UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE COMPUTACIÓN

Análisis y diseño de reingeniería de la red de la UNAN-León mediante la utilización de IPv6

Tesis para optar al título de: Master en Computación con Énfasis en Redes y Comunicaciones

2009-2011

Autor:
Ing. Karla Vanessa Cerrato Flores

Tutor:
MSc. Aldo René Martínez Delgadillo

León, Nicaragua, Julio 2012

DEDICATORIA

Es un poco difícil realizar una dedicatoria, pues es mucha gente la que ha ayudado para que pueda llegar a este punto de mi trayectoria profesional, sin embargo esta monografía va en especial dedicación:

A Dios que me ha dado sabiduría para distinguir entre el bien y el mal, fé y fortaleza para seguir adelante en los momentos difíciles de mis estudios y la oportunidad de culminar éxitosamente esta maestria.

A mi Papá Héctor Ramón Cerrato Baldizón por apoyarme incondicionalmente en cada etapa de mi formación, por darme aliento en las situaciones más difíciles a pesar de las necesidades y adversidades por las que tuve que pasar para poder lograr mis metas, por apoyar mis decisiones y sobre todo por depositar su confianza en mí.

A mi abuelita Rosa Baldizón quién ha sido más que una madre para mí, por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

Y por último, y no menos importantes a todas aquellas personas cólegas de la División de Informática de la UNAN-León por contribuir a despejar dudas del funcionamiento y administración de la red actual, docentes por transmitirme sus conocimientos y compañeros de estudios, todos ellos que siempre están presentes en mi vida brindándome todo su cariño incondicional y por animarme a seguir luchando para alcanzar mis objetivos.

A todos ellos muchas gracias por ser parte de este triunfo.

Karla Vanessa Cerrato Flores

ÍNDICE

CAPÍTULO 1 ASPECTOS INTRODUCTORIOS **1**

1. INTRODUCCIÓN 2
2. JUSTIFICACIÓN 4
3. *OBJETIVOS* 6

OBJETIVO GENERAL: 6

OBJETIVOS ESPECÍFICOS: 6

..... **7**

CAPÍTULO 2 **ASPECTOS TEÓRICOS** **7**

1. INTRODUCCIÓN A IPV6 8
   - *1.1. Historia de IPv6* *8*
     - ¿Por qué un nuevo Protocolo de Internet? 8
     - Requisitos de IPng 8
     - Candidatos para IPng 9
     - Hechos históricos 10
     - ¿Es verdad que no quedan direcciones IPv4? 12
     - Agotamiento direcciones IPv4 13
     - Ventajas y Desventajas de NAT 16
   - *1.2. Ventajas de IPv6* *16*
     - Ventajas adicionales con direcciones mayores 16
     - Ventajas adicionales con el nuevo despliegue 17
     - Características principales de IPv6 18
     - Motivación 19
2. FORMATO DE CABECERAS Y TAMAÑO DE PAQUETES 21
   - *2.1. Terminología* *21*
   - *2.2. Formato cabecera IPv6* *23*
     - Resumen de los cambios de la cabecera: 24
     - Cabeceras de extensión 24
     - Ventajas de las Cabeceras de Extensión 26
   - *2.3. Consideraciones sobre tamaño de paquete* *28*
     - MTU mínimo 28
     - Descubrimiento del Path MTU (RFC 1891) 28
     - Cabecera de fragmentación 29
     - Proceso de fragmentación 30
3. DIRECCIONAMIENTO IPV6 32
   - *3.1. Tipos de direcciones* *32*
     - Direcciones unidifusión 33
     - Direcciones IPv6 de multidifusión 39
     - Direcciones IPv6 de difusión por proximidad 43
   - *3.2. Prefijos y representación* *44*
     - Partes de una dirección IPv6 44

Prefijos 46
Ejercicios prácticos de Notación de direcciones IPv6 48
Ejemplo de asignación de prefijos y direcciones 50
3.3. Identificadores de Interfaz 57
Identificadores de interfaz basados en direcciones EUI-64 57
Direcciones IEEE 802 58
Direcciones IEEE EUI-64 59
Asignación de direcciones IEEE 802 a direcciones EUI-64 59
Asignación de direcciones EUI-64 a identificadores de interfaz IPv6 60
3.4. Otras consideraciones 62
Direcciones para hosts y enrutadores 62
4. ICMPv6, Neighbor Discovery y DHCPv6 64
4.1. ICMPv6 64
Mensajes ICMPv6 67
4.2. Neighbor Discovery 67
Interacción entre nodos 69
Nuevos tipos de paquetes ICMP 69
Ejemplo de funcionamiento 75
Comparación con IPv4 77
4.3. Autoconfiguración 79
Autoconfiguración Stateless o Serverless (RFC 4862) 80
Ventajas/beneficios de la Autoconfiguración Stateless 81
Autoconfiguración Stateful o DHCPv6 (RFC 3315) 83
Tiempo de validez de las direcciones 83
Configurar el servidor DNS con autoconfiguración Stateless 84
4.4. DHCPv6 85
Objetivos de DHCPv6 86
Detalles de DHCPv6 86
DHCPv6-PD (RFC 3633) 89
Detalles de DHCPv6-PD 91
Nuevas características de usuario con DHCPv6 92
4.5. Router Renumbering 93
Funcionamiento 93
5. Seguridad IPv6 95
5.1. Introducción 95
5.2. IPsec: la teoría 95
Seguridad IP (IPSec) 95
IPsec: Elementos básicos 96
Visión General 97
PAD (Peer Authorization Database) 99
Protocolos de seguridad 100
SA: El concepto 100
Identificación de SA 101
SA Database (SAD) 101

Campos de la SAD 102
Transmisión IPsec 103
Cabecera AH (RFC4302) 103
Cabecera ESP (RFC 4303) 104
Algoritmos ESP 105
Algoritmos AH 106
Modos de uso 106
El problema de la clave 110
Principios básicos de IKE 111
Objetivo de IKEv2 113
Diferencias de IKEv2 respecto IKEv1 114
5.3. Extensiones de privacidad 115
Introducción 115
¿Por qué Extensiones de Privacidad? 116
Extensiones de privacidad 116
5.4. Amenazas a ND 118
Visión general 118
Amenazas a ND 118
5.5. Comparativa IPv4 vs. IPv6 127
Visión general 127
Seguridad IPv6: Primer contacto 127
Clasificación de las Amenazas de Seguridad 128
5.6. Aspectos de seguridad con IPv6 129
5.7. Temas prácticos 132
5.8. Firewalling 133
Introducción 133
Consejos 133
5.9. Modelo de seguridad Distribuida 134
Visión general 134
Consideraciones del despliegue 134
Modelo se Seguridad Perimetral 135
Modelo Seguridad Distribuida 136
6. ENCAMINAMIENTO CON IPV6 139
6.1. Conceptos de encaminamiento 139
Visión General Encaminamiento 139
Tipos de protocolos de encaminamiento 139
Criterios de selección IGP 140
Encaminamiento IPv6 140
6.2. RIPng 141
6.3. EIGRP 141
6.4. OSPF 142
Visión General 142
OSPF IPv6 143
6.5. IS-IS 145

Visión General IS-IS ... 145
6.6. BGP ... 147
Visión General de BGP ... 147
BGP para IPv6 (BGP4+) ... 150
Características de BGP4+ ... 150
MPLS 6PE ... 152
6PE en Cisco (Plano de Control) ... 153
6PE Packet forwarding ... 153
6.7. Encaminamiento estático ... 153
Configuración de Rutas Estáticas ... 153
7. MECANISMOS DE TRANSICIÓN ... 155
7.1. Conceptos de transición ... 155
Técnicas de Transición / Coexistencia ... 155
7.2. Doble pila ... 156
7.3. Túneles ... 158
Túneles para atravesar Routers que no Reenvían IPv6 ... 158
Túneles IPv6 en IPv4 (6in4) ... 159
Detalles Túneles 6in4 (RFC 4213) ... 161
7.4. Tunnel Broker ... 162
Tunnel Broker (RFC 3053) ... 162
7.5. 6to4 ... 163
Túneles 6to4: RFC 3056 ... 163
7.6. 6RD ... 168
6RD: Un refinamiento de 6to4 ... 168
6RD: Formato direcciones ... 169
6RD: Pros & Contras ... 169
6RD: Arquitectura ... 170
6RD: Escenario de Implementación ... 171
7.7. Teredo ... 172
7.8. Softwires ... 174
Encapsulamiento de Softwires basado en L2TPv2 ... 175
Softwires basado en L2TPv2 L2TP header ... 176
Ejemplo de uso de Softwires ... 177
Encapsulamiento de Softwires basado en L2TPv3 ... 178
7.9. DS-Lite ... 179
7.10. Traducción ... 180
7.11. NAT64 ... 181
Traducción IPv4/IPv6 (obsoleto) ... 182
7.12. Seguridad ... 184
Seguridad en los mecanismos de transición ... 184
8. CALIDAD DE SERVICIO (QOS) ... 185
8.1. Conceptos de QoS ... 185
Aproximaciones a QoS en IP ... 185

8.2. Soporte QoS en IPv6 ... *186*
Soporte IPv6 para Int-Serv ... 186
Soporte IPv6 para Diff-Serv ... 187
IPv6 Flow Label ... 188
Especificación de Flow Label ... 190
8.3. Aspectos prácticos ... *191*
QoS para IPv6 en Cisco ... 191
Pasos generales para implementar QoS (IPv4 e IPv6) ... 192
9. MULTICAST ... 194
9.1. Conceptos Multicast ... *194*
¿Qué es Multicast? ... 194
Aplicaciones ... 195
Conceptos Multicast ... 196
¿Cómo funciona? ... 198
9.2. Direcciones Multicast ... *198*
IPv4 vs. IPv6 ... 198
Direcciones Multicast IPv6 ... 201
Direcciones Multicast Reservadas ... 202
Direcciones Multicast Importantes ... 203
9.3. Multicast Listener Discovery ... *204*
Mensajes MLD ... 208
9.4. Encaminamiento Multicast ... *208*
Ámbitos Multicast y protocolos ... 211
Escenario Básico Multicast IPv6 ... 212
Escenarios Multicast IPv6 ... 213
9.5. PIM-ASM ... *213*
RP Embebido ... 216
9.6. PIM-SSM ... *217*
9.7. Aspectos prácticos ... *218*
Aplicaciones Multicast IPv6 ... 218
10. SERVICIOS IPV6 ... 221
10.1. DNS ... *221*
10.2. Configuracion de IPv6 en Servidores ... *224*
Servidor Web ... 224
Apache ... 224
DHCP ... 228
Bind9 ... 234
IIS (Internet Information Services) ... 242
Servidor DNS ... 244

***CAPÍTULO 3* ANÁLISIS DE RED INSTITUCIONAL Y EVALUACIÓN DE ALTERNATIVAS ... 249**

11. RED INSTITUCIONAL UNAN-LEÓN ... 250
Requerimientos para la migración de red IPv4 a IPv6 ... 253
Tecnologías y filosofía de diseño ... 261

Análisis del soporte IPv6 en la red institucional 262
Alternativas de equipamiento 263
Asignación de direcciones IPv6 264
Seguridad perimetral IPv6 en la UNAN-León en los routers 267
Propuesta de ACL a implementar en routers CISCO UNAN-León 270
Costos de implementación y soporte 274
Desventajas de migración de IPv6 en la UNAN-León 277
12. CONCLUSIONES 279
13. BIBLIOGRAFÍA 280

***CAPÍTULO 4* ANEXOS 284**

1. CONFIGURACIÓN DE HOST EN WINDOWS XP 285
2. CONFIGURACIÓN DE HOST EN WINDOWS VISTA/2008 286
3. CONFIGURACIÓN DE HOST EN WINDOWS 2000 287
4. INSTALACION DE IPV6 EN LINUX 288
5. CONFIGURACION PERMANENTE EN RED HAT 289
6. CONFIGURACION PERMANENTE EN SUSE 289
7. CONFIGURACION PERMANENTE EN DEBIAN 290
8. INSTALACION DE IPV6 EN BSD 290
9. CONFIGURACION AVANZADA IPV6 EN WINDOWS 291
10. CONFIGURACION AVANZADA IPV6 EN LINUX 294
11. CONFIGURACIÓN AVANZADA IPV6 EN BSD 296
12. CONFIGURACIÓN IPV6 EN ROUTER'S CISCO 297
13. AUTOCONFIGURACIÓN STATELESS IPV6 303
14. CONFIGURAR ISATAP 317
15. PILA DUAL 321
16. AUTOMATIC 6TO4 TUNNEL 325
17. CONFIGURACIÓN DEL CLIENTE 6TO4 EN LINUX 331
18. CONFIGURACIÓN DEL CLIENTE TEREDO EN LINUX 334
19. CONFIGURACIÓN DEL CLIENTE TEREDO EN WINDOWS 336

TABLA DE ILUSTRACIONES

Ilustración 1. Evolución de IPng 11
Ilustración 2. Evolución del pool central de direcciones IPv4 12
Ilustración 3. Status de 256 /8s espacio de direcciones IPv4 13
Ilustración 4. Asignaciones IPv6 en la región de LACNIC 14
Ilustración 5. Distribución de recursos de numeración de Internet 14
Ilustración 6. Registros de Internet Regionales (RIR) 15
Ilustración 7. Direcciones IPv6 17
Ilustración 8. IPv6, un protocolo de capa de red 19
Ilustración 9. Componentes básicos de una red IPv6 21
Ilustración 10. Formato de la cabecera IPv4 23
Ilustración 11. Formato de la cabecera IPv6 23
Ilustración 12. Cabeceras de Extensión 26
Ilustración 13. Plano de control IPv4 vs. IPv6 27
Ilustración 14. Descubrimiento del Path MTU 29
Ilustración 15. Cabecera de Fragmentación 30
Ilustración 16. Fragmentación en Origen 30
Ilustración 17. Formato de fragmentación 30
Ilustración 18. Paquetes fragmentados 31
Ilustración 19. Dirección Unicast (Unidifusión) 32
Ilustración 20. Dirección Multicast (Multidifusión) 33
Ilustración 21. Dirección Anycast (Difusión por proximidad) 33
Ilustración 22. Estructura de una dirección global de unidifusión 34
Ilustración 23. Estructura de tres niveles de la dirección global de unidifusión 35
Ilustración 24. Estructura de dirección local de vínculo 36
Ilustración 25. Estructura de dirección local del sitio 37
Ilustración 26. Intercambio de mensajes en ISATAP 39
Ilustración 27. Dirección IPv6 de multidifusión 40
Ilustración 28. Dirección IPv6 de multidifusión recomendada con un identificador de grupo de 32 bits 42
Ilustración 29. Asignación de direcciones IPv6 de unidifusión a dirección IPv6 de nodo solicitado 43
Ilustración 30. Formato básico de las direcciones IPv6 45
Ilustración 31. Tabla de Prefijos de direcciones IPv6 47
Ilustración 32. Plan de direccionamiento 56
Ilustración 33. Direcciones IEEE 802 58
Ilustración 34. Direcciones IEEE EUI-64 59

Ilustración 35. Asignación de direcciones IEEE 802 a direcciones EUI-64 60
Ilustración 36. Asignación de direcciones EUI-64 a identificadores de interfaz IPv6..... 60
Ilustración 37. Ejemplo de conversión de una dirección IEEE 802 61
Ilustración 38. Mensaje ICMPv6 encapsulado en paquete IPv6 65
Ilustración 39. IPv6 ICMP Packet Header Format..... 66
Ilustración 40. Mensajes de error e informativos ICMPv6 67
Ilustración 41. Topologia de Neighbor Discovery..... 68
Ilustración 42. Formato Router Solicitation 70
Ilustración 43. Router Solicitation y Router Advertisement 70
Ilustración 44. Formato Router Advertisement 71
Ilustración 45. Formato Neighbor Solicitation 72
Ilustración 46. Neighbor Solicitation y Neighbor Advertisement 73
Ilustración 47. Formato Neighbor Advertisement 73
Ilustración 48. Redirection 74
Ilustración 49. Formato Redirect..... 74
Ilustración 50. Algoritmo para determinar el próximo salto..... 76
Ilustración 51. Comparación de la pila de protocolos IPv4 e IPv6 79
Ilustración 52. Relación entre los estados de una dirección configurada automáticamente y el tiempo de vida preferido y válido..... 80
Ilustración 53. Funcionamiento de la Auconfiguración Stateless 82
Ilustración 54. DHCPv6 89
Ilustración 55. Ejemplo básico DHCPv6-PD 90
Ilustración 56. Arquitectura de red para DHCPv6-PD 92
Ilustración 57. IPsec, visión general 98
Ilustración 58. Cabecera IPsec..... 103
Ilustración 59. Cabecera IPsec con ESP 103
Ilustración 60. Cabecera AH 103
Ilustración 61. Cabecera ESP 105
Ilustración 62. AH en modo Transporte 107
Ilustración 63. ESP en modo Transporte 108
Ilustración 64. AH en modo Túnel..... 109
Ilustración 65. ESP en modo Túnel..... 109
Ilustración 66. Modo Transporte vs Modo Túnel..... 110
Ilustración 67. Ejemplo de Fase1 y SA ISAKMP 113
Ilustración 68. IKEv1 vs IKEv2 115
Ilustración 69. Neighbor solicitation/advertisement spoofing 119
Ilustración 70. Denegación de servicio con Duplicate Address Detection..... 120

Ilustración 71. Redirigiendo trafico con Redirect ICMPv6 122
Ilustración 72. Router Advertisement que conduce a una denegacion de servicio..... 124
Ilustración 73. Neighbor Discovery: Solicitation 126
Ilustración 74. Neighbor Discovery: Advertisement 127
Ilustración 75. Modelo de seguridad perimetral..... 135
Ilustración 76. Modelo de seguridad distribuida 136
Ilustración 77. Modelo de seguridad distribuida 137
Ilustración 78. OSPFv3..... 144
Ilustración 79. IS-IS para IPv6..... 146
Ilustración 80. Visión general BGP 149
Ilustración 81. Establecimiento de sesión BGP4+ de tránsito de tráfico IPv6..... 152
Ilustración 82. Estrategias de transición a IPv6..... 155
Ilustración 83. Topologia IPv6 de doble pila 156
Ilustración 84. Mecanismo basado en doble pila..... 157
Ilustración 85. Túneles para atravesar routers 158
Ilustración 86. Mecanismo basado en Túneles 6in4 160
Ilustración 87. Diversas formas de encapsular paquetes IPv6..... 160
Ilustración 88. Detalle túneles 6in4..... 161
Ilustración 89. Establecimiento de túnel automático con Tunnel Broker..... 163
Ilustración 90. Interconectando dominios 6to4..... 164
Ilustración 91. Interconección de dominios 6to4 a dominios IPv6 nativos..... 165
Ilustración 92. Túneles 6to4 166
Ilustración 93. Relay 6to4..... 166
Ilustración 94. Elementos de arquitectura 6to4 167
Ilustración 95. Formato de direcciones 6RD 169
Ilustración 96. Arquitectura IPS para implementar IPv6 con 6RD 171
Ilustración 97. Teredo 173
Ilustración 98. Componentes de arquitectura Teredo..... 174
Ilustración 99. Encapsulamiento de Softwires basado en L2TPv2 176
Ilustración 100. Softwires basado en L2TPv2..... 176
Ilustración 101. Ejemplo de uso de Softwires 178
Ilustración 102. Encapsulamiento de Softwires basado en L2TPv3 179
Ilustración 103. Dual Stack Lite 180
Ilustración 104. NAT64 182
Ilustración 105. Ejemplo de NAT-PT..... 184
Ilustración 106. Modelo IntServ/DiffServ..... 186
Ilustración 107. Una perspectiva de red de la operación DiffServ..... 188

Ilustración 108. IPv6 Flow Label 188
Ilustración 109. Conjunto de Herramientas de QoS 192
Ilustración 110. Multicast 195
Ilustración 111. Multicast Client-Server 196
Ilustración 112. Shortest Path Tree 197
Ilustración 113. Transmisión de Informacion en modo Broadcast 199
Ilustración 114. Transmisión de información en modo Multicast 200
Ilustración 115. Direcciones Multicast IPv6 201
Ilustración 116. Protocolos Multicas de capa 2 204
Ilustración 117. Protocolos Multicast de capa 3 206
Ilustración 118. Comparación de las transmisiones de unidifusión múltiples y las transmisiones de multidifusión. 209
Ilustración 119. Diferencias entre los protocolos de multidifusión Dense Mode y Sparse Mode 211
Ilustración 120. Escenario básico Multicast IPv6 212
Ilustración 121. Escenario Multicast IPv6 213
Ilustración 122. PIM-ASM: Registro de la fuente 214
Ilustración 123. PIM-ASM: Unión del Cliente 215
Ilustración 124. Esquema de distribución de paquetes PIM-SM 216
Ilustración 125. Funcionamiento de PIM-SSM 217
Ilustración 126. Diferencia entre DNSv6 modo transporte y contenido 222
Ilustración 127. DNS IPv6: Ejemplo 223
Ilustración 128. Diagrama Físico de edificios de la UNAN-León 251
Ilustración 129. Migración IPv4 a IPv6 254
Ilustración 130. Proceso de migración: Pasar por una etapa de coexistencia IPv4/IPv6 y luego usar sólo IPv6 256
Ilustración 131. Red IPv4 a red IPv4/IPv6 257
Ilustración 132. Red IPv4/IPv6 a red IPv6 259
Ilustración 133. Aplicaciones IPv4 a aplicaciones IPv4/IPv6 260
Ilustración 134. Aplicaciones IPv4/IPv6 a aplicaciones IPv6 260
Ilustración 135.Propuesta Esquema de direccionamiento IPv6 265
Ilustración 136. Propuesta de diagrama de Red IPv6 UNAN-León 266
Ilustración 137. Instalación de IPv6 en XP/2003 285
Ilustración 138. Propiedades de Conexión de red e instalación de IPv6 en Vista 286
Ilustración 139. Estados de dirección de autoconfiguración 303
Ilustración 140. Detalle de un mensaje Router Advertisement IPv6 308

Índice de Tablas

Tabla 1. Ventajas y Desventajas de NAT 16
Tabla 2. Similitudes IPv4 & IPv6 17
Tabla 3. Mensajes ICMPv6 65
Tabla 4. Protocolos de enrutamiento en IPv6 141
Tabla 5. LSAs en OSPFv3 145
Tabla 7. Comparación entre IOS y JUNOS 262
Tabla 6. Equipos switch y routers existentes en la UNAN-León 262
Tabla 8. Direcciones IPv6 a Denegar 269
Tabla 9. ACLs entrantes con acceso a internet 270
Tabla 10. ACLs salientes con acceso a internet 273
Tabla 11. Estados del proceso autoconfiguración stateless 303

Capítulo 1 Aspectos Introductorios

1. INTRODUCCIÓN

No existe duda alguna que las tecnologías de la información y comunicaciones (TIC) se han convertido en parte fundamental de nuestras vidas. Durante la última década, se han desarrollado innumerables tecnologías y servicios que han cambiado la forma de comunicarse y relacionarse con las personas a lo largo del mundo. Poco a poco se observa como los medios tradicionales de comunicación, televisión, telefonía y mensajería, entre otros, convergen hacia una única red de comunicaciones, la Internet.

Esta tendencia mundial ha conducido a un crecimiento explosivo en el número de usuario de Internet. Junto a esto, Internet ha evolucionado desde ser una simple red que conecta computadores a una plataforma que entrega diversos tipos de servicios.

Esta evolución ha dejado en descubierto las limitantes del protocolo IPv4, base de esta gran red. IPv4 es la versión del protocolo IP más utilizada actualmente la cual constituye en estos momentos un estándar, fue desarrollado en la década de los 70's como una forma de interconectar un reducido número de redes y jamás se pensó en que tendría que ser la base de una red de millones de usuarios. Su reducido número de direcciones disponibles junto a problemas de arquitectura, han restringido y limitado el desarrollo de nuevas aplicaciones y tecnologías de Internet.

