6 y no responder en los nodos a peticiones multicast (prevención en red local).

5.2. ATAQUES SOBRE SLAAC

5.2.1. DESCRIPCIÓN

110. En IPv6 los mecanismos de configuración (los más importantes al menos) se realizan a través de ICMPv6. ICMPv6 es un objetivo habitual para ataques, muy utilizados, sobre todo, en redes locales.
111. SLAAC es una funcionalidad nueva de IPv6, que permite a un equipo obtener conectividad de forma autónoma y rápida. Los parámetros de conexión son proporcionados por un router haciendo uso de tramas ICMPv6. Un router envía mensajes de Router Advertisement (o RA) periódicamente dentro de la red, de forma que los equipos cogen los parámetros y se autoconfiguran para tener conectividad mediante IPv6.
112. El ataque consiste en ocasionar una pérdida del servicio o proporcionar la dirección del equipo fraudulento, para que un Man in the Middle que proporcione RAs falsos, de forma que un equipo se puede configurar mal (con una dirección equivocada) y puede tener una dirección falsa y puede interceptar y/o redirigir el tráfico.
113. Otro tipo de ataque es la inundación de paquetes RAs, de forma que un equipo esté calculando la dirección en muchas ocasiones, haciendo un ataque de denegación de servicio (DoS).

5.2.2. CONFIGURACIÓN SEGURA

114. La configuración óptima sería bloquear el descubrimiento de routers por SLAAC. Sin embargo, esto sólo habría que hacerlo en el caso de detección de ataques, ya que es la configuración habitual. Además, no hay que olvidar que siempre hay que deshabilitar IPv6 en aquellos equipos que no vayan a hacer uso de este protocolo.

5.3. DENEGACIÓN DE SERVICIO MEDIANTE DIRECCIÓN DESTINO MULTICAST (ATAQUE SMURF)

5.3.1. DESCRIPCIÓN

115. El documento RFC 2463: “ICMPv6 for IPv6 Specification”, declara que no se deben mandar mensajes ICMP cuando el destino es una dirección multicast. No todos los sistemas implementan esto apropiadamente. Si los mensajes ICMP de error son enviados, éstos pueden ser usados en un ataque reflector (smurf), por ejemplo con mensajes Echo ICMP de petición y respuesta.
116. Su implementación es sencilla. Un sistema malicioso genera mensajes de petición Echo ICMP a todas las direcciones multicast, con la dirección de origen establecida en una víctima. Todos los nodos responderán con un mensaje de respuesta Echo ICMP a la víctima, causando probablemente un DoS. Es un ataque muy similar al Smurf en IPv4.

5.3.2. CONFIGURACIÓN SEGURA

117. No enviar mensajes de respuesta ICMP cuando la dirección de destino de un paquete IP es una dirección multicast.

118. Descartar los paquetes susceptibles de ataque en los cortafuegos (mensajes ICMP a direcciones multicast).

5.4. DENEGACIÓN DE SERVICIO MEDIANTE DIRECCIÓN ORIGEN MULTICAST (ATAQUE SMURF)

5.4.1. DESCRIPCIÓN

119. Usar una dirección multicast como dirección origen en paquetes IP está prohibido según lo especificado en el documento RFC 2463: "ICMPv6 for IPv6 Specification". Sin embargo, no todas las implementaciones pueden descartar apropiadamente este tipo de paquetes. Cuando una respuesta es enviada, será dirigida a la dirección multicast. Esto puede ser usado como una amplificación para un ataque de denegación de servicio. Esto es una vulnerabilidad tanto de IPv4 como de IPv6.

5.4.2. CONFIGURACIÓN SEGURA

120. Descartar los paquetes con direcciones origen establecidas para las direcciones multicast (en hosts finales como en cortafuegos e IPS).

5.5. ATAQUES SOBRE NEIGHBOUR DISCOVERY

5.5.1. DESCRIPCIÓN

121. Este ataque también se basa en ICMPv6. En IPv6 no hay protocolo ARP, por lo que se implementa el protocolo NDP para el descubrimiento de vecinos. Se lleva a cabo mediante dos tipos de mensajes: NA (neighbor advertisement) y NS (neighbor solicitation).
122. Se pueden llevar a cabo distintos ataques sobre este protocolo, por ejemplo enviando una dirección falsa a un equipo mediante NA para que se configure mal, hacer spoofing de mensajes NA y NS para obtener la dirección MAC del router y poder suplantarle (MitM) o hacer inundación de mensajes NA aleatorios, de tal forma que el router llene su tabla de NDP y no permita la conexión de más equipos. Además, mediante mensajes NS se puede comprobar si una dirección de un equipo que se ha autoconfigurado con SLAAC está repetida. Si este mensaje es respondido siempre con que la dirección está ocupada, se puede hacer un ataque de denegación de servicio. El ataque consiste en ocasionar una pérdida del servicio o proporcionar la dirección del equipo fraudulento, mediante un Man in the Middle que proporcione RAs falsos, de forma que un equipo se pueda configurar mal (con una dirección equivocada), pueda tener una dirección falsa y pueda interceptar y/o redirigir el tráfico.

5.5.2. CONFIGURACIÓN SEGURA

123. Por ciertas razones, para proteger este tipo de mensajes no se utiliza IPSec. Para solventar estos problemas, se ha implementado el protocolo SEND (SEcure Neighbor Discovery). Un equipo que implementa SEND necesita un par de claves pública-privada y se definen unas nuevas opciones en los mensajes del NDP para mejorar la seguridad. Con estas opciones, que se muestran a continuación, el protocolo NDP es seguro:

- Cryptographically Generated Addresses (CGA) Option. La CGA asegura que el remitente de un mensaje NDP es el propietario de la dirección.
- RSA Signature Option. La firma de clave pública mantiene la integridad de los mensajes y autentica la identidad del que lo envía.
- Nonce Option. La opción Nonce protege los mensajes cuando se utiliza en el par Advertisement - Solicitation. Se asegura de que un advertisement es una respuesta a una solicitud reciente enviada anteriormente por el nodo.
- Timestamp Option. Ofrece protección de repetición y se asegura de que los advertisement no solicitados y redirecciones no se han reproducido.

5.6. AGOTAMIENTO DE LA TABLA DE NEIGHBOUR DISCOVERY POR INUNDACIÓN

5.6.1. DESCRIPCIÓN

124. Los sistemas IPv6 mantienen una caché de vecinos para hacer la asociación entre las direcciones IPv6 y las direcciones MAC. Esta es similar a la caché de ARP en IPv4. En IPv6, por ejemplo, puede haber más direcciones IPv6 en una subred (2^{64}) que el máximo número de entradas de las que los switches o router de última generación son capaces de contener. Un atacante puede, de este modo, causar una inundación -de muchas entradas- en la caché del vecino, mediante el escaneo de un prefijo IPv6, que consta de un número muy grande de "hosts", en poco tiempo. Este escaneo puede ser hecho, por ejemplo, enviando paquetes IPv6 a una dirección IPv6 aleatoria dentro del rango del prefijo. Los routers intentarán entonces añadir a la caché de vecinos entradas por cada dirección destino IPv6 desconocida dentro de la subred. Ya que los gateways ven la mayoría del tráfico, están específicamente afectados por esto. De manera similar, sistemas informáticos normales pueden responder mal cuando sus tablas de estado ND están llenas.

5.6.2. CONFIGURACIÓN SEGURA

125. Modificar las configuraciones de la caché de vecinos podría reducir el problema (por ejemplo, reduciendo el timeout después del cual una entrada es eliminada). La tasa de limitación puede ser habilitada en los equipos para filtrar mensajes de descubrimiento de vecinos. Como área de trabajo es posible asignar prefijos /64 de manera habitual, sin embargo aplicando prefijos /120 en vez de /64 el rango de escaneo del atacante es limitado. Nótese que esta solución deshabilita SLAAC, ya que usa 64-bit para generar identificadores de interfaz. Para escenarios en los que SLAAC no está en uso, esto proporciona una solución viable, por ejemplo para servidores o redes que usan DHCPv6 para configuración de direcciones.

5.7. PAQUETES NEIGHBOUR DISCOVERY FALSOS

5.7.1. DESCRIPCIÓN

126. Un atacante puede infectar la caché del vecino mandando Neighbour Advertisement falsos (NA es parte del protocolo ND). El nodo entonces mandará (en local)

erróneamente tráfico a un sistema especificado por el atacante. Esta vulnerabilidad es similar a ARP spoofing en IPv4.

5.7.2. CONFIGURACIÓN SEGURA

127. La vulnerabilidad puede ser mitigada de manera parcial forzando la utilización de SEND (Secure Neighbour Discovery), lo que previene que el atacante consiga una dirección que está siendo ya utilizada por otro sistema. El atacante seguirá siendo capaz de obtener una dirección que no haya sido utilizada previamente.
128. Implementar el protocolo de snooping Neighbour Discovery, el cual opera en nivel 2 o entre el nivel 2 y 3 y provee a IPv6 de características de seguridad y escalabilidad, para filtrar mensajes de neighbour discovery maliciosos.

5.8. PAQUETES ROUTER ADVERTISEMENT FALSOS

5.8.1. DESCRIPCIÓN

129. Mediante el envío de paquetes RA falsificados, un atacante puede configurarse como un punto de salida de la red y de todo su tráfico. Esto hace que el tráfico saliente de la subred sea interceptado e inspeccionado por el atacante. Este ataque puede introducir otra salida para la red existente, o introducir un nuevo prefijo (falso) y no tiene por qué ser de forma intencionada.

5.8.2. CONFIGURACIÓN SEGURA

130. Los equipos con funcionalidad 'RA Guard' filtran estos paquetes. Los equipos comunes de menor coste no dan soporte a esta funcionalidad.

5.9. PAQUETES ICMPV6 DE REDIRECCIONAMIENTO FALSOS

5.9.1. DESCRIPCIÓN

131. Los redireccionamientos ICMPv6 (tipo 137) son utilizados por routers para especificar el mejor primer salto a otro router dentro del encaminamiento. Afecta al modo en el que los paquetes son enrutados. Un atacante puede mandar paquetes ICMPv6 de redireccionamiento falsificados a la red local, lo que puede provocar que la tabla de enrutamiento de los nodos se infecte, de manera que se reenvíen paquetes a direcciones fraudulentas. Como resultado, el tráfico se redireccionará a un nodo falso en la red.

5.9.2. CONFIGURACIÓN SEGURA

132. Inhabilitar la aceptación de redireccionamiento ICMP en sistemas que no sean routers y en aquellos routers que no sea estrictamente necesario.

5.10. ROGUE DHCPV6

5.10.1. DESCRIPCIÓN

133. Se basa en levantar un servidor falso DHCP en la red local, de forma que se pueden asignar de manera errónea las direcciones y hacer un ataque de negación de servicio.

5.10.2. CONFIGURACIÓN SEGURA

134. La mejor forma de combatir esto es utilizar DHCP Snooping. Básicamente, se basa en definir en el equipo los puertos sobre los que el tráfico del servidor DHCP confiable puede transitar. Es decir, definimos como “trust” los puertos donde tenemos servidores dhcp, relays dhcp y la conexión entre los equipos.

5.11. ATAQUES SOBRE LAS CABECERAS DE EXTENSIÓN

5.11.1. DESCRIPCIÓN

135. En IPv6 se han añadido las llamadas cabeceras de extensión, que es una forma distinta de añadir opciones en los paquetes a como se hacía en la cabecera de IPv4. En IPv6 estas opciones se añaden como cabeceras de extensión, de forma que es más fácil procesar los paquetes, sabiendo si hay opciones en cabeceras de extensión gracias al campo Next Header. Sin embargo, hay algunas de ellas que se pueden usar de forma maliciosa.
136. La utilización de éstas cabeceras puede afectar al manejo de los paquetes por parte de los routers (solo las cabeceras de hop-by-hop) y los nodos finales. Para tomar decisiones correctas de seguridad, el software de seguridad, como los cortafuegos y los sistemas de prevención de intrusos, tiene que conocer el efecto que cada cabecera de extensión tiene en el paquete. Si no sabe el efecto, o cuando una cabecera de extensión oculta a otra cabecera de extensión (por ejemplo IPsec ESP), el software de seguridad no puede tomar las decisiones correctas.
137. Por otro lado, el descartar paquetes con una extensión de cabecera desconocida no es una opción válida en los nodos intermedios, con la excepción de las cabeceras hop-by-hop, ya que puede romper la funcionalidad. Para los nodos finales que no reconocen una extensión de cabecera específica, el paquete debe ser descartado y un mensaje de error ICMP “Parameter Problem” será devuelto.

5.11.2. CONFIGURACIÓN SEGURA

138. En ciertos casos, los dispositivos de seguridad pueden configurarse para descartar paquetes con una cabecera de extensión desconocida, mientras no interfiera con la funcionalidad requerida. Esto debe aplicarse por sistema, eximiendo a los sistemas específicos para pasar a través de cabeceras de extensiones desconocidas. De forma alternativa, el uso de cabeceras de extensión desconocidas puede producir un aviso en el registro de cara a una futura inspección.
139. Se recomienda que si no son necesarias se incluyan reglas en los ACL (Access Control List) de los router para no procesarlas o limitar su uso a orígenes conocidos.

5.12. FILTRADO DE PAQUETES ICMPV6

5.12.1. DESCRIPCIÓN

140. IPv6 requiere el correcto funcionamiento de ICMP, por ejemplo para PMTU discovery. Sin embargo, en IPv4 normalmente ICMP es filtrado. Como resultado de la filtración de ICMPv6, las conexiones que completan el acuerdo a tres vías (three-way handshake) de manera correcta se quedan fuera de servicio cuando los datos son transferidos. Este estado se denomina conexión de agujero negro. Los agujeros negros de PMTU actualmente son comunes, de modo que el servidor debe ser bloqueado para recibirlos y el cliente debe ser bloqueado para enviarlos.

5.12.2. CONFIGURACIÓN SEGURA

141. Habilitar mensajes específicos de ICMPv6 en los dispositivos de filtrado incluyendo mensajes de error de ICMP, por lo menos el de paquete demasiado grande (ICMPv6 Packet Too Big, tipo 2). Como solución, se puede utilizar la restricción del tamaño máximo del segmento TCP (MSS).

5.13. FILTRADO DE TRÁFICO

5.13.1. DESCRIPCIÓN

142. La Traducción de Direcciones de Red (NAT, Network Address Translation) es normalmente usada como una protección limitada en IPv4, especialmente en redes domésticas. IPv6, sin embargo, no soporta NAT y, por lo tanto, los dispositivos de frontera requieren de una implementación real de cortafuegos.

5.13.2. CONFIGURACIÓN SEGURA

143. Habilitar cortafuegos en los dispositivos frontera de la red si es posible. Otra forma sería añadir cortafuegos a los límites de la red o habilitar la protección de hosts.

5.14. TÚNELES ENCUBIERTOS

5.14.1. DESCRIPCIÓN

144. Un canal encubierto tiene la capacidad de transmitir objetos de información entre procesos que se suponen no están autorizados para comunicarse según la política de seguridad informática. Hay muchas formas posibles de encubrir canales y algunas pueden ser creadas usando funcionalidades específicas de IPv6. Estas, por ejemplo, pueden ser usadas como canales de mando y control por APTs y botnets. Algunas específicas de IPv6 se pueden ver a continuación:

- Extensión de cabeceras desconocidas. Los datos pueden ser almacenados en las cabeceras de extensión para atravesar cortafuegos de manera inadvertida.
- Datos extra después de las cabeceras de extensión. El valor 59 en el campo Next Header en una cabecera IPv6 o en cualquier cabecera de extensión indica que no hay nada que siga a esa cabecera. Si el campo de Payload Length de una cabecera IPv6 indica la presencia de octetos pasado el final de la cabecera cuyo Next Header

contiene 59, estos octetos deben ser ignorados, y se transmite sin cambios si el paquete es reenviado.

- Usando campos de la cabecera IPv6 para transportar datos. La etiqueta de flujo y el tipo de servicios son campos en la cabecera de IPv6 que típicamente no se usan y normalmente son ignorados por los cortafuegos y copiados por VPNs.
- Partes del direccionamiento IPv6. Hay muchas direcciones IPv6 sin usar en una red. Una subred de direcciones IPv6 puede ser usada como un canal encubierto sin interferir con la accesibilidad.

5.14.2. CONFIGURACIÓN SEGURA

145. Típicamente los canales encubiertos y el abuso de canales encubiertos son difíciles de encontrar y protegerse contra ellos. Reglas de filtrado y normalización de paquetes podrían ayudar en general. Canales específicos encubiertos normalmente requieren soluciones específicas para cada caso.

5.15. TÚNELES IPV6

5.15.1. DESCRIPCIÓN

146. El uso de túneles (por ejemplo Teredo, ISATAP, 6 over 4, 4 over 6) pueden evitar cortafuegos y otros mecanismos de protección, especialmente si estos mecanismos no soportan IPv6 en absoluto o los túneles están ocultos. Por lo tanto, esto llevará a una conexión IPv6 sin gestión e insegura, lo que abre la ventana a muchos ataques basados en IPv6.
147. Los túneles son un mecanismo muy utilizado a la hora de querer saltarse las medidas de seguridad, incluida la tunelización HTTP, DNS, SSH, etc. independientemente de la versión del protocolo IP. Los túneles de IPv6 simplemente son un añadido a los múltiples mecanismos de tunelización que existen.

5.15.2. CONFIGURACIÓN SEGURA

148. Se debe bloquear Teredo y otros protocolos automáticos de tunelización. Bloquear también la tunelización IPv6 si esta no es necesaria. Si es necesaria, se debe permitir sólo en sistemas específicos, tanto interna como externamente.

5.16. FALSIFICACIÓN DE RELAYS TEREDO

5.16.1. DESCRIPCIÓN

149. Teredo es una técnica de creación de túneles para poder enviar tráfico bajo el protocolo IPv6 desde un equipo que está en una red IPv4, normalmente detrás de NAT. Se trabaja con unos nodos Teredo llamados relays, que tienen acceso a la red IPv6, reciben los paquetes, los desencapsulan y los encaminan. Por tanto, son los encargados de retransmitir el tráfico IPv6.
150. El ataque se puede llevar a cabo si un atacante hace que el host anuncie el prefijo estandarizado para Teredo, que es (2001::/32). Si esto sucede, los equipos que utilicen la técnica Teredo para encapsular el tráfico IPv4 configurarán como relay el equipo del

atacante, pudiendo analizar el tráfico, intentar modificarlo o directamente eliminarlo, provocando un ataque de negación de servicio.

5.16.2. CONFIGURACIÓN SEGURA

151. Para que no se lleve a cabo la falsificación de los relays Teredo se puede realizar un procedimiento que se suele llamar test de conectividad IPv6 directa, que simplemente consiste en generar un número aleatorio y enviar desde el cliente Teredo hacia el equipo IPv6 nativo un paquete ICMPv6 echo request donde se incluya el número. La respuesta al mensaje debe venir de un relay teredo cuya dirección IPv4 coincida con la dirección del relay Teredo que se estuvo usando. Es decir, es una forma de comprobar la autenticidad del relay Teredo.
152. También se deben proteger las comunicaciones que se hagan vía Teredo con IPSec, de forma que se proporciona seguridad extremo a extremo para evitar que si el tráfico se intercepta con la finalidad de modificarlo o analizarlo, estos cambios o análisis no se puedan llevar a cabo.

5.17. DESBORDAMIENTO DE LA MEMORIA EN TEREDO

5.17.1. DESCRIPCIÓN

153. En la técnica de túnel Teredo que se ha mencionado anteriormente, la memoria se puede saturar, tanto del cliente, como del servidor Teredo o del relay, por ejemplo, mandando una gran cantidad de tráfico hacia el servidor o el relay Teredo, provocando un ataque de negación de servicio.

5.17.2. CONFIGURACIÓN SEGURA

154. Como se ha dicho, el desbordamiento de memoria se puede causar en el cliente, en el servidor o en el relay Teredo. Para evitar esto se debe filtrar el tráfico basándose en una serie de reglas como filtrar el tráfico Teredo, puerto UDP 3544.

5.18. FALSIFICACIÓN DE RELAYS 6TO4

5.18.1. DESCRIPCIÓN

155. 6to4 es otra técnica de creación de túneles para trabajar con tráfico IPv6 dentro de redes IPv4. En este caso, se forman direcciones IPv6 a partir de la dirección IPv4. Además, se usan también relays 6to4 que se encargan de llevar a cabo la comunicación entre los equipos que usan IPv6.
156. El ataque es muy similar al que se realiza en la técnica Teredo. El atacante anuncia el prefijo estandarizado que hay para 6to4, que es (2002::/16) y de esta manera el tráfico se redirige a un falso relay 6to4, donde se puede descartar el tráfico o realizar operaciones con él. El atacante también puede tener configurada la dirección anycast 192.88.99.1 que está asignada a 6to4.

5.18.2. CONFIGURACIÓN SEGURA

157. Se debe descartar el tráfico recibido de un equipo 6to4 en el cual su dirección no coincide con el prefijo 6to4. También se debería hacer uso de IPSec para protegerse ante la interceptación de la comunicación, de forma que se asegure la comunicación extremo a extremo.

5.19. DESBORDAMIENTO DE LA MEMORIA EN 6TO4

5.19.1. DESCRIPCIÓN

158. Similar al desbordamiento de memoria de la técnica Teredo, en este caso la saturación de memoria puede afectar a los relays 6to4 y a los nodos finales. Este ataque se basa en el tráfico masivo enviado hacia los relays del túnel o hacia los nodos finales, que hace que se desborde la memoria y se produzca una negación de servicio.

5.19.2. CONFIGURACIÓN SEGURA

159. Para evitarlo, hay que filtrar el tráfico de forma que se elimine el tráfico cuyo origen sean direcciones IPv4 privadas o de tipo broadcast o multicast y no aceptar el tráfico que provenga de un nodo 6to4 si la dirección IPv4 no coincide con el prefijo 6to4.

5.20. MAL REENSAMBLADO DE PAQUETES

5.20.1. DESCRIPCIÓN

160. El reensamblado se produce cuando un paquete grande es separado en fragmentos, resultando paquetes más pequeños que contienen la cabecera de fragmentación. Esto ocurre normalmente cuando un paquete no encaja en la MTU. El sistema receptor reensambla los paquetes fragmentados para obtener el paquete completo original y que pueda ser procesado como siempre.
161. Las especificaciones de IPv6 permite que los paquetes contengan cabecera de fragmentación (Fragment Header) aunque el paquete no esté realmente fragmentado en múltiples partes. Este tipo de paquetes, conocidos como fragmentos atómicos (atomic fragments), son típicamente enviados por hosts que han recibido un mensaje de error ICMPv6 del tipo "Packet Too Big" que avisa que el tamaño de MTU del siguiente salto es menor de 1280 bytes, el tamaño mínimo de la MTU de acuerdo con el estándar. Estos paquetes, que contienen la cabecera de fragmentación pero que no están fragmentados, pueden inutilizar un dispositivo o cortafuegos/IPS (Intrusion Prevention System). Esto sucede cuando un dispositivo procesa los paquetes como "tráfico fragmentado" normal (es decir, cuando son "reensamblados" con cualquier otro fragmento de los que hay en cola que supuestamente corresponde al mismo paquete original). Mediante la disminución del tamaño de la MTU haciéndola más pequeño de 1280 bytes, es posible tener clientes que generen estos paquetes, los cuales pueden causar como resultado un DoS en los dispositivos de filtrado. Esta vulnerabilidad es especialmente relevante en los dispositivos de filtrado que llevan a cabo Deep Packet Inspection, DPI o Inspección Profunda de Paquetes.
162. Este ataque puede también llevar a evitar los cortafuegos cuando las cabeceras de extensión son divididas en muchos fragmentos, en este caso el cortafuegos puede no ser

capaz de examinar todas las cabeceras de extensión. Además, es posible causar un DoS cuando inundamos un sistema con paquetes fragmentados, ya que estos necesitan ser mantenidos en memoria hasta que todos los fragmentos han sido recibidos.

5.20.2. CONFIGURACIÓN SEGURA

163. El sistema debe implementar RFC 5722: “Handling of Overlapping IPv6 Fragments”, en el que se recomienda no permitir la superposición de paquetes fragmentados y RFC 6946: “Processing of IPv6 ‘Atomic’ Fragments”, en el que se dice que cuando un host recibe un paquete con Fragment Offset=0 y MF=0, debe procesar el paquete en forma aislada, incluso si el fragmento contiene el mismo conjunto de: [Dirección IPv6 Origen, Dirección IPv6 destino, Identificación de Fragmento]. Un paquete atómico debe ser “reensamblado” a partir de los contenidos de ese único paquete.
164. La parte sin fragmentar del paquete reensamblado está formada por todas las cabeceras hasta, pero sin incluir, la cabecera de fragmentación del paquete atómico recibido.
165. El campo “Next Header” de la última cabecera de la parte sin fragmentar del paquete reensamblado se obtiene del campo “Next Header” de la cabecera de fragmentación del paquete atómico recibido.
166. La longitud del payload del paquete reensamblado es obtenida mediando la resta de la longitud de la cabecera de fragmentación (que es 8) a la longitud del payload del paquete atómico recibido.

5.21. SUPERPOSICIÓN DE FRAGMENTOS

5.21.1. DESCRIPCIÓN

167. Este ataque describe cómo se puede evitar un cortafuegos utilizando la superposición de fragmentos. El atacante envía un paquete IPv6 lo suficientemente grande para que sea necesario ser fragmentado. El paquete será dividido en varios fragmentos por el transmisor de forma que los paquetes resultantes quepan en el camino del MTU. La cabecera TCP tiene los siguientes valores de flags: S(YN)=1 y A(CK)=1. Esto puede hacer que un cortafuegos con estado que esté inspeccionando piense que es un paquete respuesta a una petición de conexión iniciada en el lado de confianza. Por lo tanto, le permitirá al fragmento que pase. También permitirá el acceso a los siguientes fragmentos que tengan el mismo valor de Identificador de Fragmento en la cabecera.
168. Un atacante puede crear un segundo fragmento, perteneciente al primero, con una cabecera TCP cuyas flags sean S(YN)=1 y A(CK)=0. El cortafuegos tratará a este paquete de manera similar al primero. En el lado del receptor, el primer paquete será ignorado, mientras que el segundo será interpretado como una petición de conexión. Mediante este proceso, el atacante evita el control de acceso del cortafuegos para iniciar una petición de conexión a un sistema protegido.

5.21.2. CONFIGURACIÓN SEGURA

169. No permitir la superposición de fragmentos para evitar el ataque.
170. Implementar el procesamiento de “Atomic” fragments de manera que los paquetes de IPv6 se filtren de manera independiente.

5.22. PAQUETES CON CABECERAS DE EXTENSIÓN LIMITADA

5.22.1. DESCRIPCIÓN

171. Las cabeceras de extensión han sido añadidas a los paquetes IPv6 en forma de lista. Cada cabecera apunta a la siguiente cabecera hasta que no haya más cabeceras; la última de ellas indica el tipo de cabecera del protocolo de la capa superior en el payload del paquete (por ejemplo, TCP o UDP). Alguien podría crear un paquete que nunca terminase la lista de las cabeceras, combinando esto con la fragmentación. No es seguro cómo las implementaciones manejarán este tipo de comportamiento sin especificar.