El protocolo IPv6 fue desarrollado durante la década de los 90 con el fin de sustituir a IPv4 como protocolo dominante en Internet. IPv6 soluciona los problemas fundamentales de IPv4 y entrega una base para futuros desarrollos y avances en Internet. Dentro de las ventajas de IPv6 se encuentran un gran número de direcciones disponibles junto a características que facilitan la implementación de modelos de seguridad y calidad de servicio en Internet.

La aceptación de IPv6 ha sido un proceso lento. A la fecha, el tráfico IPv6 en Internet representa menos de un 5% del total cursado. Aun cuando diversos estudios pronostican que en pocos años más se producirá el agotamiento total de las direcciones IPv4, las empresas y organizaciones aún no encuentran motivos suficientes para invertir en implementaciones IPv6. Se espera que dicho panorama varíe a medida que se

desarrollan nuevos servicios y negocios que requieran dar acceso masivo a Internet, tales como el despliegue de redes 3G.

El método tradicional mediante el cual empresas, universidades y particulares han realizado implementaciones de redes IPv6 es mediante el uso de túneles. Esto les permite obtener una limitada conectividad IPv6 hacia el exterior, suficiente para realizar pruebas y comprobar algunas de las muchas aplicaciones del protocolo. Sin embargo, este tipo de implementaciones entrega una panorámica parcial, que deja de lado mucho de los desafíos, decisiones y aspectos que hay que considerar cuando se debe implementar IPv6 de forma nativa en ambientes de producción.

La versión IPv6 puede ser instalada como una actualización de software en los dispositivos de red de Internet e interoperar con la versión actual IPv4. IPv6 está diseñado especialmente para redes de alto rendimiento, como por ejemplo las redes ATM, pero manteniendo la eficiencia en redes de bajo ancho de banda, como por ejemplo en redes inalámbricas. Además, ofrece una plataforma para la nueva funcionalidad de Internet que será necesaria en un futuro inmediato.

La necesidad de migrar a IPv6 está originada por las nuevas tendencias en el mundo actual de las telecomunicaciones, que podemos resumir en:

- La creciente movilidad de los usuarios de Internet, que desean acceder a los mismos servicios en cualquier momento y desde cualquier lugar.
- Las redes domésticas con avanzados sistemas de televigilancia, control y seguridad.
- La convergencia de voz, vídeo y datos, en infraestructuras basadas en IP.

El principal objetivo de esta tesis es proponer un diseño de red IPv6 en la Universidad Nacional Autónoma de Nicaragua, León, con el fin de implantar el protocolo de red IPv6 en sus redes de datos, de tal forma que, durante el tiempo que sea necesario, pueda convivir con el protocolo del internet actual, IPv4.

Además, facilitando la introducción de IPv6 en los departamentos y/o facultades se espera impulsar el desarrollo de la nueva red institucional.

2. JUSTIFICACIÓN

Las motivaciones que pueden a impulsar a una universidad y/u organización a implantar un nuevo protocolo de red en sus infraestructuras de comunicaciones pueden ser muy diversas. En el entorno en el que nos movemos, un departamento universitario involucrado en las tareas de investigación que implican tecnologías de última generación, una de las más importantes podría ser definida como la necesidad de manejar, experimentar y explotar los nuevos protocolos.

Pero no sólo es justificable la migración (previsiblemente costosa) de una tecnología a otra, en un entorno educativo. También es importante llevarla a cabo cuando dentro de la institución: hay proyectos, investigadores y recursos dedicados a la gestión de la tecnología, que de no actualizarse acabarían quedando ineludiblemente obsoletos.

En el caso del departamento de Computación, perteneciente a la Facultad de Ciencias y Tecnología de la UNAN-León, también hay fuerzas internas y externas que empujan a intentar demostrar la viabilidad y la madurez de IPv6, una tecnología que se puede ver como un factor a tener en cuenta para mejorar el rendimiento y la seguridad en las comunicaciones punto a punto. Así, por ejemplo, se cuenta con personal de las dos carreras ofertadas por el departamento, Ingenieria en Sistemas e Ingenieria en Telemática, que en muchos casos no solo investigan sobre IPv6 sino que también han contribuido activamente en el mundo académico.

Las ventajas que aportará el uso de IPv6 en nuestras redes, aplicaciones y servicios, previsiblemente irán más allá de los objetivos primarios del presente documento, permitiendo obtener resultados que no se podrían conseguir de otro modo. El proceso de migración también permitirá evaluar los costes del cambio y ayudará a crear el conocimiento base a partir del cual se podrá desarrollar proyectos de implantación de esta tecnología en otras instituciones y/u organizaciones. Se puede probar en un entorno real de trabajo las aplicaciones y sistemas creados para IPv6 y ayudar a crear la masa crítica necesaria para impulsar el cambio de tecnología de red a nivel nacional y mundial.

La migración ha de verse como un proceso evolutivo que comenzará con la implantación del nuevo protocolo en las infraestructuras de comunicaciones, para continuar luego con la modificación de aplicaciones, servicios y sistemas de gestión de las mismas, acabando con la extensión del protocolo a la mayor parte de los dispositivos interconectados a la red de redes.

Durante la implantación del nuevo protocolo los sistemas han de verse afectados lo menos posible, con el fin de que la migración en la capa de red se pueda realizar de forma escalonada y según las necesidades que vayan surgiendo. Sólo en la última fase se contempla la posibilidad de que desaparezca finalmente el protocolo de red actual, IPv4. Aunque esto puede ser que nunca llegue a producirse, ya que ambas tecnologías deben poder convivir sin demasiados problemas.

3. OBJETIVOS

Objetivo general:

- Analizar y diseñar una propuesta de reingeniería de la red de la Universidad Nacional Autonóma de Nicaragua (UNAN-León) mediante la utilización de IPv6.

Objetivos específicos:

- Documentar los aspectos más relevantes relacionados con el protocolo IP versión 6 que sirva de apoyo para justificar las fases posteriores de investigación.
- Buscar alternativas a las soluciones tecnológicas que limitan la implementación de IPv6 en la Universidad Nacional Autónoma de Nicaragua (UNAN-León).
- Diseñar y desarrollar el documento guía para la reingeniería de implantación de IPv6.
- Explicar los pasos seguidos durante la instalación del protocolo en la institución y así facilitar la implementación de éste en otras instituciones.
- Formular vías alternativas para la conexión a la red IPv6.

Capítulo 2 Aspectos Teóricos

1. INTRODUCCIÓN A IPV6

1.1. Historia de IPv6

¿Por qué un nuevo Protocolo de Internet?

El motivo básico por el que surge, en el seno del IETF[1] (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296). En cambio, IPv6 nos ofrece un espacio de direcciones de 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo, IPv4 tiene otros problemas o dificultades que IPv6 soluciona o mejora.

Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico. Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

Requisitos de IPng

- Noviembre, 1991.
    - IETF creo un grupo de trabajo para analizar el problema del crecimiento de Internet y considerar posibles soluciones.

[1] **IETF**, es una organización internacional abierta de normalización sin fines de lucro, cuyo objetivo es velar para que la arquitectura de Internet y los protocolos que la conforman funcionen correctamente.

- Julio, 1992.
  - IETF determinó que era imprescindible comenzar con el diseño de un protocolo de nueva generación para Internet (IPng)
- IPng tenía que solucionar dos problemas:
  - Soportar un gran espacio de direccionamiento.
  - Soportar esquemas de direccionamiento basados en jerarquías de agregación.
- Aunque también aparecieron nuevos requisitos para mejorar las deficiencias de IPv4:
  - Seguridad (tanto autenticación como encriptación).
  - Auto configuración de red (Plug-and-Play).
  - Mejora del soporte de calidad de servicio (QoS).
  - Soporte de movilidad.

Candidatos para IPng

- La creación y selección de los protocolos nuevos se hace bajo el "paraguas" de IETF.
- Entre 1992 y 1994 había siete candidaturas de las que en la primavera de 1994 quedaron solo tres:
  - CATNIP (Common Architecture for the Internet). Diseñado como un "protocolo convergente", entre IP, IPX[2] de Novell y el protocolo de la capa de red de la suite de OSI.
  - SIPP (Simple Internet Protocol Plus). Una evolución del IP actual (IPv4) e inter-operable con él.

[2] **Internetwork Packet Exchange o IPX**, es un protocolo de la capa de red Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo.

- TUBA (TCP y UDP con las direcciones más grandes). Una propuesta para adoptar la capa de red de OSI (CLNP[3]) como la nueva capa de red para internet.

- En julio de 1994, IETF selecciono SIPP como protocolo que debería convertirse en IPng.
  - La documentación de SIPP constituyó la base para la definición de IPng.
  - El grupo de trabajo SIPP desapareció para integrarse en el grupo IPng.
- Aspectos claves de SIPP:
  - Aspectos de transición de IPv4 a IPng:
    - Gran período de coexistencia entre ambos protocolos IPv4 e IPng.
    - Algunos nodos nunca se actualizarán a IPng.
    - Lo nodos nuevos IPng pueden usar redes solo-IPv4 para transportar paquetes IPng (túneles).
    - No se requería un día-D para desplegar IPng.
- Más adelante el grupo de trabajo de IETF IPng se renombro oficialmente como IPv6.

Hechos históricos

- ***1993:*** Red investigación con aproximadamente 100 computadoras.
- ***1991 Nov:*** IETF crea un grupo de trabajo para evaluar y buscar soluciones al agotamiento de direcciones.
- ***1992:*** Actividad comercial, crecimiento exponencial.

[3] **CLNS** es la abreviatura de **C**onnection**l**ess **N**etwork **S**ervice – traducido Servicio No Orientado a Conexión, es un servicio que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas.

- ***1992 Julio:*** IETF determina que era esencial comenzar a crear el next-generation Internet Protocol (IPng).
- ***1993:*** Agotamiento de direcciones clase B. Previsión de colapso de la red para 1994.
- ***1993 Sept:*** *RFC 1519, "Classless Inter-Domain Routing (CIDR[4]): an Address Assignment and Agreggation Strategy".*
- ***1994 Mayo:*** *RFC 1631, "The IP Network Address Translation (NAT[5])".*
- ***1995 Dic:*** Primer RFC de IPv6: "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883.
- ***1996 Feb:*** *RFC 1918, "Address Allocation for Private Internets".*
- ***1998 Dic:*** RFC 2460 Obsoleted RFC 1883. Especificación IPv6 actual.

La ***Ilustración 1*** resume los hechos históricos antes mencionados.

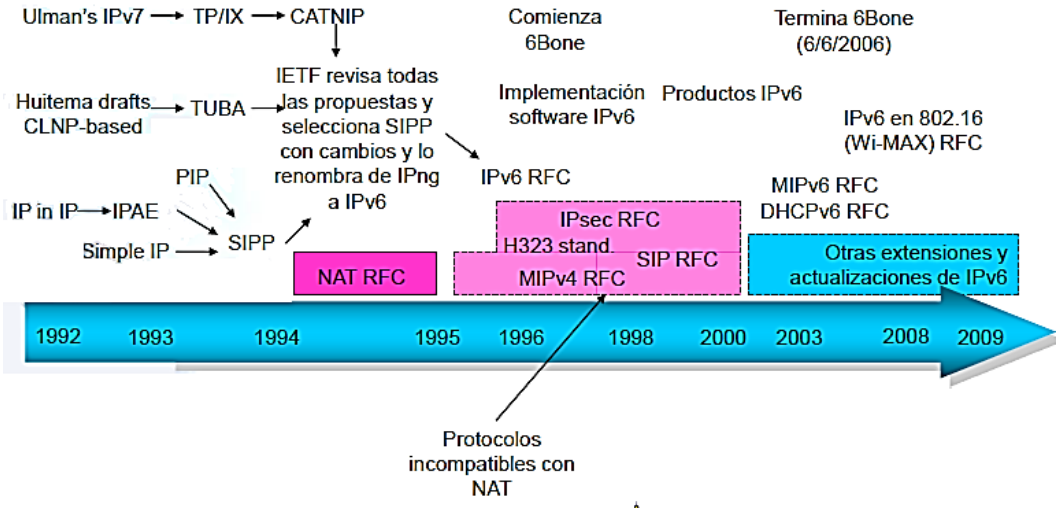


Ilustración 1. Evolución de IPng

[4] **CIDR (Classless Inter-Domain Routing)**, en español «enrutamiento entre dominios sin clases», representa la última mejora en el modo de interpretar las direcciones IP. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas.

[5] **NAT**, es mecanismo utilizado por enturadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

¿Es verdad que no quedan direcciones IPv4?

Disponibilidad de direcciones IPv4:

- 10% a principios de 2010.
- 6% a mediados de 2010.
- 5% dos meses después.
- 2% antes de final de 2010.
- 0% el 3 de Febrero de 2011.

Actualmente se niegan direcciones IPv4 públicas a la mayoría de los nuevos hosts. La solución temporal es emplear mecanismos como NAT, PPP[6], etc. para compartir direcciones.

En la ***Ilustración 2*** se puede apreciar la escacez de direcciones IPv4 en el tiempo.

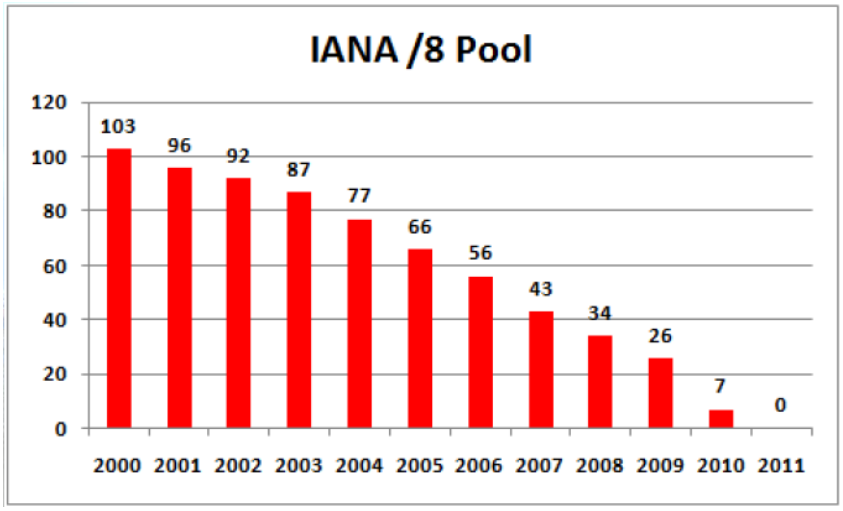


Ilustración 2. Evolución del pool central de direcciones IPv4

Sin embargo nuevos tipos de aplicaciones y nuevos mecanismos de acceso, requieren direcciones únicas.

[6] **PPP** (en español Protocolo punto a punto), es un protocolo de nivel de enlace que permite establecer una comunicación a nivel de capa de enlace TCP/IP entre dos computadoras.

Agotamiento direcciones IPv4

Existe una opinión extendida indicando que quedan pocos años de direcciones IPv4 públicas con lo cual el debate radica en ¿cuándo se agotarán?

Esto nos da tres estrategias a seguir:

- Aumentar el uso de NAT, lo cual introduce problemas técnicos y costes.
- Tratar de obtener direcciones IPv4 libres o liberadas.
- Implementar IPv6, solución válida a largo plazo.

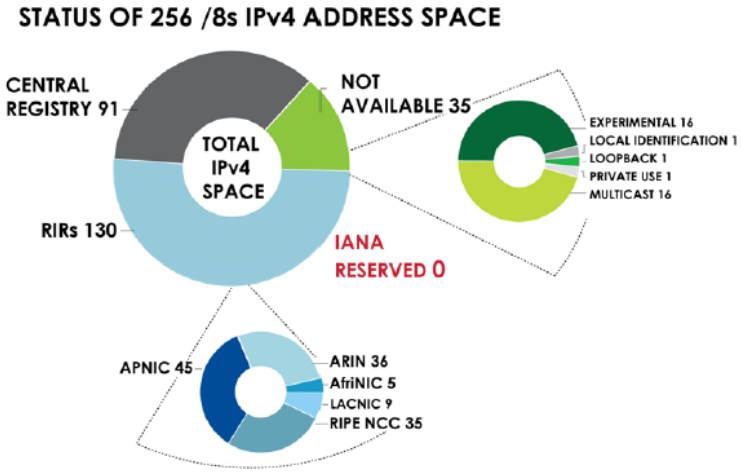


Ilustración 3. Status de 256 /8s espacio de direcciones IPv4[7]

La ***Ilustración 3.*** Status de 256 /8s espacio de direcciones IPv4 muestra el estado del espacio de direcciones IPv4 al 31 de marzo 2011.

Existen múltiples comunicados de los actores de Internet recomendando la implementación de IPv6 debido al agotamiento de direcciones IPv4[8]. La ***Ilustración 4*** muestra el avance en el uso de IPv6 en el tiempo según registros de LACNIC al 31 marzo 2011.

[7] Fuente http://www.nro.net a 31 de Marzo 2011

[8] The IPv6 Portal: Policy Recommendatios: http://www.ipv6tf.org/index.php?page=meet/policy_recommendations

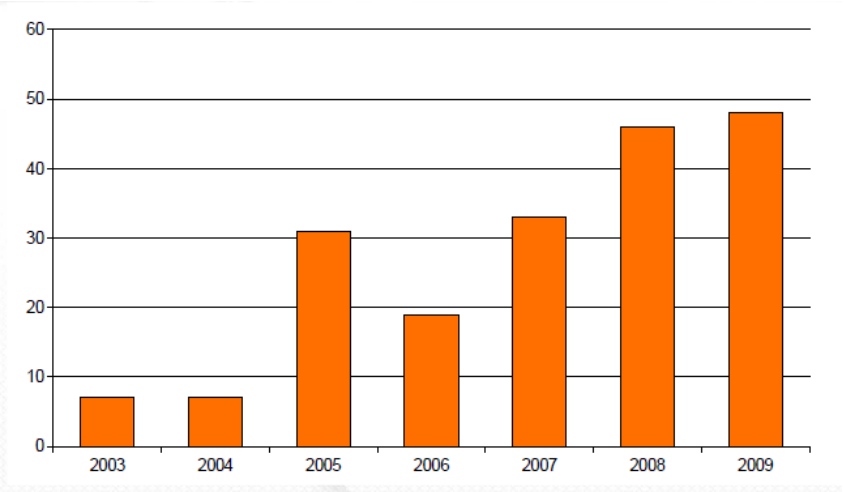


Ilustración 4. Asignaciones IPv6 en la región de LACNIC

El Registro de Internet Regionales (RIR: Regional Internet registry), tiene la función de administrar el espacio de direcciones y otros recursos de internet para una región determinada. En el caso de América Latina y parte del Caribe, el encargado de administrar los recursos de numeración de internet es LACNIC.

La ***Ilustración 5*** muestra la jerarquía de asignación de recursos para el internet.

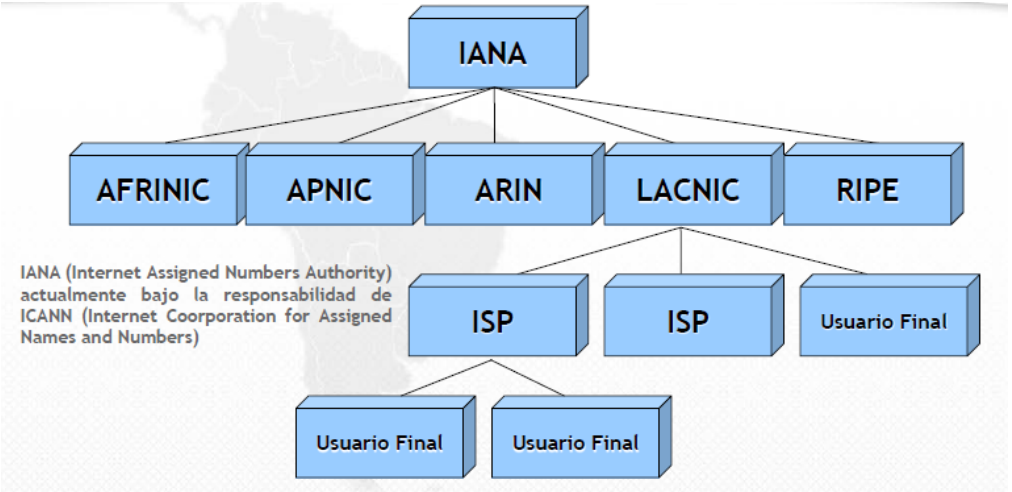


Ilustración 5. Distribución de recursos de numeración de Internet

Los tres recursos fundamentales para el crecimiento y despliegue de Internet son:

- Direcciones IPv4.
- Direcciones IPv6.

- Números de Sistema Autónomo.

EL RIR recibe del IANA[9] y dan al ISP[10]s.

Ilustración 6. Registros de Internet Regionales (RIR)

La ***Ilustración 6*** muestra los cinco Registros Regionales de Internet (RIR) en el mundo[11].

Es complicado estimar la fecha exacta en que se agotarán todas las direcciones IPv4 disponibles, ya que diversos factores pueden adelantar o retrasar la fecha. Dentro de esos factores se encuentran posibles cambios en la política de asginación, recuperación de bloques no utilizados o incluso la venta de direcciones IP entre privados. Una de las fuentes más utilizadas para proyectar el agotamiento de direcciones IPv4 es el sitio "IPv4 Address Report[12]", que a partir de la información publicada por el IANA y los registros regionales, entrega una fecha estimada de agotamiento de direcciones IPv4. El 3 de febrero se agotó el pool de IPv4 de IANA.

[9] **IANA** (Internet Assigned Numbers Authority), es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

[10] **ISP** (proveedor de servicios de Internet o ISP, por la sigla en inglés de *Internet Service Provider*) es una empresa que brinda conexión a Internet a sus clientes).

[11] http://www.iana.org/numbers/

[12] http://www.potaroo.net/tools/ipv4/

Ventajas y Desventajas de NAT

Tabla 1. Ventajas y Desventajas de NAT

Ventajas	Desventajas
Reduce la necesidad de direcciones públicas.	La traducción se hace compleja a veces (FTP, etc.).
Facilita plan de numeración interna.	No es escalable.
Es transparente para algunas aplicaciones.	Puede dar problemas al unificar varias redes.
Oculta topología en forma automática ("seguridad vs ocultamiento").	Rompe el paradigma end-to-end de Internet.
Punto de delimitación clara para los ISPs.	No funciona con gran número de "servidores", P2P.
	Inhiben el desarrollo de nuevos servicios y aplicaciones.
	Problemas con IPsec
	Aumenta el coste de desarrollo de aplicaciones.
	Comprometen las prestaciones, robustez, seguridad y manejabilidad de Internet.

1.2. Ventajas de IPv6

Ventajas adicionales con direcciones mayores

- Facilidad para la auto-configuración.
- Facilidad para la gestión/delegación de las direcciones.
- Espacio para más niveles de jerarquía y para la agregación de rutas.
- Habilidad para las comunicaciones extremo-a-extremo con IPsec (porque no necesitamos NATs).

En la siguiente tabla se muestran las caractisticas similares que tiene IPv4 e IPv6:

Tabla 2. Similitudes IPv4 & IPv6

	IPv4	IPv6
Direccionamiento	32 bits	128 bits
Resolución de direcciones hardware	ARP	ICMPv6 ND/NA
Auto-configuración de host	DHCP & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (opcional)
IPsec	Opcional	Recomendado (no obligatorio)
Fragmentación	Ambos host y routers puede fragmentar	Solo host fragmentan paquetes
QoS	Sin identificación QoS	Identificacion QoS

Ventajas adicionales con el nuevo despliegue

- Oportunidad para eliminar parte de la complejidad, ejemplo en la cabecera IP.
- Oportunidad para actualizar la funcionalidad, ejemplos como multicast, QoS, movilidad.
- Oportunidad para incluir nuevas características, ejemplo “binding updates”.

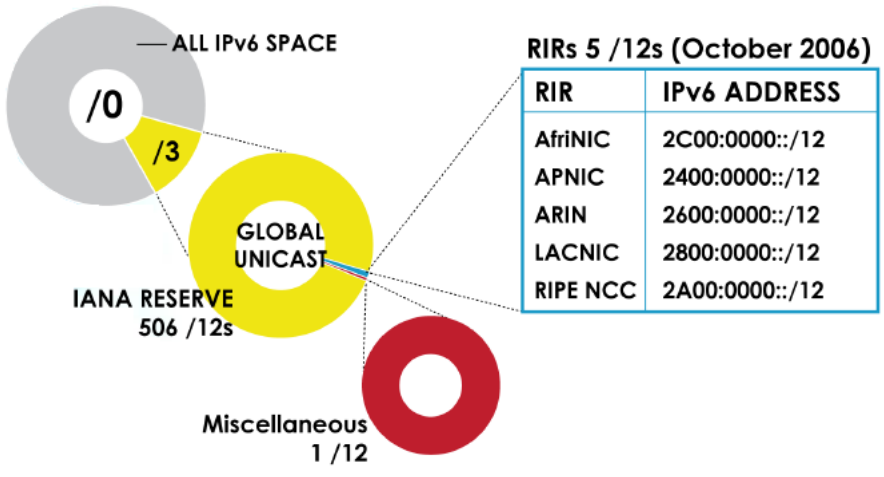


Ilustración 7. Direcciones IPv6[13]

[13] Fuente http://www.nro.net a 31 de Marzo 2011

En ***Ilustración 7***[14] se muestra el espacio de direcciones IPv6, donde los prefijos IPv6 2000::/3 estan asignados para Global Unidicast, de este bloque de direcciones se han reservado por la IANA el prefijo 2C00:0000::/12 a AfriNIC, 2400:0000::/12 para APNIC, 2600:0000::/12 para ARIN, 2800:0000::/12 para LACNIC y 2A00:0000::/12 para RIPE NCC.

Características principales de IPv6

En resumen, las características fundamentales de IPv6 son:

- Mayor espacio de direcciones.
- Autoconfiguración y reconfiguración "sin servidor" ("Plug & Play").
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS: Quality of Service) y Clase de Servicio (CoS: Class of Service).
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los encaminadores (routers), alineados a 64 bits (preparados para su proceso óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65,535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y "multi-homing", que facilita el cambio de proveedor de servicios.
- Características de movilidad más eficientes y robustas.
- Capacidades expandidas de direccionamiento.
- Habilidad para las comunicaciones extremo-a-extremo con IPsec (porque no necesitamos NATs).

[14] http://www.iana.org/numbers/

- Incorporación de encriptación y autenticación en la capa IP.
- Soporte mejorado de opciones/extensiones.

Cabe mencionar, que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de otro manera, se escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando.

Precisamente, la escalabilidad es la baza más importante de IPv6 frente a IPv4. En la ***Ilustración 8*** se muestra en el modelo OSI a IPv6 como un protocolo de red, que al igual que IPv4 es un protocolo no orientado a conexión, sin garantía de envío (no hay retransmisiones), ni control de flujo o congestión.

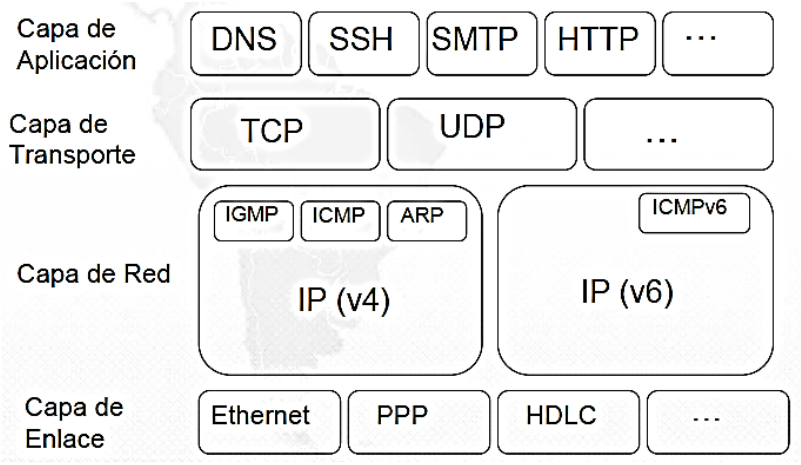


Ilustración 8. IPv6, un protocolo de capa de red

Motivación

Hay varias razones para implementar IPv6 en su red de datos operativa:

- Seguir en Internet.
- Recomendación de LACNIC.
- Agotamiento de direcciones IPv4: IANA no tiene más direcciones públicas. En poco tiempo LACNIC.

- Tecnologías que se conciben con IPv6: Los estándares de 3G recomiendan el uso de IPv6. La movilidad IP con IPv6 (MIPv6[15]) abre un abanico de posibilidades que pueden aprovecharse para ofrecer nuevos servicios.
- Preparados para el futuro: Lo que está por venir sin duda se basará en IPv6, hay que estar preparados para ello.
- Estar a la vanguardia tecnológica de la región: Oportunidad única para subir un escalón en tecnologías de red y en imagen dentro de Latinoamérica y el Caribe.
- Nuevas oportunidades: IPv6 es un "habilitador" de nuevos servicios y por tanto de nuevas oportunidades de negocio.

[15] **Mobile IPv6** (MIPv6) es un protocolo desarrollado como un subconjunto del protocolo de Internet versión 6 (IPv6) para soportar las conexiones móviles.

2. FORMATO DE CABECERAS Y TAMAÑO DE PAQUETES

2.1. Terminología

A continuación se presentan términos básicos en la topología de redes IPv6. En la ***Ilustración 9*** siguiente se muestran los componentes básicos de una red IPv6.

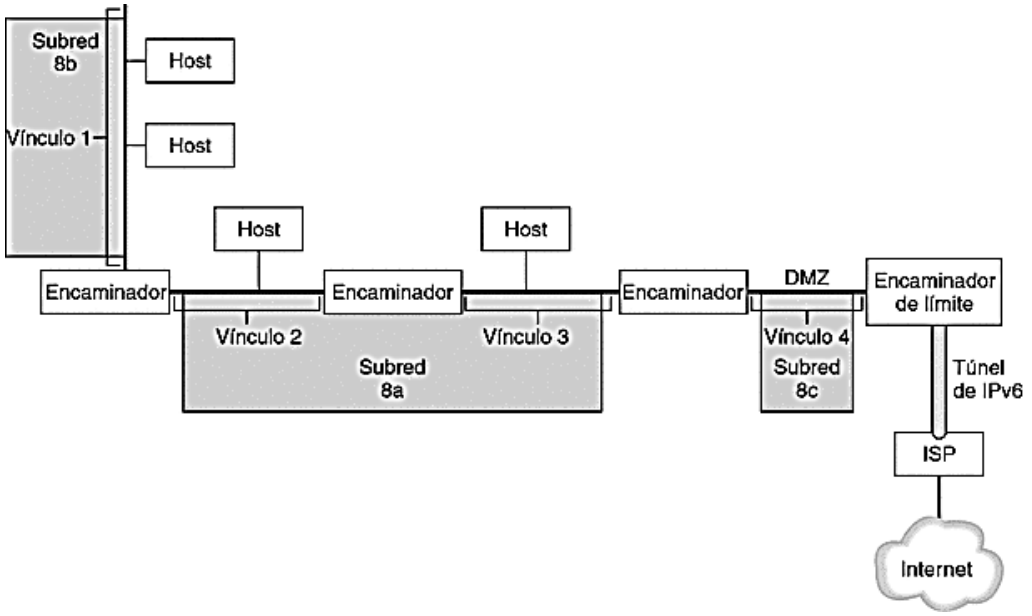


Ilustración 9. Componentes básicos de una red IPv6

La ***Ilustración 9.*** Componentes básicos de una red IPv6 muestra una red IPv6 y sus conexiones con un ISP. La red interna consta de los vínculos 1, 2, 3 y 4. Los hosts rellenan los vínculos y un enrutador los termina. El vínculo 4, considerado la DMZ[16] de la red, queda terminado en un extremo por el enrutador de límite. El enrutador de límite ejecuta un túnel IPv6 a un ISP, que ofrece conexión a Internet para la red. Los vínculos 2 y 3 se administran como subred 8a. La subred 8b tan sólo consta de sistemas en el vínculo 1. La subred 8c es contigua a la DMZ del vínculo 4.

Como se muestra en la ***Ilustración 9*** anterior, una red IPv6 tiene prácticamente los mismos componentes que una red IPv4. No obstante, la terminología de IPv6 presenta

[16] **DMZ** o zona desmilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

ligeras diferencias respecto a la de IPv4. A continuación se presenta una serie de términos sobre componentes de red empleados en un contexto de IPv6:

- ***Nodo***. Sistema con una dirección IPv6 y una interfaz configurada para admitir IPv6. Término genérico que se aplica a hosts y enrutadores.
- ***Enrutador de IPv6***. Nodo que reenvía paquetes de IPv6. Para admitir IPv6, debe configurarse como mínimo una de las interfaces del enrutador. Un enrutador de IPv6 también puede anunciar el prefijo de sitio IPv6 registrado para la empresa en la red interna.
- ***Host de IPv6***. Nodo con una dirección IPv6. Un host IPv6 puede tener configurada más de una interfaz para que sea compatible con IPv6. Al igual que en IPv4, los hosts de IPv6 no reenvían paquetes.
- ***Vínculo***. Un solo soporte contiguo de red conectado por un enrutador en cualquiera de sus extremos.
- ***Vecino***. Nodo de IPv6 que se encuentra en el mismo vínculo que el nodo local.
- ***Subred IPv6***. Segmento administrativo de una red IPv6. Los componentes de una subred IPv6 se pueden corresponder directamente con todos los nodos de un vínculo, igual que en IPv4. Si es preciso, los nodos de un vínculo se pueden administrar en subredes independientes. Además, IPv6 no permite subredes multivínculo, en las cuales los nodos de vínculos distintos pueden ser componentes de una sola subred. Los vínculos 2 y 3 de la ***Ilustración 9*** son componentes de la subred 8a multivínculo.
- ***Túnel de IPv6***. Túnel que proporciona una ruta de extremo a extremo virtual entre un nodo de IPv6 y otro punto final de nodo de IPv6. IPv6 permite la configuración manual de túneles y automática de túneles de 6to4.
- ***Enrutador de límite***. Enrutador en el límite de una red que proporciona un extremo del túnel de IPv6 a un punto final fuera de la red local. Este enrutador debe tener como mínimo una interfaz de IPv6 a la red interna. En cuanto a la red externa, el enrutador puede tener una interfaz de IPv6 o IPv4.

- ***Paquete***: una cabecera IPv6 junto a los datos que incorpora.
- ***Ruta MTU***: MTU mínima en el camino que recorren los paquetes IPv6 entre dos nodos finales.

2.2. Formato cabecera IPv6

Hay varios cambios al formato de encabezados de IPv6. Los diagramas describen en alto nivel la comparación entre IPv4 e IPv6. La ***Ilustración 10*** muestra el formato de cabecera IPv4.

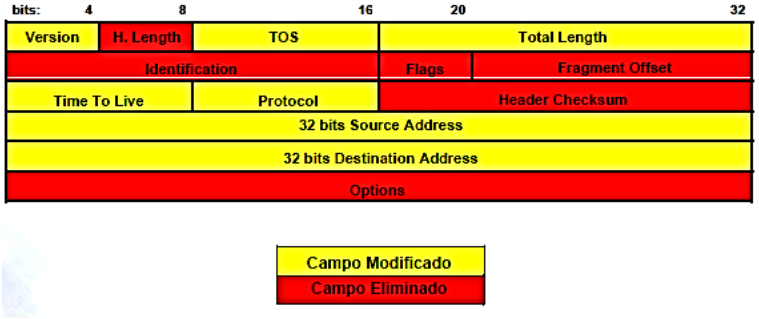


Ilustración 10. Formato de la cabecera IPv4

En el formato de la cabecera IPv6 el número de campos, respecto a IPv4, se ha reducido de 13 a 8, como se muestra en la siguiente ***Ilustración 11***:

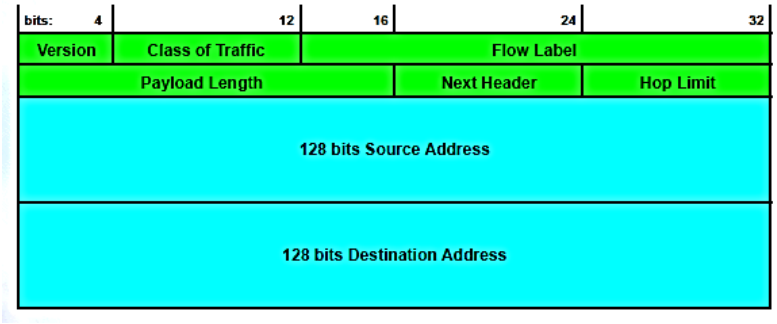


Ilustración 11. Formato de la cabecera IPv6

El protocolo IPv6 reeemplaza el campo "Options" de IPv4 por las denominadas cabeceras adicionales. Estas cabeceras permiten expandir el funcionamiento de IPv6, sin verse restringidas a un campo de tamaño fijo como el presente en IPv4. Las cabeceras

adicionales se ubican inmediatamente después de la cabecera IPv6 y antes de la cabecera del protocolo superior (UPD o TCP).

Resumen de los cambios de la cabecera:

- Reducción de 13 a 8 campos (40 bytes).
- Direcciones incrementadas de 32 a 128 bits.
- Campos de fragmentación y opciones retirados de la cabecera básica.
- Retirado del checksum de la cabecera.
- Longitud de la cabecera es sólo la de los datos (dado que la cabecera tiene una longitud fija).
- Nuevo campo de etiqueta de flujo.
- TOS[17] → Traffic Class.
- Protocol → Next Header (cabeceras de extensión).
- Time to live → Hop Limit.
- Alineación ajustada a 64 bits.
- Las cabeceras NO son compatibles.

Cabeceras de extensión

El encabezado de IPv4 incluye todas las opciones. Por lo tanto, cada enrutador intermedio debe comprobar su existencia y procesarlas cuando están presentes. Esto puede causar un deterioro del rendimiento en el reenvío de paquetes IPv4. Con IPv6, las opciones de entrega y reenvío pasan a los encabezados de extensión. El único encabezado de extensión que debe procesarse en cada enrutador intermedio es el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto). Así aumenta

[17] **ToS** (Type of Service), es una parte de la cabecera de los paquetes de datos en una red IP, pensado para llevar banderas o marcas.

la velocidad de procesamiento del encabezado de IPv6 y mejora el rendimiento del proceso de reenvío.

En RFC 2460[18] se definen los siguientes encabezados de extensión de IPv6 que deben admitir todos los nodos de IPv6:

- Encabezado Hop-by-Hop Options (Opciones de salto a salto).
- Encabezado Destination Options (Opciones de destino).
- Encabezado Routing (Enrutamiento).
- Encabezado Fragment (Fragmento).
- Encabezado Authentication (Autenticación).
- Encabezado Encapsulating Security Payload (ESP o Carga de seguridad de encapsulación).

En un paquete IPv6 típico, no hay encabezados de extensión. Si se precisa un tratamiento especial por parte de los enrutadores intermedios o del destino, el host de envío agrega uno o varios encabezados de extensión.

Cada encabezado de extensión debe adaptarse a los límites de 64 bits (8 bytes). Los encabezados de extensión de tamaño variable contienen un campo Header Extension Length (Longitud de extensión de encabezado) y deben utilizar el relleno cuando sea necesario para asegurarse de que el tamaño sea múltiplo de 8 bytes.

En la ***Ilustración 12*** siguiente se muestra el campo Next Header (Encabezado siguiente) y ninguno o varios encabezados de extensión que componen una cadena de punteros. Cada puntero indica el tipo de encabezado que viene después del encabezado inmediato hasta que el protocolo de nivel superior se identifica definitivamente.

[18] RFC2460: “Especificación del Protocolo de Internet versión 6 (IPv6)”.

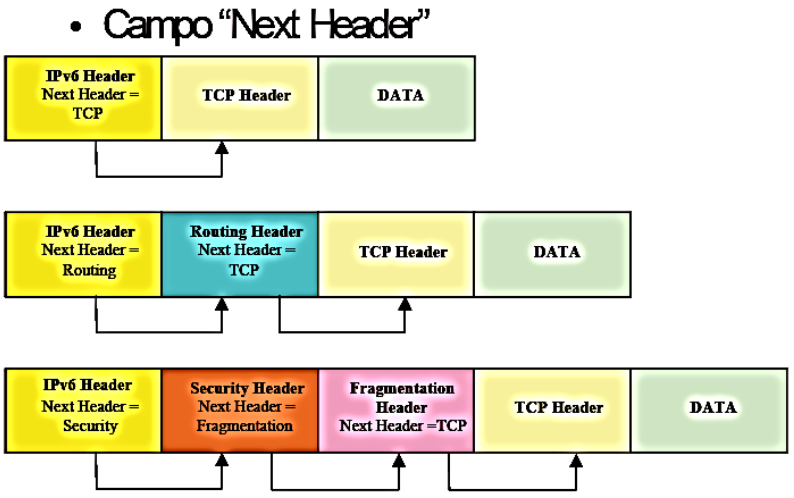


Ilustración 12. Cabeceras de Extensión

Ventajas de las Cabeceras de Extensión

- Procesadas sólo por los nodos destino.
  - Excepción: Hop-by-Hop Options Header.
- Sin limitaciones de "40 bytes" en opciones (IPv4).
- Cabeceras de extensión definidas hasta el momento (usar en este orden):
  - Hop-by-Hop Options (0).
  - Destination Options (60) / Routing (43).
  - Fragment (44).
  - Authentication (RFC4302[19], next header = 51).
  - Encapsulating Security Payload (RFC4303[20], next header = 50).
  - Destination Options (60).
  - Mobility Header (135).

[19] RFC 4302: "Cabecera de Autenticación IP".
[20] RFC 4303: "IP Encapsulating Security Payload (ESP)".

- No Next Header (59).
  - TCP (6), UDP (17), ICMPv6 (58).

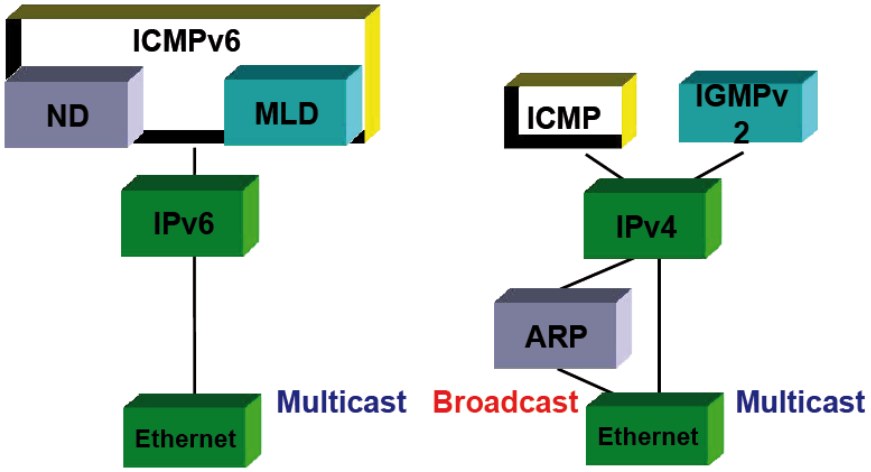


Ilustración 13. Plano de control IPv4 vs. IPv6

En la ***Ilustración 13***, ICMPv6 es la parte integral del protocolo IPv6 y debe ser implementado en cada nodo. Puesto que las funciones de ICMPv6 son:

- Diagnósticos (ping).
- Descubrimiento de vecinos, de routers y de parámetros.
- Autoconfiguración de interfaz.
- Resolución de direcciones (IP a capa de enlace).
- Detección de próximo salto (ruta por defecto).
- Detección de caída de vecinos.
- Detección de direcciones duplicadas.
- Redireccionamiento.
- Asociación a grupos de multicast.

2.3. Consideraciones sobre tamaño de paquete

MTU mínimo

- Link MTU: El máximo MTU (MTU: Maximum Transmission Unit) del link, es decir, el tamaño máximo del paquete IP que puede transmitirse sobre el link.
- Path MTU: El mínimo MTU de todos los links en la ruta desde el nodo origen hasta el nodo destino.
- El mínimo link MTU para IPv6 es de 1280 bytes en vez de 68 bytes como en el caso de IPv4.
- En links donde Path MTU < 1280, es necesario usar fragmentación y reensamblado en el nivel de enlace.
- En links donde se puede configurar el MTU, se recomienda usar el valor de 1500 bytes.

Descubrimiento del Path MTU (RFC 1891[21])

- Las implementaciones deben realizar el descubrimiento del path MTU enviando paquetes mayores de 1280 bytes.
    - Para cada destino, se comienza asumiendo el MTU del primer salto.
    - Si un paquete llega a un link en el que el MTU es menor que su tamaño, se envía al nodo origen un paquete ICMPv6 “packet too big”, informando del MTU de ese link. Dicho MTU se guarda para ese destino específico.
    - Ocasionalmente se descartan los valores almacenados de MTU para detectar posibles aumentos del MTU para los diversos destinos.

[21] RFC 1891: “SMTP Service Extension for Delivery Status Notifications”.

- Las implementaciones minimalistas pueden omitir todo el proceso de descubrimiento de MTU si observan que los paquetes de 1280 bytes pueden llegar al destino.
    - Útil en implementaciones residentes en ROM.

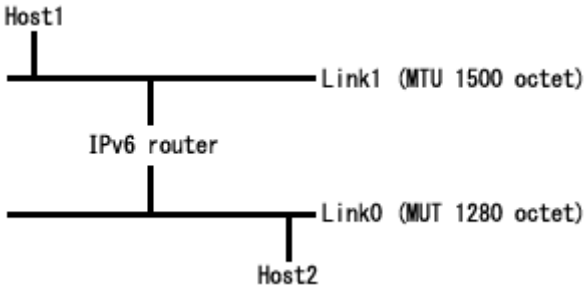


Ilustración 14. Descubrimiento del Path MTU

Como ejemplo, tomemos un caso en el cual se conecta un router a dos enlaces con MTU diferentes (***Ilustración 14.*** Descubrimiento del Path MTU), y considerar la forma en que la comunicación debe ser respondida en el router sin función del valor de MTU. Con las conexiones a como se muestra en la ***Ilustración 14.*** Descubrimiento del Path MTU, el router no puede transferir paquetes desde el host 1 al host 2 que tiene un enlace MTU mayor, puesto que los paquetes son de tamaño máximo de la MTU más grande (host 1) y este supera el tamaño del paquete de la MTU del vínculo con el host 2. Por lo tanto, el router debe enviar un mensaje de error ICMP (Paquete demasiado grande) al host 1. Pero si un router se conecta siempre a los vínculos con el MTU mismo, y si no tiene ninguna función para cambiar el valor MTU lógica (por ejemplo, un túnel), nunca tendrá que enviar un mensaje de error ICMP (Paquete demasiado grande), ni tampoco tiene que tener la función de ajuste MTU.

Cabecera de fragmentación

Se emplea cuando el paquete que se desea transmitir es mayor que el Path MTU existente hacia el destino. En la ***Ilustración 15*** se muestra el formato de la cabecera de fragmentación.

En IPv6 la fragmentación se realiza en el origen, nunca en los nodos intermedios.

8 bits	8 bits	13 bits unsigned	2 bits	1 bit
Next Header	Reserved = 0	Fragment Offset	Res. = 0	M
Identification				

Ilustración 15. Cabecera de Fragmentación

Aunque no es recomendable, se puede usar la cabecera Fragment Header para ayudar a los protocolos superiores a realizar el descubrimiento del path MTU.