5.22.2. CONFIGURACIÓN SEGURA

172. Una solución posible es establecer un máximo en la cantidad de cabeceras de extensión de los paquetes. Este máximo podría ser impuesto en los cortafuegos.

5.23. INUNDACIÓN DE ROUTER ADVERTISEMENT

5.23.1. DESCRIPCIÓN

173. Mediante el envío de una gran cantidad de paquetes RA falsos en una red local un atacante puede congelar o inhabilitar el sistema. Esta vulnerabilidad afecta a muchos sistemas, incluyendo Windows (cualquier versión anterior a Windows 8), Juniper Netscreen, Solaris, OS/X, FreeBSD y Android.
174. El ataque es llevado a cabo por RAs normales, con las opciones de ICMPv6: MTU, Multiple Route Information section 17, Multiple Prefix Information section 18 y una dirección origen de la capa de enlace.

5.23.2. CONFIGURACIÓN SEGURA

175. Equipos con funcionalidad “RA Guard” filtran estos paquetes. Los equipos más comunes normalmente no soportan esta funcionalidad. Los parches de los fabricantes (por ejemplo, Windows7) solventan en parte el problema, por lo que se recomienda estar al tanto de las actualizaciones de seguridad en todos los sistemas y/o componentes.

5.24. DENEGACIÓN DE SERVICIO CON BUCLES DE ENRUTAMIENTO MEDIANTE TÚNELES

5.24.1. DESCRIPCIÓN

176. Los túneles IP se pueden utilizar para crear un bucle de enrutamiento que puede ser utilizado para hacer ataques de denegación de servicio (DoS), de modo que un solo paquete sea procesado por un router varias veces. Estos ataques se basan en las inconsistencias entre el enrutamiento por túnel de IPv6 y el enrutamiento nativo de IPv6. Una mezcla de diferentes tipos de túneles se puede utilizar incluyendo ISATAP, Teredo, 6to4, 4to6. Se deben filtrar los túneles creados por los sistemas finales para evitarlo y seguir las directrices expuestas a continuación.

5.24.2. CONFIGURACIÓN SEGURA

177. Si la dirección de destino es una dirección ISATAP (Intra-Site Automatic Tunnel Addressing Protocol, se usa para túneles IPv6 sobre IPv4), sus últimos cuatro octetos no deben ser iguales a una dirección IPv4 de alguna de las interfaces del nodo.
178. Si la dirección de destino es una dirección 6to4, sus 3-6 octetos no deben ser iguales a una dirección IPv4 de alguna de las interfaces del nodo.
179. Si la dirección de destino es una dirección Teredo, el campo <obfuscated external IP> no puede ser igual al complemento a 1 (operación binaria para representar los números enteros negativos) de una dirección IPv4 de una de las interfaces del nodo ni igual a una dirección IPv4 que está asignada a ese nodo por un NAT.
180. Todos estos controles deben aplicarse en todos los nodos IPv6 que puedan enviar paquetes y que participe en, al menos, uno de estos túneles. Esto ayudaría a evitar los bucles de enrutamiento.

5.25. ICMP SPOOFING PARA REDIRIGIR TRÁFICO Y DENEGACIÓN DE SERVICIO

5.25.1. DESCRIPCIÓN

181. El uso de mensajes falsos de ICMPv6 en una red puede causar una denegación de servicio (DoS) en algunos equipos o, incluso, en prefijos de red enteros. El tipo de mensaje “redirect” de ICMPv6 puede hacer que el tráfico cursado pase por otro camino o Gateway, quedando incomunicados incluso.
182. Los equipos, con los mensajes “redirect”, reconfiguran la tabla de enrutamiento, cambiando las rutas de los paquetes y haciendo que el tráfico se pueda desviar.

5.25.2. CONFIGURACIÓN SEGURA

183. En un compromiso entre la seguridad y la robustez de la red, ya que los mensajes “redirect” se utilizan para cambiar las tablas de enrutamiento ante fallos, se podrían ignorar los mensajes “redirect” o restringir su uso en la red.

5.26. UTILIZACIÓN DE DIRECCIONES ULA EN REDES EXTERIORES

5.26.1. DESCRIPCIÓN

184. Como ya se ha comentado, IPv6 introduce nuevos tipos de direcciones, siendo una de ellas la ULA (Unique local Address). Estas direcciones no se espera que salgan a redes exteriores, es decir, enrutadas por Internet, sino que son para uso en redes locales. En el caso de que se haga una configuración errónea, estas direcciones pueden tener una conectividad más allá del ámbito local, lo que puede provocar un comportamiento errático, además de posibles fugas de información y de topología de la red.

5.26.2. CONFIGURACIÓN SEGURA

185. Para que esto no suceda, lo correcto es filtrar este tipo de direcciones, ya sea en los Gateway frontera o con cortafuegos.

5.27. AGOTAMIENTO DE LA TABLA CAM

5.27.1. DESCRIPCIÓN

186. Como ya se ha comentado, IPv6 introduce nuevos tipos de direcciones, siendo una de ellas la ULA (Unique local Address). Estas direcciones no se espera que salgan a redes exteriores, y sean enrutadas por Internet, sino que son para uso en redes locales. En el caso de que se haga una configuración errónea, estas direcciones pueden tener una conectividad más allá del ámbito local, lo que puede provocar un comportamiento errático, además de posibles fugas de información y de topología de la red.
187. CAM (Content Addressable Memory) es un tipo especial de memoria usada por algunos equipos. Estas memorias utilizan un dato que comparan con tu tabla de contenido y si hay coincidencias, devuelve la dirección/es en la/s que se ha encontrado ese dato. Las tablas de CAM pueden dar dos resultados 0 (true) ó 1 (false). CAM es muy útil para construir tablas que buscan coincidencias exactas como las tablas de direcciones MAC.
188. TCAM (Ternary Content Addressable Memory) puede comparar un tercer estado, que puede ser cualquier valor. TCAM es más útil para hacer tablas para la búsqueda de coincidencias más largas, tales como tablas IP organizadas por prefijos IP.
189. Por tanto, el número máximo de rutas IP y direcciones MAC que un switch o router puede aprender está limitado por el tamaño máximo de su CAM y TCAM.
190. Habilitar el enrutamiento IPv6 tiene el efecto de reducir significativamente la cantidad total de entradas de TCAM debido al mayor tamaño de las direcciones IPv6. Las siguientes consideraciones hacen a un equipo más vulnerable al agotamiento de CAM o TCAM: actualización automática de ACL (Access Control List), aceptando paquetes falsos de enrutamiento y tener un link de alcance mayor que las direcciones que puedan encajar en CAM o TCAM.
191. El agotamiento de TCAM tiene diferentes efectos en las diferentes plataformas, algunas pueden continuar procesando paquetes en la CPU causando un gran uso de recursos. Algunos equipos L3 empiezan a inundar con tráfico saliente a todos los puertos.

5.27.2. CONFIGURACIÓN SEGURA

192. Si están disponibles, se deben habilitar herramientas de mitigación, como ndpexhaustion, en el equipo. Asegurar los dispositivos para no aceptar más rutas de dispositivos sin autenticar reducirá el vector de ataque. Cuando la capacidad de la TCAM está casi alcanzada, durante una operación de refactorización normal del plan de direccionamiento de una red para reducir el número de rutas aprendidas y reducir el tamaño, aliviando así el problema, hay que limitar las reglas de ACL/QoS y/o deshabilitar las características sin usar para reducir el número de entradas TCAM requeridas. Si la refactorización no es posible, reemplazar o actualizar el hardware es la única opción.

6. CONFIGURACIÓN EN ENRUTADORES CISCO

193. Para la configuración de IPv6 en un enrutador Cisco se va a tomar como referencia el IOS Release 15.2S (1). En cuanto a otros equipos con diferente sistema y/o de otros fabricantes, el proceso será similar, salvo pequeñas diferencias en cuanto a la forma de

escribir ciertas instrucciones. Se recomienda acudir al manual del fabricante para poder ver posibles equivalencias.

6.1. IMPLEMENTACIÓN DE CONECTIVIDAD BÁSICA IPV6

6.1.1. CONECTIVIDAD IPV6

194. En primer lugar se realiza una asignación de dirección a una interfaz, siguiendo los siguientes pasos en la consola de comandos del terminal:

```
enable
configure terminal
interface type number
ipv6 address ipv6-prefix/prefix-length eui64|link-local|anycast o ipv6 enable
exit
ipv6 unicast-routing
```

195. Primero se entra en la configuración del equipo y se selecciona la interfaz sobre la que se va a aplicar la configuración. Una vez ahí, el siguiente comando se utiliza para fijar la dirección IPv6 a utilizar en este caso, pudiendo configurarse una dirección con el algoritmo eui64 (que utiliza la dirección mac para obtener la dirección), una dirección link-local o una dirección anycast. También es posible habilitar el procesado de IPv6 en una interfaz que no ha sido configurada con una dirección explícita de IPv6 con el comando `ipv6 enable`. Una vez realizado esto, saliendo del modo de configuración de la interfaz y con el último comando se habilita la transmisión de paquetes IPv6.

6.1.2. CONFIGURAR UN LÍMITE DE CACHÉ PARA EL PROTOCOLO NEIGHBOUR DISCOVERY

196. Es necesario tener un límite de caché apropiado según las condiciones del equipo para poder evitar que la tabla de entradas se colapse. Para ello, se configura el límite de la caché así:

```
enable
configure terminal
interface type number
ipv6 nd cache interface-limit size
```

197. Con ello se entra a la configuración del terminal y se selecciona la interfaz sobre la que aplicar el límite de la caché. Si se prefiere, se puede obviar el comando “interface type number” para aplicar la misma configuración sobre todas las interfaces del equipo. Por último, en el último comando en el parámetro `size` se introduce la cantidad de entradas que se desean como máximo.

6.1.3. PERSONALIZAR PARÁMETROS DE NEIGHBOUR DISCOVERY

198. En el protocolo se pueden configurar ciertas opciones o características dependiendo del entorno en el que se trabaje.

```
enable
configure terminal
```

```
interface type number
ipv6 nd nud retry base interval max-attempts
ipv6 nd cache expire expire-time-in-seconds
ipv6 nd na glean
```

199. Igual que en el caso anterior, los 3 primeros comandos sirven para entrar a la configuración del equipo. El cuarto comando marca el número de veces que la funcionalidad Neighbour Unreachability Detection (NUD) reenvía peticiones de Neighbour Solicitation, poniendo en base 1, en interval el tiempo que tiene que transcurrir entre las peticiones y en max-attempts el número máximo de intentos.
200. Por otro lado, el quinto comando configura el tiempo que tarda en expirar (expire time in seconds) una entrada de la tabla del protocolo Neighbour Discovery, mientras que el último de ellos configura Neighbour Discovery para limpiar una entrada de un Neighbour Advertisement no solicitado.

6.1.4. CONFIGURAR PREFIJOS

6.1.4.1. CONFIGURAR UN PREFIJO MANUAL

201. Para configurar un prefijo de forma manual, hay que seguir los siguientes comandos:

```
enable
configure terminal
ipv6 general-prefix prefix-name {ipv6-prefix/prefixlength | 6to4 interface-type
interface-number}
```

202. Básicamente, se trata de entrar a la configuración del equipo y añadir un prefijo, con un nombre dado y el prefijo en sí. Además, si se desea hacer que la interfaz sea una 6to4, se puede hacer la opción del final. Un ejemplo del comando con cada opción sería:

```
Device(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
ipv6 general-prefix my-prefix 6to4 ethernet 0
```

6.1.4.2. DEFINIR UN PREFIJO CON DHCPV6

203. De esta forma, se define un prefijo para usarlo con la opción de DHCPv6. Para más información sobre cómo realizar esta labor, ver la sección sobre implementación de DHCP para IPv6. Los comandos a utilizar son:

```
enable
configure terminal
interface type number
ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits/prefix-lentgh}
```

204. Con los 3 primeros comandos se entra a la configuración del terminal y se selecciona la interfaz donde se va a hacer la configuración. Con el último comando se inserta el prefijo, como por ejemplo:

```
ipv6 address my-prefix 2001:DB8:0:7272::/64
```

6.1.5. CONFIGURAR UNA INTERFAZ PARA QUE SOPORTE IPV4 E IPV6

205. Se configura una interfaz para que sea capaz de manejar tráfico tanto de paquetes IPv4 como de paquetes IPv6. Es decir, puede recibir y enviar tráfico de los 2 protocolos por la misma interfaz. Los comandos son:

```
enable
configure terminal
ipv6 unicast-routing
interface type number
ip address ip-address mask [secondary [vrf vrf-name]]
ipv6 address {ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
```

206. Con los 2 primeros comandos se entra en la configuración del equipo, con el tercero se permite el uso de IPv6 y en el cuarto se elige la interfaz. Se selecciona más tarde la dirección de IPv4 de la interfaz y la dirección de IPv6 después.

6.1.6. PERSONALIZAR LA TASA LÍMITE DE ICMP

207. Se efectúa con los siguientes comandos:

```
enable
configure terminal
ipv6 icmp error-interval milliseconds
```

6.1.7. CONFIGURAR LA EXTENSIÓN DRP PARA INGENIERÍA DE TRÁFICO

208. Los equipos descubren y seleccionan dispositivos predeterminados al escuchar los Router Advertisement (RA). Por defecto, los mecanismos de selección de dispositivo no son óptimos en ciertos casos, como cuando se necesita la ingeniería de tráfico. Por ejemplo, dos dispositivos en una red pueden proporcionar un coste de enrutamiento equivalente, pero no igual costo, y la política puede dictar que se prefiera uno de los dispositivos para tener mayor optimización. Para llevarlo a cabo:

```
enable
configure terminal
interface type number
ipv6 nd router-preference {high|medium|low}
```

6.1.8. HABILITAR UNICAST RPF

209. Los administradores de red deben utilizar Unicast Reverse Path Forwarding (Unicast RPF) para ayudar a limitar el tráfico malicioso en la red. Esta función de seguridad permite que un router verifique la accesibilidad a la dirección de origen en los paquetes. Esta capacidad puede limitar la aparición de direcciones falsas en una red. Si la dirección IP de origen no es válida, el paquete se descarta. Unicast RPF trabaja en 2 modos distintos: el modo strict y el modo loose.
210. Cuando se utiliza Unicast RPF en modo strict, el paquete debe ser recibido en la interfaz del router que utilizaría para reenviar el paquete de respuesta. Por tanto, configurado en modo estricto puede descartar tráfico legítimo que se recibe en una interfaz que no era la elección del enrutador para enviar el tráfico de respuesta.

211. En cambio, cuando se utiliza Unicast RPF en el modo loose, la dirección de origen debe aparecer en la tabla de enrutamiento. Los administradores pueden cambiar este comportamiento usando la opción `allow-default`, que permite el uso de la ruta por defecto en el proceso de verificación de origen. Una lista de acceso también se puede especificar para que permita o niegue ciertas direcciones de origen.
212. Se debe tener cuidado en el modo seleccionado de Unicast RPF (loose o strict) que se configura durante el despliegue de esta característica, ya que puede verse afectado el tráfico legítimo. En muchos entornos, es necesario el uso de una combinación de modo strict y el modo loose Unicast. La elección del modo de RPF dependerá del diseño del segmento de red conectado a la interfaz en la que se despliega.
213. Se debe utilizar el modo strict en interfaces de red para que se garantice que todos los paquetes recibidos en una interfaz se originan en la subred asignada a la interfaz. Una subred compuesta por estaciones terminales o recursos de red cumple con este requisito. Tal diseño sería una red de acceso, donde sólo hay un camino de entrada y salida. No se permite otro tráfico distinto al originado por la red.
214. El modo loose, en cambio, se puede utilizar en una interfaz de red de enlace ascendente que tiene una ruta por defecto asociado a él. Para configurarlo, hay que aplicar los siguientes comandos:

```
enable
configure terminal
interface type number
ipv6 verify unicast source reachable-via {rx|any}[allow-default][allow-self-ping][access-list-name]
```

215. En el último comando `rx` permite Unicast RPF en modo strict, mientras que para aplicar el modo loose se utiliza la opción `any`. La opción `allow-default` puede ser usada con `rx` o `any` para incluir direcciones IP que no figuren específicamente en la tabla de enrutamiento. La opción `allow-auto-ping` no se debe utilizar, ya que podría crear una denegación de servicio. Una lista de acceso también puede ser configurada para permitir o denegar específicamente una lista de direcciones a través de Unicast RPF.

6.1.9. VISUALIZACIÓN DE INFORMACIÓN DE IPV6

216. Con estos comandos se puede ver una gran cantidad de información acerca del estado del router y del tráfico en la red. A continuación se puede ver una lista de ellos (es necesario acceder en modo privilegiado para poder ejecutar el resto de comandos sobre el equipo).

`show ipv6 interface [brief] [type number] [prefix]` : muestra el estado de uso de las interfaces configuradas para ipv6.

`show ipv6 neighbors [interface-type interface-number | ipv6-address | ipv6-hostname | statistics]`: muestra la información de caché de neighbour discovery.

`show ipv6 route [ipv6-address | ipv6-prefix | prefix-length | protocol | interface-type interface-number]` : muestra los contenidos actuales de la tabla de routing de ipv6.

`show ipv6 traffic`: muestra las estadísticas sobre el tráfico de ipv6.

6.2. IMPLEMENTACIÓN DE DHCP PARA IPV6

6.2.1. DELEGACIÓN DE PREFIJO EN DHCPV6

217. La delegación de prefijos puede usarse para manejar enlaces, subredes y cambios de direcciones. Las extensiones de DHCPv6 también proporcionan delegación de prefijos, incluso un ISP puede automatizar el proceso de asignación de prefijos a un cliente para usar en su propia red. Esta delegación se da entre el equipo del proveedor (ISP) que se denomina PE y el equipo del cliente, que se llama CE y una vez esto ocurra, el cliente puede hacer subredes y asignar distintos prefijos.
218. Como se vio anteriormente, hay 2 posibilidades. Por un lado, se tiene la opción stateless, en la que no se requiere ningún servidor central, utilizada para configurar nodos sin delegación de prefijo. Su uso es controlado por los routers, con los mensajes router advertisement (RA). El cliente solicita el RA y el DHCPv6 responde a esta petición con los parámetros de configuración apropiados para el cliente.
219. Cada cliente y servidor están identificados por un identificador DHCP único, formándose este identificador con la dirección MAC del equipo. Cada una de las funciones (Cliente, Servidor, Relay) son excluyentes dentro de la misma interfaz, de forma que si una interfaz ya tiene habilitada alguna de las funciones, no podrá tener otra más. A continuación se describen estas funcionalidades.

6.2.1.1. CLIENTE DHCP

220. El cliente DHCPv6 puede solicitar y aceptar los parámetros de configuración que no requieren un servidor, tales como direcciones de servidor DNS y opciones de la lista de búsqueda de dominios.
221. El cliente DHCPv6 también puede solicitar la delegación de prefijos. Los prefijos adquiridos de una delegación de router se almacenarán en un "pool" local de prefijos IPv6.
222. Un cliente DHCPv6 genera una lista de posibles servidores mediante el envío de un mensaje de petición y mediante la recopilación de mensajes de respuesta de los servidores. Estos mensajes se clasifican en base al valor de preferencia, y los servidores pueden añadir una opción de preferencia al anunciar mensajes indicando explícitamente el valor usado. Si el cliente necesita adquirir prefijos de servidores, se consideran sólo los servidores que han anunciado prefijos.

6.2.1.2. SERVIDOR DHCP

223. El servidor DHCPv6 puede proporcionar los parámetros de configuración para mantener cualquier estado dinámico para los clientes, tales como direcciones de servidor DNS y opciones de la lista de búsqueda de dominios. El servidor DHCPv6 puede estar configurado para realizar la delegación de prefijo.
224. Todos los parámetros de configuración para los clientes están configurados de forma independiente en los "pool" de configuración de DHCPv6. Los prefijos que son delegados a los clientes podrán especificarse como una lista de prefijos asignados previamente para un cliente particular o a "pools" IPv6.

225. El servidor DHCPv6 mantiene una tabla de vinculación automática en la memoria para realizar un seguimiento de la asignación de algunos parámetros de configuración, como prefijos entre el servidor y sus clientes.
226. Un “pool” de información de configuración de DHCPv6 es una entidad que incluye información acerca de los parámetros de configuración disponibles y las políticas que controlan la asignación de los parámetros a los clientes que pertenezcan a ese “pool”. Un “pool” está configurado de forma independiente del servicio DHCPv6 y se asocia con el servicio de DHCPv6 a través de la interfaz de línea de comandos.
227. Cada “pool” de DHCPv6 tiene asociada una “binding table” o tabla de vinculación, que contiene todo los prefijos que en la configuración han sido delegados a los clientes. Contiene distinta información, como la dirección IPv6 del cliente o el tiempo de vida de cada prefijo, entre otros.

6.2.1.3. RELAY DHCP

228. Un relay o agente de retransmisión DHCP se utiliza para retransmitir mensajes entre el cliente y el servidor, siendo transparente para el cliente. Es un requisito para la comunicación directa entre el cliente y el servidor que entre ellos tengan conexión directa. Sin embargo, en algunas situaciones, hace falta un relay que se encargue de esto.

6.2.2. CONFIGURACIÓN DE LA FUNCIÓN DE SERVIDOR DHCPV6

6.2.2.1. CONFIGURACIÓN DEL POOL DE DHCPV6

229. Con los siguientes comandos se puede crear y configurar un pool DHCPv6 y asociarlo con un servidor en una interfaz.

`enable`

Habilita privilegios para la ejecución de comandos.

`configure terminal`

Entra a la configuración global

`ipv6 dhcp pool poolname`

Configura el nombre de un pool y se entra en su configuración.

`domain-name domain`

Configura un nombre de dominio para un cliente DHCPv6.

`dns-server ipv6-address`

Especifica la dirección del DNS disponible para un DHCPv6.

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

Especifica un prefijo de forma manual para ser delegado a un cliente específico con su identificador.

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

Especifica un pool local de IPv6 desde la que los prefijos son delegados a los clientes DHCPv6.

`exit`

Sale de la configuración del pool y vuelve a la configuración global del router.

`interface type number`

Especifica una interfaz.

```
ipv6 dhcp server poolname [rapid-commit] [preference value] [allow-hint]
    Habilita DHCPv6 en esa interfaz.
end
    Se vuelve al modo de ejecución.
```

6.2.2.2. CONFIGURAR BASE DE DATOS DE VINCULACIÓN DE PREFIJOS ASIGNADOS

230. Configurar una base de datos de vinculación de prefijos asignados se hace con los siguientes comandos:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
ipv6 dhcp database agent [write-delay seconds] [timeout seconds]
    Especifica los parámetros de la base de datos de vinculación de DHCPv6.
end
    Se vuelve al modo de ejecución.
```

6.2.3. CONFIGURAR LA FUNCIÓN CLIENTE DE DHCPV6

231. Los prefijos generales se pueden definir de forma dinámica desde un prefijo recibido mediante delegación de prefijo en DHCPv6. El prefijo delegado se almacena en un prefijo general. Para ello seguir los comandos:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
interface type number
    Especifica una interfaz con su tipo y número y entra en la configuración de dicha interfaz.
ipv6 dhcp client pd {prefix-name | hint ipv6-prefix}[rapid-commit]
    Habilita el cliente DHCPv6 y permite una solicitud de delegación de prefijo a través de la interfaz especificada.
end
    Se vuelve al modo de ejecución.
```

6.2.4. CONFIGURAR LA FUNCIÓN RELAY DE DHCPV6

232. Configurar la función relay de DHCPv6:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
interface type number
    Especifica una interfaz con su tipo y número y entra en la configuración de dicha interfaz.
ipv6 dhcp relay destination ipv6-address [interface-type interface-number]
```

Especifica una dirección de destino a la que los paquetes del cliente se reenvían y habilita la retransmisión DHCPv6 en dicho interfaz.

end

Se vuelve al modo de ejecución.

6.2.5. CONFIGURAR DHCPV6 PARA LA ASIGNACIÓN DE DIRECCIONES

233. Para ello, se va a habilitar la función de server en una interfaz, con los siguientes comandos:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
ipv6 dhcp pool poolname
    Configura el nombre de un pool y se entra en su configuración.
address prefix ipenav6-prefix [lifetime {valid-lifetime preferred-lifetime |
infinite}]
    Opcional: especifica un prefijo para la asignación de direcciones (el prefijo
debe estar en hexadecimal).
link-address ipv6-prefix
    Opcional: especifica un prefijo IPv6 como link-address. Cuando una
dirección en la interfaz entrante o una dirección de enlace en el paquete
coincide con el prefijo IPv6 especificado, el servidor utiliza la información
de configuración del pool.
vendor-specific vendor-id
    Opcional: se entra en la configuración específica con el valor de
identificación.
suboption number {address ipv6-address | ascii ascii-string | hex hex-string}
    Opcional: se introduce un número de subopción específico.
exit
    Vuelve a la configuración del pool DHCP
exit
    Vuelve a la configuración global.
interface type numer
    Se entra a la configuración de la interfaz.
ipv6 dhcp server [poolname | automatic][rapid-commit][preference value][allow-
hint]
    Se habilita la función de servidor en la interfaz.
end
    Se vuelve al modo de ejecución.
```

Realizar una de las 2 siguientes tareas a continuación:

```
show ipv6 dhcp pool
    Verifica la configuración del pool DHCPv6.
show ipv6 dhcp interface
    Verifica que la función servidor está habilitada en una interfaz.
```

234. Y ahora habilitar la función de cliente DHCPv6 en una interfaz:

```

enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
interface type number
    Entra a la configuración de esa interfaz.
ipv6 address dhcp [rapid-commit]
    Habilita la interfaz para que pueda adquirir una dirección IPv6 del servidor
    DHCPv6.
end
    Se vuelve al modo de ejecución.
show ipv6 interface
    Verifica que el cliente DHCPv6 está habilitado en una interfaz.

```

6.2.6. CONFIGURAR LA FUNCIÓN STATELESS DE DHCPV6

235. Configurar la función stateless de DHCPv6 mediante la configuración del servidor stateless y del cliente stateless. Para el servidor:

```

enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
ipv6 dhcp pool poolname
    Configura el nombre de un pool y se entra en su configuración.
dns-server ipv6-address
    Especifica los servidores DNS IPv6 disponibles para el cliente.
domain-name domain
    Configura un nombre de dominio para el cliente DHCPv6.
exit
    Se vuelve al modo de ejecución.
interface type number
    Entra a la configuración de esa interfaz.
ipv6 dhcp server poolname [rapid-commit][preference value][allow-hint]
    Habilita DHCPv6 en una interfaz.
ipv6 nd other-config-flag
    Activa el indicador de "other stateful configuration" en los RAs de IPv6.
end
    Se vuelve al modo de ejecución.

```

236. Y ahora para el cliente:

```

enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
interface type number
    Entra a la configuración de esa interfaz.
ipv6 address autoconfig [default]
    Habilita la configuración automática de direcciones IPv6 utilizando la
    configuración automática de stateless en una interfaz y habilita el
    procesamiento de IPv6 en dicha interfaz.

```

end

Se vuelve al modo de ejecución.

6.2.7. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE DHCPV6

237. Para verificar la configuración de DHCPv6 llevada a cabo con los anteriores comandos se puede usar:

enable

Habilita privilegios para la ejecución de comandos.

show ipv6 dhcp

Muestra el DUID (identificador de dispositivo) de un dispositivo específico.

show ipv6 dhcp binding [*ipv6-address*]

Muestra las vinculaciones de los clientes en la base de datos de DHCPv6.

show ipv6 dhcp interface [*type number*]

Muestra la información de DHCPv6 de la interfaz.

show ipv6 dhcp pool [*poolname*]

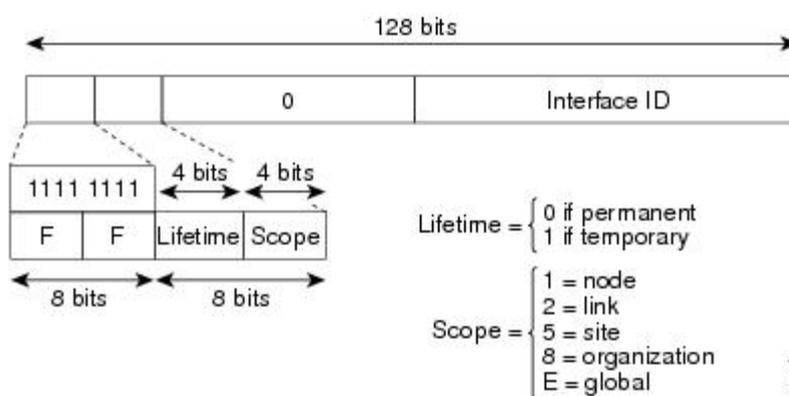
Muestra la información acerca de la configuración del pool de DHCPv6.

6.3. IMPLEMENTACIÓN DE MULTICAST PARA IPV6

238. Un grupo multicast de IPv6 es un grupo arbitrario de receptores que desean recibir un flujo de datos en particular. Este grupo no tiene fronteras físicas o geográficas, ya que los receptores pueden estar ubicados en cualquier lugar en Internet o en cualquier red privada. Los receptores que estén interesados en recibir los datos de un grupo en particular debe unirse al grupo mediante la señalización de su router local. Esta señalización se consigue con el protocolo MLD.
239. Los enrutadores utilizan el protocolo MLD para saber si los miembros de un grupo están conectados en sus subredes de forma directa. Los anfitriones se unen a grupos multicast mediante el envío de mensajes MLD. La red entonces envía los datos a un número potencialmente ilimitado de receptores, usando sólo una copia de los datos de multicast en cada subred.
240. Los paquetes entregados a los miembros del grupo se identifican por una sola dirección de grupo multicast. Estos paquetes se entregan al grupo mediante best-effort o de mejor esfuerzo. El mecanismo de entrega de mejor esfuerzo (Best-effort delivery, en inglés) designa un tipo de servicio de red en el que la red no puede garantizar que los datos lleguen a su destino, ni ofrecer al usuario una determinada calidad de servicio (QoS) en sus comunicaciones.
241. En una red de mejor esfuerzo todos los usuarios reciben el mejor servicio posible en ese momento, lo que significa que obtendrán distintos anchos de banda y tiempos de respuesta en función del volumen de tráfico en la red.
242. El entorno multicast consiste en emisores y receptores. Cualquier equipo, independientemente de si es un miembro de un grupo, puede enviar a un grupo. Sin embargo, sólo los miembros de un grupo reciben el mensaje.
243. La pertenencia a un grupo es dinámica, ya que los equipos pueden unirse y salir en cualquier momento. No hay ninguna restricción en la ubicación o el número de

miembros en un grupo multicast. Además, un equipo puede ser un miembro de más de un grupo multicast a la vez.

244. Una dirección de multicast IPv6 es una dirección que tiene un prefijo FF00::/8. Esta dirección es un identificador para un conjunto de interfaces que normalmente pertenecen a diferentes nodos. Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por la dirección de multidifusión. El segundo octeto que sigue al prefijo define el tiempo de vida y el alcance de la dirección de multidifusión. Una dirección de multidifusión permanente tiene un parámetro de tiempo de vida igual a 0; una dirección de multidifusión temporal tiene un parámetro de tiempo de vida igual a 1. Una dirección de multidifusión que tiene el alcance de un nodo, enlace, sitio, u organización, o un alcance global tiene un parámetro alcance de 1, 2, 5, 8, o E, respectivamente. La siguiente figura muestra el formato de la dirección de multidifusión IPv6.



6.3.1. PROTOCOLO MULTICAST LISTENER DISCOVERY (MLD)

245. El protocolo MLD es utilizado por los routers IPv6 para descubrir la presencia de los oyentes de multidifusión (por ejemplo, los nodos que desean recibir los paquetes de multidifusión) en sus enlaces directamente conectados, y específicamente para descubrir qué direcciones de multidifusión son de interés para aquellos nodos vecinos. Se utiliza para el descubrimiento del grupo local y la pertenencia a un grupo específico de la fuente. El protocolo MLD proporciona un medio para controlar de forma automática y limitar el flujo de tráfico de multidifusión a través de su red con el uso de interrogadores especiales de multicast y host. La diferencia entre interrogadores de multidifusión y los host es la siguiente:
246. Un interrogador es un dispositivo de red, como un router, que envía mensajes de consulta para descubrir qué dispositivos de red son miembros de un grupo de multidifusión dado. Por otro lado, un host es un receptor, incluyendo routers, que envían mensajes de informe para informar al interrogador de una calidad de miembro de acogida. Un conjunto de interrogadores y anfitriones que reciben flujos de datos de multidifusión de la misma fuente se llama grupo de multidifusión o multicast.
247. MLD utiliza el protocolo ICMP para llevar sus mensajes. Todos los mensajes MLD son de enlace local con un límite de saltos de 1, y todos ellos tienen el router conjunto de opciones de alerta. La opción de alerta de enrutador implica una implementación de la cabecera hop-by-hop.
248. MLD tiene tres tipos de mensajes:

- Query. En un mensaje de query, el campo de dirección de multidifusión se establece en 0 cuando MLD envía una consulta general.
- Report. En un mensaje de report, el campo de dirección de multidifusión es el de la dirección de multidifusión específica IPv6 a la que el remitente está escuchando.
- Done. En un mensaje done, el campo de dirección de multidifusión es el de la dirección de multidifusión específica IPv6 a la que la fuente del mensaje MLD ya no está escuchando.

249. Para la configuración stateless, se requiere un nodo para unirse a varios grupos de multidifusión IPv6 con el fin de realizar la detección de direcciones duplicadas (DAD).

6.3.2. HABILITAR MULTICAST EN IPV6

250. Con estos pasos se consigue habilitar multicast en IPv6:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
ipv6 multicast-routing
    Habilita Multicast en IPv6.
```

6.3.3. PERSONALIZAR MLD

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Entra a la configuración global.
interface type number
    Entra en la configuración de la interfaz.
ipv6 mld join-group [group-address] [include | exclude] {source-address | source-
list [acl]}
    Configura MLD para un grupo específico y un origen.
ipv6 mld access-group access-list-name
    Habilita el control de acceso a multicast.
ipv6 mld static-group group-address [[include| exclude] {source-address | source-
list [acl]}
    Reenvía el tráfico de forma estática para el grupo multicast en la interfaz
especificada.
ipv6 mld query-max-response-time seconds
    Configura el máximo tiempo de respuesta en peticiones MLD.
ipv6 mld query-timeout seconds
    Configura el valor del “time-out” del MLD.
ipv6 mld query-interval seconds
    Configura el intervalo de tiempo en el cuál se envía un mensaje MLD.
exit
    Se sale del modo de configuración de la interfaz.
show ipv6 mld [vrf vrf-name] groups [link-local][group-name | group-
address][interface-type interface-number] [detail | explicit]
    Muestra los grupos multicast que están conectados directamente al router.
```

```
show ipv6 mld groups summary
    Muestra un resumen de los grupos multicast.
show ipv6 mld [vrf vrf-name] interface [type number]
    Muestra información de multicast en esa interfaz.
```

6.4. IMPLEMENTACIÓN DE POLÍTICAS DE ENRUTAMIENTO EN IPV6

251. Las políticas de enrutamiento (Policy-Based Routing, de ahora en adelante PBR) proporcionan un medio flexible de enrutamiento de paquetes por lo que permite configurar una política para los flujos de tráfico, lo que reduce la dependencia de rutas derivadas de los protocolos de enrutamiento. Con este fin, PBR da más control sobre el enrutamiento ampliando y complementando los mecanismos existentes proporcionados por los protocolos de enrutamiento. PBR permite establecer la precedencia IPv6, al igual que permite especificar una ruta de acceso para determinados flujos de tráfico, tales como tráfico de prioridad sobre un enlace de alto coste. Además, PBR para IPv6 se puede aplicar tanto a paquetes IPv6 reenviados como originados en la propia máquina.
252. Las políticas pueden basarse en la dirección IPv6, puertos usados, protocolos o el tamaño del paquete. En una política simple se pueden utilizar cualquiera de estos descriptores; para una política compleja, se pueden utilizar varios o todos ellos. PBR permite, entre otras cosas, realizar las siguientes tareas:
 - Clasificar el tráfico en base a una lista de acceso. Estas listas de acceso, por tanto, establecen los criterios a seguir.
 - Establecer bits de prioridad en IPv6, dando a la red la capacidad de activar las clases de servicio diferenciadas.
 - Enrutar paquetes a rutas específicas de ingeniería de tráfico, para que se encaminen para permitir una determinada calidad de servicio (QoS) a través de la red.
253. PBR permite clasificar y marcar los paquetes en el borde de la red, marcando un paquete estableciendo su valor de precedencia. El valor de prioridad puede ser utilizado directamente por los routers en el núcleo de red para aplicar la QoS correspondiente a un paquete, lo que mantiene la clasificación de paquetes en el borde de red.
254. Todos los paquetes recibidos en una interfaz con PBR habilitado se hacen pasar por los filtros de paquetes conocidos como mapas de ruta. Los mapas de rutas utilizados por PBR dictan la política, para determinar dónde enviar los paquetes.
255. Los mapas de ruta se componen de declaraciones. Los mapas de rutas se pueden marcar como permitir o denegar, y se interpretan de la siguiente manera:
 - Si un paquete coincide con todas las declaraciones coincidentes de un mapa de ruta que está marcado como permitir, entonces el router intenta enrutar el paquete de políticas mediante las instrucciones establecidas. De lo contrario, el paquete se reenvía normalmente.
 - Si el paquete no coincide con ninguna de las declaraciones coincidentes de un mapa de ruta que está marcado como denegar, entonces el paquete se envía normalmente.
 - Si la declaración se marca como permitido y los paquetes no coinciden con ninguna de las declaraciones, los paquetes se envían a través de los canales normales y se realiza el enrutamiento basado en destino.

256. Se especifica PBR en la interfaz que recibe el paquete, no en la interfaz desde la que se envía el paquete. PBR para IPv6 seleccionará los paquetes utilizando distintos criterios de coincidencia de paquetes como:

- interfaz de entrada.
- IPv6 dirección de origen.
- Dirección de destino IPv6.
- Protocolo.
- Puerto de origen y puerto de destino.
- DSCP.
- Flujo de etiqueta.
- Fragmento.

6.4.1. HABILITAR PBR EN UNA INTERFAZ

257. Para habilitar PBR para IPv6, se debe crear un mapa de ruta que especifique los criterios de coincidencia de paquetes y la acción de la ruta deseada. A continuación, se asocia el mapa de ruta en la interfaz necesaria. Todos los paquetes que llegan a la interfaz especificada que responden a las cláusulas de coincidencia estarán a esas políticas. Se hace con los siguientes comandos:

enable

Habilita privilegios para la ejecución de comandos.

configure terminal

Entra a la configuración global.

route-map *map-tag* [permit | deny] [*sequence-number*]

Define las condiciones para la redistribución de rutas de un protocolo de enrutamiento a otro, o habilitar la política de enrutamiento. Utilice el comando route-map para entrar en modo de configuración del mapa de ruta.

Hacer una de las siguientes ahora. Se pueden especificar algunas o todas de estas. Si no se aplica ningún comando match, el map-route se aplica a todos los paquetes.

match length *minimum-length maximum-length*

match ipv6 address {*prefix-list prefix-list-name* | *access-list-name*}

Hacer una de las siguientes ahora:

Se especifican la acción o las acciones que hay que realizar para los paquetes que coincidan con el criterio del match.

set ipv6 precedence *precedende-value*

Fija el valor de precedencia en la cabecera de ipv6.

set ipv6 next-hop *global-ipv6-address* [*global-ipv6-address*]

Fija el siguiente salto para encaminar el paquete (debe ser adyacente).

set interface *type number* [*type number*]

Fija la interfaz de salida del paquete.
 set ipv6 default next-hop *global-ipv6-address* [*global-ipv6-address*]
 Establece el siguiente salto al que se debe enviar el paquete si no hay una ruta explícita para este destino.
 set default interface *type number* [*type number*]
 Establece una interfaz de salida para el paquete si no hay una ruta explícita para este destino.

exit
 Se vuelve a la configuración global del router

interface *type number*
 Especifica una interfaz y el router entra en la configuración de dicha interfaz.

ipv6 policy route-map *route-map-name*
 Identifica un mapa de ruta a utilizar para IPv6 PBR en una interfaz.

6.4.2. HABILITAR PBR LOCAL EN IPV6

258. Los paquetes que se generan por el router normalmente no son enrutados por ninguna política de enrutado. Realice esta tarea para habilitar PBR en IPv6 para tales paquetes, que indica qué route-map debe utilizar.

enable
 Habilita privilegios para la ejecución de comandos.

configure terminal
 Se entra a la configuración global del router.

ipv6 local policy route-map *route-map-name*
 Configura PBR en ipv6 para paquetes generados por el router.

6.4.3. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE PBR EN IPV6

enable
 Habilita privilegios para la ejecución de comandos.

show ipv6 policy
 Muestra la política activa de routing de paquetes de IPv6.

6.5. IMPLEMENTACIÓN DE FILTROS DE TRÁFICO Y CORTAFUEGOS PARA SEGURIDAD EN IPV6

259. La funcionalidad ACL estándar en IPv6 es similar a las ACL estándar en IPv4. Las listas de acceso determinan qué tráfico está bloqueado y qué tráfico se reenvía a las interfaces del router, además de permitir el filtrado basado en direcciones de origen y de destino, tanto entrante como saliente, a una interfaz específica. Cada lista de acceso tiene una declaración implícita de negación al final.
260. Por otro lado, Cisco IOS tiene un cortafuegos que proporciona una funcionalidad avanzada de filtrado de tráfico como parte integral del servidor de seguridad de red. Las características que posee son las siguientes:
- Inspección de paquetes fragmentados: el cortafuegos examina fragmentos fuera de secuencia y conmuta los paquetes en el orden correcto, examina el número de

fragmentos de una sola dirección IP dado un identificador único y realiza un reensamblado virtual para mover los paquetes a los protocolos de capas superiores.

- Mitigación de ataques de denegación de servicio en IPv6: los mecanismos de mitigación se han implementado de la misma manera que para la implementación de IPv4, incluyendo conexiones a medias (SYN half-open).
- Inspección de paquetes de túnel.
- Inspección de paquetes: proporciona la inspección de estado de paquetes de TCP, UDP, control de mensajes de Internet Protocol versión 6 (ICMPv6), y sesiones de FTP.
- Interpretación y reconocimiento de la mayoría de la información de cabeceras de extensión IPv6: proporciona información de encabezado de extensión IPv6 incluyendo enrutamiento de cabecera y opciones como hop-by-hop.
- Mapeo de puertos a la aplicación (PAM): permite personalizar los puertos TCP o UDP para los servicios de red o aplicaciones. PAM utiliza esta información para apoyar los entornos de red que ejecutan los servicios en puertos que son diferentes de los puertos registrados o conocidos asociados con una determinada aplicación. Utilizando la información del puerto, PAM establece una tabla de información de asignación predeterminada de puerto a la aplicación.

6.5.1. CONFIGURAR FILTROS DE TRÁFICO IPV6

6.5.1.1. CREAR Y CONFIGURAR UNA ACL PARA EL FILTRADO DE TRÁFICO

261. Cada ACL IPv6 contiene normas sobre permisos implícitos para permitir el descubrimiento de vecinos (Neighbour Discovery) en IPv6. Estas reglas pueden ser anuladas por el usuario mediante la colocación de una regla “any any” ipv6 en la ACL. El proceso de descubrimiento de vecinos de IPv6 hace uso del servicio de capa de red IPv6. Por lo tanto, de forma predeterminada, IPv6 ACL permiten implícitamente paquetes de descubrimiento de vecinos de IPv6 para ser enviados y recibidos en una interfaz. Para hacer una ACL seguir los siguientes comandos:

enable

Habilita privilegios para la ejecución de comandos.

configure terminal

Se entra a la configuración global del router.

ipv6 access-list *access-list-name*

Define una ACL IPv6 y se introduce en la configuración de acceso de la lista.

Se introducen las siguientes líneas en el orden y las veces necesarias:

Especifica las condiciones de permitir y denegar de la ACL IPv6.

```
permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address
| auth}[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address | auth}[operator [port-number]][dest-option-type [doh-
number | doh-type]][dscp value][flow-label value][fragments][log][log-
input][mobility][mobility-type [mh-number | mh-type]] [reflect name [timeout
value]][routing][routing-type routing-number [sequence value]][time-range name]
```

```
deny protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address |
auth}[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address | auth}[operator [port-number]][dest-option-type [doh-
number | doh-type]][dscp value][flow-label value][fragments][log][log-
input][mobility][mobility-type [mh-number | mh-type]] [reflect name [timeout
value]][routing][routing-type routing-number [sequence value]][time-range name]
```

6.5.1.2. APLICAR UNA ACL IPV6 A UNA INTERFAZ ESPECÍFICA

262. Para aplicar una ACL a una interfaz concreta se deben ejecutar los siguientes comandos:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Se entra a la configuración global del router.
interface type number
    Entra a la configuración de esa interfaz.
ipv6 traffic-filter access-list-name {in | out}
    Aplica la ACL específica del comando a la interfaz anteriormente
    seleccionada.
```

6.5.2. CONFIGURAR EL CORTAFUEGOS PARA IPV6

263. Se va a explicar la configuración necesaria para implementar inspección de paquetes como ACLs. Se hace con los siguientes comandos:

```
enable
    Habilita privilegios para la ejecución de comandos.
configure terminal
    Se entra a la configuración global del router.
ipv6 unicast-routing
    Habilita IPv6 routing unicast.
ipv6 inspect name inspection-name protocol [alert {on | off}][audit-trail{on |
off}][timeout seconds]
    Define reglas de inspección IPv6 en el cortafuegos.
interface type number
    Especifica la interfaz en la que se llevará a cabo la inspección.
ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits/prefix-length}
    Proporciona la dirección de la interfaz de inspección.
ipv6 enable
    Habilita el routing IPv6.
ipv6 traffic-filter access-list-name {in | out}
    Se aplica la lista de acceso IPv6 especificada a la interfaz especificada en
    el paso anterior.
ipv6 inspect inspection-name {in | out}
    Se aplica el conjunto de reglas de inspección.
ipv6 access-list access-list-name
    Define una ACL IPv6 y entra en el modo de configuración de la lista de
    acceso IPv6.
```

264. Para permitir o denegar el tráfico hay que ir introduciendo las siguientes líneas en el orden y número necesario en cada caso:

```
permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address
| auth}[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address | auth}[operator [port-number]][dest-option-type [doh-
number | doh-type]][dscp value][flow-label value][fragments][log][log-
input][mobility][mobility-type [mh-number | mh-type]] [reflect name [timeout
value]][routing][routing-type routing-number [sequence value]][time-range name]
```

```
deny protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address |
auth}[operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address | auth}[operator [port-number]][dest-option-type [doh-
number | doh-type]][dscp value][flow-label value][fragments][log][log-
input][mobility][mobility-type [mh-number | mh-type]] [reflect name [timeout
value]][routing][routing-type routing-number [sequence value]][time-range name]
```

6.5.3. VERIFICAR LA CONFIGURACIÓN DE SEGURIDAD DE IPV6

```
show crypto ipsec sa [map map-name | address | identity | interface interface-type
interface-number | peer [vrf vrf-name] address | vrf ivrf-name | ipv6 [interface-
type interface-number]][detail]
```

Muestra la configuración de las actuales SAs (Asociación de seguridad).

```
show crypto isakmp peer [config | detail]
```

Muestra las descripciones de peer.

```
show crypto isakmp profile
```

Lista todos los perfiles ISAKMP definidos en un router.

```
show crypto isakmp sa [active | standby | detail | nat]
```

Muestra las actuales IKE SAs.

```
show ipv6 access-list [access-list-name]
```

Muestra el contenido de las actuales ACLs de IPv6 fijadas.

```
show ipv6 port-map [application | port port-number]
```

Muestra la configuración de PAM.

```
show ipv6 prefix-list [detail | summary][list-name]
```

Muestra información sobre los prefijos IPv6.

```
show logging [slot slot-number | summary]
```

Muestra el estado de los logging.

6.6. IMPLEMENTACIÓN DE RUTAS ESTÁTICAS PARA IPV6

265. Los dispositivos de red reenvían paquetes utilizando información de las rutas que se configuran, ya sea manualmente o mediante el uso de un protocolo de enrutamiento dinámico. Las rutas estáticas se configuran manualmente y permiten definir una ruta explícita entre dos dispositivos de red. A diferencia de un protocolo de enrutamiento dinámico, las rutas estáticas no se actualizan automáticamente y se deben reconfigurar manualmente si cambia la topología de red. Los beneficios del uso de rutas estáticas incluyen la eficiencia y la seguridad de los recursos, ya que utilizan menos ancho de banda que los protocolos de enrutamiento. La principal desventaja de utilizar rutas estáticas es la falta de reconfiguración automática si cambia la topología.

266. Las rutas estáticas se pueden redistribuir en los protocolos de enrutamiento dinámico pero las rutas generadas por protocolos de enrutamiento dinámico no pueden ser redistribuidos en la tabla de enrutamiento estático. No existe ningún algoritmo para evitar los bucles de enrutamiento que puedan surgir al configurar rutas estáticas.
267. Las rutas estáticas son útiles para redes más pequeñas con sólo una ruta de acceso a una red externa y para garantizar la seguridad de una red más amplia para ciertos tipos de tráfico o enlaces a otras redes en los que se necesita más control. En general, la mayoría de las redes utilizan protocolos de enrutamiento dinámico para la comunicación entre los dispositivos de red, pero pueden tener una o dos rutas estáticas configuradas para casos especiales. Hay distintas rutas estáticas según los parámetros que fijen:
- Directly attached Static Routes: solo la interfaz de salida es especificada.
 - Recursive Static Routes: solo se especifica el siguiente salto.
 - Fully Specified Static Routes: se especifican tanto la interfaz de salida como el siguiente salto.
 - Floating Static Routes: son rutas estáticas que se utilizan para copia de seguridad de las rutas dinámicas aprendidas a través de los protocolos de enrutamiento configurados. Como resultado, las rutas aprendidas a través del protocolo de encaminamiento se utilizan siempre con preferencia. Si se pierde la ruta dinámica aprendida a través del protocolo de enrutamiento, la ruta estática será la que se use.

6.6.1. CONFIGURAR UNA RUTA ESTÁTICA IPV6

268. Para llevarlo a cabo, efectuar los siguientes comandos:

```
enable
```

Habilita privilegios para la ejecución de comandos.

```
configure terminal
```

Entra a la configuración global.

```
ipv6 route ipv6-prefix / prefix-length ipv6-address / interface-type interface-number ipv6-address] [administrative-distance] [administrative-multicast-distance | unicast | multicast] [tag tag]
```

6.6.2. CONFIGURACIÓN DE UNA RUTA ESTÁTICA RECURSIVA PARA EL USO POR DEFECTO

269. Llevarlo a cabo de la siguiente manera:

```
enable
```

Habilita privilegios para la ejecución de comandos.

```
configure terminal
```

Entra a la configuración global.