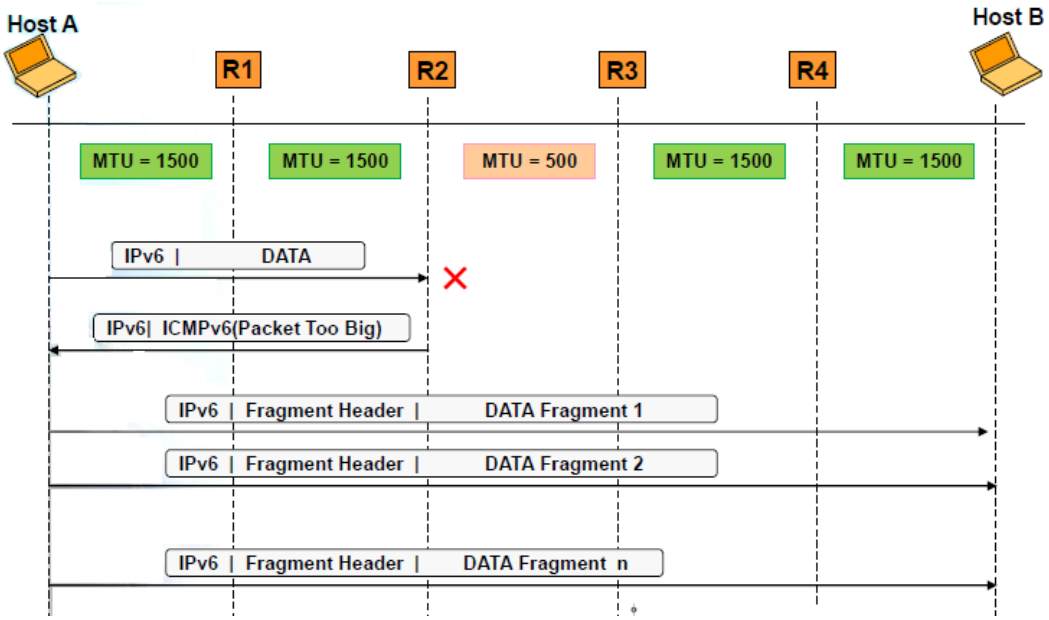


Ilustración 16. Fragmentación en Origen

La fragmentación y reensamblado de los paquetes IPv6 es una función que se realiza en los extremos finales. Los encaminadores no fragmentan los paquetes si estos resultan ser demasiado grandes para el link por el que van a encaminar sino que envían un paquete ICMPv6 de tipo “packet too big”, lo cual se aprecia en la ***Ilustración 16***.

Proceso de fragmentación

La parte fragmentable del paquete original se divide en fragmentos de tamaño múltiplo de 8 bytes, excepto el último. Cada fragmento se envía en paquetes separados, a como se puede observar en la ***Ilustración 17***:

Unfragmentable Part	1st Fragment	2nd Fragment	...	Last Fragment

Ilustración 17. Formato de fragmentación

Quedando los paquetes fragmentados, como lo indica la ***Ilustración 18***:

Unfragmentable Part	Fragment Header	1st Fragment
Unfragmentable Part	Fragment Header	2nd Fragment
• • •		
Unfragmentable Part	Fragment Header	Last Fragment

Ilustración 18. Paquetes fragmentados

3. DIRECCIONAMIENTO IPV6

3.1. Tipos de direcciones

Las direcciones IPv6 se asignan a interfaces en lugar de a nodos, teniendo en cuenta que en un nodo puede haber más de una interfaz. Así mismo, se puede asignar más de una dirección IPv6 a una interfaz.

IPv6 abarca tres clases de direcciones:

A. **Unidifusión**. Identifica una interfaz de un solo nodo. Una dirección de unidifusión identifica una única interfaz en el ámbito del tipo de dirección de unidifusión. La ***Ilustración 19*** muestra la definición.

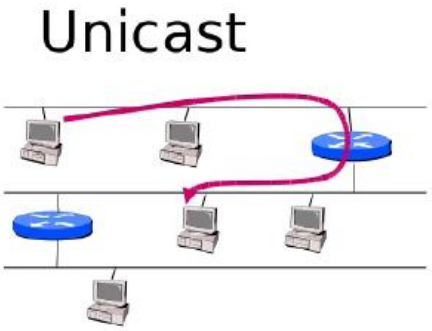


Ilustración 19. Dirección Unicast (Unidifusión)

B. **Multidifusión**. Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección multidifusión se dirigen a todos los miembros del grupo de multidifusión. Una dirección de multidifusión identifica varias interfaces, como se presenta en la ***Ilustración 20***.

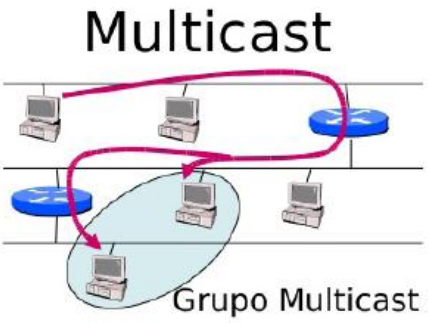


Ilustración 20. Dirección Multicast (Multidifusión)

C. **Difusión por proximidad**. Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección de difusión por proximidad se dirigen al nodo de miembros del grupo de difusión por proximidad que se encuentre más cerca del remitente. Una dirección por proximidad identifica varias interfaces. La ***Ilustración 21*** muestra la definición de difusión por proximidad.

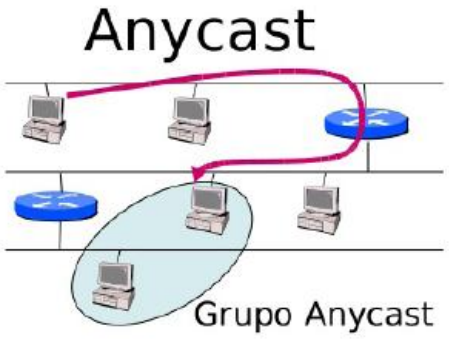


Ilustración 21. Dirección Anycast (Difusión por proximidad)

Las direcciones IPv6 siempre identifican interfaces, no nodos. Un nodo es identificado por una dirección de unidifusión que se haya asignado a una de sus interfaces.

Las direcciones IPv6 tienen diferentes alcances: link-local, global. Un host puede usar diferentes direcciones de diferentes tipos y alcances al mismo tiempo.

Direcciones unidifusión

Las direcciones IPv6 de unidifusión pueden ser de cinco tipos:

a) Direcciones globales de unidifusión.

Las direcciones globales de unidifusión equivalen a las direcciones IPv4 públicas. Se pueden enrutar y se puede tener acceso a ellas globalmente en la red Internet IPv6.

A diferencia de la red Internet actual basada en IPv4, que es una combinación de enrutamiento jerárquico y plano, la red Internet basada en IPv6 se ha diseñado desde la base para admitir una infraestructura de direccionamiento y enrutamiento eficaz y jerárquica. El ámbito (es decir, la región de la red IPv6 en la que la dirección es única) de una dirección global de unidifusión es la red Internet IPv6 completa.

En la siguiente ***Ilustración 22.*** Estructura de una dirección global de unidifusiónse muestra la estructura de una dirección global de unidifusión según la definición del documento RFC 3587[22].

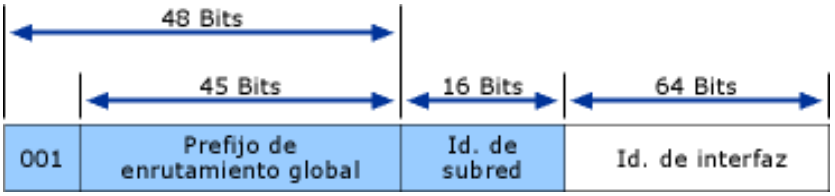


Ilustración 22. Estructura de una dirección global de unidifusión

Las direcciones globales de unidifusión contienen cuatro campos.

- Los tres bits de valor superior están establecidos en 001. El prefijo de la dirección para las direcciones globales asignadas actualmente es 2000::/3.
- El prefijo de enrutamiento global indica el prefijo de enrutamiento global del sitio de una organización específica. La combinación de los tres bits fijos y el prefijo de enrutamiento global de 45 bits crea un prefijo del sitio de 48 bits, que se asigna a un sitio individual de una organización. Una vez asignado este prefijo, los enrutadores de Internet IPv6 envían el tráfico IPv6 que coincide con el prefijo de 48 bits a los enrutadores del sitio de la organización.
- El identificador de subred se usa en el sitio de la organización para identificar subredes. Este campo tiene 16 bits de longitud. El sitio de la organización puede

[22] RFC 3587: "Formato global de direcciones Unicast IPv6".

usar estos 16 bits en el sitio para crear 65.536 subredes o varios niveles de jerarquía de direccionamiento y una infraestructura de enrutamiento eficaz.

- El identificador de interfaz indica la interfaz de una subred específica del sitio. Este campo tiene 64 bits de longitud.

En la siguiente ***Ilustración 23.*** Estructura de tres niveles de la dirección global de unidifusiónse muestra cómo los campos de una dirección global de unidifusión crean una estructura de tres niveles.

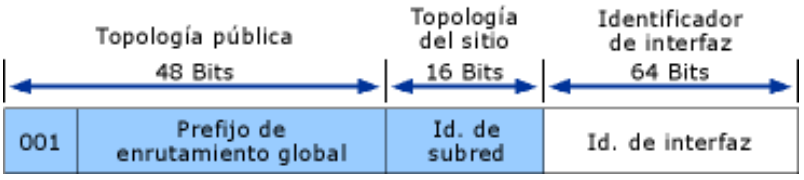


Ilustración 23. Estructura de tres niveles de la dirección global de unidifusión

La topología pública es la colección de proveedores ISP (Internet Service Provider) grandes y pequeños que proporcionan acceso a la red Internet IPv6. La topología del sitio es la colección de subredes del sitio de una organización. El identificador de interfaz identifica una interfaz específica en una subred del sitio de una organización.

Las direcciones de unidifusión de uso local pueden ser de dos tipos:

- Direcciones locales del vínculo, que se usan entre vecinos en vínculo y en procesos de detección de vecinos.
- Direcciones locales del sitio, que se usan entre nodos del mismo sitio.

b) Direcciones locales del vínculo

Los nodos usan direcciones locales del vínculo para comunicarse con nodos vecinos que están en el mismo vínculo. Por ejemplo, en una red IPv6 de vínculo único sin enrutador, las direcciones locales del vínculo se usan para la comunicación entre los hosts del vínculo. Las direcciones locales del vínculo equivalen a las direcciones IPv4 de dirección IP privada automática (APIPA[23]: Automatic Private Internet Protocol Addressing)

[23] **APIPA** (Direccionamiento privado Automático del Protocolo de Internet) es un protocolo que utilizan los sistemas que corren bajo Windows 98 o versiones posteriores para obtener la

configuradas de forma automática en equipos que ejecutan Windows. Las direcciones APIPA usan el prefijo 169.254.0.0/16. El ámbito de una dirección local del vínculo es el vínculo local.

En los procesos de detección de vecinos es necesaria una dirección local del vínculo, que siempre se configura de forma automática, incluso si no hay ninguna otra dirección de unidifusión.

En la siguiente ***Ilustración 24*** se muestra la estructura de la dirección local del vínculo.

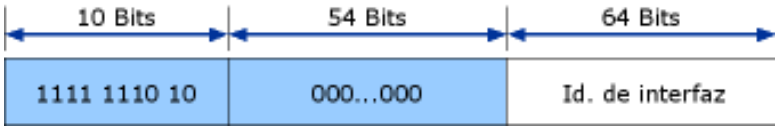


Ilustración 24. Estructura de dirección local de vínculo

Las direcciones locales del vínculo siempre empiezan por FE80. Con el identificador de interfaz de 64 bits, el prefijo de las direcciones locales del vínculo es siempre FE80::/64. Un enrutador IPv6 nunca reenvía el tráfico local del vínculo fuera del vínculo.

c) Direcciones locales del sitio

Las direcciones locales del sitio equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16). Por ejemplo, las intranets privadas que no tienen una conexión directa enrutada a la red Internet IPv6 pueden usar las direcciones locales del sitio sin entrar en conflicto con las direcciones globales. Las direcciones locales del sitio no son accesibles desde otros sitios y los enrutadores no deben reenviar el tráfico local del sitio fuera del sitio. Las direcciones locales del sitio se pueden usar junto con las direcciones globales. El ámbito de una dirección local del sitio es el sitio.

A diferencia de las direcciones locales del vínculo, las direcciones locales del sitio no se configuran de forma automática y deben asignarse mediante procesos de configuración de direcciones sin estado o con estado.

En la siguiente ***Ilustración 25*** se muestra la estructura de la dirección local del sitio.

configuración de red cuando el sistema esta configurado para obtener una dirección dinámicamente, y al iniciar, éste no encuentra un servidor DHCP.

Ilustración 25. Estructura de dirección local del sitio

Los primeros 10 bits siempre son fijos en las direcciones locales del sitio y empiezan por FEC0::/10. Después de los 10 bits fijos hay un identificador de subred de 54 bits (campo del identificador de subred) que proporciona 54 bits con los que se puede crear dentro del sitio una infraestructura de enrutamiento jerárquica que se puede resumir. Después del campo del identificador de subred está el campo del identificador de interfaz de 64 bits, que identifica una interfaz específica en una subred.

d) Direcciones especiales

Las direcciones IPv6 especiales son las siguientes:

- Dirección no especificada:

La dirección no especificada (0:0:0:0:0:0:0:0 ó ::) indica la ausencia de dirección. Equivale a la dirección IPv4 no especificada de 0.0.0.0. La dirección no especificada se suele usar como dirección de origen de paquetes que intentan comprobar la exclusividad de una dirección provisional. La dirección no especificada nunca se asigna a una interfaz ni se usa como dirección de destino.

- Dirección de bucle invertido:

La dirección de bucle invertido (0:0:0:0:0:0:0:1 ó ::1) se usa para identificar una interfaz de bucle invertido, lo que permite que un nodo se envíe paquetes a sí mismo. Equivale a la dirección IPv4 de bucle invertido de 127.0.0.1. Los paquetes destinados a la dirección de bucle invertido no deben enviarse nunca en un vínculo ni deben reenviarse mediante un enrutador.

e) Direcciones de compatibilidad.

Para facilitar la migración de IPv4 a IPv6 y la coexistencia de ambos tipos de hosts, se han definido las siguientes direcciones:

- Dirección compatible con IPv4:

Los nodos IPv6/IPv4 que se comunican mediante IPv6 usan la dirección compatible con IPv4, 0:0:0:0:0:0:w.x.y.z ó ::w.x.y.z (donde w.x.y.z es la representación decimal con punto de una dirección IPv4 pública). Los nodos IPv6/IPv4 son compatibles con los protocolos IPv4 y IPv6. Cuando se usa una dirección compatible con IPv4 como destino IPv6, el tráfico IPv6 se encapsula automáticamente con un encabezado IPv4 y se envía al destino mediante la infraestructura IPv4.

- Dirección asignada a IPv4:

La dirección asignada a IPv4, 0:0:0:0:0:FFFF:w.x.y.z ó ::FFFF:w.x.y.z, se usa para representar un nodo exclusivo de IPv4 en un nodo IPv6. Sólo sirve para la representación interna. La dirección asignada a IPv4 nunca se usa como dirección de origen o de destino de un paquete IPv6.

- Dirección 6to4:

La dirección 6to4 se usa para la comunicación entre dos nodos que ejecutan IPv4 e IPv6 en una infraestructura de enrutamiento IPv4. La dirección 6to4 se crea mediante la combinación del prefijo 2002::/16 con los 32 bits de una dirección IPv4 pública del nodo, con lo que se forma un prefijo de 48 bits. 6to4 es una técnica de túnel que se describe en el documento RFC 3056[24].

- Dirección ISATAP:

El borrador de Internet titulado "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)[25]" define las direcciones ISATAP que se usan entre dos nodos que ejecutan IPv4 e IPv6 en una infraestructura de enrutamiento IPv4. Las direcciones ISATAP usan el identificador de interfaz administrado localmente ::0:5EFE:w.x.y.z donde w.x.y.z es una dirección IPv4 de unidifusión, que incluye direcciones públicas y privadas.

El identificador de interfaz de ISATAP puede combinarse con cualquier prefijo de 64 bits que sea válido para direcciones IPv6 de unidifusión. Esto incluye el prefijo de dirección local del vínculo (FE80::/64), los prefijos locales del sitio y los prefijos globales.

[24] RFC 3056: "Conexión de dominios IPv6 a través de nubes IPv4".
[25] RFC 4214: "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)".

En la siguiente ***Ilustración 26*** se puede apreciar, que una vez que la resolución de nombres tiene éxito, el host ISATAP envía un mensaje Router Solicitation (RS) encapsulado en IPv4 al enrutador ISATAP. El router ISATAP responde con un mensaje Router Advertisement (RA) encapsulado en un IPv4 unicast. El mensaje contiene información de prefijo RA, y opcionalmente una ruta por defecto de ruta con él mismo como el siguiente salto.

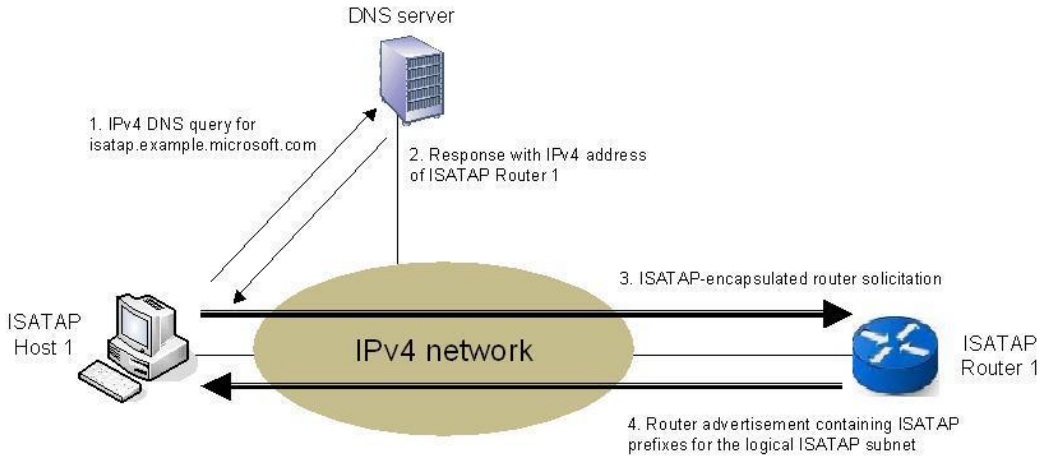


Ilustración 26. Intercambio de mensajes en ISATAP

Una vez que la máquina obtiene una dirección IPv6 adecuada, es capaz de llegar a los dominios IPv6 a través del túnel ISATAP, y también puede llegar a los dominios IPv4 normal.

- Dirección Teredo:

Las direcciones Teredo usan el prefijo 3FFE:831F::/32. Más allá de los primeros 32 bits, las direcciones Teredo se usan para codificar las direcciones IPv4 de un servidor Teredo, los marcadores y la versión codificada de la dirección externa y el puerto de un cliente Teredo. Un ejemplo de una dirección Teredo es 3FFE:831F:CE49:7601:8000:EFFF:62C3:FFFE.

Direcciones IPv6 de multidifusión

En IPv6, el tráfico de multidifusión funciona de la misma forma que el tráfico en IPv4. Los nodos IPv6 ubicados de forma arbitraria pueden escuchar el tráfico de multidifusión en

direcciones IPv6 de multidifusión arbitrarias. Los nodos IPv6 pueden escuchar en varias direcciones de multidifusión a la vez. Los nodos pueden unirse a un grupo de multidifusión o salir de él en cualquier momento.

Las direcciones IPv6 de multidifusión tienen los primeros 8 bits establecidos en 1111 1111. Es fácil clasificar una dirección IPv6 como de multidifusión porque siempre empieza por "FF". Las direcciones de multidifusión no se pueden usar como direcciones de origen ni como destinos intermedios en un encabezado de enrutamiento.

Después de los primeros 8 bits, las direcciones de multidifusión contienen otra estructura que identifica los marcadores, el ámbito y el grupo de multidifusión. En la siguiente ***Ilustración 27*** se muestra la estructura de la dirección IPv6 de multidifusión.

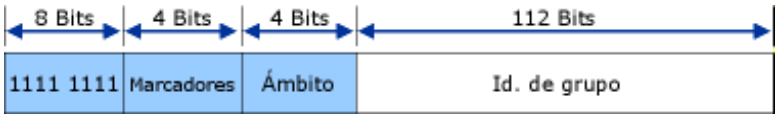


Ilustración 27. Dirección IPv6 de multidifusión

Los campos de la dirección de multidifusión son los siguientes:

- *Marcadores*. Corresponde a los marcadores establecidos en una dirección de multidifusión. El tamaño de este campo es de 4 bits. A partir del documento RFC 3513[26], el único marcador definido es Transitorio (T). El marcador T usa el bit de nivel inferior del campo Marcadores. Si está establecido en 0, el marcador T especifica que la dirección de multidifusión es una dirección de multidifusión conocida asignada permanentemente por la Autoridad de números asignados de Internet (IANA, Internet Assigned Numbers Authority). Si está establecido en 1, el marcador T especifica que la dirección de multidifusión es una dirección de multidifusión transitoria, que IANA no ha asignado permanentemente.
- *Ámbito*. Indica el ámbito de la red IPv6 al que va dirigido el tráfico de multidifusión. El tamaño de este campo es de 4 bits. Además de la información proporcionada por los protocolos de enrutamiento de multidifusión, los enrutadores usan el ámbito de multidifusión para determinar si puede reenviar el

[26] RFC 3513: "Internet Protocol Version 6 (IPv6) Addressing Architecture"

tráfico de multidifusión. Los valores predominantes para el campo Ámbito son 1 (ámbito local de la interfaz), 2 (ámbito local del vínculo) y 5 (ámbito local del sitio).

Por ejemplo, el tráfico con una dirección de multidifusión de FF02::2 tiene un ámbito local del vínculo. Un enrutador IPv6 nunca reenvía este tráfico fuera del vínculo local.

- *Identificador de grupo*. Identifica el grupo de multidifusión y es único en el ámbito. El tamaño de este campo es de 112 bits. Los identificadores de grupo asignados permanentemente son independientes del ámbito. Los identificadores de grupo transitorios son relevantes sólo para un ámbito específico. Las direcciones de multidifusión en el intervalo de FF01:: a FF0F:: son direcciones conocidas y reservadas.

Para identificar todos los nodos de los ámbitos local de la interfaz y local del vínculo, se han definido las siguientes direcciones:

- FF01::1 (dirección de multidifusión para todos los nodos de ámbito local de la interfaz).
- FF02::1 (dirección de multidifusión para todos los nodos de ámbito local del vínculo).

Para identificar todos los enrutadores de los ámbitos local de la interfaz, local del vínculo y local del sitio, se han definido las siguientes direcciones:

- FF01::2 (dirección de multidifusión para todos los enrutadores de ámbito local de la interfaz).
- FF02::2 (dirección de multidifusión para todos los enrutadores de ámbito local del vínculo).
- FF05::2 (dirección de multidifusión para todos los enrutadores de ámbito local del sitio).

Con 112 bits para el identificador de grupo, es posible tener 2112 identificadores de grupo. No obstante, debido a la forma en que las direcciones IPv6 de multidifusión se

asignan a las direcciones de Media Access Control (MAC) de multidifusión de Ethernet, en el documento RFC 3513 se recomienda asignar el identificador de grupo de los 32 bits de nivel inferior de la dirección IPv6 de multidifusión y establecer el resto de los bits del identificador de grupo original en 0. Si sólo se usan los 32 bits de nivel inferior, cada identificador de grupo se asigna a una única dirección MAC de multidifusión de Ethernet. En la siguiente ***Ilustración 28*** se muestra la dirección IPv6 de multidifusión recomendada.