```
ipv6 route static resolve default
```

Permite una ruta estática recursiva IPv6 para usarla como ruta estática por defecto.

6.6.3. CONFIGURAR UNA RUTA ESTÁTICA FLOTANTE

270. Hacer la siguiente configuración:

enable

Habilita privilegios para la ejecución de comandos.

configure terminal

Entra a la configuración global.

ipv6 route *ipv6-prefix / prefix-length {ipv6-address / interface-type interface-number ipv6-address}* [*administrative-distance*] [*administrative-multicast-distance* | unicast | multicast] [tag *tag*]

6.6.4. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE LAS RUTAS ESTÁTICAS

271. Hacer los siguientes comandos:

enable

Habilita privilegios para la ejecución de comandos.

Hacer una de las siguientes ahora:

Muestran el contenido actual de la tabla derouting IPv6.

show ipv6 static [*ipv6-address / ipv6-prefix / prefix-length*][*interface interface-type interface-number*] [*recursive*] [*detail*]

show ipv6 route [*ipv6-address* | *ipv6-prefix* | *prefix-length* | *protocol* | *interface-type interface-number*]

debug ipv6 routing

Muestra los mensajes de depuración para las actualizaciones de la tabla de routing IPv6.

6.7. IMPLEMENTACIÓN DE TÚNELES EN IPV6

272. Un túnel encapsula los paquetes IPv6 en paquetes IPv4 para la entrega a través de una infraestructura de red IPv4. Mediante el uso de túneles se pueden comunicar las redes IPv6 sin necesidad de actualizar la infraestructura IPv4 entre ellos. Estos túneles se pueden configurar entre los enrutadores de borde o entre un router de borde y un equipo. Sin embargo, ambos extremos del túnel deben soportar tanto IPv4 como IPv6. Este protocolo es compatible con los siguientes tipos de mecanismos de tunelización:

- Manual.
- GRE: Generic Routing Encapsulation.
- 6to4.
- ISATAP: Intrasite Automatic Tunnel Addressing Protocol.

6.7.1. CONFIGURAR TÚNELES MANUALES EN IPV6

273. Un túnel configurado manualmente equivale a un enlace permanente entre dos dominios de IPv6 en una red troncal IPv4. El uso principal es para conexiones estables que requieren comunicaciones seguras entre dos enrutadores de borde o entre un sistema final y un router de borde, o para la conexión a las redes IPv6 remotas.

274. Una dirección IPv6 se configura manualmente en un interfaz de túnel y las direcciones IPv4 configurados manualmente se asignan a la fuente de túnel y el destino del túnel. El host o router en cada extremo de un túnel configurado deben apoyar tanto a las pilas de protocolos IPv4 e IPv6.
275. Con túneles IPv6 configurados manualmente, una dirección IPv6 se configura en una interfaz de túnel, y las direcciones IPv4 configuradas manualmente se asignan a la fuente y el destino del túnel, respectivamente. El host o router de cada extremo del túnel configurado deben soportar tanto IPv4 como IPv6. Se puede hacer con los siguientes comandos:
- enable
Habilita privilegios para la ejecución de comandos.
 - configure terminal
Entra a la configuración global.
 - interface-tunnel *tunnel-number*
Especifica una interfaz para el túnel y se entra en la configuración de dicha interfaz.
 - ipv6 address *ipv6-prefix / prefix-length* [eui-64]
Especifica el prefijo IPv6 asignado a la interfaz y habilita el procesamiento de IPv6 en la interfaz.
 - tunnel source {*ip-address / interface-type interface-number*}
Especifica la dirección IPv4 o la interfaz de origen del túnel.
 - tunnel destination *ip-address*
Especifica la dirección IPv4 de destino o el nombre del host destino para la interfaz del túnel.
 - tunnel mode ipv6ip
Especifica un túnel IPv6 manual.

6.7.2. CONFIGURAR TÚNELES IPV6 GRE

276. Al igual que en túneles IPv6 configurados manualmente, los túneles GRE son vínculos entre dos puntos, con un túnel separado para cada enlace. Los túneles no están vinculados a un protocolo específico de pasajeros o de transporte, pero en este caso, llevan IPv6 como protocolo de pasajeros e IPv4 o IPv6 como protocolo de transporte.
277. Los túneles GRE pueden ser configurados para funcionar a través de una capa de red IPv6 y para el transporte de los paquetes IPv6 en túneles de IPv6 y paquetes IPv4 en túneles IPv6.
278. Cuando se configuran túneles IPv6 GRE, las direcciones IPv6 se asignan al origen de y el destino del túnel. La interfaz de túnel puede tener ya sea direcciones asignadas IPv4 o IPv6. El host o router en cada extremo de un túnel configurado deben soportar tanto IPv4 e IPv6. Para llevarlo a cabo, realizar los siguientes comandos:
- enable
Habilita privilegios para la ejecución de comandos.
 - configure terminal
Entra a la configuración global.
 - interface tunnel *tunnel-number*
Especifica una interfaz para el túnel y se entra en la configuración de dicha interfaz.

- `ipv6 address ipv6-prefix / prefix-length [eui-64]`
Especifica el prefijo IPv6 asignado a la interfaz y habilita el procesado de IPv6 en la interfaz.
- `tunnel source {ip-address / ipv6-address / interface-type interface-number}`
Especifica la dirección IPv4/IPv6 o la interfaz de origen del túnel.
- `tunnel destination {host-name / ip-address / ipv6-address}`
Especifica la dirección IPv4 de destino o el nombre del host destino para la interfaz del túnel.
- `tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre ipv6 | ipip [decapsulate-any] | iptalk | ipv6 | mpls | nos}`
Especifica un túnel GRE IPv6. El comando `tunnel mode gre ipv6` especifica el modo de túnel GRE como el protocolo de encapsulación para el túnel.

6.7.3. CONFIGURAR TÚNELES AUTOMÁTICOS 6TO4

279. Un túnel 6to4 permite que dominios aislados IPv6 se conecten a través de una red IPv4. La diferencia clave entre los túneles de 6to4 y túneles configurados manualmente es que el túnel no es punto a punto, es punto a multipunto. En los túneles de 6to4, los routers no están configurados en pares porque tratan la infraestructura IPv4 como un enlace virtual de acceso múltiple. La dirección IPv4 integrada en la dirección IPv6 se utiliza para encontrar el otro extremo del túnel automático.
280. El escenario de implementación más simple para túneles 6to4 es interconectar varios sitios IPv6, cada uno de los cuales tiene al menos una conexión a una red IPv4 compartida. El requisito clave es que cada sitio tiene una dirección IPv4 global única y se utiliza esta dirección para construir un único prefijo 6to4/48 de IPv6.
281. Con túneles 6to4, el destino del túnel está determinado por la dirección IPv4 del router de borde, que se concatena con el prefijo 2002::/16 en el formato 2002:-border-router-IPv4-address::/48. El router de borde en cada extremo de un túnel 6to4 debe soportar tanto IPv4 como IPv6. Si se elige configurar este túnel con otro túnel IPv6, se recomienda encarecidamente que no compartan el mismo origen por problemas de incompatibilidad. Para hacer un túnel de este tipo:

- `enable`
Habilita privilegios para la ejecución de comandos.
- `configure terminal`
Entra a la configuración global.
- `interface tunnel tunnel-number`
Especifica una interfaz para el túnel y se entra en la configuración de dicha interfaz.
- `ipv6 address ipv6-prefix / prefix-length [eui-64]`
Especifica el prefijo IPv6 asignado a la interfaz y habilita el procesado de IPv6 en la interfaz.
- `tunnel source {ip-address / interface-type interface-number}`
Especifica la dirección IPv4 o la interfaz de origen del túnel. Esta interfaz debe ser configurada con una dirección IPv4.
- `tunnel mode ipv6ip 6to4`
Especifica un túnel utilizando 6to4.
- `exit`

Salen del modo de configuración de la interfaz y vuelven a la configuración global del router.

`ipv6 route ipv6-prefix / prefix-length tunnel tunnel-number`

Configura una ruta estática para el prefijo IPv6 6to4 2002::/16 a la interfaz de túnel especificada. Al configurar un túnel 6to4 se debe configurar una ruta estática para el prefijo IPv6 6to4 2002::/16 a la interfaz del túnel 6to4. El `tunnel-number` especificado en el comando debe ser el mismo `tunnel number` especificado en el comando donde se usó anteriormente.

6.7.4. CONFIGURAR TÚNELES COMPATIBLES IPV4 CON IPV6

282. Con un túnel compatible IPv4, el destino del túnel se determina automáticamente por la dirección IPv4 en los 32 bits de la dirección IPv6 compatibles con IPv4. El host o router en cada extremo de un túnel compatible con IPv4 deben soportar tanto IPv4 como IPv6.

`enable`

Habilita privilegios para la ejecución de comandos.

`configure terminal`

Entra a la configuración global.

`interface tunnel tunnel-number`

Especifica una interfaz para el túnel y se entra en la configuración de dicha interfaz.

`tunnel source {ip-address / interface-type interface-number}`

Especifica la dirección IPv4 o la interfaz de origen del túnel. Esta interfaz debe ser configurada con una dirección IPv4.

`tunnel mode ipv6ip auto-tunnel`

Especifica un túnel compatible con IPv4 utilizando una dirección IPv6 compatible con IPv4.

6.7.5. CONFIGURAR TÚNELES ISATAP

283. ISATAP está diseñado para el transporte de paquetes IPv6 dentro de un sitio donde la infraestructura IPv6 todavía no está disponible. El origen del túnel utilizado en la configuración de un túnel ISATAP debe apuntar a una interfaz con una dirección IPv4 configurada. La dirección ISATAP IPv6 y el prefijo (o prefijos) publicado se configuran como una interfaz de IPv6 nativa. La interfaz de túnel IPv6 se debe configurar con una dirección EUI-64 modificada debido a que los últimos 32 bits del identificador de interfaz se construyen utilizando la dirección de origen del túnel IPv4. Para llevarlo a cabo se hace lo siguiente:

`enable`

Habilita privilegios para la ejecución de comandos.

`configure terminal`

Entra a la configuración global.

`interface tunnel tunnel-number`

Especifica una interfaz para el túnel y se entra en la configuración de dicha interfaz.

`ipv6 address ipv6-prefix / prefix-length [eui-64]`

Especifica la dirección IPv6 asignada a la interfaz y permite el procesamiento de IPv6 en la interfaz.

`no ipv6 nd ra suppress`

El envío de router advertisement IPv6 está desactivado por defecto en las interfaces de túnel. Este comando permite el envío de router advertisement IPv6 para permitir la configuración automática del cliente.

tunnel source {ip-address | interface-type interface-number}

Especifica la dirección IPv4 o la interfaz de origen del túnel. Esta interfaz debe ser configurada con una dirección IPv4.

tunnel mode ipv6ip isatap

Especifica un túnel IPv6 mediante ISATAP.

6.7.6. VERIFICAR LA CONFIGURACIÓN Y OPERACIÓN DE TÚNELES IPV6

284. Realizarlo para obtener información acerca de las configuraciones de los túneles y de su operación.

enable

Habilita privilegios para la ejecución de comandos.

show interfaces tunnel *number* [accounting]

Muestra la información de la interfaz acerca de los túneles configurados.

ping [*protocol*] *destination*

Permite hacer un diagnóstico de conectividad básica.

show ip route [*address*[*mask*]]

Muestra el estado actual de la tabla de routing.

6.8. IMPLEMENTACIÓN DE RA GUARD Y SEND

285. La implementación de estos 2 protocolos son necesarios para evitar algunas de las vulnerabilidades descritas anteriormente y, por tanto, su utilización es muy recomendada, aunque no todos los equipos tienen soporte para ello.

6.8.1. CONFIGURACIÓN DE RA GUARD

286. La función de IPv6 RA Guard proporciona soporte para permitir bloquear o rechazar algunos mensajes RA que llegan al dispositivo de red. Los mensajes RA son utilizados por los dispositivos para anunciarse en el enlace. La función IPv6 RA Guard los analiza y filtra los RA que son enviados por los dispositivos no autorizados. Para configurarlo, realizar los siguientes comandos:

enable

Habilita privilegios para la ejecución de comandos.

configure terminal

Entra a la configuración del equipo.

interface *type number*

Entra en la configuración de la interfaz especificada.

ipv6 nd raguard attach-policy [*policy-name* [vlan {add | except | none | remove | all} *vlan* [*vlan1*, *vlan2*, *vlan3*...]]]

Se aplica la función RA guard a una interfaz específica.

Nota: en algunos sistemas es posible que la instrucción necesaria en este momento sea ipv6 nd raguard.

exit

Sale de la configuración de la interfaz.

6.8.2. CONFIGURACIÓN DE ND INSPECTION

287. ND Inspection aprende y asegura vinculaciones para las direcciones de configuración automática sin estado (SLAAC) en la capa 2. Analiza los mensajes con el fin de construir una tabla de confianza. Los mensajes ND que no tienen fijaciones válidas se dejan caer. Para llevarlo a cabo:

- enable
Habilita privilegios para la ejecución de comandos.
- configure terminal
Entra a la configuración del equipo.
- ipv6 nd inspection policy *policy-name*
Define la política usada y se entra en su configuración.
- drop-unsecure
Se tiran los mensajes inseguros, sin opciones o con opciones inválidas.
- sec-level minimum *value*
Especifica el valor mínimo del parámetro nivel de seguridad cuando se utilizan las opciones de CGA.
- device-role {host | monitor | router}
Define el rol del equipo
- tracking {enable [reachable-lifetime {*value* | infinite}]| disable [stale-lifetime {*value* | infinite}]}
Anula la política por defecto en un puerto.
- trusted-port
Se configura como un puerto de confianza.

288. Y para aplicarlo sobre una interfaz:

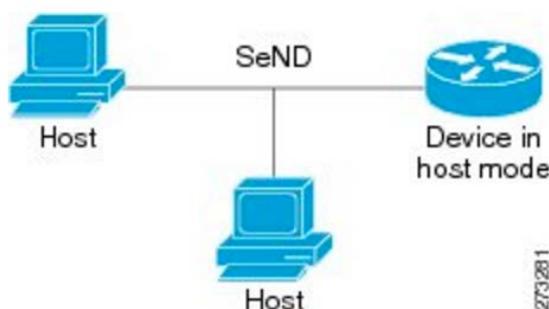
- enable
Habilita privilegios para la ejecución de comandos.
- configure terminal
Entra a la configuración del equipo.
- interface *type number*
Se entra en la configuración de la interfaz.
- ipv6 nd inspection [attach-policy [policy *policy-name*]]|vlan {add | except | none | remove | all} *vlan[vlan1, vlan2, vlan3...]*
Aplica ND Inspection a la interfaz.

6.8.3. CONFIGURACIÓN DE SECURE ND (SEND)

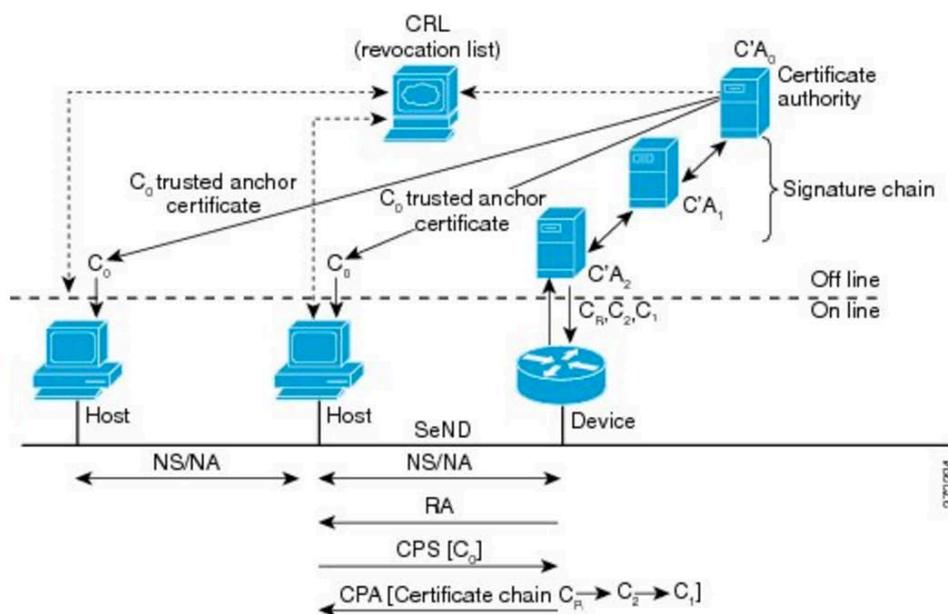
289. El protocolo SEND contrarresta las posibles amenazas que contiene Neighbour Discovery. Se define un conjunto de nuevas opciones, y dos nuevos tipos de mensajes (Certification Path Solicitation [CPS] y Certification Path Answer [CPA]). También define un nuevo mecanismo de configuración automática para ser utilizado conjuntamente con las nuevas opciones de ND.

290. Por un lado, cabe destacar las Cryptographically Generated Addresses (CGA), que son direcciones IPv6 generadas a partir del hash criptográfico de una clave pública y de una serie de parámetros auxiliares. Esto proporciona un método para asociar de forma segura una clave criptográfica pública con una dirección IPv6 en el protocolo SEND.

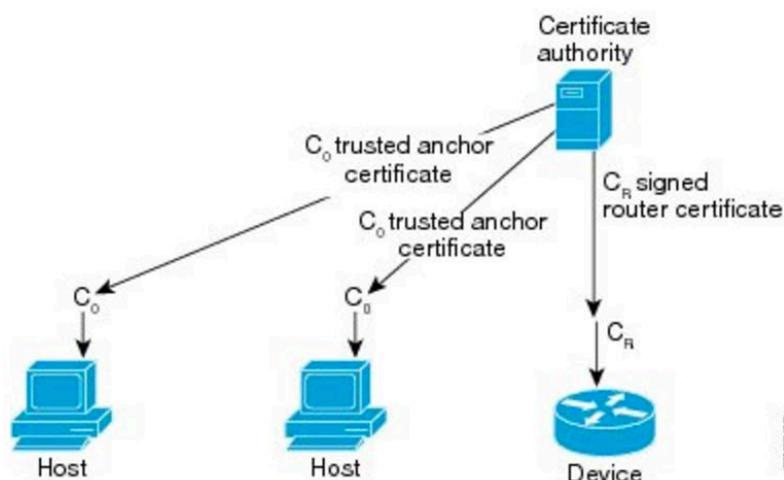
291. El nodo que genera una dirección de CGA debe obtener primero un par de claves RSA (SEND utiliza un par de claves pública y privada RSA). El nodo calcula entonces el identificador de interfaz y añade el resultado al prefijo para formar la dirección CGA.
292. La generación CGA es un evento que se da una sola vez. Una CGA válida no puede ser falsificada y los parámetros CGA asociados a ella se vuelven a usar porque el mensaje se firma con la clave privada que coincide con la clave pública utilizada para la generación CGA, que solo tendrá el propietario de la dirección.
293. Hay varias formas de implementar SEND. Una de ellas es poner el router en modo host, de forma que los hosts pueden generar un par de claves RSA localmente, configurar automáticamente sus direcciones CGA, y utilizarlas para validar su autoridad remitente, en lugar de utilizar un tercero de confianza para establecer la autoridad remitente. La figura a continuación ilustra este modelo.



294. Por otro lado, se puede realizar también un despliegue en modo host-router. En algunos casos, los hosts no tendrán acceso a la infraestructura que les permita obtener y anunciar sus certificados. En estas situaciones, los anfitriones asegurarán su relación usando CGA, y aseguran su relación con los routers usando un tercero (trust anchor). La figura a continuación ilustra este escenario.



295. Por último, hay otro tipo de modelo donde los hosts y routers confían en una sola CA, como el servidor de certificación de Cisco (CS). La figura a continuación ilustra este modelo.



6.8.4. CONFIGURACIÓN DEL SERVIDOR DE CERTIFICACIONES

296. Hosts y enrutadores deben configurarse con pares de claves RSA y sus certificados correspondientes antes de que se configuren los parámetros de envío. Se han de realizar las siguientes tareas para configurar el servidor de certificados.

enable

Habilita privilegios para la ejecución de comandos.

configure terminal

Entra a la configuración del equipo.

ip http server

Configura el servidor http.

crypto pki trustpoint *name*

(Opcional) Declara el trustpoint que el servidor de certificados debe utilizar y entra en el modo de configuración ca-trustpoint.

ip-extension[multicast | unicast]{inherit [ipv4 | ipv6]| prefix *ipaddress* | range *min-ipaddress max-ipaddress*}

(Opcional) Especifica que las extensiones IP están incluidas en una solicitud de certificado, ya sea para la inscripción o la generación de una autoridad de certificación (CA).

revocation-check {[crl] [none] [ocsp]}

(Opcional) Define uno o más métodos para la comprobación de revocación.

exit

Salte del modo de configuración.

crypto pki server *name*

Configura el servidor PKI (Public Key Infrastructure) y pone el router en modo servidor.

grant auto

(Opcional) Concede acceso a todas las solicitudes de certificados de forma automática.

`cdp-url url-name`
 (Opcional) Establece el nombre de la URL si el host utiliza una lista de revocación de certificados (CRL).

`no shutdown`
 Habilita el servidor de certificados.

6.8.5. CONFIGURACIÓN DEL MODO HOST

`enable`
 Habilita privilegios para la ejecución de comandos.

`configure terminal`
 Entra a la configuración del equipo.

`crypto key generate rsa [general-keys | usage-keys | signature | encryption][label key-label][exportable][modulus modulus-size][storage devicename :][on devicename :]`
 Configura la clave RSA.

`ipv6 cga modifier rsakeypair key-label sec-level {0 | 1}`
 Habilita el uso de la clave para SeND.

`crypto pki trustpoint name`
 Especifica el nodo trustpoint y entra en el modo de configuración ca-trustpoint.

`enrollment [mode] [retry period minutes] [retry count number] url url [pem]`
 Especifica los parámetros de inscripción de una CA.

`revocation-check {[crl] [none] [ocsp]}`
 Establece uno o más métodos de revocación.

`exit`
 Sale del menú de configuración.

`crypto pki authenticate name`
 Autentica la autoridad de certificación.

`ipv6 nd secured sec-level minimum value`
 (Opcional) Configura CGA, dando parámetros como el nivel de seguridad.

`interface type number`
 Se entra en la configuración de esa interfaz.

`ipv6 cga rsakeypair key-label`
 (Opcional) Configura CGA en las interfaces.

`ipv6 address ipv6-address / prefix-length link-local cga`
 Configura una dirección de enlace local IPv6 para la interfaz y permite el procesamiento de IPv6 en la interfaz.

`ipv6 nd secured trustanchor trustanchor-name`
 (Opcional)

`ipv6 nd secured timestamp {delta value | fuzz value}`
 (Opcional) Configura los parámetros de tiempo.

`exit`
 Vuelve a la configuración global.

`ipv6 nd secured full-secure`
 (Opcional) Configura los parámetros generales de SeND.

6.8.6. CONFIGURACIÓN DEL MODO ROUTER

`enable`

Habilita privilegios para la ejecución de comandos.
 configure terminal
 Entra a la configuración del equipo.
 crypto key generate rsa [general-keys | usage-keys | signature | encryption][label *key-label*] [exportable] [modulus *modulus-size*] [storage *devicename:*] [on *devicename:*]
 Configura la clave RSA.
 ipv6 cga modifier rsakeypair *key-label* sec-level {0 | 1}
 Habilita la clave RSA para que sea usada por SeND.
 crypto pki trustpoint *name*
 Configura PKI para una CA de nivel único o múltiple, especifica el trustpoint router, y coloca el router en el modo de configuración de CA-trustpoint.
 subject-name [attr *tag*][eq | ne | co | nc] *string*
 Crea una regla de entrada.
 rsakeypair *key-label*
 Une el par de claves RSA.
 revocation-check {[crl][none][ocsp]}
 Establece uno o más métodos de revocación.
 exit
 Vuelve a la configuración global.
 crypto pki authenticate *name*
 Autentica la autoridad certificadora.
 crypto pki enroll *name*
 Obtiene el certificado para el router desde la CA.
 ipv6 nd secured sec-level minimum *value*
 (Opcional) Configura CGA, dando parámetros como el nivel de seguridad.
 interface *type number*
 Especifica una interfaz y se entra en su configuración.
 ipv6 cga rsakeypair *key-label*
 (Opcional) Configura CGA en la interfaz.
 ipv6 address *ipv6-address / prefix-length* link-local cga
 Configura una dirección IPv6 link-local address para la interfaz y habilita IPv6 en la interfaz.
 ipv6 nd secured trustanchor *trustpoint-name*
 (Opcional)
 ipv6 nd secured timestamp {delta *value* | fuzz *value*}
 (Opcional) Configura los parámetros de tiempo.
 exit
 Vuelve a la configuración global.
 ipv6 nd secured full-secure
 (Opcional) Configura los parámetros generales de SeND.

6.8.7. CREACIÓN DE LA CLAVE RSA Y CGA PARA LA CLAVE

enable
 Habilita privilegios para la ejecución de comandos.
 configure terminal
 Entra a la configuración del equipo.

```
crypto key generate rsa [general-keys | usage-keys | signature | encryption][label
key-label][exportable][modulus modulus-size][storage devicename:][on
devicename :]
```

Genera la clave RSA.

```
ipv6 cga modifier rsa keypair key-label sec-level {0 | 1}
```

Genera CGA para la clave RSA especificada, que la habilita para ser utilizada para SeND.

6.8.8. CONFIGURAR EL TRUSTPOINT DE SEND

297. En el modo router, el par de claves utilizado para generar las direcciones CGA en una interfaz debe estar certificado por la CA y el certificado enviado a través del protocolo SeND. Un par de claves RSA y el certificado asociado es suficiente para poder operar SeND. Sin embargo, los usuarios pueden utilizar varias claves, identificadas por diferentes etiquetas. SeND y CGA son referidos a una clave directamente por etiqueta o indirectamente por trustpoint.
298. Se requieren múltiples pasos para unir SEND a un trustpoint. En primer lugar, se genera un par de claves. A continuación, el dispositivo se refiere a ella en un trustpoint, y entonces la interfaz SEND apunta al trustpoint. Hay dos razones por las múltiples pasos:
- El mismo par de claves se puede utilizar en varias interfaces SEND.
 - El trustpoint contiene información adicional, como el certificado, es requerido por SEND al realizar la delegación de autorización.
299. Varios trustpoint se pueden configurar, apuntando a las mismas claves RSA, en una interfaz determinada. Esta función es útil si los diferentes hosts tienen diferentes trusted anchors (es decir, las entidades emisoras que confían). Se hace con los siguientes comandos:

```
enable
```

Habilita privilegios para la ejecución de comandos.

```
configure terminal
```

Entra a la configuración del equipo.

```
crypto key generate rsa [general-keys | usage-keys | signature | encryption][label
key-label][exportable][modulus modulus-size][storage devicename:][on
devicename:]
```

Genera la clave RSA.

```
ipv6 cga modifier rsa keypair key-label sec-level {0 | 1}
```

Genera CGA para la clave RSA especificada, que la habilita para ser utilizada para SeND.

```
crypto pki trustpoint name
```

Declara el trustpoint que el router usará y se entra en su configuración.

```
subject-name [x.500-name]
```

Especifica el nombre.

```
rsa keypair key-label key-size encryption-key-size ]]
```

Especifica que clave se asocia con el certificado.

```
enrollment terminal [pem]
```

Especifica la inscripción de certificados.

```
ip-extension [multicast | unicast]{inherit [ipv4|ipv6]} prefix ipaddress | range min-
ipaddress max ip-address }
```

Añade IP-extensions.
 exit
 Vuelve a la configuración global.
 crypto pki authenticate *name*
 Autentica la autoridad de certificación.
 crypto pki enroll *name*
 Obtiene los certificados del router desde la CA.
 crypto pki import *name* certificate
 Importa un certificado manualmente.
 interface *type number*
 Especifica una interfaz y se entra en su configuración.
 ipv6 nd secured trustpoint *trustpoint-name*
 Habilita SeND en una interfaz y especifica el trustpoint a usar.

6.8.9. CONFIGURAR TRUST ANCHORS (TERCERO) DE SEND EN UNA INTERFAZ

300. Esto se puede realizar sólo en el modo host. El host debe estar configurado con uno o más trust anchors. Tan pronto como SeND está enlazado a un trustpoint en una interfaz, este trustpoint es también un trust anchor. Una configuración consta de los siguientes elementos:

- Un algoritmo de clave pública y la firma de clave pública asociada.
- Un nombre.
- Un identificador de clave pública opcional.
- Una lista opcional de los rangos de direcciones para los que está autorizado el ancla de confianza.

301. Debido a que PKI ya se ha configurado, la configuración del trust anchor se logra mediante la unión de SEND a uno o varios puntos de confianza de PKI. PKI se utiliza para cargar los certificados correspondientes, que contienen los parámetros necesarios (como el nombre y la clave).

enable
 Habilita privilegios para la ejecución de comandos.
 configure terminal
 Entra a la configuración del equipo.
 crypto pki trustpoint *name*
 Declara el trustpoint que el router debe utilizar y entra en el modo de configuración ca-trustpoint.
 enrollment terminal [pem]
 Especifica la inscripción de certificados.
 exit
 Vuelve a la configuración global.
 crypto pki authenticate *name*
 Autentica la autoridad de certificación.
 interface *type number*
 Especifica una interfaz y se entra en su configuración.
 ipv6 nd secured trustanchor *trustanchor-name*
 Especifica un trusted anchor en una interfaz y une SeND al trustpoint.

6.9. EJEMPLO DE CONFIGURACIÓN DE ENRUTADOR

302. En este punto se va a configurar IPv6 a modo de ejemplo en un router teniendo en cuenta las recomendaciones enumeradas anteriormente. Se recomienda que si un router no va a cursar tráfico IPv6 o no es estrictamente necesario, se deje desactivada la opción de IPv6.
303. En los puntos anteriores se pueden ver todas las instrucciones necesarias para realizar los pasos que se van a dar a continuación, además de otras opciones de configuración que podría utilizarse en escenarios muy concretos o para aplicar ciertas políticas de tráfico. Todo ello se encuentra en el capítulo 6 de esta guía.

6.9.1. CONECTIVIDAD BÁSICA

304. Para que un router pueda funcionar correctamente con IPv6, lo primero es habilitar el procesado de paquetes IPv6, tanto en la interfaz como en el router, de la siguiente forma:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#
```

305. Una vez que esté habilitado IPv6 en el router, hay que dar a cada interfaz una dirección IPv6 para que pueda encaminar tráfico correctamente. Se verá después que está asignación de direcciones se puede hacer de forma automática y manualmente como se va a hacer a continuación, pero si hiciese falta configurar alguna dirección estática o concreta, se podría hacer de esta manera en la interfaz del router.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ipv6 address 2001:1:1:1:1:1:1:1/64 eui-64
Router(config-if)#no shutdown
Router(config-if)#
*Mar  1 00:27:03.283: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:27:04.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

306. También se podría agregar una dirección de link-local con el comando “ipv6 address FE80::1 link-local”, con la que se podría hacer que los hosts de distintas subredes puedan comunicarse entre ellos sin salir al exterior.

```
Router(config)#interface FastEthernet 1/0
Router(config-if)#ipv6 address FE80::1 link-local
Router(config-if)#ipv6 address 2001:1:1:2::1/64 eui-64
Router(config-if)#no shutdown
Router(config-if)#
*Mar  1 00:35:15.491: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar  1 00:35:16.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

307. Para observar si IPv6 está activo en las interfaces, se puede usar el comando “show ipv6 interface” para ver la configuración de IPv6 en las distintas interfaces.