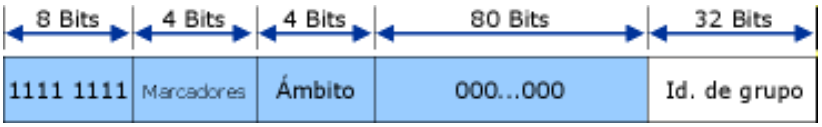


Ilustración 28. Dirección IPv6 de multidifusión recomendada con un identificador de grupo de 32 bits

Dirección de nodo solicitado

La dirección de nodo solicitado facilita la consulta eficaz de los nodos de la red durante la resolución de las direcciones. En IPv4, la trama *Solicitud de ARP* se envía a la difusión de nivel MAC, con lo que afecta a todos los nodos del segmento de red, incluidos los que no ejecutan IPv4. IPv6 usa el mensaje de solicitudes de vecino para llevar a cabo la resolución de direcciones. No obstante, en lugar de usar la dirección de multidifusión para todos los nodos de ámbito local del vínculo como destino del mensaje de solicitudes de vecino, que afectaría a todos los nodos IPv6 del vínculo local, se usa la dirección de multidifusión de nodo solicitado.

En la siguiente ***Ilustración 29*** se muestra cómo la dirección de multidifusión de nodo solicitado se compone del prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 que se esté resolviendo.

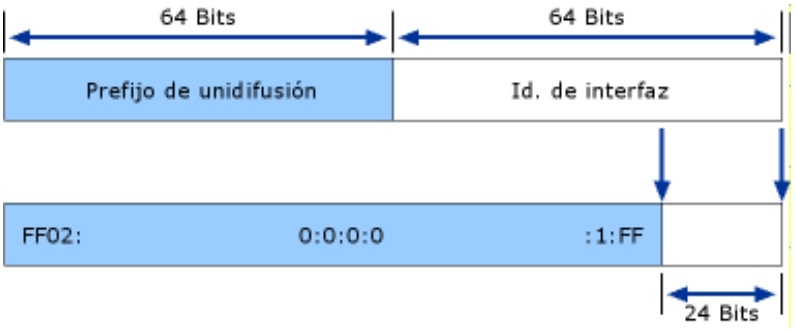


Ilustración 29. Asignación de direcciones IPv6 de unidifusión a dirección IPv6 de nodo solicitado

Por ejemplo, para el nodo con la dirección IPv6 local del vínculo de FE80::2AA:FF:FE28:9C5A, la dirección de nodo solicitado correspondiente es FF02::1:FF28:9C5A. Este nodo escucha el tráfico de multidifusión en la dirección de nodo solicitado de FF02::1:FF28:9C5A y, para las interfaces que corresponden a un adaptador de red físico, ha registrado la dirección de multidifusión correspondiente en el adaptador de red. Para resolver la dirección de FE80::2AA:FF:FE28:9C5A en su dirección de nivel de vínculo, un nodo vecino envía una solicitud de vecino a la dirección de nodo solicitado de FF02::1:FF28:9C5A.

El resultado de usar la dirección de multidifusión de nodo solicitado es que la resolución de direcciones, que suele producirse en un vínculo, no necesita usar un mecanismo que afecte a todos los nodos de la red. De hecho, son muy pocos los nodos que se ven afectados al usar la dirección de nodo solicitado durante la resolución de direcciones. En la práctica, debido a la relación entre la dirección MAC de Ethernet, el identificador de interfaz IPv6 y la dirección de nodo solicitado, ésta actúa como una dirección de pseudounidifusión para lograr una resolución de direcciones muy eficaz.

Direcciones IPv6 de difusión por proximidad

A una dirección de difusión por proximidad se asignan varias interfaces. Con una infraestructura de enrutamiento adecuada, los paquetes destinados a una dirección de difusión por proximidad se entregan en la interfaz más próxima a la que la dirección de difusión por proximidad está asignada.

Para facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces que tienen asignadas direcciones de difusión por proximidad y su distancia en términos de métrica de enrutamiento. Por el momento, las direcciones de difusión por proximidad sólo se usan como direcciones de destino y sólo se asignan a enrutadores.

Las direcciones de difusión por proximidad se asignan desde el espacio de direcciones de unidifusión y el ámbito de una dirección de difusión por proximidad es el ámbito del tipo de dirección de unidifusión desde que se asigna la dirección de difusión por proximidad.

La dirección de difusión por proximidad de un enrutador de subred está predefinida y es obligatoria. Se crea a partir del prefijo de subred de una interfaz determinada. Para crear la dirección de difusión por proximidad de un enrutador de subred, se fijan los valores adecuados para los bits del prefijo de subred y los bits restantes se establecen en 0. A todas las interfaces de enrutador conectadas a una subred se les asigna la dirección de difusión por proximidad de un enrutador de dicha subred. La dirección de difusión por proximidad de un enrutador de subred se usa para comunicarse con uno de varios enrutadores conectados a una subred remota.

3.2. Prefijos y representación

Partes de una dirección IPv6

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la ***Ilustración 30*** siguiente, las equis representan números hexadecimales.

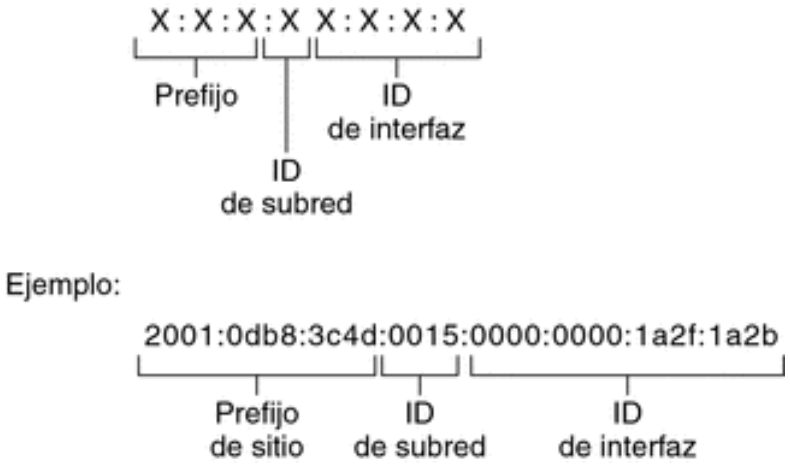


Ilustración 30. Formato básico de las direcciones IPv6

Los tres campos que están más a la izquierda (48 bits) contienen el prefijo de sitio. El prefijo describe la topología pública que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el ID de subred de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la topología privada, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el ID de interfaz, también denominado token. El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Examine de nuevo la dirección de la figura ***Ilustración 30***:

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, 2001:0db8:3c4d, contienen el prefijo de sitio y representan la topología pública. Los siguientes 16 bits, 0015, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, 0000:0000:1a2f:1a2b, contienen el ID de interfaz.

Prefijos

Cada dirección IPv6 incluye bits que identifican una red y un nodo o interfaz. Un prefijo de IPv6 es la parte de una dirección IPv6 que identifica la red. La longitud del prefijo es un entero positivo que denota un número de bits consecutivos, a partir del bit más significativo (el del extremo izquierdo). La longitud del prefijo lleva delante una diagonal y, en la mayoría de los casos, representa la parte de la dirección que es propiedad de la organización. Todos los bits restantes (hasta el bit situado más a la derecha) representan nodos o interfaces individuales.

Por ejemplo, 32f1::250:af:34ff:fe26/64 tiene una longitud de prefijo de 64.

Con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones IPv6:

a) No se hace distinción entre mayúsculas y minúsculas.
   "ABC9" es equivalente a "abc9".
b) Los ceros al inicio de un campo son opcionales.
   "00c1" es equivalente a "c1".
c) Una sucesión de campos con ceros pueden ser reemplazados por "::"[27].
   "1234:0000:0000:abc9" es igual a "1234::abc9"

Tomando la dirección de ejemplo siguiente:

2001:0000:1234:0000:0000:C1C0:ABCD:0876

Mediante la regla a), se puede escribir como:

2001:0000:1234:0000:0000:**c**1**c**0:**abcd**:0876

La direccion se puede escribir de forma resumida utilizando la regla b):

2001:**0**:1234:**0**:**0**:c1c0:abcd:**876**

Aplicando la regla c) se puede resumir aún más a:

[27] Esta regla sólo se puede utilizar una vez en una direccion IPv6, de lo contrario el sistema no sabría cuantos campos se han comprimido en cada caso.

2001:0:1234**::**c1c0:abcd:876

Tal como en el caso de IPv4, para señalar las secciones de la que identifican a la red y al dispositivo, se utiliza el formato CIDR en la forma <dirección>/<prefijo>. Por ejemplo, una dirección en la forma 3ffe:b00:c18:1::1/64 señala que los primeros 64 [bit] identifican a la red (3ffe:b00:c18:1) y los restantes 64[bit] identifican al dispositivo de dicha red (::1).

Tradicionalmente el uso del símbolo ":" en las direcciones IPv4 señala un puerto en un determinado nodo, por ejemplo 192.168.1.1:80 señala al puerto 80 (WWW) del nodo 192.168.1.1. Esto representa un problema de incompatibilidad al utilizar direcciones IPv6, por lo que se ha establecido que para señalar un puerto en una determinada dirección IPv6, esta debe estar encerrada por paréntesis cuadrados en la forma [dirección]:puerto.

En la ***Ilustración 31*** se muestran los tipos de direcciones IPv6 con sus respectivos prefijos en binarios y la notación asignada al mismo.

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	00...0:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (deprecated)	1111 1110 11	FEC0::/10
IPv4-compatible (deprecated)	00...0 (96 bits)	::IPv4/128

Global Unicast assigments actually use 2000::/3 (001 prefix)
Anycast addresses allocated from unicast prefixes

Ilustración 31. Tabla de Prefijos de direcciones IPv6

Ejercicios prácticos de Notación de direcciones IPv6

1. Indicar a qué tipo de direcciones pertenece cada una de las siguientes:

Dirección	Tipo
2001:db8:fe80:ffff::a:b:c	
fe80::9ce4:ecde:cf33:a2a2	
2002:1bc3:1b::1:2	
::1	
FD00:a:b:17c2::1	
FF0E::1:2:3:4	
FF05::a:b:c	

Siendo la solución a la tabla anterior la siguiente:

Dirección	Tipo
2001:db8:fe80:ffff::a:b:c	Dirección Unicast global
fe80::9ce4:ecde:cf33:a2a2	Link-Local Unicast
2002:1bc3:1b::1:2	Dirección 6to4
::1	Dirección de Loopback, para auto-envío de paquetes
FD00:a:b:17c2::1	Direccion local única
FF0E::1:2:3:4	Dirección de multidifusión de alcance global
FF05::a:b:c	Dirección de multidifusión de ámbito local del sitio

2. Comprimir al máximo las siguientes direcciones

Ejemplo 1:	*Ejemplo 2:*
2001:0db8:3003:0001:0000:0000:6543:0ffe	**2001:0db8:0000:0000:0300:0000:0000:0abc**
2001:0db8:3003:0001:0:0:6543:0ffe	2001:0db8:0:0:0300:0:0:0abc
2001:0db8:3003:0001::6543:0ffe	2001:0db8:0:0:0300::0abc
2001:db8:3003:1::6543:ffe	2001:db8:0:0:300::abc

Ejemplo 3:	*Ejemplo 4:*
2001:0db8:F181:0000:0000:0000:0000:0000	**0000:0000:0000:0000:0000:ffff:0a55:6677**
2001:0db8:F181:0:0:0:0:0	0:0:0:0:0:ffff:0a55:6677
2001:0db8:F181::0:0:0:0	::0:0:0:0:ffff:0a55:6677
2001:0db8:F181::0:0	::0:0:ffff:0a55:6677
2001:0db8:F181::	::ffff:0a55:6677
2001:db8:F181::	::ffff:a55:6677

3. Descomprimir al máximo las siguientes direcciones

Ejemplo 1:	*Ejemplo 2:*
2001:0DB8::1428:57ab	**2002:9ba0:d:0:ff4::7**
2001:0DB8:0::0:1428:57ab	2002:9ba0:d:0:ff4:0:0:7
2001:0DB8:0:0:0:0:1428:57ab	2002:9ba0:000d:0000:0ff4:0000:0000:0007
2001:0DB8:0000:0000:0000::1428:57ab	
2001:0DB8:0000:0000:0000:0000:1428:57ab	
Ejemplo 3:	*Ejemplo 4:*
2001:0:0:fb0f::acd2:1250	**::ffff:147.51.23.149**
2001:0:0:fb0f:0:0:acd2:1250	::0:0:ffff:147.51.23.149
2001:0000:0000:fb0f:0000:0000:acd2:1250	::0:0:0:0:ffff:147.51.23.149
	0:0:0:0:0:ffff:147.51.23.149
	0000:0000:0000:0000:0000:ffff:147.51.23.149

Ejemplo de asignación de prefijos y direcciones

1. Subneteo de direcciones IPv6

Ejemplo 1:

Cómo obtenemos /47s en 2001:1::/32?

- Hex 2001 = Binario **0010 0000 0000 0001** = 16 bits
- Hex 0001 = Binario **0000 0000 0000 0001** = 32
- Hex 0000 = Binario **0000 0000 0000 000**0 = 47 (32 bits in prefix –"fixed", 15 bits de subred)

Entonces los 15 bits de subred (verde) son usados para identificar las /47s: Subredes numeradas usando estos bits

- El primer /47 es 2001:0001:0000::/47

  Binario **0000 0000 0000 000**0 = Hex 0000
- El segundo /47 es 2001:0001:0002::/47

  Binario **0000 0000 0000 001**0 = Hex 0002
- El tercero /47 es 2001:0001:0004::/47

  Binario **0000 0000 0000 010**0 = Hex 0004
- El cuarto /47 es 2001:0001:0006::/47

  Binario **0000 0000 0000 011**0 = Hex 0006

Ejemplo 2:

Cómo obtenemos /64s en 2001:2:3::/48 esto es:

- 2001:0002:0003:0001::/64
- 2001:0002:0003:0002::/64

- 2001:0002:0003:0003::/64
- Etc.

Con 16 bits de espacio de dirección

- Se puede tener 65,536 /64s en una dirección /48 IPv6
- Nota: indica que los 64 bits restantes son ceros y se pueden utilizar para identificar hosts::

2. Plan de direccionamiento

Si disponemos del siguiente prefijo: 2001:0db8::/32, para proveer varios servicios, tales como:

- Conectividad de tránsito IP estático
- Conectividad de tránsito BGP
- Todos los servicios son proveedores de multiples países.

Asignación de conectividad IP para la empresa Foobar:

En un /32 podemos tener 256 subredes /40, quedando así:

2001:0db8:0000::/40	**Foobar Infra + uso futuro**
2001:0db8:0100::/40	**Bloque de clientes**
2001:0db8:0200::/40	**Uso futuro**
…	
2001:0db8:fd00::/40	**Uso futuro**
2001:0db8:fe00::/40	**Uso futuro**
2001:0db8:ff00::/40	**Uso futuro**

En cada /40 podemos tener 16 subredes /44.

2001:0db8:0000::/40	**Foobar Infra + uso futuro**
2001:0db8:0000::/44	**Foobar Infra**
2001:0db8:0010::/44	**Uso futuro**
…	
2001:0db8:00e0::/44	**Uso futuro**
2001:0db8:00f0::/44	**Uso futuro**
2001:0db8:0100::/40	**Bloque de clientes**
2001:0db8:0200::/40	**Uso futuro**
…	
2001:0db8:fd00::/40	**Uso futuro**
2001:0db8:fe00::/40	**Uso futuro**
2001:0db8:ff00::/40	**Uso futuro**

En cada /44 podemos obtener 16 subredes /48.

2001:0db8:0000::/40	**Foobar Infra + uso futuro**
2001:0db8:0000::/44	**Foobar Infra**
2001:0db8:0000::/48	**Direcciones de Backbone**
…	
2001:0db8:000f::/48	
2001:0db8:0010::/44	**Uso futuro**
…	
2001:0db8:00e0::/44	**Uso futuro**
2001:0db8:00f0::/44	**Uso futuro**
2001:0db8:0100::/40	**Bloque de clientes**
2001:0db8:0200::/40	**Uso futuro**
…	
2001:0db8:fd00::/40	**Uso futuro**
2001:0db8:fe00::/40	**Uso futuro**
2001:0db8:ff00::/40	**Uso futuro**

En cada /48 podemos obterer 256 subredes /56

2001:0db8:0000::/40	Foobar Infra + uso futuro
2001:0db8:0000::/44	Foobar Infra
2001:0db8:0000::/48	Direcciones de Backbone
2001:0db8:0000:0000::/56	Loopbacks de Routers + Intercos
2001:0db8:0000:0100::/56	Clientes Interco
2001:0db8:000f::/48	
2001:0db8:0010::/44	Uso futuro
...	
2001:0db8:00e0::/44	Uso futuro
2001:0db8:00f0::/44	Uso futuro
2001:0db8:0100::/40	Bloque de clientes
2001:0db8:0200::/40	Uso futuro
...	
2001:0db8:fd00::/40	Uso futuro
2001:0db8:fe00::/40	Uso futuro
2001:0db8:ff00::/40	Uso futuro

En cada /56 podemos obtener 256 subredes /64

2001:0db8:0000::/40	Foobar Infra + uso futuro
2001:0db8:0000::/44	Foobar Infra
2001:0db8:0000::/48	Direcciones de Backbone
2001:0db8:0000:0000::/56	Loopbacks de Routers + Intercos
2001:0db8:0000:0000::/64	Loopbacks de Routers
2001:0db8:0000:0001::/64	PNI Intercos
2001:0db8:0000:0002::/64	Enlaces internacionales Intercos
2001:0db8:0000:0003::/64	Routers Intercos en Francia
2001:0db8:0000:0004::/64	Routers Intercos en Ucrania
2001:0db8:0000:0005::/64	Routers Intercos en Alemania
2001:0db8:0000:0006::/64	Routers Intercos en Holanda
2001:0db8:0000:0100::/56	Clientes Interco
2001:0db8:0000:0100::/64	Sin usar
2001:0db8:0000:0101::/64	Sin usar
2001:0db8:0000:0102::/64	Sin usar
2001:0db8:0000:0103::/64	Clientes Intercos en Francia
2001:0db8:0000:0104::/64	Clientes Intercos en Ucrania
2001:0db8:0000:0105::/64	Clientes Intercos en Alemania

2001:0db8:0000:0106::/64	Clientes Intercos en Holanda
2001:0db8:000f::/48	
2001:0db8:0010::/44	Uso futuro
…	
2001:0db8:00e0::/44	Uso futuro
2001:0db8:00f0::/44	Uso futuro
2001:0db8:0100::/40	Bloque de clientes
2001:0db8:0200::/40	Uso futuro
…	
2001:0db8:fd00::/40	Uso futuro
2001:0db8:fe00::/40	Uso futuro
2001:0db8:ff00::/40	Uso futuro

En cada /64 podemos obtener 2^{64} subredes /128

2001:0db8:0000::/40	Foobar Infra + uso futuro
2001:0db8:0000::/44	Foobar Infra
2001:0db8:0000::/48	Direcciones de Backbone
2001:0db8:0001:0000::/56	Loopbacks de Routers + Intercos
2001:0db8:0001:0000::/64	Loopbacks de Routers
2001:0db8:0001:0000::1/128	cr1.paris
2001:0db8:0001:0000::2/128	cr2.paris
2001:0db8:0001:0000::3/128	cr1.london
O se lleva a cabo una reparticion con las IP4 loopbacks	
2001:0db8:0001:0000:192:168:0:1/128	cr1.paris (loopback IPv4: 192.1680.1)
2001:0db8:0001:0001::/64	PNI Intercos
2001:0db8:0001:0001::0000/126	PNI Wan One AS1111
2001:0db8:0001:0001::0004/126	PNI Too Two AS2222
2001:0db8:0001:0002::/64	Enlaces internacionales Intercos
2001:0db8:0001:0002::0000/126	cr1.paris – cr1.london
2001:0db8:0001:0002::0004/126	cr2.paris – cr1.amsterdam
2001:0db8:0001:0002::0008/126	cr1.london – cr1.frankfurt
2001:0db8:0001:0003::/64	Routers Intercos en Francia
2001:0db8:0001:0003::0000/126	cr1.paris – cr2.paris
2001:0db8:0001:0003::0004/126	cr1.paris – er1.paris
2001:0db8:0001:0004::/64	Routers Intercos en Ucrania
2001:0db8:0001:0004::0000/126	cr1.london – cr2.london

2001:0db8:0001:0004::0004/126	cr1.london – er1.london
2001:0db8:0001:0005::/64	Routers Intercos en Alemania
2001:0db8:0001:0005::0000/126	cr1.frankfurt – cr2.frankfurt
2001:0db8:0001:0005::0004/126	cr1.frankfurt - er1.frankfurt
2001:0db8:0001:0006::/64	Routers Intercos en Holanda
2001:0db8:0001:0006::0000/126	cr1.amsterdam – cr2.amsterdam
2001:0db8:0001:0006::0004/126	cr1.amsterdam - er1.amsterdam
2001:0db8:0001:0100::/56	Clientes Interco
2001:0db8:0001:0100::/64	Sin usar
2001:0db8:0001:0101::/64	Sin usar
2001:0db8:0001:0102::/64	Sin usar
2001:0db8:0001:0103::/64	Clientes Intercos en Francia
2001:0db8:0001:0103::0000/126	Clientes de Interseco en Francia #1
2001:0db8:0001:0104::/64	Clientes Intercos en Ucrania
2001:0db8:0001:0104::0000/126	Clientes Intercos Ingleses #1
2001:0db8:0001:0104::0004/126	Clientes Intercos Ingleses #2
2001:0db8:0001:0104::0008/126	Clientes Intercos Ingleses #3
2001:0db8:0001:0104::000c/126	Clientes Intercos Ingleses #4
2001:0db8:0001:0104::0010/124	Clientes Intercos Ingleses #5 (2 HA Firewalls on customer side)
2001:0db8:0001:0104::0020/126	Clientes Intercos Ingleses #6
2001:0db8:0001:0105::/64	Clientes Intercos en Alemania
2001:0db8:0001:0106::/64	Clientes Intercos en Holanda
2001:0db8:000f::/48	
2001:0db8:0010::/44	Uso futuro
…	
2001:0db8:00e0::/44	Uso futuro
2001:0db8:00f0::/44	Uso futuro
2001:0db8:0100::/40	Bloque de clientes
2001:0db8:0200::/40	Uso futuro
…	
2001:0db8:fd00::/40	Uso futuro
2001:0db8:fe00::/40	Uso futuro
2001:0db8:ff00::/40	Uso futuro

En la siguiente ***Ilustración 32*** se muestra el diagrama de subneteo de las tablas anteriores, de manera simplificada.

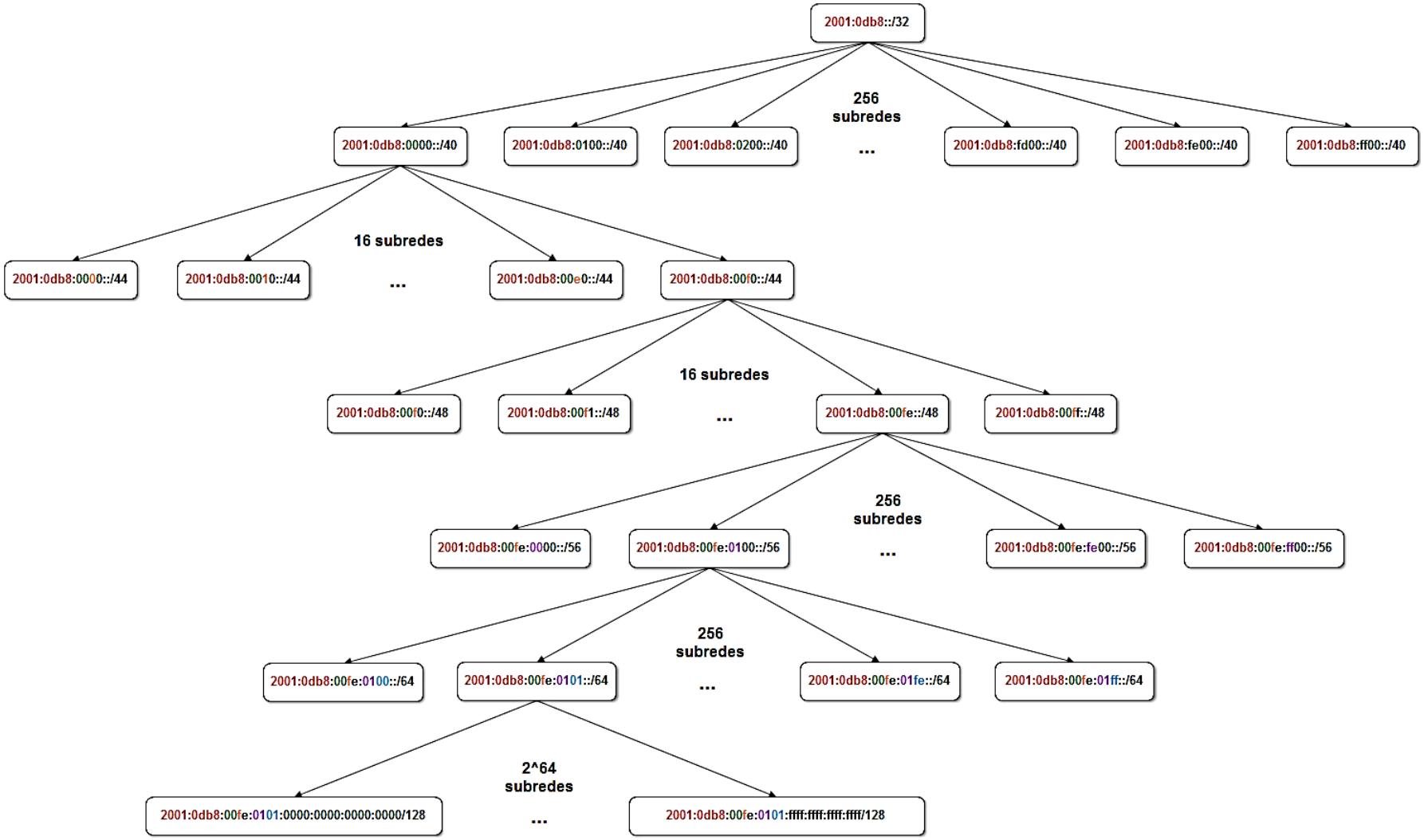


Ilustración 32. Plan de direccionamiento

3.3. Identificadores de Interfaz

Los últimos 64 bits de una dirección IPv6 corresponden al identificador de la interfaz, que es único para el prefijo de 64 bits de la dirección IPv6. Las formas de determinar un identificador de interfaz son las siguientes:

- En el documento RFC 2373[28] se indica que todas las direcciones de unidifusión que utilicen los prefijos del 001 al 111 deben utilizar también un identificador de interfaz de 64 bits derivado de la dirección EUI-64 (Extended Unique Identifier o Identificador único extendido).
- En el documento RFC 3041[29] se describe un identificador de interfaz generado aleatoriamente que cambia al cabo del tiempo para proporcionar un nivel de anonimato.
- Un identificador de interfaz que se asigna durante la configuración automática de direcciones con estado (por ejemplo, mediante DHCPv6). Los estándares DHCPv6 se están definiendo actualmente. En la familia de Windows Server 2003 y en Windows XP, el protocolo IPv6 no admite la configuración de direcciones con estado ni DHCPv6.
- Un identificador de interfaz configurado manualmente.

Identificadores de interfaz basados en direcciones EUI-64

El Institute of Electrical and Electronic Engineers (IEEE[30]) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

[28] RFC 2373: "IP Version 6 Addressing Architecture".

[29] RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[30] **IEEE**, en español Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

Direcciones IEEE 802

Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un identificador de compañía (también llamado identificador de fabricante) de 24 bits y un identificador de extensión (también llamado identificación de tarjeta) de 24 bits. La combinación del identificador de compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el identificador de tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, Media Access Control). En la siguiente ***Ilustración 33*** se puede observar la composición de los 48 bits de la dirección IEEE.

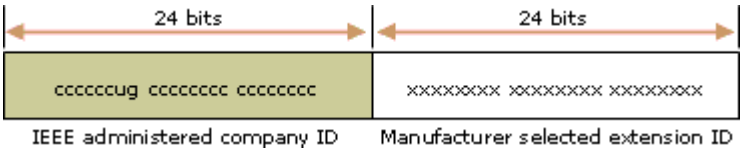


Ilustración 33. Direcciones IEEE 802

Los bits definidos en la dirección IEEE 802 son los siguientes:

- Universal o local (U/L)

  El bit U/L es el séptimo bit del primer byte y se utiliza para determinar si la dirección se administra de forma universal o local. Si el bit U/L está establecido en 0, la administración de la dirección corresponde a IEEE, mediante la designación de un ID. de compañía único. Si el bit U/L está establecido en 1, la dirección se administra de forma local. El administrador de la red ha suplantado la dirección de fábrica y ha especificado una dirección distinta.

- Individual o grupo (I/G)

  El bit I/G es el bit de orden inferior del primer byte y se utiliza para determinar si la dirección es individual (unidifusión) o de grupo (multidifusión). Si está establecido en 0, la dirección es de unidifusión. Si está establecido en 1, la dirección es de multidifusión.

En una dirección típica de adaptador de red 802.x, los bits U/L e I/G están establecidos en 0, lo que corresponde a una dirección MAC de unidifusión administrada de forma universal.

Direcciones IEEE EUI-64

La dirección IEEE EUI-64 representa un nuevo estándar para el direccionamiento de interfaces de red. El Id. de compañía sigue teniendo 24 bits de longitud, pero el Id. de extensión tiene 40 bits, por lo que se crea un espacio de direcciones mucho mayor para los fabricantes de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G de la misma forma que la dirección IEEE 802. La ***Ilustración 34*** muestra una dirección IEEE EUI-64.

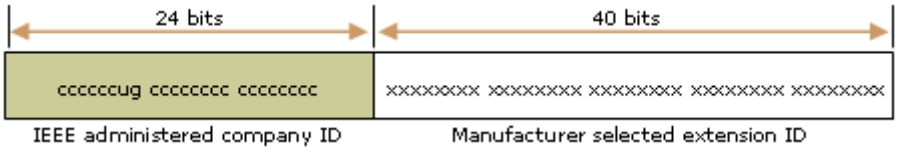


Ilustración 34. Direcciones IEEE EUI-64

Asignación de direcciones IEEE 802 a direcciones EUI-64

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id. de compañía y el Id. de extensión. En la siguiente ***Ilustración 35*** se muestra la conversión de una dirección IEEE 802 en una dirección EUI-64.

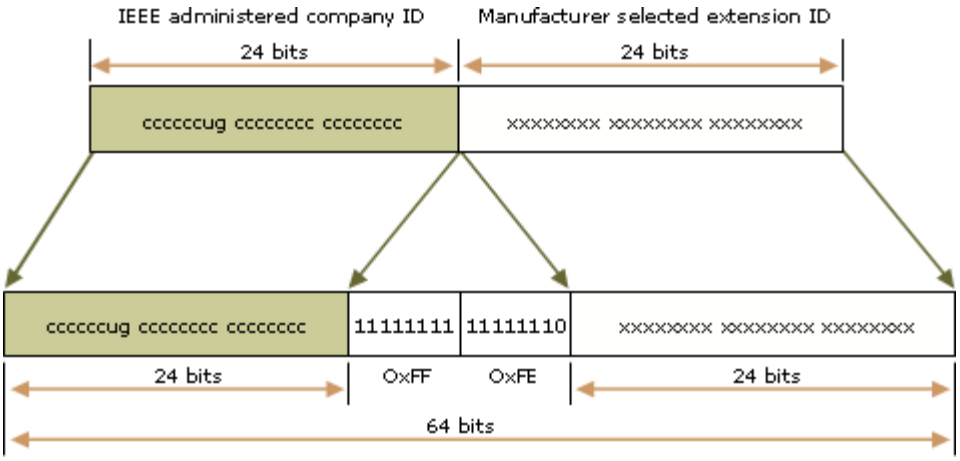


Ilustración 35. Asignación de direcciones IEEE 802 a direcciones EUI-64

Asignación de direcciones EUI-64 a identificadores de interfaz IPv6

Para obtener el identificador de interfaz de 64 bits para las direcciones IPv6 de unidifusión, se complementa el bit U/L de la dirección EUI-64 (si es 1, se establece en 0; y si es 0, se establece en 1). En la ***Ilustración 36*** siguiente se muestra la conversión de una dirección EUI-64 de unidifusión administrada de forma universal.

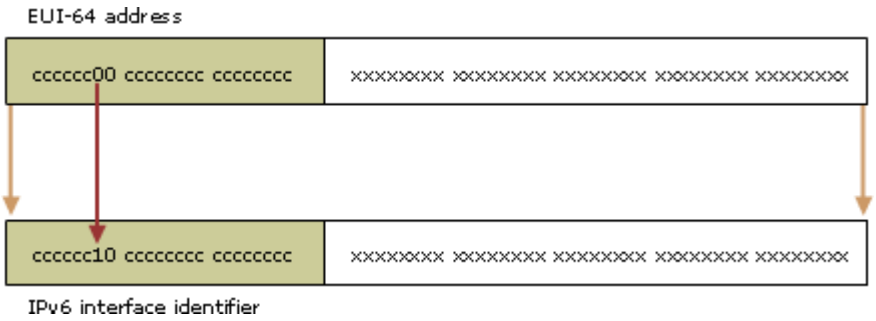


Ilustración 36. Asignación de direcciones EUI-64 a identificadores de interfaz IPv6

Para obtener un identificador de interfaz IPv6 a partir de una dirección IEEE 802, primero se debe asignar la dirección IEEE 802 a una dirección EUI-64 y, después, complementar el bit U/L. En la ***Ilustración 37*** siguiente se muestra el proceso de conversión de una dirección IEEE 802 de unidifusión administrada de forma universal.

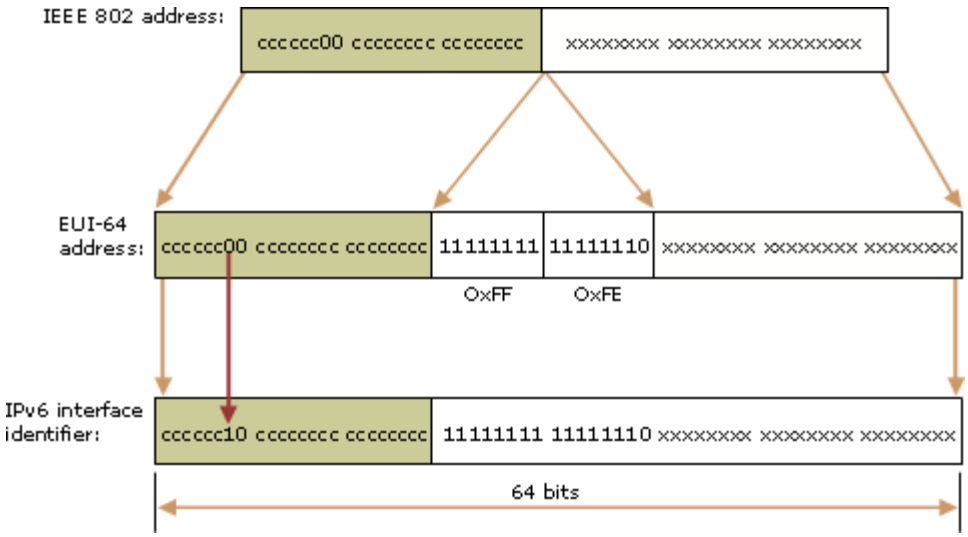


Ilustración 37. Ejemplo de conversión de una dirección IEEE 802

El host A tiene la dirección MAC de Ethernet de 00-AA-00-3F-2A-1C. Primero, se convierte al formato EUI-64 insertando FF-FE entre el tercer y cuarto bytes, con el resultado de 00-AA-00-FF-FE-3F-2A-1C. Después, se complementa el bit U/L, que es el séptimo bit del primer byte. El primer byte en formato binario es 00000000. Al complementar el séptimo bit, se convierte en 00000010 (0x02). El resultado final es 02-AA-00-FF-FE-3F-2A-1C que, cuando se convierte a notación hexadecimal con dos puntos, da como resultado el identificador de interfaz 02AA:FF:FE3F:2A1C. En consecuencia, la dirección local del vínculo correspondiente al adaptador de red que tiene la dirección MAC de 00-AA-00-3F-2A-1C es FE80::2AA:FF:FE3F:2A1C.

Nota

- Al complementar el bit U/L, se debe sumar 0x2 al primer byte si la dirección EUI-64 se administra de forma universal, y restar 0x2 del primer byte si la dirección EUI-64 se administra de forma local.

3.4. Otras consideraciones

Direcciones para hosts y enrutadores

Un host IPv4 con un solo adaptador de red tiene generalmente una única dirección IPv4 asignada al adaptador. Sin embargo, un host IPv6 suele tener varias direcciones IPv6, aunque sólo tenga una interfaz.

Un host IPv6 puede tener asignadas las direcciones de unidifusión siguientes:

- Una dirección local del vínculo para cada interfaz.
- Direcciones de unidifusión para cada interfaz (que puede ser una dirección local del sitio y una o varias direcciones globales).
- La dirección de bucle de retroceso (::1) para la interfaz de bucle de retroceso.

Los hosts IPv6 típicos son lógicamente hosts múltiples porque tienen al menos dos direcciones con las que pueden recibir paquetes. Cada host tiene una dirección local del vínculo para el tráfico del vínculo local y una dirección global o local del sitio enrutable.

Además, cada host escucha el tráfico de las siguientes direcciones de multidifusión:

- La dirección para todos los nodos de ámbito local del nodo (FF01::1).
- La dirección para todos los nodos de ámbito local del vínculo (FF02::1).
- La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz.
- Las direcciones de multidifusión de los grupos unidos a cada interfaz.

Un enrutador IPv6 puede tener asignadas las direcciones de unidifusión siguientes:

- Una dirección local del vínculo para cada interfaz.
- Direcciones de unidifusión para cada interfaz (que puede ser una dirección local del sitio y una o varias direcciones de unidifusión globales agregables).
- La dirección de bucle de retroceso (::1) para la interfaz de bucle de retroceso.

Un enrutador IPv6 puede tener asignadas las direcciones de difusión por proximidad siguientes:

- Una dirección de difusión por proximidad de un enrutador de subred para cada subred.
- Direcciones de difusión por proximidad adicionales (opcional).

Además, cada enrutador escucha el tráfico de las siguientes direcciones de multidifusión:

- La dirección para todos los nodos de ámbito local del nodo (FF01::1).
- La dirección para todos los enrutadores de ámbito local del nodo (FF01::2).
- La dirección para todos los nodos de ámbito local del vínculo (FF02::1).
- La dirección para todos los enrutadores de ámbito local del vínculo (FF02::2).
- La dirección para todos los enrutadores de ámbito local del sitio (FF05::2).
- La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz.
- Las direcciones de los grupos unidos a cada interfaz.

4. ICMPV6, NEIGHBOR DISCOVERY Y DHCPV6

4.1. ICMPv6

El Protocolo de control de mensajes Internet para IPv6 (ICMPv6, Internet Control Message Protocol for IPv6) es un estándar de IPv6 necesario que está definido en el documento RFC 2463, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification" [Especificación del Protocolo de control de mensajes de Internet (ICMP) para el Protocolo Internet versión 6 (IPv6)]. Con ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar de errores y enviar mensajes de eco simples.

El protocolo ICMPv6 proporciona también un marco de trabajo para los protocolos siguientes:

- Descubrimiento de escucha de multidifusión (MLD: Multicast Listener Discovery).

MLD consiste en una serie de tres mensajes ICMPv6 que reemplazan la versión 2 del Protocolo de administración del grupo Internet (IGMP[31], Internet Group Management Protocol) para IPv4 en la administración de la pertenencia a multidifusión de subred.

- Descubrimiento de vecinos (ND).

Descubrimiento de vecinos consiste en una serie de cinco mensajes ICMPv6 que administran la comunicación de un nodo a otro en un vínculo. El descubrimiento de vecinos reemplaza al Protocolo de resolución de direcciones (ARP[32], Address Resolution Protocol), Descubrimiento de enrutadores ICMPv4 y el mensaje de Redirección ICMPv4, además de proporcionar funciones adicionales.

[31] El protocolo de red **IGMP** se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión.

[32] **ARP** (Protocolo de resolución de direcciones), es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

Los mensajes ICMPv6 se suelen enviar automáticamente cuando un paquete IPv6 no puede llegar a su destino.

Los mensajes ICMPv6 se encapsulan y envían como carga de los paquetes IPv6, como se muestra en la ***Ilustración 38*** siguiente.

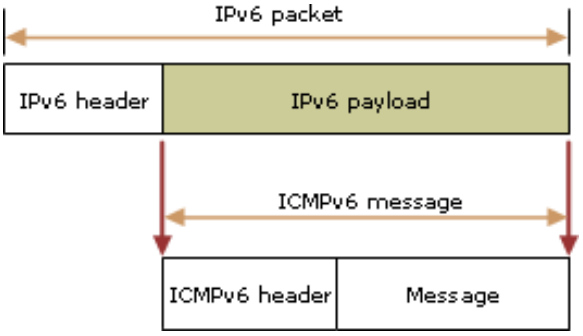


Ilustración 38. Mensaje ICMPv6 encapsulado en paquete IPv6

En el encabezado ICMPv6 se identifican diferentes tipos de mensajes ICMPv6. Como los mensajes ICMPv6 se transmiten en paquetes IPv6, no son confiables.

En la tabla siguiente se muestran y describen los mensajes ICMPv6 que no están relacionados con MLD o ND:

Tabla 3. Mensajes ICMPv6

Mensaje ICMPv6	Descripción
Destination Unreachable (Destino inaccesible).	Mensaje de error que informa al host remitente de que un paquete no se puede entregar.
Packet Too Big (Paquete demasiado grande).	Mensaje de error que informa al host remitente de que el paquete es demasiado grande para el reenvío.
Time Exceeded (Tiempo agotado).	Mensaje de error que informa al host remitente de que el límite de saltos de un paquete IPv6 ha caducado.
Parameter Problem (Problemas de	Mensaje de error que informa al host remitente de que se produjo un error al procesar el encabezado IPv6 o un

parámetros).	encabezado de extensión IPv6.
Echo Request (Solicitud de eco).	Mensaje informativo que se utiliza para determinar si un nodo IPv6 está disponible en la red.
Echo Reply (Respuesta de eco).	Mensaje informativo que se emplea para responder al mensaje de solicitud de eco ICMPv6.

Se puede utilizar el comando **ping** para enviar mensajes de solicitud de eco ICMPv6 y registrar la recepción de los mensajes de respuesta de eco ICMPv6. Mediante ping, se puede detectar errores de comunicación en la red o en los hosts y solucionar problemas comunes de conectividad IPv6.

Se puede utilizar el comando **tracert** para enviar mensajes de solicitud de eco ICMPv6 con valores de incremento gradual en el campo Hop Limit (límite de saltos). Tracert trazará y mostrará la ruta seguida por los paquetes IPv6 entre un origen y un destino, con lo que podrá solucionar problemas comunes de enrutamiento IPv6. En la ***Ilustración 39*** se muestra el formato de cabecera ICMPv6:

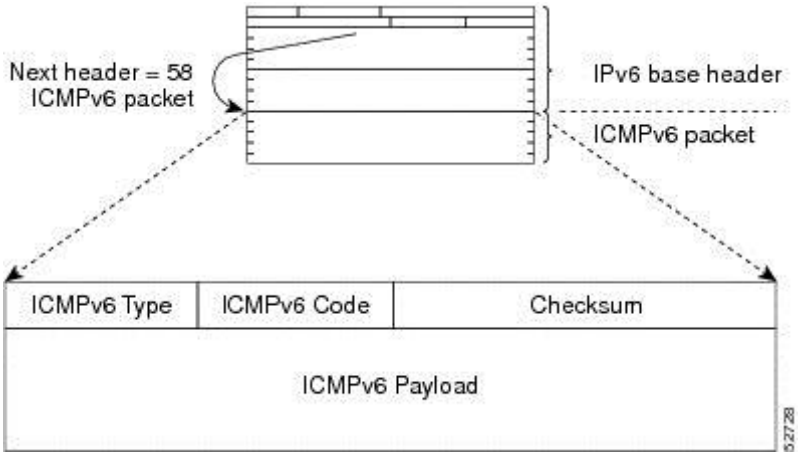


Ilustración 39. IPv6 ICMP Packet Header Format

El campo “tipo” indica el tipo de mensaje, su valor determina el formato de los datos restantes; el campo “codigo” depende del tipo de mensaje y se utiliza par crear un nivel adicional de granularidad al mensaje; y el campo “checksum (comprobación)” es usado para detectar la corrupción de datos en el mensaje ICMPv6 y partes de la cabecera IPv6.

Mensajes ICMPv6

Agrupados en dos clases:

- Mensajes de error.
- Mensajes informativos.

Los mensajes de error tienen un cero en el bit de mayor orden del valor del campo Type. Por tanto el valor del campo Type es de 0 a 127. A continuación la ***Ilustración 40*** muestra la tabla de mensajes de error ICMPv6.

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Ilustración 40. Mensajes de error e informativos ICMPv6

Los mensajes informativos tienen valores para el campo Type de 128 a 255.

4.2. Neighbor Discovery

El Descubrimiento de vecinos (ND, Neighbor Discovery) de IPv6 es un conjunto de mensajes y procesos que determinan las relaciones entre nodos vecinos. El

Descubrimiento de vecinos reemplaza al Protocolo de resolución de direcciones (ARP, Address Resolution Protocol), el Descubrimiento de enrutadores del Protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol) y la Redirección ICMP, que se utilizan en IPv4, y proporciona funciones adicionales. El descubrimiento de vecinos está definido en el documento RFC 2461, "Neighbor Discovery for IP Version 6 (IPv6)" [Descubrimiento de vecinos para IP versión 6 (IPv6)].

En la ***Ilustración 41*** se muestra una topología simple del proceso de neighbor discovery en una red de accesos multiples.

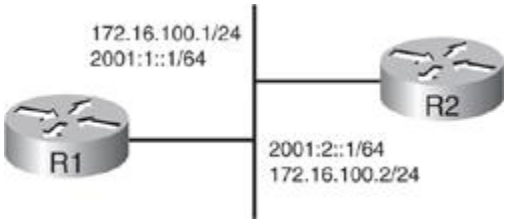


Ilustración 41. Topologia de Neighbor Discovery

Los hosts utilizan el Descubrimiento de vecinos para efectuar las funciones siguientes:

- Descubrir enrutadores vecinos.
- Descubrir direcciones, prefijos de direcciones y otros parámetros de configuración.

Los enrutadores utilizan el Descubrimiento de vecinos para efectuar las funciones siguientes:

- Anunciar su presencia, los parámetros de configuración de host y los prefijos en vínculo.
- informar a los hosts acerca de la mejor dirección de salto siguiente para reenviar los paquetes dirigidos a un destino determinado.

Los nodos utilizan el Descubrimiento de vecinos para efectuar las funciones siguientes:

- Resolver la dirección de nivel de vínculo de un nodo vecino al que se reenvía un paquete IPv6 y determinar cuándo ha cambiado la dirección de nivel de vínculo de un nodo vecino.

- Determinar si los paquetes IPv6 se pueden enviar a y recibir de un vecino.

ND habilita el mecanismo de autoconfiguración en IPv6.

Interacción entre nodos

Define el mecanismo para solventar:

- Descubrimiento de encaminadores.
- Descubrimiento de prefijos de red.
- Descubrimiento de parámetros.
- Autoconfiguración de direcciones.
- Resolución de direcciones.
- Determinación del "Next-Hop".
- Detección de Vecinos Inalcanzables (NUD).
- Detección de Direcciones Duplicadas (DAD).
- Redirección del "First-Hop".