```

Router#
*Mar 1 00:38:58.339: %SYS-5-CONFIG I: Configured from console by consoleshov ipv6 interface
FastEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::CE02:6FF:FE89:0
Global unicast address(es):
  2001:1:1:1:CE02:6FF:FE89:0, subnet is 2001:1:1:1::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF89:0
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
FastEthernet1/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
Global unicast address(es):
  2001:1:1:2::1, subnet is 2001:1:1:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

```

308. Como se puede ver, también salen ciertos valores acerca de Neighbour Discovery e ICMP. Dependiendo de la cantidad de equipos que haya conectados, a la vez que la actividad de la subred, estos valores por defecto pueden no ser correctos y provocar el agotamiento de ciertas tablas al haber demasiadas entradas o demasiados mensajes ICMP. En el apartado de implementación de conectividad básica del capítulo 6 se encuentra cómo cambiar estos valores si se observa algún comportamiento anómalo, aunque en condiciones normales no deberían suponer un problema los valores por defecto. Por otro lado, se puede ver que los mensajes redirect están activos. Como se ha visto en el capítulo de vulnerabilidades, este tipo de mensajes pueden comprometer la seguridad, aunque también pueden disminuir la robustez de la red. Se puede restringir su uso con una regla dentro de un access-list del tipo “deny icmp any any redirect”.
309. Por otro lado, es posible que sea necesario configurar las interfaces para que puedan trabajar tanto con IPv4 como IPv6, por lo que habría que configurarles una dirección de cada tipo, o lo que es lo mismo, aplicar una configuración de doble pila. Los protocolos entre sí no son excluyentes, por lo que una interfaz puede trabajar a la vez con IPv4 y con IPv6. A continuación un ejemplo.

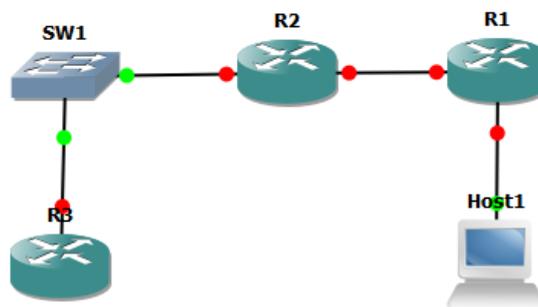
```

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.3.56 255.255.252.0
Router(config-if)#ipv6 address 2001:1:1:1:1:1:1:1/64 eui-64
Router(config-if)#

```

6.9.2. CONFIGURACIÓN DE DHCPV6

310. Aunque se ha visto anteriormente cómo configurar direcciones IPv6 manualmente para cada interfaz, este método no es dinámico y no funciona de forma automática, teniendo que efectuar todos los cambios manualmente si la topología de red cambia.
311. Por esta razón se suele usar algún protocolo de asignación automática de direcciones. Aunque en IPv6 se puede usar stateless como método para que cualquier equipo pueda acceder a la red global, este es más vulnerable que DHCPv6, por lo que se usará preferiblemente para la obtención de direcciones.
312. En este ejemplo se va a configurar tanto el cliente, que recibirá las direcciones o el prefijo a usar, como un relay que sea capaz de retransmitir las peticiones y un servidor que sea el encargado de proporcionar estas direcciones. El escenario básico por tanto es este.



313. R3 sería el encargado de actuar como servidor, R2 como relay y R1 como cliente. El host conectado a R1 obtendría su dirección mediante SLAAC. Se puede ver en la sección anterior como en la captura del comando “show ipv6 interface” los hosts reciben direcciones por SLAAC. Para llevar esto a cabo habrá que configurar las interfaces de los routers para que cada uno haga su función. Para el servidor se tiene:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface ethernet 1/0
Router(config-if)#ipv6 address 2001:DB8::1/64
Router(config-if)#ipv6 dhcp server DHCPv6-SERVER
Router(config-if)#exit
Router(config)#ipv6 dhcp pool DHCPv6-SERVER
Router(config-dhcp)#prefix-delegation pool MY-PD-1
Router(config-dhcp)#ipv6 local pool MY-PD-1 2001:DB8:ABCD::/48 56
```

314. Primero se le indica al equipo (si se ha hecho ya anteriormente no es necesario) que puede enrutar paquetes IPv6. Se configura la interfaz que une R3 con el Switch (en realidad este equipo no es obligatorio que esté) con una dirección IPv6 y se coloca en modo server. Después se fija en prefix-delegation y se le da un prefijo, en este caso un /48, seguido de 56, que indica la longitud de los prefijos que va a dar. Esto se elegirá en función de la red que se esté configurando.
315. Por otro lado, se tiene el cliente, que es el que se encargará de pedir un prefijo con Router Advertisements para proporcionar direcciones a los equipos que estén conectados a él. En este caso el procedimiento es:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet 0/0
Router(config-if)#ipv6 dhcp client pd rapid-commit
```

316. Para terminar, la función de relay se puede llevar a cabo de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface ethernet 2/0
Router(config-if)#ipv6 dhcp relay destination 2001:DB8::1
Router(config-if)#exit
```

317. Se ve que se configura la interfaz para que las peticiones las envíe a la interfaz donde está configurado el servidor DHCPv6. Los relays son necesarios si no se tiene conectividad directa con el servidor que hace la delegación de prefijos.
318. En el capítulo anterior se pueden ver más detalles acerca de la implementación de DHCPv6, a la vez que la configuración de Stateless por si se quisiera llevar a cabo, aunque lo recomendado es utilizar DHCPv6.

6.9.3. RUTAS ESTÁTICAS

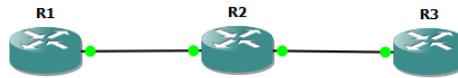
319. Las rutas estáticas con aquellas que son puestas a mano o que vienen puestas por defecto y que no tienen ninguna reacción ante nuevas rutas o caídas de tramos de la red. Son las habituales en sistemas cliente o en redes donde solo se sale a Internet. En el capítulo anterior se encuentra un apartado sobre el tema de rutas estáticas, explicando cada tipo de ruta que se puede hacer.
320. No se puede asegurar que no existan bucles de enrutamiento al configurar rutas estáticas, por lo que se aconseja usar solo las necesarias para el correcto funcionamiento de la red. A continuación se muestra un ejemplo de una ruta estática, aunque se pueden configurar otras rutas estáticas de diferentes tipos, recogidas en la sección de rutas estáticas del capítulo anterior.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 route 2001:1::/32 FastEthernet 0/0
Router(config)#exit
```

6.9.4. CONFIGURACIÓN DE TÚNELES

321. Los túneles para IPv6 se usan cuando una parte de la red sólo es capaz de manejar tráfico IPv4 y, por tanto, no puede enrutar paquetes de tipo IPv6. Es la típica tecnología de transición entre los 2 protocolos.
322. Para ello, el paquete IPv6 se encapsula sobre IPv4 para que así esta res pueda manejarlo. En general, la utilización de túneles tiene algunas vulnerabilidades asociadas y, además, es una forma de poder esconder tráfico y conexiones a cortafuegos y demás dispositivos de seguridad presentes en la red. Por todo ello, se desaconseja el uso de túneles si la red entera es capaz de hablar IPv6. Si algún router de la red solo maneja IPv4 (es preferible que toda la red sea IPv6 si es posible, así contendrá menos

vulnerabilidades) se ofrece un ejemplo de cómo configurar un túnel en el siguiente escenario.



323. En esta red, R1 y R3 son capaces de hablar IPv6, pero R2 solo maneja tráfico IPv4. Por tanto, haría falta un túnel entre los 2 routers para poder comunicarse mediante IPv6. Vamos a establecer una posible configuración de túnel de todas las que hay. Si se desea hacer otro tipo de túneles, se puede encontrar más información en el capítulo anterior, en la sección de túneles.
324. Para configurar un túnel es necesario configurar IPv6 en los 2 routers en los que se va a utilizar el túnel y luego establecer el túnel en uno de ellos. Primero se va a ver la configuración de R3.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

325. Lo primero de todo es habilitar el tráfico IPv6 y configurar una dirección IPv4 (o tenerla ya establecida) para poder utilizar ipv6 sobre IPv4. A modo de prueba, se va a configurar en loopback, habilitando IPv6.

```
Router(config)#interface loopback0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 add 2000::1/64
```

326. Y a continuación en R1 se va a configurar el túnel, aunque primero se harán los pasos llevados a cabo en R3 y, posteriormente, se configurará el túnel.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip add 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
*Jun 23 11:07:44.923: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 23 11:07:44.923: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Jun 23 11:07:45.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface loopback0
Router(config-if)#
*Jun 23 11:08:32.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 add 2001::1/64
Router(config-if)#exit
```

```
Router(config)#interface tunnel0
Router(config-if)#tunnel source FastEthernet 0/0
Router(config-if)#tunnel destination 192.168.2.1
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#ipv6 enable
Router(config-if)#exit
```

327. Con estos últimos comandos se define el túnel en R1, especificando la interfaz fuente, la dirección destino y el modo del túnel, en este caso ipv6 sobre ipv4.

6.9.5. CONSIDERACIONES ADICIONALES DE SEGURIDAD

328. Para paliar algunas vulnerabilidades descritas en el capítulo de vulnerabilidades, hay que tener especial cuidado con las direcciones multicast y los mensajes ICMP que tienen direcciones de tipo multicast. Concretamente, hay que evitar los mensajes ICMP cuando la dirección destino es una dirección de tipo multicast y, además, descartar los paquetes con dirección origen de tipo multicast. Para ello se recomienda aplicar en un access-list en el router estas 2 reglas:

```
Router(config-ipv6-acl)#deny tcp ff00::/11 any
Router(config-ipv6-acl)#deny icmp any ff00::/11
```

329. En el caso de la primera regla, se ha elegido tcp como ejemplo, pero se debería aplicar a todos los demás protocolos que estén habilitados en la red, como podría ser UDP.
330. Por otro lado, hay ciertos ataques que se pueden hacer sobre los protocolos Neighbour Discovery y Router Advertisement que deben ser tenidos en cuenta. La forma de solucionarlos es aplicar SeND o Secure Neighbour Discovery y RA Guard, respectivamente. En el capítulo anterior se encuentra como implementar estos 2 protocolos, aunque la aplicación de SeND es marginal y casi no es usada, mientras que RA Guard solo es soportado por una serie de equipos muy limitados. Se aconseja utilizarlos siempre que estén disponibles. También se recomienda usar ND Inspection para no aceptar paquetes ND falsos.
331. También existen ciertos problemas de seguridad en cuanto a las cabeceras de extensión. Si no se van a usar, se recomienda crear reglas en los access-list para restringir su uso, aunque esto puede interferir en la utilización de estas cabeceras y solo se debe aplicar en los dispositivos en los que no se vayan a usar. A continuación se ofrece un ejemplo de Cisco (2) para limitar el uso de la cabecera hop-by-hop.

```
Device(config-if)# ipv6 traffic-filter hbh_acl in
Device(config-if)# exit
Device(config)# exit
Device# clear counters
Clear "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface FastEthernet3/1

Building configuration...

Current configuration : 114 bytes
!
interface FastEthernet3/1
no switchport
ipv6 address 1001::1/64
ipv6 traffic-filter hbh_acl
end
```

```

Device(config)# ipv6 access-list hbh_acl
Device(config-ipv6-acl)# permit tcp any any hbh
Device(config-ipv6-acl)# permit tcp any any
Device(config-ipv6-acl)# permit udp any any
Device(config-ipv6-acl)# permit udp any any hbh
Device(config-ipv6-acl)# permit hbh any any
Device(config-ipv6-acl)# permit any any
Device(config-ipv6-acl)# hardware statistics
Device(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Device(config)# interface FastEthernet3/1
Device(config-if)# ipv6 address 1001::1/64

```

332. Por último, se recomienda, siempre que sea posible, habilitar cortafuegos en la frontera de la red, de forma que se pueda vigilar el tráfico y aplicar reglas para limitar el uso de túneles, como se sugiere en el capítulo de vulnerabilidades, como bloquear los mensajes que vengan desde un servidor Teredo o desde un nodo 6to4, o bloquear el puerto UDP 3544 que es donde escucha Teredo, además de bloquear la salida a la red exterior de direcciones prohibidas, como pueden ser las direcciones Link-local o ULA explicadas en el documento anteriormente. Se recomienda también repasar el capítulo de vulnerabilidades para una mejor comprensión e implantación de las medidas de seguridad necesarias.

6.10. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR

VULNERABILIDAD	MEDIDA
Ataques de escaneo de direcciones de red	No utilizar asignación manual de direcciones ni asignación basada en reglas. Usar preferiblemente DHCPv6 y/o SLAAC.
Ataques de tipo SLAAC	Utilizar DHCPv6.
Ataques sobre multicast	Filtrar los mensajes ICMP hacia direcciones multicast y descartar los paquetes con direcciones origen multicast.
Ataques sobre Neighbour Discovery	Implementación de SeND si fuese posible, variación de parámetros para evitar el agotamiento de tablas y aplicar ND Inspection.
Aceptación de paquetes RA falsos e inundación de paquetes RA.	Utilización de RA Guard en los equipos en los que esté disponible.
Aceptación de paquetes ICMPv6 de redireccionamiento falsos.	Inhabilitar la recepción de estos mensajes.
Ataques sobre las cabeceras de extensión.	Bloquear y/o restringir el uso de cabeceras de extensión.
Vulnerabilidades sobre túneles	No utilizar túneles bajo ningún concepto si no es estrictamente necesario. Si lo fuese, limitarlo a los equipos que lo necesiten filtrando el tráfico de los túneles como Teredo o 6to4.

7. CONFIGURACIÓN DE SISTEMAS WINDOWS: WINDOWS 10

7.1. INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE IPV6 EN EL EQUIPO

7.1.1. INSTALACIÓN DE IPV6

333. A partir de la versión Windows 7 y posteriores, IPv6 viene configurado por defecto en los sistemas operativos de Microsoft. En caso de estar desactivado en el sistema operativo se puede activar como se indica a continuación.
334. Para versiones anteriores a Windows 7, accediendo al Panel de Control/Conexiones de red e Internet/Conexiones de red, se selecciona cualquiera de los iconos Conexión de área local o Conexiones de red inalámbricas y después se accede a Propiedades/General. Se escribe Microsoft TCP/IP versión 6 y se selecciona Instalar/Protocolo.
335. Después se abre una ventana de comandos (Inicio/ejecutar/cmd) y se introduce “ipv6 install” saliendo un mensaje de confirmación de que la instalación ha sido correcta. En caso de tener problemas con este comando se puede hacer también con “netsh interface ipv6 install”, para lo que se deberá ejecutar una ventana de comandos en modo administrador.
336. Para versiones posteriores a Windows 7, se puede llevar a cabo accediendo a Conexiones de Red mediante Inicio/Panel de control y en el cuadro de búsqueda escribiendo “adaptador” y en Centro de redes y recursos compartidos entrando en “Ver conexiones de red” y se accede a Propiedades. En caso de solicitar una contraseña de administrador o una confirmación, se escribirá la contraseña y se proporcionará confirmación. Una vez hecho esto habrá que activar la casilla “Protocolo de Internet versión 6 (TCP/IPv6)”.
337. Y, al igual que en el caso anterior, si se tiene algún problema se puede llevar a cabo abriendo una ventana de comandos y escribiendo “netsh interface ipv6 install”.

7.1.2. OBTENCIÓN DE LA DIRECCIÓN IPV6

338. Cuando en un equipo se tiene instalado y activado este protocolo, en Windows la asignación de la dirección se hará automáticamente a través de servidores DNS obteniendo una dirección local. Si un equipo en una red IPv6 desea encaminar tráfico fuera de la red local se usará el protocolo SLAAC, el cual es usado por los routers de conexión. Estos envían mensajes RA (Router Advertisement) diciéndole a los equipos cómo configurarse para tener conectividad a través de ellos.
339. Otra forma de obtener direcciones IPv6 es DHCPv6 que puede trabajar de forma conjunta con el mecanismo SLAAC. También permite a los clientes la solicitud de múltiples direcciones IPv6, que no es posible en IPv4 ni a través del mecanismo SLAAC.
340. Ambos métodos, uso de SLAAC o DHCPv6, son protocolos que implementa IPv6 y que no necesitan de instalación ni configuración previa a su uso. Por tanto, para obtención de la dirección IPv6 se hará de forma automática y el usuario no tendrá que realizar ninguna configuración adicional a la de instalación y activación del protocolo.

7.1.3. CONFIGURACIÓN DE IPV6

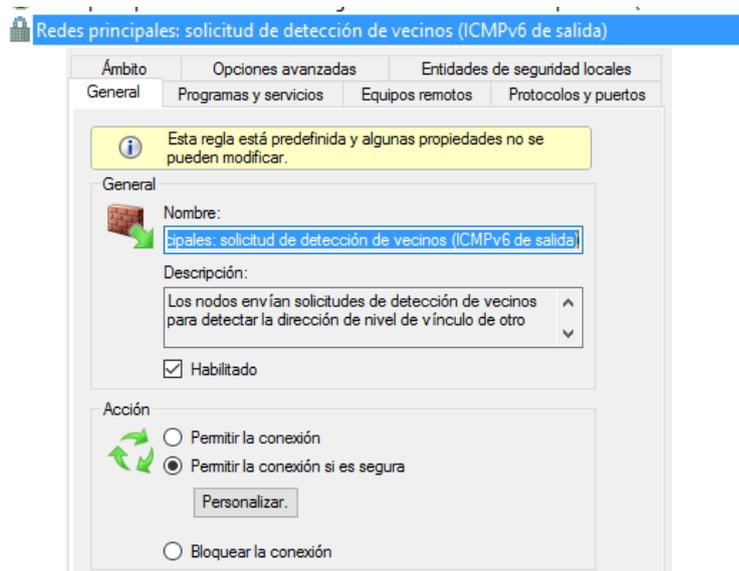
7.1.3.1. CONFIGURACIÓN ICMP

341. IPv6 utiliza ICMP para detectar errores encontrados en la interpretación de los paquetes y para realizar otras funciones de la capa de internet como el diagnóstico.

342. Estos mensajes pueden ser falsificados para atacar una red. Uno de los más comunes en redes IPv6 es el uso de paquetes de redireccionamiento falsos, por lo que se debe desactivar la aceptación de este tipo de paquetes ICMPv6 en los sistemas finales. Desde una ventana de comandos ejecutándose en modo administrador se usará el comando “netsh”:

```
netsh firewall> set icmpsetting type=5 mode=DISABLE profiles=ALL
```

343. De este modo se inhabilita la recepción de estos mensajes en el PC (7).
344. Este protocolo es usado también para el descubrimiento de vecinos y, por tanto, lo que es usado por los atacantes para comprometer los sistemas. Los ataques se producen bien falsificando estos mensajes o bien inundando la tabla de routers vecinos. Para evitar estos ataques:
345. Falsificación de mensajes ND (Neighbor Discovery): en las reglas entrantes del Firewall (cortafuegos) se configurará para que solo se permitan este tipo de conexiones si la comunicación es segura.



346. Agotamiento de la tabla ND: en IPv6 es posible configurar el time out y la validez de una dirección. Con la siguiente configuración se podrá seguir haciendo uso del protocolo ICMPv6 pero se evitará que se use como vector de ataque a un sistema dentro de una red IPv6.

```
netsh interface ipv6>show privacy
Consultando el estado activo...

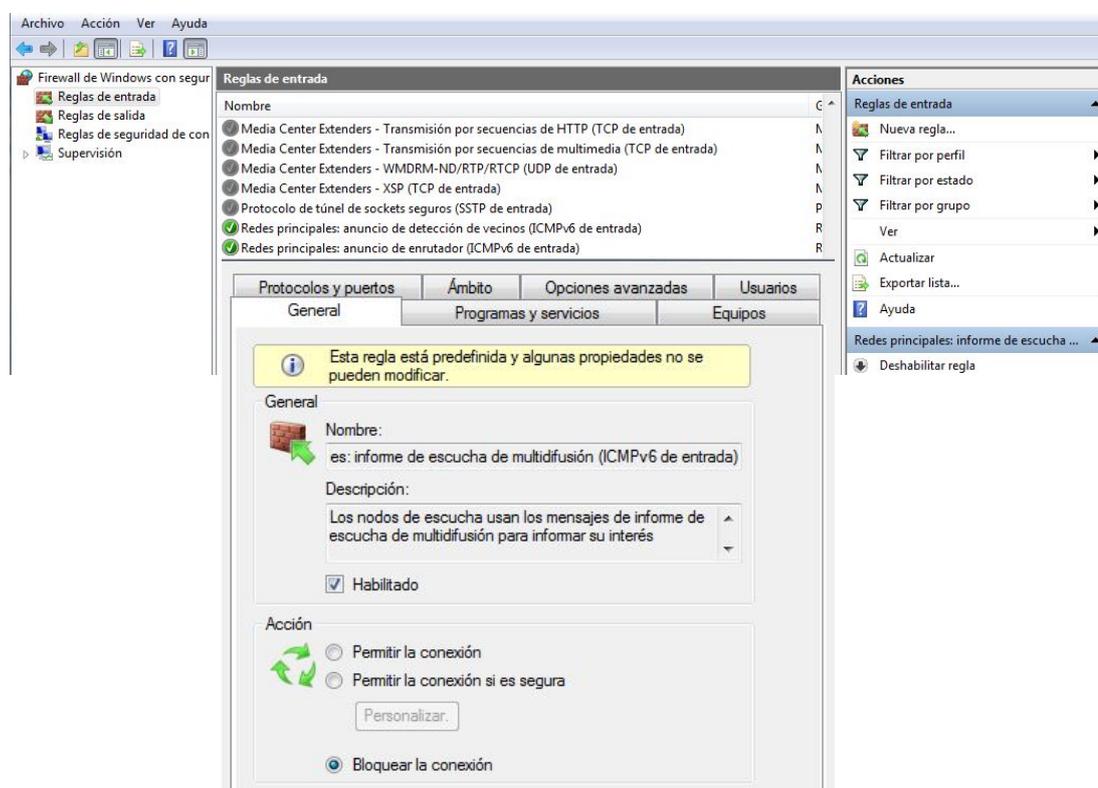
Parámetros de dirección temporal
-----
Usar direcciones temporales           : enabled
Intentos de detección de dirección duplicada: 3
Vigencia válida máxima               : 7d
Vigencia preferida máxima            : 1d
Regenerar tiempo                     : 5s
Tiempo aleatorio máximo              : 10m
Tiempo aleatorio                     : 4m41s
```

7.1.3.2. MULTICAST

347. A diferencia de su predecesor, IPv6 no implementa direcciones broadcast. Sin embargo, existen las direcciones multicast para poder transmitir datagramas a un grupo de receptores interesados. Para este tipo de comunicaciones, se usan paquetes MLD (Multicast Listener Discovery) (8), que van encapsulados en ICMP (9), para conocer la pertenencia a un grupo multicast o unirse al mismo (10). Por ello y para evitar ataques DDoS utilizando las direcciones multicast, se detectarán los paquetes que tengan como origen una dirección multicast para no responder a ellos. Usando el comando “netsh” se hará:

```
netsh firewall> set multicastbroadcastresponse mode=DISABLE profiles=ALL
```

348. De este modo se bloquean las respuestas a direcciones multicast. Es conveniente también bloquear la recepción de paquetes que vengan de este tipo de direcciones y para ello se pueden deshabilitar la recepción de los mismos en las reglas del cortafuegos.



349. Por tanto, queda de manifiesto que es necesario tener activado un cortafuegos que filtre el tráfico entrante y saliente, puesto que en IPv6 no se usa NAT, que actuaba como método de protección en IPV4.

7.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6

350. Para comprobar la conectividad de IPv6 en el equipo se realizará una verificación de la misma mediante el comando ping. Este comando chequea la dirección destino que se desea alcanzar, enviando peticiones de eco (echo request) (11). Si la máquina destino está operativa, esta dará una respuesta por su parte junto al retardo de la operación. En este caso se utilizará la dirección ::1, que es la dirección de loopback que utilizan las máquinas para enviarse paquetes a sí mismas.

351. Abriendo una terminal se ejecuta el comando “ping -6 -n 5 ::1” y aparecerá lo siguiente:

```
C:\Users\Usuario>ping -6 -n 5 ::1

Haciendo ping a ::1 con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m

Estadísticas de ping para ::1:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

352. Otra forma de comprobar la conectividad de la propia máquina sería haciendo ping a la dirección IPv6 de la misma. Para conocer dicha dirección se ejecuta en el terminal “ipconfig” o “ipconfig/all”.