Nuevos tipos de paquetes ICMP

ND define 5 tipos de paquetes:

1. ***"Router Solicitation" (RS)***

- Cuando arrancan los hosts envían RS para indicar a los encaminadores que generen un RA inmediatamente.
- Se envía a la dirección multicast que engloba a todos los encaminadores del segmento de red.

Bits 8	16	32
Type = 133	Code = 0	Checksum
Reserved = 0		
Options …		

Ilustración 42. Formato Router Solicitation

- Opciones Posibles: Source Link-Layer Address.

En la ***Ilustración 42*** se puede apreciar el formato de cabecera de un mensaje ICMP Router Solicitation que es enviado por un host (durante el proceso de inicializacion) para encontrar routers cerca. Asi mismo en la ***Ilustración 43***, (escenario simplificado) se observa el proceso de descubrimiento donde se da el intercambio de mensajes Router solicitation de parte de los host en busca de routers y el mensaje Router Advertisement enviado por los routers de forma periodica para indicar las rutas por defecto a los host.

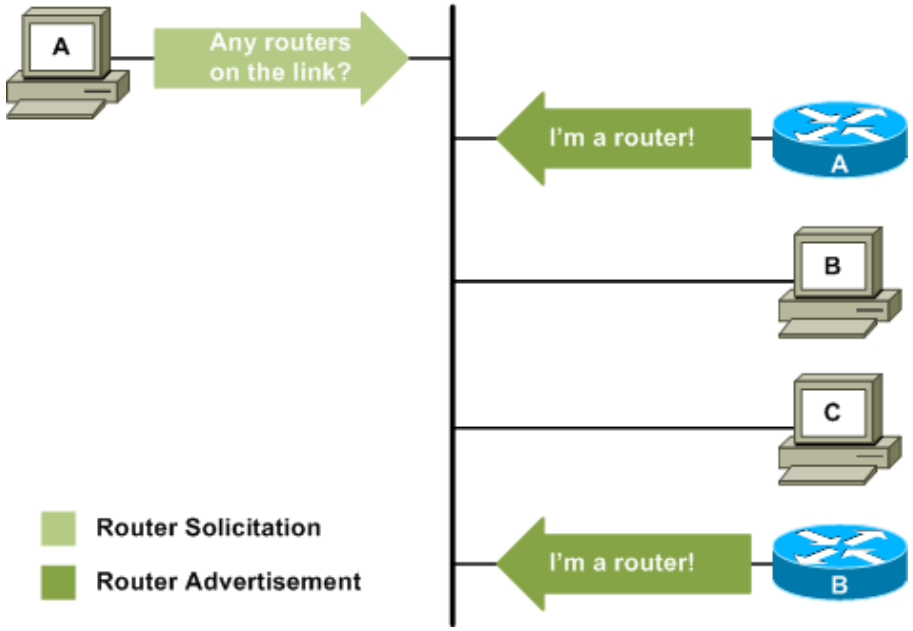


Ilustración 43. Router Solicitation y Router Advertisement

2. ***"Router Advertisement" (RA)***

- En una red (link) con capacidad broadcast, cada encaminador envía periódicamente paquetes multicast RA.

- Un host recibe los RAs de todos los encaminadores, construyendo una lista de encaminadores por defecto.
- El algoritmo de Neighbor Unreachability Detection (NUD) detecta si existen problemas en alcanzar los encaminadores.
- Los RAs contienen una lista de prefijos usados por los hosts para determinar si una dirección destino de un paquete pertenece a dicho link y para la autoconfiguración de direcciones.
- Los RAs y los "Flags" asociados a cada prefijo permiten a los encaminadores indicar a los hosts como realizar la autoconfiguración (stateless o DHCPv6).

Bits 8	16			32
Type = 134	Code = 0			Checksum
Cur Hop Limit	M	O	Reserved = 0	Router Lifetime
Reachable Time				
Retrans Timer				
Options …				

Ilustración 44. Formato Router Advertisement

La ***Ilustración 44*** muestra el formato de cabecera de un mensaje ICMP Router Advertisement enviado por los routers.

- Cur Hop Limit: valor predeterminado que debería ponerse en el campo Hop Count de la cabecera IPv6 de los paquetes que van a ser enviados.
- M: 1-bit "Managed address configuration" flag.
- O: 1-bit "Other configuration" flag.
- Router Lifetime: entero sin signo de16-bits.
- Reachable Time: entero sin signo de 32-bits.
- Retrans Timer: entero sin signo de 32-bits.

- Possible Options: Source LinkLayer Address, MTU, Prefix Information, Flags Expansion (RFC 5175[33]).

3. *"Neighbor Solicitation" (NS)*

- Los nodos envían NS para obtener la dirección MAC del nodo con el que se pretende comunicar, a la vez que se proporciona la propia dirección MAC del nodo solicitante.
- Los paquetes NS son multicast cuando el nodo precisa resolver una dirección y unicast cuando el nodo pretende averiguar si un vecino es alcanzable.

Bits 8	16	32
Type = 135	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Options …		

Ilustración 45. Formato Neighbor Solicitation

En la ***Ilustración 45*** se observa el formato de cabecera de un mensaje ICMP Neighbor Solicitation. Estos mensajes Neighbor Solicitation son enviados por un nodo para determinar la dirección de la capa de enlace de un vecino, como se muestra en la ***Ilustración 46***, así mismo el intercambio de mensajes Neighbor Advertisement, es enviado en respuesta a un mensaje Neighbor Solitation. Siendo el formato de cabecera de los mensajes Neighbor Advertisement el mostrado en la ***Ilustración 47***.

- Target Address: La dirección IPv6 objetivo de la solicitud. No debe ser una dirección multicast.
- Opciones Posibles: Source Link-Layer Address.

[33] RFC 5175: "IPv6 Router Advertisement Flags Option".

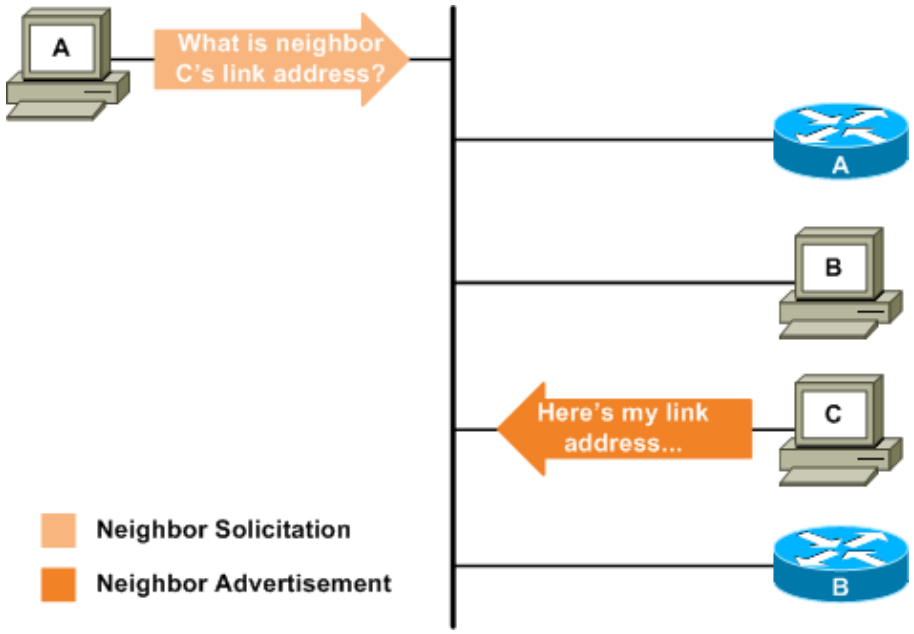


Ilustración 46. Neighbor Solicitation y Neighbor Advertisement

4. *"Neighbor Advertisement" (NA)*

- Un nodo envía NA como respuesta a un NS y envía NA no solicitados para propagar nueva información rápidamente.

Bits 8	16	32
Type = 136	Code = 0	Checksum
R S O	Reserved = 0	
Target Address		
Options …		

Ilustración 47. Formato Neighbor Advertisement

- Flags:
  - R: Router Flag=1 indica que el que envía en un encaminador.
  - S: Solicited Flag=1 indica que se envía como respuesta a un NS.
  - O: Override Flag=1 indica que deben actualizarse las caches.
- Para NA solicitados, igual al campo "Target Address" del NS. Para un NA no solicitado, la dirección cuya MAC ha cambiado. No puede ser una dirección multicast.

- Posibles Opciones: Target Link-Layer Address (MAC del Tx).

5. ***"Redirect"***

- Los encaminadores envían paquetes Redirect para informar a un host que existe otro encaminador mejor en el camino hacia el destino final.

Los mensajes Redirect son usados por los routers para informar a los host de un mejor "primer salto" para un destino, a como se muestra en la ***Ilustración 48***. El formato de cabecera para estos mensajes Redirect es el mostrado en la ***Ilustración 49***.

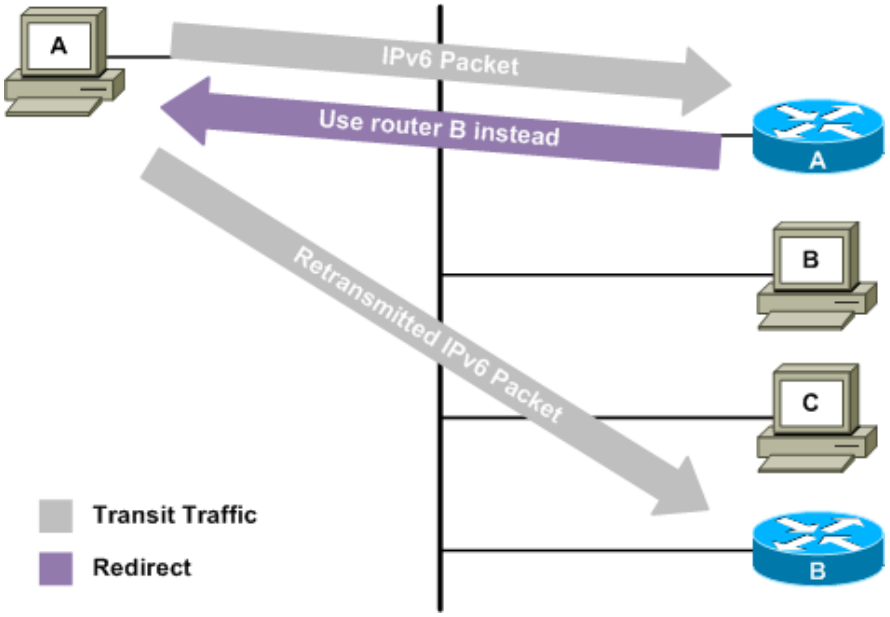


Ilustración 48. Redirection

- Los hosts pueden ser redireccionados a otro encaminador mejor pero también pueden ser informados mediante un paquete Redirect que el destino es un vecino.

Bits 8	16	32
Type = 137	Code = 0	Checksum
Reserved = 0		
Target Address		
Destination Address		
Options …		

Ilustración 49. Formato Redirect

- Target Address: La dirección IPv6 del “first hop” que es mejor usar para llegar al “Destination Address” del paquete ICMPv6.
- Destination Address: La dirección IPv6 de destino que es redireccionada al “target address” del paquete ICMPv6.

Ejemplo de funcionamiento

- Neighbor Cache: Vecinos a los que se les ha enviado tráfico recientemente. Se indexa por la “on-link unicast IP address”. Cada entrada contiene: dirección de capa enlace, si es router/host, información de NUD (reachability state, etc.).
- Destination Cache: Mapea IP destino con “next hop”. Direcciones a las que se ha enviado recientemente.
- Prefix List: Contiene los prefijos del enlace. Se basa en los RA, de donde se saca también el tiempo de validez.
- Default Router List: Lista de routers a donde los paquetes “off-link” deben ser enviados. Cada entrada apunta a una entrada en la Neighbor Cache y tiene un tiempo de validez obtenido del RA (router lifetime).

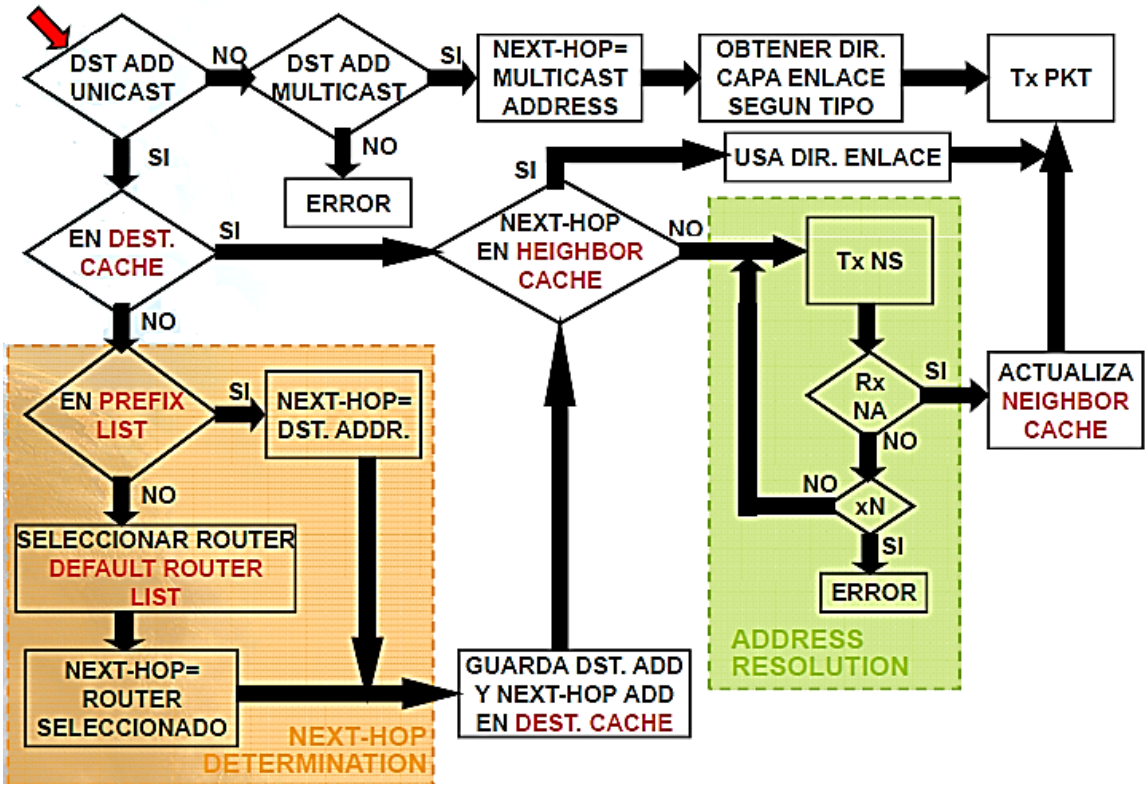


Ilustración 50. Algoritmo para determinar el próximo salto

En la ***Ilustración 50*** se muestra un modelo de determinación del siguiente salto (next-hop) basado en el RFC 2461[34].

Cuando se envía un paquete a un destino, un nodo usa una combinación de la caché de destino, la lista de prefijos y la lista por defecto del router para determinar la dirección IP apropiada del siguiente salto, operación conocida como "determinación del siguiente salto". Una vez que la dirección IP del siguiente salto es conocida, la caché de vecinos se consulta para obtener información sobre la capa de enlace de ese vecino.

El host primero realiza una búsqueda en la caché de destino, en caso de que el destino del paquete ha sido visto recientemente. Si es así, el cache de destino ofrece el siguiente salto que se ha utilizado (puede ser el propio destino), y una búsqueda posterior en la cache de vecinos es probable que proporcione la dirección de la capa de enlace. Este camino, será el utilizado en un flujo ya establecido. Si el destino no esta en la caché de

[34] RFC 2461: "Neighbor Discovery for IP Version 6 (IPv6)".

destino, se busca en la lista de prefijo (información recibida en los RA). Como último recurso, un router por defecto se selecciona, de entre todos los rourters del enlace (enviándola por medio de RA), a través de la selección del router por defecto.

Comparación con IPv4

El protocolo Neighbor Discovery (NDP) IPv6 corresponde a una combinación de los protocolos ARP de IPv4, ICMP Router Discovery (RDISC[35]) e ICMP Redirect (ICMPv4). En IPv4 no hay un acuerdo general sobre el protocolo o mencanismo para la detección de inaccesibilidad de vecino.

El protocolo Neighbor Discovery (NDP) IPv6 ofrece una serie de mejoras en los correspondientes protocolos IPv4, de la siguiente manera:

- El descubrimiento de enrutadores se convierte en una parte integral del protocolo, con lo cual no hay necesidad de que los host “espien” los protocolos de enrutamiento.
- Información adicional, como la MTU o la dirección de capa de enlace, se ha insertado en los mensajes de ND, reduciendo el número de intercambios necesarios en el enlace para lograr el mismo resultado que en IPv4.
- La resolución de direcciones utiliza los grupos de multidifusión (nodo solicitado la dirección multicast), la incorporación de parte de la dirección de destino. Lo más probable, por lo tanto, es que sólo unos pocos (la mayoría de las veces sólo el propietario de la dirección destino) nodos se ven interrumpidos con esas consultas de resolución de dirección. Comparando esto con ARP de IPv4, que no tiene otra opción que la radiodifusión (los broadcast de la capa de enlace) a las solicitudes de resolución de direcciones (porque ARP se encuentra justo por encima de la capa de enlace).

[35] Los hosts utilizan **RDISC** para obtener información de enrutamiento de los enrutadores. De este modo, cuando los hosts ejecutan RDISC, los enrutadores también deben ejecutar otro protocolo, como RIP, para poder intercambiar información de enrutadores.

Se espera que la manera de IPv6 de resolver las direcciones de la capa de enlace haga subredes con un número mucho mayor de host, más manejable limitando drásticamente los broadcasts que la capa de enlace que las capas de aplicación de los host tiene que manejar.

- Algunas de las características nuevas, tales como configuración automática de direcciones (autoconfiguration) y la Detección de inaccesibilidad de vecinos son parte de la base de protocolo, simplificación en las configuraciones y la mejora de la robustez de la entrega de paquetes.
- Los anuncios del enrutador (Router advertisements) y los mensajes de redirección llevan la dirección del enrutador en forma de direcciones locales de vínculo, haciendo la asociación del router en el host más robusto para volver a numerar (de prefijos global). En IPv4, la información de puerta de enlace predeterminada tiene que ser modificada en el host cada vez que la red cambia su esquema de direccionamiento.
- El posicionamiento de la resolución de la dirección por encima de ICMP hace posible utilizar la seguridad estándar IP y los mecanismos de seguridad para los mensajes ND. Estos mecanismos no están disponibles en ARP para IPv4.

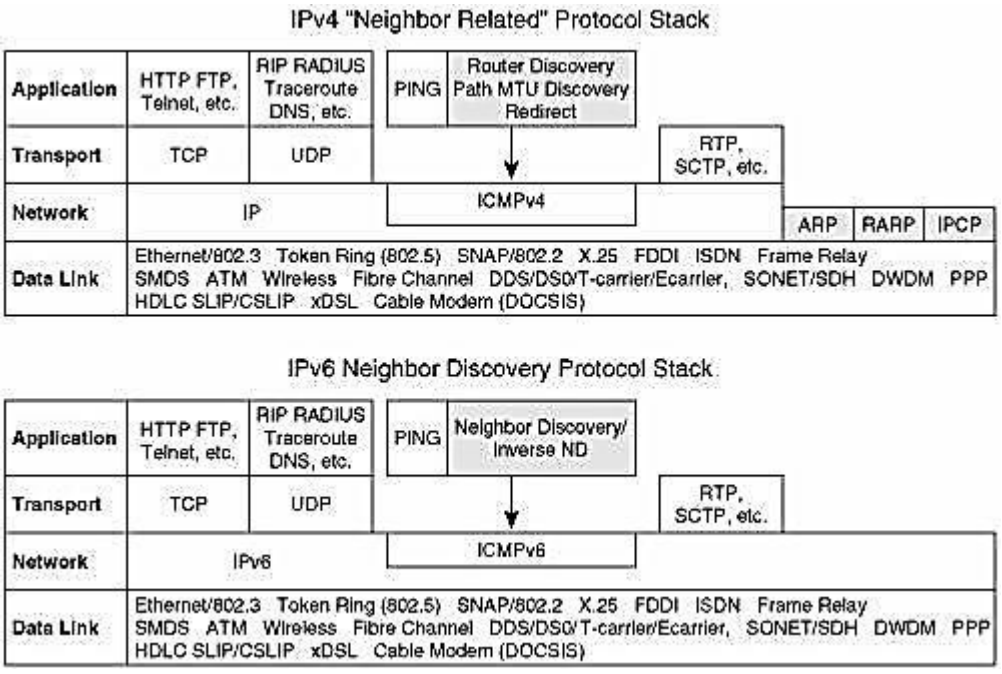


Ilustración 51. Comparación de la pila de protocolos IPv4 e IPv6

En la ***Ilustración 51*** se resaltan las diferencias entre la pila de protocolos IPv4 e IPv6. Siendo una de las diferencias fundamentales entre IPv6 ND y su contraparte el conjunto de protocolos IPv4 (ARP, IPCP[36], etc) el posicionamiento de la pila de protocolo IP. Aunque el mismo enlace IPv4 divide los protocolos relacionados entre ARP/RARP[37], justo encima de la capa de enlace e ICMP corriendo por encima de IP, en IPv6 el ND se lleva a cabo enteramente dentro de ICMPv6.

4.3. Autoconfiguración

El estándar especifica los pasos que un host debe seguir para decidir cómo auto-configurar sus interfaces de red en IPv6.

[36] Internet Protocol Control Protocol (**IPCP**) es un protocolo de control de red (NCP) para configurar IP en un enlace PPP.

[37] **RARP** son las siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso). Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dada (como una dirección Ethernet).

El proceso de auto-configuración incluye la creación de una dirección IPv6 de ámbito local (link-local) y la verificación de que no está duplicada en el mismo segmento de red, determinando qué información debería ser auto-configurada y en el caso de direcciones, si estas deberían obtenerse mediante "stateful", "stateless" o ambos.

IPv6 define tanto un mecanismo de auto-configuración de direcciones de tipo "stateful" como "stateless".

La auto-configuración "stateless" (SLAAC) no precisa de configuración manual en el host, mínima (si acaso alguna) configuración de encaminadores y ningún servidor adicional.

En la ***Ilustración 52*** se muestra la relación entre los estados de una dirección autoconfigurada, así como el tiempo de vida preferido y válido.

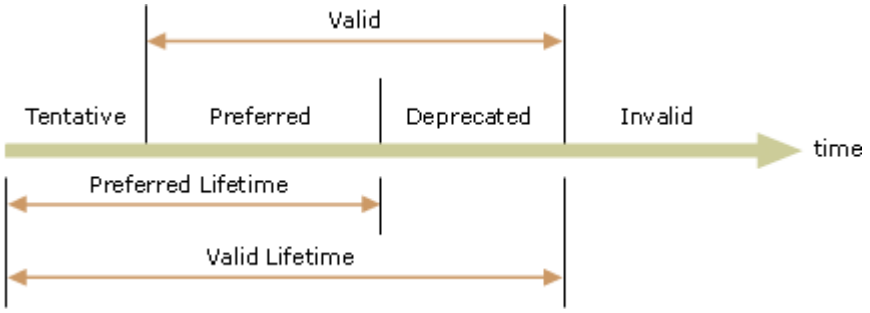


Ilustración 52. Relación entre los estados de una dirección configurada automáticamente y el tiempo de vida preferido y válido

Autoconfiguración Stateless o Serverless (RFC 4862[38])

El mecanismo "stateless" permite a un host generar su propia dirección usando una combinación de información localmente disponible y de información proporcionada por los encaminadores.