```
Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de red inalámbrica 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::5557:1d02:93dd:d2af%14
    Dirección IPv4. . . . . : 192.168.1.36
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

353. Una vez conocida la dirección IPv6 se ejecuta “ping -6 -n 5 DIR_IPV6_MAQUINA”.

```
C:\Users\Usuario>ping -n 5 fe80::5557:1d02:93dd:d2af%14

Haciendo ping a fe80::5557:1d02:93dd:d2af%14 con 32 bytes de datos:
Respuesta desde fe80::5557:1d02:93dd:d2af%14: tiempo<1m

Estadísticas de ping para fe80::5557:1d02:93dd:d2af%14:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

354. Otra posible forma es comprobar la conectividad con el exterior, para ello se realizará un ping a máquinas IPv6 fuera de la red local. Se puede probar haciendo “ping www.ipv6tf.org”. Además, se puede conocer también la conectividad con los nodos intermedios observando los saltos con tracert.

7.3. CONFIGURACIÓN DE TÚNELES EN IPV6

355. Actualmente en internet conviven redes que funcionan con IPv4 e IPv6. Para que la comunicación entre los distintos nodos y usuarios sea posible en esta red híbrida se hacen necesarios los túneles. Este tipo de mecanismos que permite usar ambos protocolos es también usado como vector de ataque, puesto que haciendo uso de ellos se

pueden saltar las defensas perimetrales de la red y enmascarar tráfico malicioso, por lo que no se recomienda el uso de túneles.

356. Si se ejecuta el comando “ipconfig” desde una terminal de comandos en Windows veremos lo siguiente:

```

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::d573:428c:8a18:3d7f%2
    Dirección IPv4. . . . . : 192.168.1.38
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de túnel isatap.{1E513098-BDDE-4FDD-B722-F13E0C86FF12}:

    Sufijo DNS específico para la conexión. . . :
    Sitio: dirección IPv6 local. . . . . : fec0:0:0:ffff::2%1
    Vínculo: dirección IPv6 local. . . . . : fe80::5efe:192.168.1.38%14
    Puerta de enlace predeterminada . . . . . :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de túnel Conexión de área local* 11:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de túnel 6TO4_Adapter:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

```

357. Se observa que este permite mecanismos de tunelización TEREDO e ISATAP.

7.3.1. TEREDO

358. Teredo es una tecnología de transición que proporciona conectividad IPv6 a hosts que soportan IPv6 pero que se encuentran conectados a Internet mediante una red IPv4. Comparado con otros protocolos similares, la característica que lo distingue es que es capaz de realizar su función incluso detrás de dispositivos NAT, como los routers domésticos (12).
359. En este caso, para configurarlo, se hará uso del comando “netsh” y se tendrá que escribir “netsh interface teredo” (13):

```

C:\Windows\system32>netsh
netsh>interface teredo
netsh interface teredo>show state
Parámetros de Teredo
-----
Tipo                               : client
Nombre del servidor                 : win10.ipv6.microsoft.com.
Intervalo de actualización del cliente: 30 segundos
Puerto de cliente                   : unspecified
Estado                              : qualified
Tipo de cliente                     : teredo client
Red                                 : unmanaged
NAT                                 : restricted (port)
Comportamiento especial de NAT      : UPNP: No, conservación de puertos: Sí
Asignación local                    : 192.168.1.36:65399
Asignación de NAT externa            : 81.38.152.121:65399

```

360. Se observa que el protocolo tiene configurado por defecto el servidor de traducción de direcciones IPv6, que en este caso es win10.ipv6.microsoft.com, y el tipo de conexión, que en este caso es cliente. Se ve también que no tiene ningún puerto saliente asignado, por lo que no se podrá establecer conexiones con el exterior.
361. Se asigna un puerto en el que no haya otro servicio escuchando. Para ello se ejecutará en la misma terminal (14) “set state client win10.ipv6.microsoft.com 60 3544” (15). Quedará de la siguiente manera:

```
netsh interface teredo>show state
Parámetros de Teredo
-----
Tipo                : client
Nombre del servidor : teredo.ipv6.microsoft.com
Intervalo de actualización del cliente: 60 segundos
Puerto de cliente   : 3544
Estado              : offline
Error                : no se puede resolver el nombre del servidor
```

362. Se comprueba el correcto funcionamiento del mismo haciendo un ping forzando el uso de IPv6.

```
C:\Users\Elisa>ping -6 www.google.com -n 6

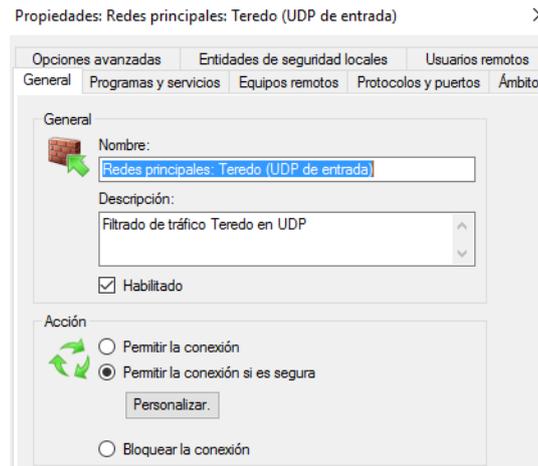
Haciendo ping a www.google.com [2a00:1450:4006:803::2004] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Respuesta desde 2a00:1450:4006:803::2004: tiempo=119ms
Respuesta desde 2a00:1450:4006:803::2004: tiempo=70ms
Respuesta desde 2a00:1450:4006:803::2004: tiempo=91ms
Respuesta desde 2a00:1450:4006:803::2004: tiempo=106ms
Respuesta desde 2a00:1450:4006:803::2004: tiempo=119ms

Estadísticas de ping para 2a00:1450:4006:803::2004:
    Paquetes: enviados = 6, recibidos = 5, perdidos = 1
              (16% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 70ms, Máximo = 119ms, Media = 101ms
```

363. Para hacer un uso seguro de este mecanismo, se debe desactivar en esta interfaz el parámetro “routerdiscovery” para evitar ataques de tipo SLAAC, protocolo que permite la configuración automática (16). Usando el comando “netsh”:

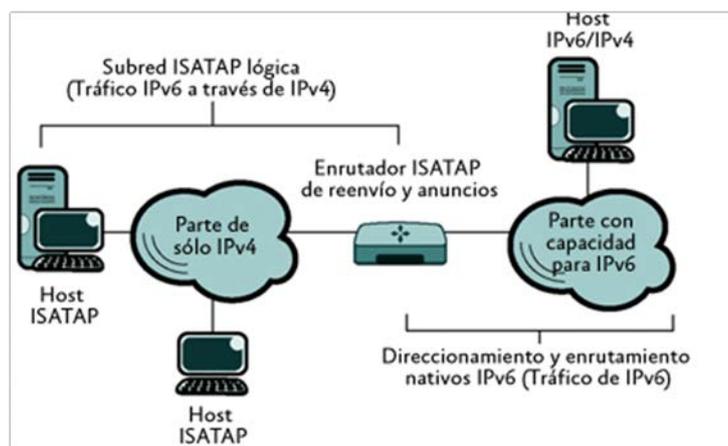
```
netsh interface ipv6> set interface “27” routerdiscovery=disabled
```

364. El uso de este mecanismo puede provocar ataques de DDoS. Para evitarlos se puede filtrar el tráfico que llegue de este protocolo y cifrar la conexión. El tráfico que se recibe es UDP y escucha en el puerto 3544. Se debe crear una nueva regla de entrada en el cortafuegos del sistema, donde especificamos puerto, protocolo y tipo de conexión.



7.3.2. ISATAP

365. ISATAP es una tecnología de asignación de direcciones y de tunelización automática (definida en RFC 4214) que ofrece conectividad unidifusión IPv6 entre hosts IPv6/IPv4 a través de una intranet de sólo IPv4 (17) (18).
366. Es por ello que será necesario configurar un router ISATAP para traducción y reenvío de peticiones, cuyo proceso se encuentra explicado en el capítulo sobre la configuración de router. Por tanto, desde el host final (PC del usuario) no se podrá realizar ninguna configuración.
367. Sin embargo, hay que tener en cuenta que Windows 10 tiene desactivado por defecto el uso de DNS ISATAP (19), de manera que si dentro de una red corporativa se quiere usar este protocolo, se deberán cambiar ciertos valores del registro.
368. Se abrirá, buscando en el explorador de Windows, regedit.exe. Una vez dentro se navegará por las carpetas hasta el siguiente directorio:
- ```
HKEY_LOCAL_MACHINE\SYSTEM\CURRENT_CONTROL_SET\SERVICES\DNSCACHE\PARAMETERS
```
369. Y una vez dentro, se crearán los siguientes parámetros:
- DisableParallelAandAAA* de tipo DWORD y con valor 1 en decimal.
  - DisableServerUnreachability* de tipo DWORD y con valor 1 en decimal.
370. Una vez hecho, se reinicia el equipo para que se hagan efectivos los cambios en el registro. Esto permitirá conexiones como por ejemplo Microsoft Windows DireccAccess, una herramienta de Microsoft para crear VPN.
371. Por tanto, si se hace uso de este protocolo, se deberá configurar el router ISATAP que haga de DNS.



372. Para ello, se abre una ventana de comandos en modo administrador y se ejecuta “netsh interface isatap” y se establece el router tal y como se muestra en la pantalla.

```

netsh interface isatap>set router isatap enabled 1
Aceptar

netsh interface isatap>show router
Nombre de enrutador : isatap
Usar retransmisión : enabled
Intervalo de resolución : 1 minutos

netsh interface isatap>

```

373. Esta configuración solo debería hacerla el administrador de red si es necesario, puesto que habilitando este tipo de conexiones se es susceptible a posibles ataques en los que se saltan las defensas perimetrales.
374. De la misma forma que en Teredo, debemos desactivar en la interfaz el “routerdiscovery” para evitar ataques usando SLAAC.

```
netsh interface ipv6> set interface “14” routerdiscovery=disabled
```

### 7.3.3. 6TO4

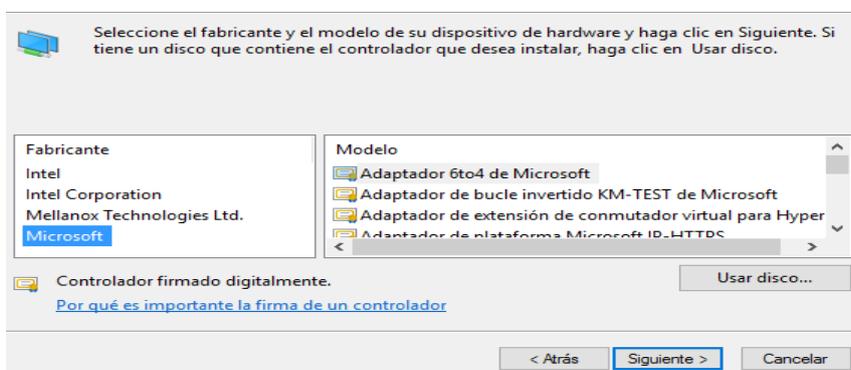
375. 6to4 es un sistema que permite enviar paquetes IPv6 sobre redes IPv4 obviando la necesidad de configurar túneles manualmente. Fue diseñado para permitir conectividad IPv6 sin la cooperación de los proveedores de Internet (20).
376. Este sistema puede funcionar en un router, proveyendo conectividad a toda una red o a una máquina en particular. En ambos casos se necesita una dirección IP pública. El funcionamiento básico del sistema consiste en la asignación de direcciones IPv6 que contienen embebida la dirección IPv4 pública del router. Estas direcciones tienen todas el prefijo 2002::/16. De esta manera, cuando es necesario convertir un paquete IPv6 para que atraviese la red IPv4, el router sabe la dirección a la que debe estar dirigido el paquete IPv4 generado (21).
377. En Windows 10 el adaptador 6to4 no viene instalado por defecto. Para poder instalarlo pulsando en el icono de Windows se accede a Configuración y en el buscador se escribe “administrador de dispositivos”.



378. Se pincha en Administrador de dispositivos y se accede a “Adaptadores de red”. Una vez seleccionado este apartado se hace Acción/Agregar hardware heredado y se abrirá un cuadro de diálogo en el que se tendrá que pulsar en “Siguiente”. Seguidamente se selecciona la opción de “Instalar el hardware seleccionado manualmente de una lista (avanzado)” y una vez seleccionada esta opción se pincha en adaptadores de red. Se elige como fabricante “Windows” y en la parte de la derecha el adaptador 6to4 para instalarlo.

Agregar hardware

Seleccione el controlador de dispositivo que desea instalar para este hardware.



379. Una vez hecho, se comprueba que se ha instalado correctamente el adaptador. Para ello se abre una terminal y se introduce “ipconfig”.

```

Adaptador de Ethernet Ethernet:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Vínculo: dirección IPv6 local. . . : fe80::d573:428c:8a18:3d7f%2
Dirección IPv4. : 192.168.1.38
Máscara de subred. : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1

Adaptador de túnel isatap.{1E513098-BDDE-4FDD-B722-F13E0C86FF12}:

Sufijo DNS específico para la conexión. . . :
Sitio: dirección IPv6 local. . . : fec0:0:0:ffff::2%1
Vínculo: dirección IPv6 local. . . : fe80::5efe:192.168.1.38%14
Puerta de enlace predeterminada :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de túnel Conexión de área local* 11:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

Adaptador de túnel 6TO4_Adapter:

Estado de los medios. : medios desconectados
Sufijo DNS específico para la conexión. . . :

```

380. Del mismo modo que ocurre con los mecanismos de Teredo e ISATAP, si no se va a hacer uso de este mecanismo, es recomendable desactivar este adaptador para evitar ataques DDoS u otro tipo de ataques en el que se use este mecanismo como vector. Si fuese necesario su uso, una buena práctica sería filtrar este tráfico y dotarlo de seguridad usando IPsec.

#### 7.4. TRADUCCIÓN DE DIRECCIONES IPV6

381. Una parte importante del uso de IPv6 en redes IPv4, es la traducción de direcciones IP. Es por ello, que se podrán configurar en el cliente los servidores DNS para permitir la configuración entre los servidores y los clientes DNS.
382. Para permitir la comunicación entre los servidores y los clientes DNS, puede configurar los clientes con la dirección IPv6 del servidor DNS, o bien configurar el servidor DNS con una de las tres direcciones IPv6 de servidor DNS predeterminadas que se definen automáticamente en todos los clientes IPv6.
383. Para configurar los clientes con la dirección IPv6 del servidor DNS, se utiliza el comando “netsh interface ipv6 add dns” en cada equipo cliente o en una secuencia de comandos de inicio de sesión que se ejecute cada vez que el cliente inicie sesión en la red.
384. Si desea configurar el servidor DNS con una de las tres direcciones IPv6 disponibles de forma predeterminada en los equipos cliente IPv6, hay que usar el comando “netsh interface ipv6 add address”. Las tres direcciones de servidor DNS son (22):
- FEC0:0:0: FFFF::1
  - FEC0:0:0: FFFF::2
  - FEC0:0:0: FFFF::3

```
netsh interface ipv6>show address
Interfaz 1: Loopback Pseudo-Interface 1

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Preferido infinite infinite ::1

Interfaz 9: Ethernet

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Obsoleto infinite infinite fe80::b5d0:29fe:ef6a:720c%9

Interfaz 2: Wi-Fi

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Preferido infinite infinite fe80::d573:428c:8a18:3d7f%2

Interfaz 14: isatap.{1E513098-BDDE-4FDD-B722-F13E0C86FF12}

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Preferido infinite infinite fe80::5efe:192.168.1.39%14

Interfaz 11: Conexión de área local* 2

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Obsoleto infinite infinite fe80::a03e:7dfa:f729:2cb7%11

Interfaz 27: Teredo Tunneling Pseudo-Interface

Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Público Preferido infinite infinite 2001:0:9d38:6abd:ac:78f8:a7ff:5272
Otros Preferido infinite infinite fe80::ac:78f8:a7ff:5272%27
```

385. En la captura se observa la configuración por defecto, y a continuación se añaden las direcciones del DNS a las interfaces de TEREDEO e ISATAP.

```
netsh interface ipv6>add address "Teredo Tunneling Pseudo-Interface" FEC0:0:0:FFFF::1
netsh interface ipv6>add address "isatap" FEC0:0:0:FFFF::2
```

386. Se comprueba que se han añadido correctamente.

```
Interfaz 27: Teredo Tunneling Pseudo-Interface
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Público Preferido infinite infinite 2001:0:9d38:6abd:ac:78f8:a7ff:5272
Otros Preferido infinite infinite fe80::ac:78f8:a7ff:5272%27
Manual Preferido infinite infinite fec0:0:0:ffff::1%1

Interfaz 14: isatap.{1E513098-BDDE-4FDD-B722-F13E0C86FF12}
Tipo direc. Estado DAD Vigencia válida Vigencia pref. Dirección

Otros Preferido infinite infinite fe80::5efe:192.168.1.39%14
Manual Preferido infinite infinite fec0:0:0:ffff::2%1
```

387. A la hora de configurar DNS, se deben elegir aquellos que sean de confianza y sean conocidos, puesto que si se configura mal los DNS podrían ser usados como un vector de ataque. Éstos podrían dar traducciones de direcciones IP a host maliciosos y ser víctimas de un ataque.

## 7.5. DESHABILITAR IPV6 Y SUS COMPONENTES

388. Windows recomienda deshabilitar IPv6 y sus componentes, puesto que Windows 7 y sus versiones posteriores se hicieron pensando para soportar dicho protocolo. Si se deshabilita, puede que algunas aplicaciones o servicios que usan IPv6 por defecto dejen de funcionar (23).
389. Si por razones de seguridad hay que deshabilitar IPv6 o algunos de sus componentes, a continuación se detallan las posibles configuraciones.

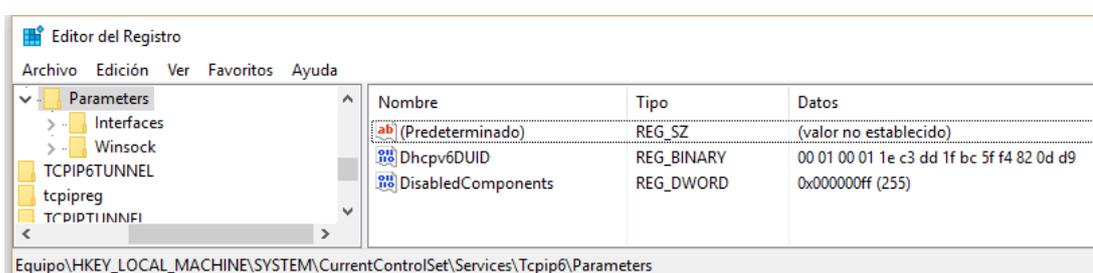
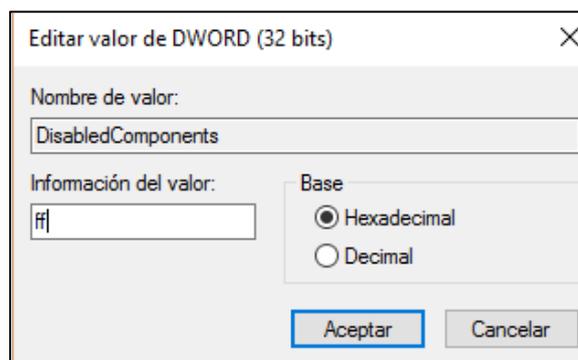
### 7.5.1. DESHABILITAR IPV6

390. Se puede deshabilitar IPv6 en el equipo a través del valor de registro DisabledComponents. Este valor de registro afecta a todas las interfaces de red en el host. En la lista de programas se abrirá regedit.exe y se navegará por las carpetas hasta la ruta:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
```

391. Una vez dentro, se debe modificar la variable DisabledComponents, que en caso de no aparecer se creará de la siguiente manera:
- En el menú **Edición**, seleccionar **nuevo** y, a continuación, haciendo clic en valor **DWORD (32 bits)**.
  - Escribir **DisabledComponents** y, a continuación, presionar ENTER.

- Una vez creada la variable, haciendo doble clic sobre ella se modificará su valor para desactivar IPv6 y todos sus componentes. Para ello se escribe el valor ff en hexadecimal.



392. Reiniciando el equipo para hacer efectivos los cambios de registro, se comprueba que se han desactivado IPv6 y sus componentes. Este valor también configura la preferencia de IPv4 sobre IPv6 en la tabla de políticas de prefijos.

### 7.5.2. PREFERENCIA DE IPV4 SOBRE IPV6 EN LAS POLÍTICAS DE PREFIJOS

393. Cambiando el valor del registro a “0x02” cambiará la tabla de políticas de prefijos para preferir IPv4 sobre IPv6. Cambiando esta configuración es posible configurar qué prefijos van a ser usados para establecer comunicaciones. Si se dota de una preferencia baja a los prefijos de las direcciones ULA (24) (25) (26) (con prefijo fc00::/7), se podrá evitar que estas direcciones se asignen y puedan ser utilizadas en internet y no en un ámbito local.

```
C:\Users\Elisa>ping -6 www.google.com -n 5
La solicitud de ping no pudo encontrar el host www.google.com. Compruebe el nombre y
vuelva a intentarlo.

C:\Users\Elisa>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

 Estado de los medios. : medios desconectados
 Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

 Estado de los medios. : medios desconectados
 Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

 Sufijo DNS específico para la conexión. . . :
 Dirección IPv4. : 192.168.1.39
 Máscara de subred : 255.255.255.0
 Puerta de enlace predeterminada : 192.168.1.1
```

**7.5.3. DESHABILITAR IPV6 EN TODAS LAS INTERFACES SIN TÚNELES**

394. Cambiando el valor del registro a 0x10, se desactiva IPv6 en todas las interfaces que no sean de túnel (LAN y P2P).

**7.5.4. DESHABILITAR IPV6 EN TODAS LAS INTERFACES DE TÚNELES**

395. Cambiando el valor del registro a 0x01, se desactiva IPv6 en todas las interfaces de túnel, esto incluye TEREDO, ISATAP y 6to4. Es recomendable establecer esta configuración si no se va a hacer un uso específico de estos mecanismos puesto que son muy usados para realizar ataques saltándose las defensas perimetrales.

**7.5.5. DESHABILITAR IPV6 EN TODAS LAS INTERFACES EXCEPTO LA DE LOOPBACK**

396. Cambiando el valor del registro a 0x11 se desactiva IPv6 en todas las interfaces excepto en la de loopback. Es recomendable establecer esta configuración si no se va a hacer un uso específico de este protocolo.

**7.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR**

| VULNERABILIDAD                                                                 | MEDIDA                                                                                                                                                                               |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ataques de tipo SLAAC                                                          | Dos medidas: <ul style="list-style-type: none"> <li>Desactivar IPv6.</li> <li>Desactivar el "routerdiscovery" en las interfaces en las que se haga uso del protocolo IPv6</li> </ul> |
| Dispositivo de filtrado no bloquea el tráfico saliente                         | Firewall activado para filtrar el tráfico saliente.                                                                                                                                  |
| Dispositivo de filtrado no filtra túneles IPv6                                 | Cambiar registro "DisabledComponents" a "0x01" para desactivar interfaces del túnel IPv6.                                                                                            |
| La red acepta paquetes ICMPv6 de redireccionamiento falsos                     | Inhabilitar la recepción de paquetes de redireccionamiento ICMPv6 en equipos no routers.                                                                                             |
| Ataque DoS mediante el reflector de dirección destino multicast (ataque smurf) | Bloquea la respuesta a los mensajes ICMPv6 en direcciones multicast y broadcast.                                                                                                     |
| Ataque sobre neighbour discovery (ND)                                          | Cifrar concesiones de mensajes ND de ICMP para asegurar la comunicación.                                                                                                             |
| Agotamiento de la tabla ND (Neighbour discovery) por inundación                | Reducir time out de la caché de vecinos.                                                                                                                                             |
| Desbordamiento de la memoria en Teredo                                         | Crear una nueva regla en el firewall que escuche en el puerto 3544 y filtram el tráfico.                                                                                             |

**8. CONFIGURACIÓN DE SISTEMAS MAC OS X**

397. Mac OS X ha incluido compatibilidad con el protocolo IPv6 desde la versión Mac OS X v10.1 y lo ha activado por omisión desde la versión Mac OS X v10.3. Actualmente se

encuentra en la versión OS X v10.11, por tanto el protocolo se encontrará por defecto activado en todos los equipos que tengan las versiones anteriormente mencionadas. Sin embargo, debido a la escasez de posibilidades de configuración del sistema, como ocurre con el firewall, no se tienen tantas opciones de configuración como en Windows, por lo que la aplicación de políticas de seguridad es más reducida que en los sistemas Windows.

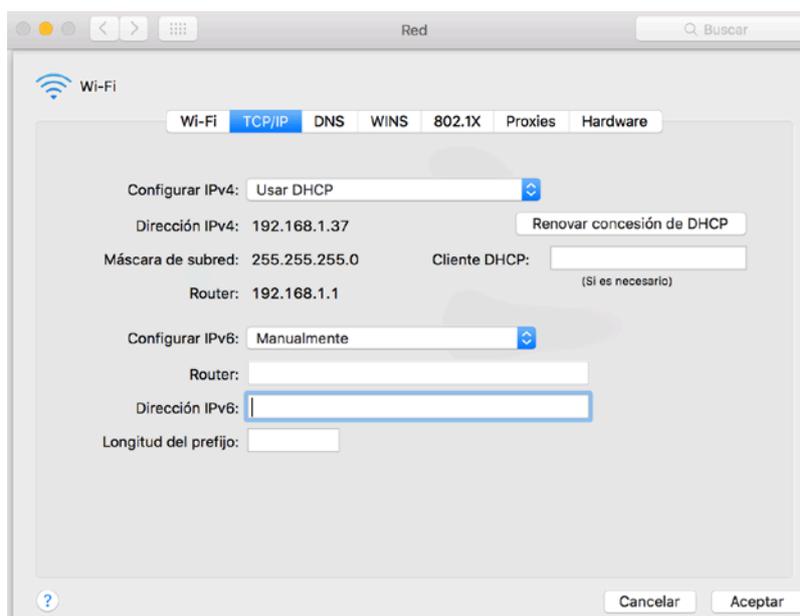
## 8.1. INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE IPV6 EN EL EQUIPO

### 8.1.1. INSTALACIÓN DE IPV6

398. IPv6 está soportado por Apple desde Mac OS X 10.1 y se halla habilitado por defecto desde la versión OS X 10.3. Por lo tanto, no es preciso hacer nada para instalarlo (27).

### 8.1.2. OBTENCIÓN DE UNA DIRECCIÓN IPV6

399. Como ya se ha comentado una de las ventajas clave que ofrece el protocolo IPv6 es que se configura de forma automática (28). En la mayor parte de los casos, el ordenador y las aplicaciones detectarán y aprovecharán las redes y los servicios con el protocolo IPv6 activado sin que tengas que hacer nada más. No obstante, puede que en algunas ocasiones se desee desactivar o configurar manualmente el protocolo IPv6. Se puede hacer para cada interfaz de red a través de los ajustes avanzados del panel Red de Preferencias del Sistema.

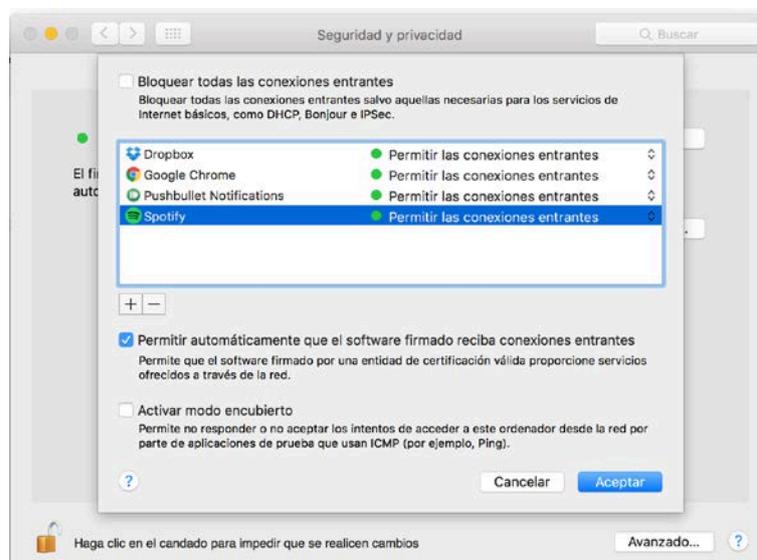


### 8.1.3. CONFIGURACIÓN BÁSICA DE IPV6

#### 8.1.3.1. ICMP

400. Como ya se ha comentado, este es el protocolo que usa IPv6 para recibir diagnósticos y errores de la red. En Mac OS no se puede configurar este protocolo con tanta granularidad como ocurre con los sistemas operativos Windows. Es posible activar desde el Firewall (cortafuegos) del sistema operativo (Preferencias del Sistema >

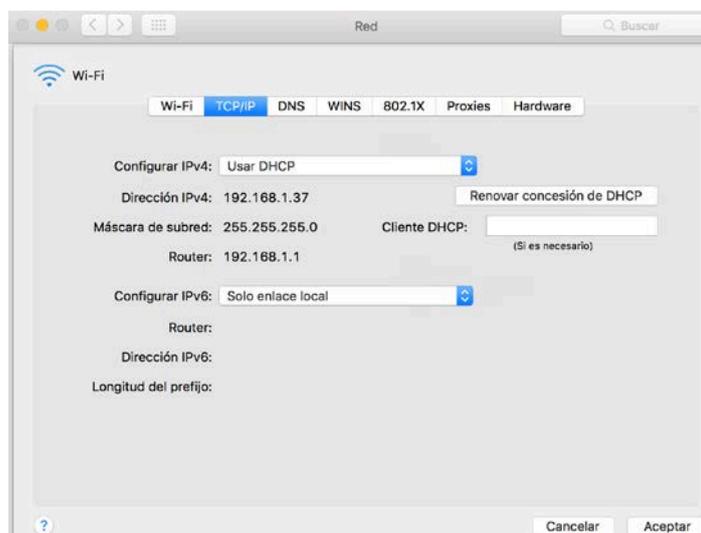
Seguridad y Privacidad > Firewall > Opciones Avanzadas) la opción “Activar modo encubierto”:



401. Esto permite que el ordenador no responda y/o no acepte los mensajes de sondeo. El ordenador seguirá respondiendo a solicitudes entrantes de las apps autorizadas. Se ignoran las solicitudes inesperadas, como ICMP (29).

### 8.1.3.2. MULTICAST

402. Como ya se ha comentado, en IPv6 se utilizan los mensajes MLD para configurar los grupos multicast. Para el caso de MAC, se accederá a Preferencias del Sistema > Red. En las interfaces que se tengan activas dentro de la configuración avanzada y en la pestaña TCP/IP se selecciona configuración “Solo enlace local” para IPv6 (30).



## 8.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6

403. Se abre una terminal (cmd + barra espaciadora y se escribe terminal) y a continuación se realiza “ping6 -c5 ::1”:

```

[MacBook-Pro-de-Andrea:~ apantojab$ ping6 -c5 ::1
PING6(56=40+8+8 bytes) ::1 --> ::1
16 bytes from ::1, icmp_seq=0 hlim=64 time=0.071 ms
16 bytes from ::1, icmp_seq=1 hlim=64 time=0.173 ms
16 bytes from ::1, icmp_seq=2 hlim=64 time=0.143 ms
16 bytes from ::1, icmp_seq=3 hlim=64 time=0.212 ms
16 bytes from ::1, icmp_seq=4 hlim=64 time=0.117 ms

--- ::1 ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.071/0.143/0.212/0.048 ms

```

404. Otra forma sería hacer ping a la dirección IPv6 de la máquina, como ya se ha visto para Windows. En este caso para conocer la dirección IPv6 de la máquina, se hace “ifconfig -a” y buscamos la interfaz que tenga “status: active” para conocer dicha dirección.

```

en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether 60:f8:1d:c3:79:c0
inet6 fe80::62f8:1dff:fec3:79c0%en0 prefixlen 64 scopeid 0x4
inet 192.168.1.37 netmask 0xfffff00 broadcast 192.168.1.255
nd6 options=1<PERFORMNUD>
media: autoselect
status: active

```

405. En caso de no tener activado IPv6 en la interfaz de que se está haciendo uso se podrá hacer desde la terminal lo siguiente (31):

```

networksetup -setv6automatic SERVICIO_A_ACTIVAR
networksetup -setv6automatic SERVICIO_A_ACTIVAR

```

406. Para saber qué servicios tenemos activos escribimos en la terminal “networksetup -listallnetworkservices”
407. Una vez conocida la dirección se hacer “ping6 DIR\_IPV6\_MAQUINA”

```

[MacBook-Pro-de-Andrea:~ apantojab$ ping6 fe80::62f8:1dff:fec3:79c0%en0
PING6(56=40+8+8 bytes) fe80::62f8:1dff:fec3:79c0%en0 --> fe80::62f8:1dff:fec3:79c0%en0
16 bytes from fe80::62f8:1dff:fec3:79c0%en0, icmp_seq=0 hlim=64 time=0.150 ms
16 bytes from fe80::62f8:1dff:fec3:79c0%en0, icmp_seq=1 hlim=64 time=0.152 ms
16 bytes from fe80::62f8:1dff:fec3:79c0%en0, icmp_seq=2 hlim=64 time=0.097 ms
16 bytes from fe80::62f8:1dff:fec3:79c0%en0, icmp_seq=3 hlim=64 time=0.215 ms
16 bytes from fe80::62f8:1dff:fec3:79c0%en0, icmp_seq=4 hlim=64 time=0.157 ms
^C
--- fe80::62f8:1dff:fec3:79c0%en0 ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.097/0.154/0.215/0.037 ms

```

### 8.3. CONFIGURACIÓN DE TÚNELES EN IPV6

#### 8.3.1. TEREDO

408. En el caso de los sistemas operativos Mac OS no viene instalado por defecto este adaptador de red para crear túneles. Para poder hacer uso del mismo se pueden encontrar en Internet distintas distribuciones de software libre (32) para poder instalarlo en la máquina. En cualquier caso, se tratan de distribuciones no oficiales, por tanto se desaconseja su instalación en el equipo.

### 8.3.2. ISATAP

409. Del mismo modo que ocurre con TEREDO, Mac OS tampoco dispone de agente para poder hacer uso de ISATAP. Existen, como ocurre con TEREDO, distribuciones de código libre por Internet que permiten instalar el agente en el equipo (33), pero de igual modo que ocurre con el caso arriba mencionado, se desaconseja su instalación.

### 8.3.3. 6TO4

410. En el caso de este mecanismo de tunelización es soportado por los sistemas operativos Mac OS por defecto. No obstante para hacer uso del mismo, es necesaria una configuración manual. Para ello se abrirá una terminal y se escribirán los siguientes comandos (34):
- Se establecen las direcciones IPv4 del túnel:  
`ifconfig gif0 tunnel $host-ipv4 $router-ipv4`
  - Se establecen las direcciones IPv6 del túnel:  
`ifconfig gif0 inet6 alias $tunnel-v6host $tunnel-v6router prefixlen 128`
  - Se establece la ruta (IPv6) por defecto del túnel:  
`route add -inet6 default -interface gif`
411. Se utilizan las interfaces “gifX”, que son las que tiene reservadas el sistema para túneles entre los protocolos IPv4 e IPv6.
412. Para completar la configuración, debe añadirse la interfaz de túnel en el panel de control de red (34) (Preferencias del Sistema > Red). En el panel de la izquierda se pulsa sobre “+” y se añade la interfaz 6to4.



## 8.4. TRADUCCIÓN DE DIRECCIONES IPV6

413. De la misma forma que ocurre en Windows, en Mac OS también se pueden configurar servidores DNS para que hagan la traducción de direcciones IPv6. En el caso de Mac OS no tiene direcciones asignadas por defecto para servidores DNS IPv6. Si fuera necesario añadirlos lo haríamos desde la configuración de red en la interfaz que se use para la conexión a internet:



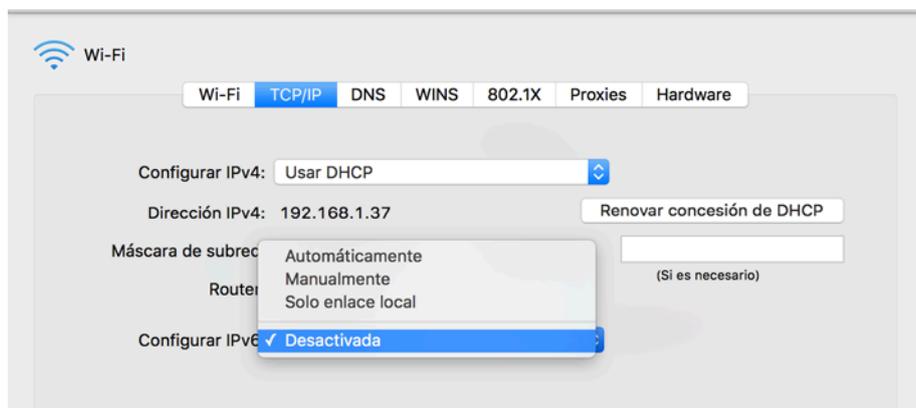
## 8.5. DESHABILITAR IPV6 Y SUS COMPONENTES

414. Para desactivar IPv6 si se accede a las preferencias de red, en las interfaces que estén activas en opciones avanzadas dentro de TCP/IP, se ve que la opción para deshabilitarlo no se encuentra disponible por defecto (35).



415. Sin embargo, esta opción está solo oculta, y puede ser activada por medio del interfaz de comandos (35) (36).

```
MacBook-Pro-de-Andrea:~ apantojab$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
Thunderbolt Ethernet
Wi-Fi
iPhone USB
Bluetooth PAN
Thunderbolt Bridge
MacBook-Pro-de-Andrea:~ apantojab$ networksetup -setv6off Wi-Fi
MacBook-Pro-de-Andrea:~ apantojab$
```



## 8.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR

| VULNERABILIDAD                                         | MEDIDA                                                                                                    |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Ataques de tipo SLAAC                                  | Activar el "modo encubierto" en el firewall del ordenador para evitar la recepción de mensajes de sondeo. |
| Dispositivo de filtrado no bloquea el tráfico saliente | Firewall activado para filtrar el tráfico saliente.                                                       |
| Vulnerabilidades de túneles                            | No habilitar la utilización de túneles en los sistemas.                                                   |

## 9. CONFIGURACIÓN DE SISTEMAS LINUX

### 9.1. INSTALACIÓN Y CONFIGURACIÓN DE IPV6 EN EL EQUIPO

#### 9.1.1. INSTALACIÓN DE IPV6

416. En Linux IPv6 se implementa como un módulo kernel. Las distribuciones con kernel 2.4.X ya dan este soporte y el módulo IPv6 en este caso ya viene instalado (37). En el caso de que dicho módulo no se encuentre activado se debe activar manualmente de la siguiente forma.
417. Primero se abre una ventana de terminal y se ejecuta el siguiente comando: `test -f /proc/net/if_inet6 && echo "Si activado"`. Si nos devuelve el mensaje "si activado" quiere decir que el módulo IPv6 ya está operativo, de lo contrario se debería activar.
418. Para la activación manual se debe escribir `modprobe ipv6`, con privilegios de usuario root. Para que el módulo IPv6 cargue automáticamente cuando se inicia el sistema, se agrega la palabra IPv6 al final del archivo `/etc/modules`.
419. Tras cargar el módulo, se comprueba que se haya hecho de manera correcta ejecutando `lsmod | grep -w 'ipv6' && echo "el modulo fue cargado"`.

#### 9.1.2. OBTENCIÓN DE DIRECCIÓN IPV6

420. La asignación de la dirección IPv6 se realiza de forma completamente automática. Existen diferentes maneras (38), todas implementadas dentro de IPv6 y en las que el usuario no tiene que participar, que se explican a continuación:

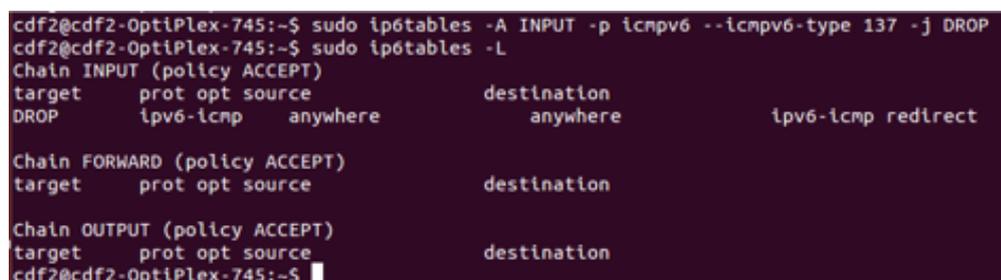
- SLAAC sin router (encaminar tráfico dentro de la red local): el adaptador de red no encuentra un router que le suministre una dirección IPv6, por lo tanto la dirección local se construye utilizando un algoritmo (en IPv6 la dirección configurada empezará siempre por FE80::).
- SLAAC con router (encaminar tráfico fuera de la red local): se construye la dirección IPv6 basándose en el paquete "Router Advertisement" que envía el router IPv6 conectado al mismo segmento de red.
- Configuración automática DHCPv6: con DHCPv6 un equipo puede recibir una dirección IPv6 además de otros parámetros de configuración. Esta opción puede establecerse utilizando un servidor o un router que pueda ejercer de tal. Un uso común de DHCPv6 es recibir y configurar automáticamente la dirección IPv6 de los servidores DNS, los cuales no se reciben a través del paquete Router Advertisement que envían los routers IPv6 de la red. El paquete Router Advertisement que recibe el equipo durante la fase de descubrimiento de routers contiene un campo que indica si se va a utilizar también DHCPv6 para configurar la dirección IPv6.

### 9.1.3. CONFIGURACIÓN DE IPV6

#### 9.1.3.1. ICMP

421. El protocolo de ICMP utilizado en IPv6 es ICMPv6 (39). Este protocolo lo utilizan los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico de red.
422. Falsificando los mensajes de este protocolo se puede atacar la red objetivo. La utilización de paquetes de redireccionamiento falsos es una técnica común en redes IPv6, por lo que es conveniente desactivar la aceptación de este tipo de paquetes.
423. En Linux, para filtrar este tipo de paquetes se puede utilizar Netfilter (40), un framework disponible en el kernel Linux que permite interceptar y manipular paquetes de red. El componente más popular construido sobre Netfilter es iptables (41), una herramienta cortafuegos incluida en el kernel desde la versión 2.4, que permite filtrar paquetes. Para IPv6 se utiliza la versión ip6tables (42). La configuración para filtrar los paquetes ICMPv6 de redireccionamiento es realmente sencilla, simplemente se debe añadir una regla al cortafuegos ejecutando la siguiente línea de código (43):

```
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 137 -j DROP
```



```

cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 137 -j DROP
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP ipv6-icmp anywhere anywhere ipv6-icmp redirect

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
cdf2@cdf2-OptiPlex-745:~$

```

424. Como se puede ver, se ha añadido la regla al cortafuegos que ha traducido el tipo de paquete ICMPv6 137 (44) como paquete de redireccionamiento, a la tabla de tráfico de entrada.

425. El protocolo ICMP es también utilizado para el descubrimiento de vecinos y puede usarse en un ataque a nuestra red o bien falsificando los paquetes o bien inundando la tabla de los vecinos. Para evitar este tipo de ataques se debe añadir unas nuevas reglas al cortafuegos (45) que permiten aceptar este tipo de mensajes únicamente si provienen realmente de un vecino [RFC 4861]. Para ello se ejecutan la siguientes líneas:

```
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 134 -hl --hl-eq 255 -j ACCEPT
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 135 -hl --hl-eq 255 -j ACCEPT
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 136 -hl --hl-eq 255 -j ACCEPT
```

```
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 134 -m hl --hl-eq 255 -j ACCEPT
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 135 -m hl --hl-eq 255 -j ACCEPT
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 136 -m hl --hl-eq 255 -j ACCEPT
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT ipv6-icmp anywhere anywhere ipv6-icmp router-advertisement HL match HL == 255
ACCEPT ipv6-icmp anywhere anywhere ipv6-icmp neighbour-solicitation HL match HL == 255
ACCEPT ipv6-icmp anywhere anywhere ipv6-icmp neighbour-advertisement HL match HL == 255

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
cdf2@cdf2-OptiPlex-745:~$
```

426. Lo que se hace es asegurarse de que los mensajes recibidos tengan un Hop Limit de 255.
427. Para evitar el agotamiento de la tabla de ND por inundación, se debe poner un límite de paquetes por minuto a los tres tipos 134, 135 y 136, y se rechazarán todos los que lo excedan. Para hacer esto hay que repetir el procedimiento anterior, esta vez con el siguiente comando:

```
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 134 -m limit --limit 500/min -j ACCEPT
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 135 -m limit --limit 500/min -j ACCEPT
sudo ip6tables -A INPUT -p icmpv6 --icmpv6-type 136 -m limit --limit 500/min -j ACCEPT
```

### 9.1.3.2. Multicast

428. En IPv6 ya no existe el broadcast, únicamente hay multicast, unicast y anycast. Para la configuración segura hay que prestar atención al multicast, ya que puede utilizarse para ataques de tipo Denegación de Servicio (DDoS). Para las comunicaciones multicast se utilizan paquetes MLD (Multicast Listener Discovery) que están encapsulados en los paquetes de ICMP. Por lo tanto, y de manera similar a ICMPv6, se deben rechazar los paquetes que provengan de una dirección multicast. El método es el siguiente (46):

```
sudo ip6tables -A INPUT -m pkttype --pkt-type multicast -j DROP
```

```
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -A INPUT -m pkttype --pkt-type multicast -j DROP
cdf2@cdf2-OptiPlex-745:~$ sudo ip6tables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP ipv6-icmp anywhere anywhere ipv6-icmp redirect
DROP all anywhere anywhere PKTTYPE = multicast

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
cdf2@cdf2-OptiPlex-745:~$
```

429. En este caso tenemos configuradas tanto la regla anterior (evitar paquetes de redireccionamiento) como la recepción de paquetes multicast.
430. Si se quiere poder recibir paquetes que provengan de una dirección multicast pero evitar responder a los mismos, simplemente se debería cambiar en el comando anterior INPUT por OUTPUT.

## 9.2. COMPROBACIÓN DE CONECTIVIDAD BÁSICA DE IPV6

431. Para comprobar la conectividad de IPv6 en el equipo se realizará una verificación de la misma mediante el comando ping. Este comando chequea la dirección destino que se desea alcanzar, enviando peticiones de eco (echo request). Si la máquina destino está operativa, esta dará una respuesta por su parte junto al retardo de la operación.
432. En este caso se hará un comando ping a la dirección de loopback (::1), que es la que utilizan las máquinas para enviarse paquetes a sí mismas, otro a la dirección del link local y finalmente a una dirección externa a la red local.
433. Se abre una ventana de terminal y se ejecuta el siguiente comando:

```
ping6 -c 6 ::1
```

```
cdf2@cdf2-OptiPlex-745:~$ ping6 -c 6 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.039 ms
64 bytes from ::1: icmp_seq=4 ttl=64 time=0.080 ms
64 bytes from ::1: icmp_seq=5 ttl=64 time=0.037 ms
64 bytes from ::1: icmp_seq=6 ttl=64 time=0.042 ms

--- ::1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4998ms
rtt min/avg/max/mdev = 0.032/0.044/0.080/0.017 ms
cdf2@cdf2-OptiPlex-745:~$
```

434. Para conocer la dirección local, simplemente se debe ejecutar el comando ifconfig en el terminal.
435. Se selecciona la dirección que empieza por fe80:: que es la que se ha generado automáticamente con el algoritmo SLAAC sin router y se realiza el ping:

```
ping6 -c 6 -I eth0 fe80::21a:a0ff:fee8:ef19
```

```
cdf2@cdf2-OptiPlex-745:~$ ping6 -c 6 -I eth0 fe80::21a:a0ff:fee8:ef19
PING fe80::21a:a0ff:fee8:ef19(fe80::21a:a0ff:fee8:ef19) from fe80::21a:a0ff:fee8:ef19 eth0: 56 data bytes
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=3 ttl=64 time=0.045 ms
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=4 ttl=64 time=0.047 ms
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from fe80::21a:a0ff:fee8:ef19: icmp_seq=6 ttl=64 time=0.040 ms

--- fe80::21a:a0ff:fee8:ef19 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.030/0.044/0.055/0.008 ms
cdf2@cdf2-OptiPlex-745:~$
```

```
ping6 -c 6 ipv6.google.com
```

```

cdf2@cdf2-OptiPlex-745:~$ ping6 -c 6 ipv6.google.com
PING ipv6.google.com(mad01s24-in-x0e.1e100.net) 56 data bytes
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=1 ttl=56 time=2.34 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=2 ttl=56 time=2.36 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=3 ttl=56 time=2.32 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=4 ttl=56 time=2.30 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=5 ttl=56 time=2.41 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=6 ttl=56 time=2.36 ms

--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 2.307/2.355/2.417/0.052 ms
cdf2@cdf2-OptiPlex-745:~$

```

### 9.3. CONFIGURACIÓN DE TÚNELES EN IPV6

#### 9.3.1. TEREDO

436. Este mecanismo tiene como objetivo dar conectividad IPv6 a los usuarios que están detrás de un NAT y que, por tanto, el host tiene una IP privada.
437. Con los túneles Teredo (47) lo que se consigue es proporcionar direcciones IPv6 a hosts IPv4 a través de una o más capas NAT, creando túneles sobre el protocolo UDP. Se encapsulan paquetes IPv6 dentro de datagramas UDP-IPv4 para poder atravesar los dispositivos NAT y la red IPv4.
438. A día de hoy Teredo no viene configurado por defecto en Linux, por lo que se debe activar manualmente. Para configurar Teredo se va a utilizar Miredo, el cliente de Teredo para Linux.
439. En primer lugar lo que se hará será instalar el paquete de Miredo (48), que está incluido en la librería de Linux:
 

```

sudo apt-get update
sudo apt-get install miredo

```
440. Para seguir se debe seleccionar un servidor hacia el cual se quiere hacer el túnel. Por defecto en Linux viene activado el de `teredo.remlab.net / teredo-debian.remlab.net` (Alemania), que es aconsejable, pero existen otros que también pueden ser una opción:
  - `teredo.ngix.ne.kr` (Corea del Sur)
  - `teredo.managemydedi.com` (EEUU, Chicago)
  - `teredo.trex.fi` (Finlandia)
  - `teredo.ipv6.microsoft.com`
441. Para configurar el servidor (49) se debe abrir en el editor de texto el fichero de configuración de miredo:
 

```

sudo gedit /etc/miredo.conf

```

```
miredo.conf x
Please refer to the miredo.conf(5) man page for details.
InterfaceName teredo

Pick a Teredo server:
#ServerAddress teredo.ipv6.microsoft.com
ServerAddress teredo-debian.remlab.net

Some firewall/NAT setups require a specific UDP port number:
#BindPort 3545
```

442. Se ve que por defecto viene activado el server de debían. Para cambiarlo únicamente habría que comentar esa línea y añadir: ServerAddress DIRECCIÓN\_SERVIDOR
443. En caso de que se hay hecho algún cambio en el fichero de configuración se debe reiniciar el servicio miredo:

```
sudo /etc/init.d/miredo restart
```

444. Finalmente se puede comprobar que se ha creado el túnel teredo ejecutando ifconfig

```
cdf2@cdf2-OptiPlex-745:~$ ifconfig teredo
teredo Link encap:UNSPEC direcciónHW 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
Dirección inet6: 2001:0:53aa:64c:18b0:4546:75fb:f863/32 Alcance:Global
Dirección inet6: fe80::ffff:ffff:ffff/64 Alcance:Enlace
ACTIVO PUNTO A PUNTO FUNCIONANDO NOARP MULTICAST MTU:1280 Métrica:1
Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:4 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colaTX:500
Bytes RX:0 (0.0 B) TX bytes:304 (304.0 B)
```

teredo:

445. Para comprobar el correcto funcionamiento se fuerza un ping a una dirección IPv6:

```
ping6 -c 6 ipv6.google.com
```

```
cdf2@cdf2-OptiPlex-745:~$ ping6 -c 6 ipv6.google.com
PING ipv6.google.com(mad01s24-in-x0e.1e100.net) 56 data bytes
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=1 ttl=56 time=2.34 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=2 ttl=56 time=2.36 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=3 ttl=56 time=2.32 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=4 ttl=56 time=2.30 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=5 ttl=56 time=2.41 ms
64 bytes from mad01s24-in-x0e.1e100.net: icmp_seq=6 ttl=56 time=2.36 ms

--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 2.307/2.355/2.417/0.052 ms
cdf2@cdf2-OptiPlex-745:~$
```

446. Teredo sólo puede proporcionar una dirección IPv6 única por túnel a un punto final. Como tal, no es posible utilizar un único túnel Teredo para conectar varios hosts.
447. Para que los túneles Teredo funcionen los cortafuegos no deben filtrar los paquetes UDP entrantes ni salientes.
448. Con la utilización de estos túneles se deben evitar los ataques tipo SLAAC configurándolo de manera segura. Para ello lo que se debe hacer es filtrar con iptables

el tráfico de tipo 134 “Router Advertisement”, descartando todo el que no tenga un Hop Limit de 255, como bien se indica en el apartado 10.1.3.1.

449. Deshabilitar Teredo: esta operación es muy sencilla, simplemente se debe realizar el comando `sudo apt-get remove miredo` y reiniciar el sistema para que se guarden los cambios realizados con el comando `sudo reboot`.

### 9.3.2. CONFIGURACIÓN DE ISATAP

450. Como ya se ha comentado, es necesaria una configuración del router ISATAP (traducción y reenvío de peticiones), que desde el host final no se puede realizar.
451. Sí que se puede hacer configuración como cliente de ISATAP (50), que es relativamente sencilla, y que consiste en activar la interfaz de ISATAP. Debe especificarse la dirección del router ISATAP cuando se cree el túnel, esto se hace especificando la opción `v4any` en el comando `ip`:

```
ip tunnel add is0 mode isatap local V4ADDR_NODE v4any V4ADDR_RTR ttl 64
ip link set is0 up
```

452. Los clientes solicitarán la información de dirección y ruta del router ISATAP y automáticamente se configurarán ellos mismos para el acceso IPv6.
453. De la misma forma que en teredo, se debe aplicar una regla en el firewall `ip6tables` que bloquee el tráfico “Router Advertisement” con un Hop limit distinto de 255. También debe tenerse en cuenta que los paquetes tendrán protocolo tipo 41, lo que ayudará al filtrado.

### 9.3.3. CONFIGURACIÓN DE 6TO4

454. El mecanismo de tunelización `6to4` envía los paquetes IPv6 encapsulados dentro de paquetes IPv4 con protocolo tipo 41. Se utilizan diversos servidores distribuidos por el mundo con la dirección IP `anycast 192.88.99.1` que están conectados tanto a la red IPv4 como a la red IPv6. Los mismos reciben paquetes IPv6 encapsulados en paquetes IPv4 y los reenvían a la red IPv6, realizando el proceso inverso con las respuestas. En resumen, `6to4` conecta una red IPv6 con otra red IPv6 utilizando la infraestructura IPv4 existente (51).
455. Las direcciones `6to4` tienen la siguiente estructura: `2002:XXXX:YYYY::/16`, donde `XXXX:YYYY` son los 32 bits de la dirección IPv4 en formato hexadecimal (52). De esta forma, al convertir la dirección a IPv6, el router necesita saber a qué dirección debe dirigirse el paquete IPv4 generado.
456. Para la configuración del túnel `6to4`, en primer lugar se debe conocer la dirección IPv4. Con el comando `ifconfig` se muestran las interfaces y se coge la dirección `inet` local.
457. Una vez se tiene la dirección IPv6 hay que convertirla a formato IPv6, para esto hay dos formas:
  - Se puede pasar término a término a hexadecimal de forma manual y luego colocarlos de la forma mencionada anteriormente. Como ejemplo se cogerá la dirección `138.4.7.156` que en hexadecimal es: `8A.04.07.9C` y que por lo tanto quedaría como resultado: `2002:8a04:079c::/16`.

- Por otro lado, se puede hacer el mismo mecanismo pero de forma automática ejecutando en el terminal el siguiente comando:

```
printf "2002:%02x%02:%x%02x\n" DIRECCIÓN_IPv4
```

458. Una vez se tiene la dirección IPv6 correspondiente hay que editar el fichero /etc/network/interfaces y añadir la nueva interfaz túnel 6to4. El procedimiento es el siguiente:

```
sudo gedit /etc/network/interfaces
```

459. En el archivo se añaden las siguientes líneas:

```
auto tun6to4
iface tun6to4 inet6 v4tunnel
 address 2002:XXXX:YYYY::1
 netmask 16
 gateway ::192.88.99.1
 endpoint any
 local DIRECCIÓN_IPv4_LOCAL
```

```
interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto tun6to4
iface tun6to4 inet6 v4tunnel
 address 2002:8a04:079c::1
 netmask 16
 gateway ::192.88.99.1
 endpoint any
 local 138.4.7.156
```

460. Una vez se ha editado y guardado los cambios del fichero, se reinicia el sistema con sudo reboot. Al hacer ifconfig se puede ver como se ha creado la nueva interfaz. Se habilita el dispositivo tun6to4 con ifup tun6to4.

```
tun6to4 Link encap:IPv6-en-IPv4
 Dirección inet6: 2002:8a04:79c::1/16 Alcance:Global
 Dirección inet6: ::138.4.7.156/96 Alcance:Compatibilidad
 ACTIVO FUNCIONANDO NOARP MTU:1480 Métrica:1
 Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
 Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
 colisiones:0 long.colaTX:0
 Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)
```

461. Aquí se muestra el túnel 6to4 creado con la dirección que se ha configurado previamente. Tiene un alcance global y como indica, encapsula IPv6 en Ipv4.
462. Como se ha dicho previamente, el paquete IPv4 en el que va encapsulado el de IPv6 tiene protocolo tipo 41, por lo tanto se debe filtrar el contenido de ese tipo de paquetes para asegurarse de que no son maliciosos, teniendo en cuenta que el puerto origen/destino será 192.88.99.0\24.

463. Debe evitarse la utilización de este mecanismo, al igual que la de los mecanismos anteriores, y en caso de tener que llevarse a cabo, es imprescindible asegurarlo filtrando el tráfico y asegurándolo con IPsec.

#### 9.4. TRADUCCIÓN DE DIRECCIONES IP

464. Una parte importante del uso de IPv6 en redes IPv4, es la traducción de direcciones IP. Es por ello, que se pueden configurar en el equipo servidores DNS diferentes a los que ofrece el proveedor de servicio de Internet.
465. La función más conocida de los protocolos DNS es la de asignar nombres a las direcciones IP para poder acceder a diferentes sitios de manera más sencilla sin tener que recordar valores numéricos (53). El usuario final casi nunca se comunica directamente con el servidor DNS, sino que la resolución de los nombres la llevan a cabo las aplicaciones. La mayoría de los usuarios utilizan como servidor DNS el que les proporciona su ISP (proveedor de servicio de Internet). Pero a través del protocolo DHCPv6 estos servidores pueden ser configurados de manera manual.
466. Se va a poner el ejemplo con la conexión a los servidores públicos que google puso a disposición de los usuarios en 2009. Aclarar que no se recomienda por seguridad la utilización de servidores públicos sin saber que son fiables al 100%, pero dentro de los servidores públicos, los de google son sin duda una de las mejores opciones en este campo.
1. Desde el menú de preferencias hay que buscar el apartado conexiones de red, o hacer clic en el icono de red del panel superior y después en editar las conexiones
  2. Se selecciona la conexión a editar (ethernet o inalámbrica), y se hace clic en la pestaña IPv4
  3. En la opción método se selecciona Sólo direcciones automáticas (DHCP)
  4. En el campo servidores DNS se escriben las direcciones 8.8.8.8 y 8.8.4.4 separadas por un espacio
  5. Se repite lo mismo pero en la pestaña de IPv6 con las direcciones 2001:4860:4860::8888 y 2001:4860:4860::8844
  6. Guardar los cambios.

#### 9.5. DESHABILITAR IPV6 Y SUS COMPONENTES

467. Para deshabilitar IPv6 en el equipo existen dos mecanismos (54):

##### 9.5.1. DESHABILITARLO DESDE SYSCTL

468. Con este método se editan ciertos parámetros a nivel del kernel a través de la interfaz sysctl.
469. Se abre una ventana del terminal y se ejecuta el siguiente comando para editar el fichero sysctl.conf que se encuentra dentro de /etc:
- ```
sudo gedit /etc/sysctl.conf
```
470. Una vez abierto el editor de texto con el contenido del fichero se añaden las siguientes líneas al final:

```
# IPv6 disabled
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

471. Se guardan los cambios y se reinicia la interfaz sysctl con el siguiente comando:

```
sudo sysctl -p
```

472. Con ifconfig se puede ver el resultado, sin dirección IPv6 ni de loopback ni local:

```
cdf2@cdf2-OptiPlex-745:~$ sudo sysctl -p
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
cdf2@cdf2-OptiPlex-745:~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 00:1a:a0:e8:ef:19
          Direc. inet:138.4.7.156  Difus.:138.4.7.255  Másc:255.255.255.128
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:60205 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:39089 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:55480418 (55.4 MB)  TX bytes:4849193 (4.8 MB)
          Interrupción:16

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:6211 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:6211 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:911311 (911.3 KB)  TX bytes:911311 (911.3 KB)

cdf2@cdf2-OptiPlex-745:~$
```

473. Posteriormente, se reinicia el sistema con `sudo reboot`. Para volver a habilitar IPv6 tras haberlo deshabilitado, se abre el fichero `sysctl.conf` como anteriormente se indica:

```
sudo gedit /etc/sysctl.conf
```

474. Se comentan las líneas anteriormente añadidas y se introduce lo siguiente:

```
net.ipv6.conf.all.forwarding=1
```

475. Se guardan los cambios y se reinicia de nuevo la interfaz sysctl con el siguiente comando:

```
sudo sysctl -p
```

476. Por último, se reinicia el sistema con `sudo reboot`.

9.5.2. DESHABILITARLO DESDE EL FICHERO DE CONFIGURACIÓN GRUB

477. Desde una ventana de terminal se ejecuta el comando:

```
sudo gedit /etc/default/grub
```

478. Dentro del fichero se busca la línea que contenga “GRUB_CMDLINE_LINUX” y se edita de forma que quede como sigue:

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

479. También se puede hacer el mismo cambio al valor de la variable “GRUB_CMDLINE_LINUX_DEFAULT”.
480. Se guardan los cambios, se cierra el editor de texto y en el terminal se regenera la configuración de GRUB:
- ```
sudo update-grub
```
481. Por último, se reinicia el sistema con `sudo reboot`. Para volver a habilitar IPv6 tras haberlo deshabilitado, simplemente se debe volver a poner la variable con el mismo valor que tenía previamente y se vuelve a guardar los cambios con `sudo update-grub`. Se reinicia el sistema con `sudo reboot`.

## 9.6. TABLA RESUMEN DE VULNERABILIDADES Y MEDIDAS A TOMAR

| VULNERABILIDAD                                                                 | MEDIDA                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ataques de tipo SLAAC                                                          | Dos medidas: <ul style="list-style-type: none"> <li>Desactivar IPv6.</li> <li>Filtrar con ip6tables el tráfico tipo 134 “Router Advertisement”</li> </ul>                                                                                                  |
| Dispositivo de filtrado no bloquea el tráfico saliente                         | Con ip6tables, filtrar el tráfico saliente.                                                                                                                                                                                                                |
| Dispositivo de filtrado no filtra túneles IPv6                                 | Desactivar las interfaces de tunelización.                                                                                                                                                                                                                 |
| La red acepta paquetes ICMPv6 de redireccionamiento falsos                     | Filtrar la recepción de paquetes de redireccionamiento con ip6tables.                                                                                                                                                                                      |
| Ataque DoS mediante el reflector de dirección destino multicast (ataque smurf) | Filtrar la recepción de paquetes que provengan de una dirección multicast con el cortafuegos.                                                                                                                                                              |
| Ataque sobre neighbour discovery (ND)                                          | Filtrar los mensajes: <ul style="list-style-type: none"> <li>Router Advertisement (RA)</li> <li>Neighbour Solicitation (NS)</li> <li>Neighbour Advertisement (NA)</li> </ul> Para asegurarse de que el Hop Limit es 255 y realmente proviene de un vecino. |
| Agotamiento de la tabla ND (Neighbour discovery) por inundación                | Poner un límite de paquetes por minuto de los tipos RA, NS y MNA. Descartar lo que excedan.                                                                                                                                                                |
| Desbordamiento de la memoria en Teredo                                         | Con el cortafuegos, filtrar el tráfico del puerto 3544.                                                                                                                                                                                                    |

## 10. CONFIGURACIÓN DE SISTEMAS MÓVILES (ANDROID Y IOS)

### 10.1. CONECTIVIDAD BÁSICA IPV6 ANDROID

#### 10.1.1. PROBLEMAS DE CONECTIVIDAD IPV6

482. A la hora de buscar una manera básica de implementar conectividad IPv6 en Android, nos encontramos con un problema: Android a la fecha de redacción de este documento

no da soporte a DHCPv6. Esto conlleva a que tengamos problemas de implementación IPv6 y de seguridad.

483. Para la gestión de redes, en particular para lugares con una política de BYOD (bring your own device), la ausencia de soporte del estándar DHCPv6 afecta significativamente. Con la llegada de Android 5.0 se introdujo RDNSS (recursive DNS server) y se dijo que era un buen sustituto de DHCPv6, y es cierto que provee un método administrativo que puede utilizarse en su lugar, pero sigue siendo algo no usado en la mayoría de los casos.
484. Aunque es posible desplegar una red con RDNSS y DHCPv6, no es nada recomendable, ya que implica la aparición de algunos problemas e introduce posibles agujeros de seguridad. Por ejemplo, un atacante puede simplemente hacerse pasar por el servidor recursivo DNS local mediante el envío de falsos mensajes Router Advertisement que incluyen la opción RDNSS correspondiente, y luego realizar un ataque de spoofing DNS para una атака de Man in the Middle interceptar el tráfico correspondiente.

#### 10.1.2. CONEXIÓN MANUAL A IPV6 DESDE EL TERMINAL (SIN ROOTEAR)

485. Sólo algunas compañías ofrecen la posibilidad de conectarse a través de un APN (Access Point Names) con IPv6. En España, la compañía IPv6 Móvil, facilita una guía: [http://www.ipv6movil.com/manuales/manual\\_apn\\_android\\_ipv6.pdf](http://www.ipv6movil.com/manuales/manual_apn_android_ipv6.pdf)

#### 10.1.3. SOLUCIÓN DE PROBLEMAS DE CONECTIVIDAD

486. Desafortunadamente, no hay muchas formas de solucionar este problema, y para todas nos será necesario el roteo del terminal. Sólo hay un único proveedor de Android que apoya DHCPv6 y es Fairphone, un proyecto de acción social que está creando un terminal ambientalmente y económicamente responsable. La solución que ellos han dado es incluir WIDE-DCHPv6 (proyecto que libera/desarrolla/mantiene al día la implementación de DHCPv6 para BSD y Linux), que ha sido también implementada como un APK por un desarrollador independiente. Esto está disponible como DHCPv6 Client en el Google Play Store, pero requiere permisos de root.
487. En un futuro se espera que Android dé un mejor soporte a DHCPv6 y por tanto a IPv6 de manera más segura, lo que derivará en la posibilidad de una mejor configuración del protocolo a nivel de usuario con más posibilidades de desarrollo cosa que hoy por hoy no está disponible.

### **10.2. CONECTIVIDAD BÁSICA EN IOS**

488. El sistema operativo iOS sí que da un gran soporte y prioridad a IPv6, dejando cada vez más atrás el uso de la versión 4. Tanto es así que en la presentación en 2015 de iOS 9, anunciaron que todas las aplicaciones deben dar soporte a IPv6, ya sea como una red IPv6 única o dual IPv4/IPv6. Cualquier aplicación que desde comienzos de 2016 no cumpla esta condición, no es admitida en el Apple Store. De esta forma, no solo se obliga al uso de los frameworks propios de Apple para red, si no que se prohíbe el uso de APIs específicas que utilicen IPv4 o incluir direcciones en dicho protocolo directamente en la aplicación. Las aplicaciones que no almacenen direcciones IP o las utilicen para identificar usuarios, etc. No tiene que cambiar nada de desarrollo en la aplicación porque funcionará de por sí.

489. Para que los desarrolladores puedan probar si sus aplicaciones funcionan en redes IPv6, la próxima versión de MAC OS X dará la posibilidad de generar un WiFi hotspot personal, únicamente con IPv6, y que se podrá utilizar para dicha comprobación.
490. Para iOS es realmente importante el soporte de IPv6 por el hecho de que las redes 4G estén basadas en el intercambio de paquetes y que al mismo tiempo las direcciones IPv4 se estén agotando, lo que hace IPv6 necesario para que sea posible el desarrollo de manera escalable del 4G.

### 10.2.1. CONEXIÓN MANUAL A IPV6 DESDE EL TERMINAL (SIN ROOTEAR)

491. De la misma forma que lo visto anteriormente, en España casi ninguna compañía telefónica da prácticamente ninguna posibilidad para configurar IPv6 en nuestro terminal. La misma compañía que para Android, IPv6 Movil, nos deja su propia guía, en este caso para IOs:

[http://www.ipv6movil.com/manuales/manual\\_apn\\_apple\\_ipv6.pdf](http://www.ipv6movil.com/manuales/manual_apn_apple_ipv6.pdf)

492. Existe también una aplicación llamada “IPv6 Toolkit” de pago, que realiza un diagnóstico de la red y nos proporciona una dirección IPv6, pero no da conectividad real. Aquí están las características del Apple Store:

| Descripción                                                                          |
|--------------------------------------------------------------------------------------|
| IPv6 is here!                                                                        |
| IPv6 Toolkit is a network diagnostic tool with the following features:               |
| – Displays all network interfaces on your iPhone or iPod Touch                       |
| – Ping IPv4 and IPv6 addresses                                                       |
| – DNS Lookup (Forward and Reverse queries)                                           |
| – Network Connections (netstat)                                                      |
| – Displays the IPv6 Route Table                                                      |
| – Displays all IPv4, IPv6, and Link-Layer addresses for available network interfaces |
| – Displays IPv6 Neighbors, the IPv6 equivalent of ARP                                |
| – Listens for IPv6 Router Advertisements                                             |
| – Supports copying from all data fields                                              |

493. Finalmente, y tras el estudio de la conectividad IPv6 para terminales iOS, la conclusión es que hoy por hoy no podemos configurar parámetros que permitan conectarnos a IPv6 de manera más segura. Se dan consejos a nivel de desarrollador de cómo configurar las aplicaciones para que soporten IPv6, pero como usuarios no tenemos muchas opciones.
494. En el futuro, cuando esté más extendido el protocolo IPv6 para redes móviles, se espera que el usuario pueda hacer configuraciones personales sobre su terminal para conectarse de manera segura a la red.

## 11. REFERENCIAS

1. *Informe de amenazas CCN-CERT IA-12/12 - IPv6*. **CCN-CERT**. 2012.
2. **IETF**. Internet Protocol Version 6 (IPv6) Addressing Architecture. [En línea] <https://tools.ietf.org/html/rfc3513>.
3. **TNO**. Testing the security of IPv6 Implementations. *www.tno.nl*. [En línea] 2014. [https://www.tno.nl/media/3274/testing\\_the\\_security\\_of\\_ipv6\\_implementations.pdf](https://www.tno.nl/media/3274/testing_the_security_of_ipv6_implementations.pdf).
4. **National Institute of Standards and Technology - NIST**. Guidelines for the Secure Deployment of IPv6. [En línea] 2010. <http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf>.
5. **Cisco**. IPv6 Implementation Guide, Cisco IOS Release 15.2S. *www.cisco.com*. [En línea] <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book.html>.
6. —. IPv6 ACL Extensions for Hop by Hop Filtering. *www.cisco.com*. [En línea] [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_acl/configuration/xs-3s/sec-data-acl-xs-3s-book/ipv6-acl-ext-hbh-xs.pdf](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xs-3s/sec-data-acl-xs-3s-book/ipv6-acl-ext-hbh-xs.pdf).
7. Blog El valle del viento helado. *Controlando el firewall de Windows en la Línea de*. [En línea] <http://icewinddale.blogspot.com.es/2008/05/controlando-el-firewall-de-windows-en.html>.
8. Wikipedia. *Multicast Listener Discovery*. [En línea] [https://en.wikipedia.org/wiki/Multicast\\_Listener\\_Discovery](https://en.wikipedia.org/wiki/Multicast_Listener_Discovery).
9. Wikipedia. *ICMPv6*. [En línea] <https://es.wikipedia.org/wiki/ICMPv6>.
10. DIT UPM. *Direcciones Multicast*". [En línea] <http://web.dit.upm.es/~jmseyas/linux/mcast.como/Multicast-Como-2.html>.
11. Blog Pcactual. *Prepara tu equipo para el nuevo protocolo IPv6*". [En línea] [http://www.pcactual.com/articulo/zona\\_practica/paso\\_a\\_paso/paso\\_a\\_paso\\_internet/11120/prepara\\_equipo\\_para\\_nuevo\\_protocolo\\_ipv6.html](http://www.pcactual.com/articulo/zona_practica/paso_a_paso/paso_a_paso_internet/11120/prepara_equipo_para_nuevo_protocolo_ipv6.html).
12. Wikipedia. *Teredo* . [En línea] <https://es.wikipedia.org/wiki/Teredo>.
13. TechNet. *Internet Protocol Version 6, Teredo, and Related Technologies*". [En línea] [https://technet.microsoft.com/es-es/library/cc722030\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/cc722030(v=ws.10).aspx).
14. **Fernandez, Andres Palma**. Youtube. *Teredo Windows 7* . [En línea] <https://www.youtube.com/watch?v=LjK16SQDuuQ>.
15. Blog Lobobinario. *Notas de Seguridad en IPv6: Seguridad en los paquetes IP*". [En línea] [http://lobobinario.blogspot.com.es/2011/05/notas-de-seguridad-en-ipv6-seguridad-en\\_14.html](http://lobobinario.blogspot.com.es/2011/05/notas-de-seguridad-en-ipv6-seguridad-en_14.html).
16. Ispcolohost. *How to disable IPv6 stateless autoconfig on Windows 7*. [En línea] <http://www.ispcolohost.com/2013/07/06/how-to-disable-ipv6-stateless-autoconfig-on-windows-7/>.
17. The Cable Guy. *Migración de la intranet a IPv6 con ISATAP*. [En línea] <https://technet.microsoft.com/es-es/magazine/2008.03.cableguy.aspx>.
18. **Hiếu, Phạm Trung**. Youtube. *Configuring ISATAP pt 1*. [En línea] <https://www.youtube.com/watch?v=Dw9t-Mdy4ww>.
19. **Hick, Richard**. Richard Hick's Direct Access Blog. *DirectAccess Manage Out from Windows 10 Does Not Work*. [En línea] <https://directaccess.richardhicks.com/category/isatap/>.

20. MSDN. *Tráfico IPv6 entre nodos de sitios diferentes en Internet (6to4)*. [En línea] [https://msdn.microsoft.com/es-es/library/cc779985\(v=ws.10\).aspx](https://msdn.microsoft.com/es-es/library/cc779985(v=ws.10).aspx).
21. TechNet. *Pv6 for the Windows Administrator: The 2002: (6to4 Tunnel) Address and its impact*. [En línea] <https://blogs.technet.microsoft.com/askpfeplat/2013/11/17/ipv6-for-the-windows-administratorthe->.
22. MSDN. *Elementos de configuración de IPv6*. [En línea] [https://msdn.microsoft.com/es-es/library/cc783049\(v=ws.10\).aspx](https://msdn.microsoft.com/es-es/library/cc783049(v=ws.10).aspx).
23. Microsoft Support. *How to disable IPv6 or its components in Windows*. [En línea] <https://support.microsoft.com/en-us/kb/929852>.
24. The Cable Guy. *Source and Destination Address Selection for IPv6*. [En línea] <https://technet.microsoft.com/library/bb877985.aspx>.
25. Geek By The System. *Direcciones IPv6 ULA*. [En línea] <http://madrigaladmin.blogspot.com.es/2011/05/direcciones-ipv6-ula.html>.
26. SuperUser. *IPv4 vs IPv6 priority in Windows 7*. [En línea] <http://superuser.com/questions/436574/ipv4-vs-ipv6-priority-in-windows-7>.
27. Apple Support . *Cómo configurar IPv6 en OS X*. [En línea] <https://support.apple.com/es-es/HT202237>.
28. **Cicileo, Guillermo, y otros, y otros**. *Pv6 para Todos: Guía de uso y aplicación para diversos entornos*. Buenos Aires : Asociación Civil de Argentinos en Internet, Octubre 2009. ISBN 978-987-25392-1-4.
29. Apple Support . *OS X: Acerca del firewall de aplicación*. [En línea] <https://support.apple.com/es-es/HT201642>.
30. Movistar. *Problema bloqueo MAC (IOS previas a 10.7.X)*. [En línea] [http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/modem-router-inalambricos-adsl/instrucciones\\_para\\_el\\_desbloqueo\\_de\\_dispositivos\\_MAC.pdf](http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/modem-router-inalambricos-adsl/instrucciones_para_el_desbloqueo_de_dispositivos_MAC.pdf).
31. Soydemac. *Truco para deshabilitar IPv6 en tu Mac*. [En línea] <http://www.soydemac.com/truco-para-deshabilitar-ipv6-en-tu-mac/>.
32. deep darc. *Teredo for MacOS X*. [En línea] <http://www.deepdarc.com/miredo-osx/>.
33. Momose. *Mac OS X ISATAP client*. [En línea] <http://www.momose.org/macosex/isatap.html>.
34. Ipv6int.net. *Apple Mac OS X IPv6*. [En línea] [http://ipv6int.net/systems/mac\\_os\\_x-ipv6.html](http://ipv6int.net/systems/mac_os_x-ipv6.html).
35. Seguridad Apple . *Deshabilitar IPv6 en Mac OS X para evitar ataques de red*. [En línea] <http://www.seguridadapple.com/2012/02/deshabilitar-ipv6-en-mac-os-x-para.html>.
36. Udistrital. *Protocolo de internet versión 6. Configuración de equipos: host*. [En línea] <https://rita.udistrital.edu.co/images/pdf/8Configuraciones%20de%20host.pdf>.
37. Google Sites. *Instalación y configuración básica de IPv6*. [En línea] <https://sites.google.com/site/tnikaipv6/2-3-instalacion-y-configuracion-basica-de-ipv6>.
38. Wikipedia. *ICMPv6*. [En línea] <https://es.wikipedia.org/wiki/ICMPv6>.
39. Wikipedia. *Netfilter/iptables*. [En línea] <https://es.wikipedia.org/wiki/Netfilter/iptables>.
40. Netfilter. *Uso de iptables*. [En línea] <http://www.netfilter.org/documentation/HOWTO/es/packet-filtering-HOWTO-7.html>.

41. **Giobbi, Ryan.** CERT. *Reference iptables firewall rules for ICMPv6.* [En línea] [https://www.cert.org/downloads/IPv6/iptables\\_rules.txt](https://www.cert.org/downloads/IPv6/iptables_rules.txt).
42. Youtube. *Configuring and Implementing Linux's iptables.* [En línea] <https://www.youtube.com/watch?v=TicONyWnjpl>.
43. CISCO. *ICMPv6 Packet Types and Codes.* [En línea] <http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/22974->.
44. tk-sls. *Filtering and Rate-Limiting ICMPv6 on a GNU/Linux Server.* [En línea] <https://tk-sls.de/wp/3184>.
45. **Souza, Kleber Sacilotto de.** IBM. *Configuring iptables for IP multicast.* [En línea] <https://www.ibm.com/developerworks/community/blogs/>.
46. Wikipedia. *Teredo.* [En línea] <https://es.wikipedia.org/wiki/Teredo>.
47. Howtoinstall. *Cómo instalar miredo en Ubuntu 16.04.* [En línea] <https://www.howtoinstall.co/es/ubuntu/xenial/miredo>.
48. UCA. *IPv6 con Miredo (Cliente Teredo para Linux).* [En línea] <http://blog.uca.edu.ni/cleal/2013/02/13/ipv6-con-miredo-cliente-teredo-para-linux/>.
49. Litech. *Linux ISATAP Setup.* [En línea] <http://www.litech.org/isatap/>.
50. Mikroways. *Configuración de 6to4.* [En línea] <http://www.mikroways.net/2010/10/22/configuracion-de-6to4/>.
51. **Molina, Alberto.** Wordpress. *Conexión a internet IPv6 a través de 6to4.* [En línea] <https://albertomolina.wordpress.com/2010/01/31/conexion-a-internet-ipv6-a-traves-de-6to4/>.
52. Hipertextual. *Cómo configurar tu red para usar los DNS públicos de Google.* [En línea] <https://hipertextual.com/archivo/2013/10/dns-publicos-google/>.
53. Binarytides. *How to disable IPv6 on Ubuntu, Linux Mint, Debian.* [En línea] <http://www.binarytides.com/disable-ipv6-ubuntu/>.
54. Adslayuda, Comunidad de Banda Ancha. *¿Cómo configurar el firewall de MAC OS X?* [En línea] <http://www.adslayuda.com/cortafuegos-firemacosx.html>.
55. Apple Communities . *Yosemite firewall: IPFW is gone, Moving to PF.* [En línea] <https://discussions.apple.com/thread/6645172>.
56. **albin, John.** Drupal front-end evangelist, John albin. *Everything you ever wanted to know about ICMP.* [En línea] <http://john.albin.net/essential-icmp>.
57. Water Roof. [En línea] <http://www.hanynet.com/waterroof/>.
58. Wikipedia. [En línea] [https://en.wikipedia.org/wiki/PF\\_%28firewall%29](https://en.wikipedia.org/wiki/PF_%28firewall%29).
59. Wikipedia . *Dirección IPv6.* [En línea] [https://es.wikipedia.org/wiki/Direcci%C3%B3n\\_IPv6#Direcciones\\_Multicast](https://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6#Direcciones_Multicast).
60. Agile Faqs. *Enabling Multicast on your MacOS (\*Unix).* [En línea] <http://blogs.agilefaqs.com/2009/11/08/enabling-multicast-on-your-macos-unix/>.
61. Hipertextual. *Cómo configurar tu red para usar los DNS públicos de Google.* [En línea] <https://hipertextual.com/archivo/2013/10/dns-publicos-google/>.
62. Aaronsw. *Enabling IPv6 on OS X.* [En línea] <http://www.aaronsw.com/weblog/000831>.