Los ***encaminadores anuncian los prefijos de red*** que identifican la subred asociada a un determinado segmento de red.

[38] RFC 4862: "IPv6 Stateless Address Autoconfiguration".

Los ***host generan un identificador de interfaz*** que lo indica de manera única en la subred. Dicho identificador se genera localmente, por ejemplo a partir de la dirección MAC.

Una dirección IPv6 se forma mediante la combinación de ambas informaciones.

En la ausencia de encaminadores, un host puede generar solo las direcciones IPv6 de ámbito local (link-local).

Las direcciones link-local son suficiente para permitir la comunicación IPv6 entre nodos que están conectados en el mismo segmento de red.

Ventajas/beneficios de la Autoconfiguración Stateless

- La configuración manual de cada máquina antes de conectarla a la red no es necesaria.
- Los sitios pequeños compuesto de pocas máquinas conectadas al mismo segmento no necesitarían de un servidor DHCPv6 ni de un encaminador para comunicarse, usarían direcciones link-local.
- Un sitio grande con varias subredes no necesitarían de un servidor DHCPv6 para la configuración de direcciones.
- Facilita el cambio de prefijo de un sitio mediante el uso de varias direcciones por interfaz y tiempo de vida.

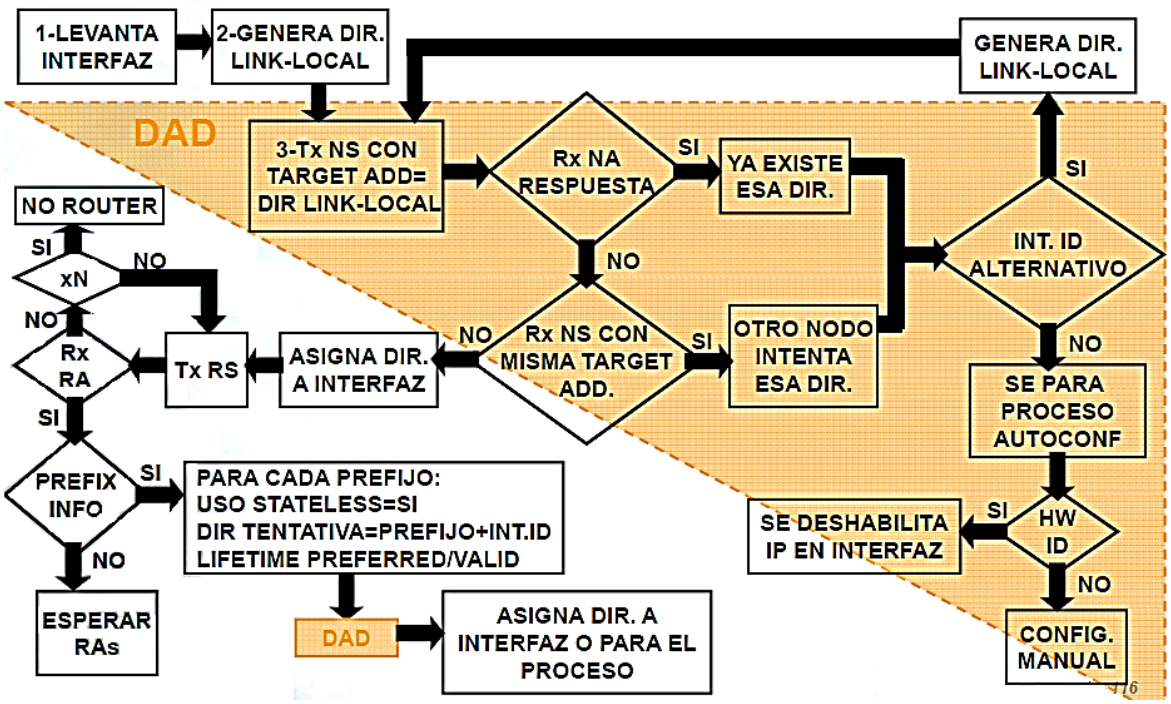


Ilustración 53. Funcionamiento de la Auconfiguración Stateless

En la ***Ilustración 53*** se muestra el proceso de autoconfiguración:

- La autoconfiguración comienza cuando una interfaz de multidifusión es habilitada, por ejemplo, durante el inicio del sistema. Los nodos, host y routers, inician el proceso de autoconfiguración generando una dirección de enlace local para la interfaz. Una dirección local de vínculo se forma añadiendo el identificador de la interfaz para el prefijo conocido de enlace local.

- Un nodo debe tratar de verificar que la dirección local de vínculo tentativa no esta en uso por otro nodo en el enlace. Tras la verificación, la dirección local de vínculo puede ser asignada a una interfaz. En concreto, el nodo envía un mensaje de solicitud de vecino (neighbor solicitation) que contiene la dirección tentativa, ya que es el objetivo. Si otro nodo ya esta usando esa dirección, el nodo devuelve un anuncio de vecino (neighbor advertisement) diciendo que el nodo esta usando esa dirección.

- Si otro nodo también esta tratando de utilizar la misma dirección, el nodo envía también una solicitud de vecino (neighbor solicitation) para el destino. El número de transmisiones o retransmisiones de solicitud de envío (neighbor advertisement) y la demora entre solicitudes consecutiva, son específicos del enlace.
- Si un nodo determina que la dirección local de vínculo tentativa no es único, el proceso de autoconfiguración se detiene y es necesario configurar la interfaz manualmente.
- Después que un nodo determina que su dirección de vínculo local es único, el nodo asigna la dirección a la interfaz. En este punto, el nodo tiene conectividad de nivel IP con nodos vecinos.

Autoconfiguración Stateful o DHCPv6 (RFC 3315[39])

Los host obtienen las direcciones de la interfaz de red y/o información de configuración desde un servidor.

Los servidores mantienen una base de datos que actualizan con las direcciones que han sido asignadas y con información de a qué host se han asignado.

La autoconfiguración “stateless” y la “stateful” se complementan la una a la otra.

Ambos tipos de autoconfiguración se pueden usar de forma simultánea.

El administrador de red especifica qué tipo de autoconfiguración se usa, por medio de la configuración de los campos adecuados de los mensajes RAs.

Tiempo de validez de las direcciones

Las direcciones IPv6 se asignan a un interfaz por un tiempo determinado (posiblemente infinito) que indica el periodo de validez de la asignación.

[39] RFC 3315: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”.

Cuando el tiempo de asignación expira, la asignación ya no es válida y la dirección puede ser reasignada a otra interfaz de red en cualquier otra red dentro de internet.

Con el fin de gestionar de una manera adecuada la expiración de las direcciones, una dirección pasa por dos fases distintas mientras está asignada a una interfaz:

- Inicialmente una dirección es la preferida (preferred), lo cual significa que su uso es una combinación arbitraria no está restringida.
- Más tarde, una dirección se convierte en "obsoleta" (deprecated) anticipándose al hecho de que su asignación al interfaz de red será inválido en breve.

Configurar el servidor DNS con autoconfiguración Stateless

Hay dos maneras de configurar el servidor DNS en un nodo:

- Manualmente.
- Con DHCPv6 o DHCPv4 (en caso de nodos dual-stack).

Puede ser un problema en algunos entornos:

- Necesidad de usar dos protocolos en IPv6 (Stateless Autoconfguration y DHCPv6).
- Retardo al obtener el servidor DNS cuando se usa DHCP.
- En entornos wireless, donde el nodo cambia de red frecuentemente, no es posible usar configuración manual o el retardo del DHCP puede ser demasiado.

Una nueva forma de configurar servidores DNS se define en el RFC 5006[40], la opción Recursive DNS Server (RDNSS[41]) para los RA:

- Se puede usar conjuntamente con DHCPv6.

[40] RFC 5006: "IPv6 Router Advertisement Option for DNS Configuration".

[41] Un **RDNSS** (Recursive DNS Server), es un servidor que ofrece un servicio de resolución de DNS recursiva para traducir nombres de dominio en direcciones IP, definidos en el RFC1034: "Domain Names – Concepts and Facilities" y RFC1035: "Domain Names – Implementation and Specification".

Funciona de la misma manera en que se aprenden los prefijos y routers usando ND: IPv6 Sateless Address Autoconfiguration [RFC 4862].

Con la opción RDNSS el nodo aprende, con solo un mensaje:

- Prefjo para usar en la autoconfiguración.
- Gateway IP.
- Servidores DNS Recursivos.

Si, además de la opción RDNSS, se usa DHCPv6, se debe activar el flag “O” en el RA.

Existen dos opciones para configurar la opción RDNSS en los routers:

- Manualmente.
- Automáticamente, es posible mediante la ejecución de un cliente DHCPv6 en el router.

4.4. DHCPv6

DHCP para IPv6 (DHCPv6) es un protocolo UDP cliente/servidor diseñado para reducir el coste de la gestión de nodos IPv6 en entornos donde los administradores de red precisan de más control sobre la asignación de direcciones IPv6 y la configuración de los parámetros de red que el ofrecido por la autoconfiguración de tipo “stateless”.

DHCPv6 reduce el coste de la asignación de direcciones centralizando la gestión de los recursos de red en vez de distribuir dicha información en ficheros de configuración local entre cada nodo en la red.

DHCPv6 se ha diseñado para ser extendida fácilmente para transportar parámetros nuevos de configuración añadiendo nuevas opciones DHCP definidas para dichas necesidades.

Objetivos de DHCPv6

- Es un mecanismo, no una política de asignación.
- Es compatible con la autoconfiguración IPv6 “stateless”.
- No requiere configuración manual de parámetros de red en los clientes DHCP.
- No requiere un servidor en cada segmento de red.
- Coexiste con nodos configurados estáticamente, nodos no participantes y con otras implementaciones de protocolos de red existentes.
- Los clientes DHCP pueden operar en un segmento de red sin que estén presentes encaminadores IPv6.
- DHCP proporciona la capacidad de remuneración de las redes.
- Un cliente DHCP puede hacer peticiones diferentes y múltiples.
- DHCP contiene temporizadores y mecanismos de retransmisión para funcionar de forma eficiente en entornos con alta latencia y bajo ancho de banda.

Detalles de DHCPv6

Los puertos UDP son:

- Los clientes escuchan los mensajes DHCP en el puerto 546.
- Servidores y agentes relays escuchan los mensajes DHCP en el puerto 547.

DHCP hace uso de las siguiente direcciones de multidifusión:

- All_DHCP_Relay_Agents_and_Servers (FF02::1:2): una dirección de multidifusión con enlace de ámbito utilizado por un cliente para comunicarse con los vecinos, agentes de retransmisión y servidores. Todos los servidores y agentes de retransmisión son miembros de este grupo de multidifusión.
- All_DHCP_Servers (FF05::1:3): una dirección de multisifusión sitio de ámbito utilizado por un agente de retransmisión para comunicarse con servidores, ya sea

porque el agente de retranmision quiere enviar mensajes a todos los servidores o porque no conoce las direcciones unicast de los servidores.

DHCP define los siguientes tipos de mensajes[42]:

- DHCP
- SOLICIT
- ADVERTISE
- REQUEST
- CONFIRM
- RENEW
- REBIND
- REPLY
- RELEASE
- DECLINE
- RECONFIGURE
- INFORMATION-REQUEST
- RELAY-FORW
- RELAY-REPL

Cada mensaje puede transportar una o más opciones DHCP:

- Domain-list.
- DNS-server.
- IA-NA, etc.

Identificador único DHCP (DHCP Unique Identifier, DUID).

- Los servidores usan DUIDs para identificar a los clientes para la selección de unos determinados parámetros de configuración.
- Los clientes usan los DUIDs para identificar un servidor en aquellos mensajes en los que el servidor necesita ser identificado.

En la parte superior de la ***Ilustración 54*** se muestran 4 mensajes de intercambio entre una estación cliente y un servidor:

- En el primer mensaje el cliente DHCPv6 envía un mensaje de solicitud para localizar el servidor DHCP, el cual se encuentra dentro del prefijo FF02::1:2, en el puerto UDP 547. Esta dirección es enviada en el enlace local a todos los servidores DHCPv6.

[42] Más detalle sobre este dipo de mensajes: RFC 2401: “Security Architecture for the Internet Protocol”.

- En el segundo mensaje el servidor DHCPv6 envía un mensaje anunciándose para indicar que esta disponible para el servicio DHCP, esto en respuesta al mensaje de solicitud del cliente.
- Posterioremente en el tercer mensaje el cliente DHCPv6 envía un mensaje solicitando los parámetros de configuración (esto incluye la direccion IP desde un servidor específico) si es primera vez que hace la solicitud o en caso contrario envía un mensaje de renovación al servidor que originalmente le suministro la dirección, así como los parámetros de configuración para extender el tiempo de vida de la direccion asignada y actualizar otros parámetros de configuración.
- Finalmente el servidor envía un mensaje de respuesta que contiene direcciones asignadas y los parámetros de configuración en respuesta a la solicitud/renovación recibidos del cliente. El servidor envía un mensaje reply para confirmar que la dirección asignada al ciente es apropiada para el enlace en el cual esta conectado el cliente.

En la parte inferior de la ***Ilustración 54***, el escenario es similar, la diferencia con el escencario anterior radica en que ahora hay un agente de retransmisión:

- En el mensaje RELAY-FORW, un agente de retransmisión envía un mensaje de retransmisión para transmitir mensajes a los servidores, ya sea directamente o a través de otro agente de retransmisión. El mensaje recibido ya sea de un cliente o de otro agente de retransmisión se encapsula en una opción en el mensaje a reenviar.
- RELAY-REPL, un servidor envía un mensaje de retranmisión en respuesta a la solicitud, conteniendo un mensaje que el agente de retransmisión entregara al cliente. Igualmente el servidor encapsula el mensaje, el cual será extraido por el agente de retransmisión y transmitido al cliente.

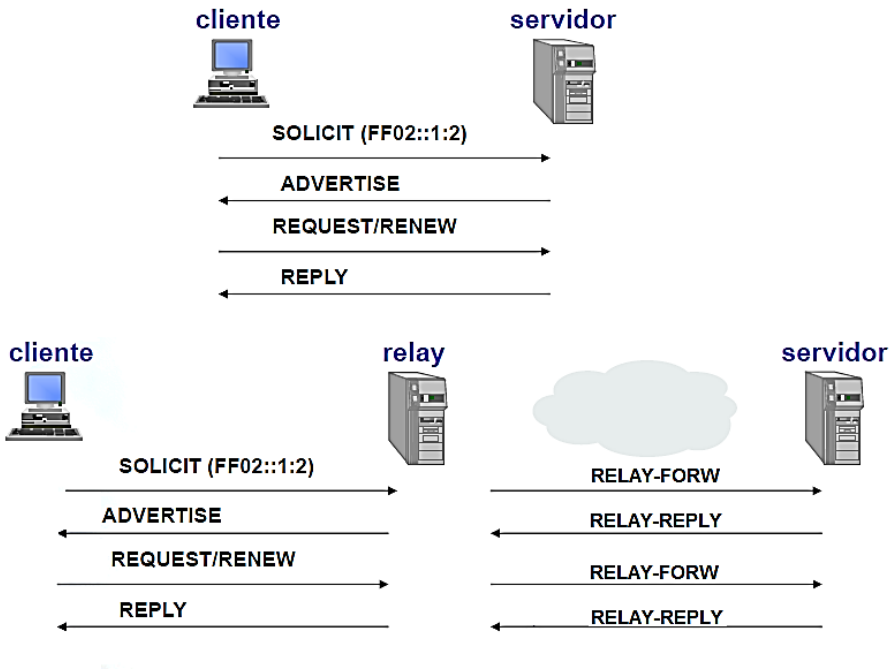


Ilustración 54. DHCPv6

DHCPv6-PD (RFC 3633[43])

Proporciona a los encaminadores autorizados que lo necesiten un mecanismo automatizado para la delegación de prefijos IPv6.

Los encaminadores que delegan no necesitan tener conocimiento acerca de la topología de red a la que están conectados los encaminadores solicitantes.

Los encaminadores que delegan no necesitan ninguna información aparte de la identidad del encaminador que solicita la delegación de un prefijo.

- Un ISP que asigna un prefijo a un CPE[44] que actúa como encaminador.

[43] RFC 3633: "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[44] El **CPE** (Equipo Local del Cliente) es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación.

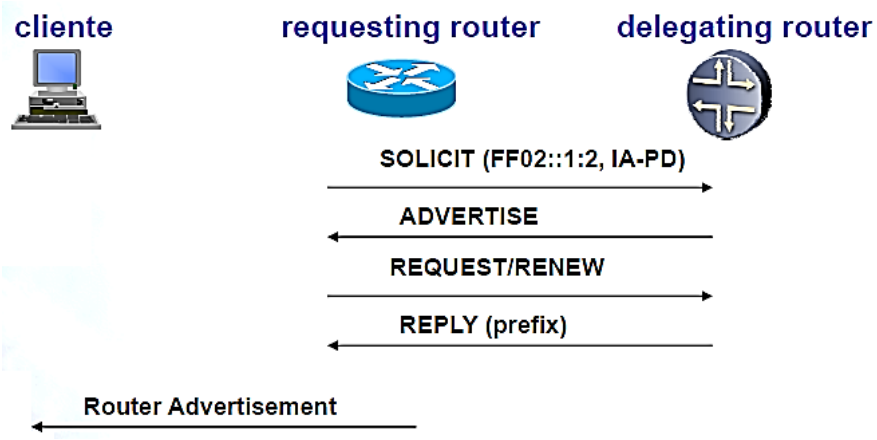


Ilustración 55. Ejemplo básico DHCPv6-PD

En la ***Ilustración 55***, se ilustra de forma general el servicio DHCPv6 con delegación de prefijo. La delegación de prefijo con DHCP es independiente de la asignación de direcciones con DHCP. Un router solicitante (requesting router) puede usar DHCP solo para la delegación de prefijo o para delegación de prefijo junto con la asignación de direcciones y otra información de configuración.

Un router solicitante crea primero un IA_PD[45] y le asigna un IAID[46]. El router solicitante a continuación, transmite el mensaje SOLICIT que contiene la opción IA_PD decribiendo la IA_PD. El router delegado (delegating router) que puede delegar prefijos a los IA_PD responde a la solicitud del router con un mensaje ADVERTISE.

El router solicitante puede incluir prefijos en la IA_PD como una sugerencia para el router delegado sobre los prefijos específicos para los cuales el router solicitante tiene preferencia.

Cuando el router solicitante ha identitificado un router delegado, el router solicitante usa un mensaje REQUEST para rellenar la IA_PD con prefijos. El router solicitante incluye una o más opciones IA_PD en el mensaje REQUEST. Luego el router delegado retorna prefijos y otra información sobre la IA_PD al router solicitante en las opciones de IA_PD en un mensaje de respuesta (REPLY).

[45] **IA_PD** (Identity Association for Prefix Delegation), es una coleccion de prefijos asignada al router solicitante. Cada IA_PD tiene un IAID asociado.

[46] **IAID**, es un identificador único para cada IA_PD.

Finalmente, luego que se ha asingando una subred a partir de un prefijo delegado, el router solicitante comienza a enviar notificaciones del enrutador (router advertisement) para el prefijo en ese enlace.

Detalles de DHCPv6-PD

El encaminador que solicita la delegación (Requesting Router, RR) necesita autenticación.

El perfil de un RR se puede almacenar en un servidor AAA.

El prefijo delegado se puede extraer de:

- Perfil del cliente almacenado en el servidor AAA.
- Lista de prefijos (prefix pool).

Los prefijos delegados tienen cierto período de validez, al igual que las direcciones IPv6 en DHCPv6.

Lo que DHCPv6-PD no hace es proporcionar un método para propagar el prefijo delegado a través de la red del usuario.

- Todos los prefijos ::/64 que se pueden extraer de un prefijo delegado se asignan en el RR de acuerdo a las políticas que tengan configuradas.

Se pueden usar los DHCPv6 relays en DHPv6-PD de igual forma que en DHCPv6.

En la ***Ilustración 56*** se muestra una arquitectura de red en donde la delegación de prefijo puede ser implementado. En este ejemplo, el router está configurado con la delegación de un conjunto de prefijos que se utilizan para la asignación a los clientes en el momento de la primera conexión de cada cliente para el servicio de ISP. El proceso de delegación de prefijo comienza cuando el solicitante solicita información de configuración al router a través de peticiones DHCP. Los mensajes DHCP son recibidos desde el router solicitante al router delegado a través del dispositivo de agregación. Cuando el router delegado recibe una petición se selecciona un prefijo o prefijos disponibles para la delegación del

router solicitante. Entonces el router delegado retorna el prefijo o prefijos al router solicitante.

El router solicitante delega prefijos de subred y asigna el prefijo mayor a los enlaces de red del suscriptor. Un típico escenario de red se muestra en la ***Ilustración 56***, donde el router solicitante puede delegar solo prefijos /48 a las subredes en un prefjo /64 y asignar un prefijo /64 para cada enlace de red con el suscriptor.

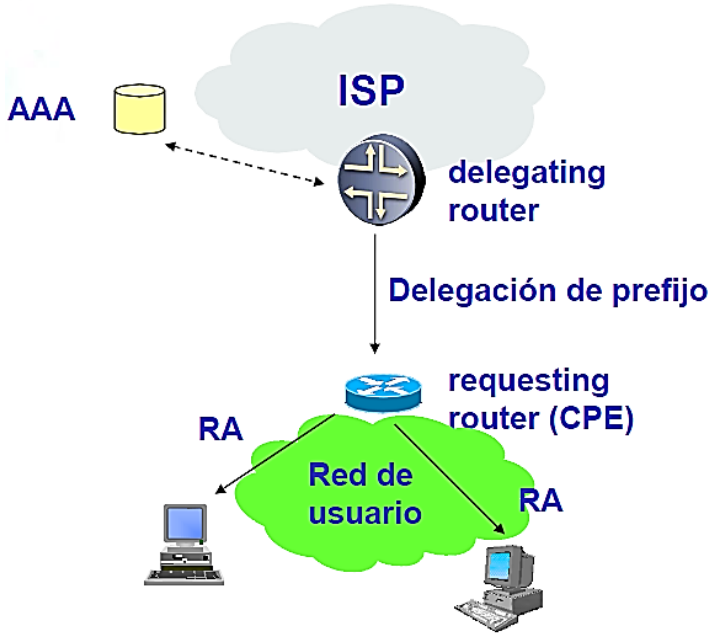


Ilustración 56. Arquitectura de red para DHCPv6-PD

Nuevas características de usuario con DHCPv6

- Configuraciones de actualizaciones dinámicas de servidores DNS.
- Deprecación de direcciones para la renumeración dinámica.
- Los “relay” se pueden configurar con direcciones de servidor o usar multicast.
- Autenticación.
- Los clientes pueden pedir múltiples direcciones IPv6.

- Las direcciones pueden ser reclamadas usando mensajes “Reconfigure-init”.
- Integración entre autoconfiguración de tipo “stateful” y “stateless”.
- Habilitando “relays” para localizar servidores no alcanzables.

4.5. Router Renumbering

ND y la autoconfiguración de direcciones IPv6 hacen la asignación inicial de los prefijos y de las direcciones de red a los diversos host.

Gracias a estos dos mecanismos, el procedimiento de reconfiguración de host es extremadamente sencillo cuando los prefijos de una red cambian.

El mecanismo de renumeración de encaminadores (Router Renumbering, “RR”) permite configurar y reconfigurar los prefijos de direcciones en los encaminadores tan fácilmente cómo funciona la combinación de ND y la autoconfiguración de direcciones en los host.

Proporciona un medio para que el administrador de la red haga actualizaciones en los prefijos usados y que se anuncian por medio de los encaminadores IPv6 a toda una red.

Funcionamiento

Los paquetes “Router Renumbering Command” contienen una secuencia de operaciones de control de prefijos (PCO[47]: Prefix Control Operations).

Cada PCO especifica una operación, un prefijo-planilla y cero o más prefijos de uso.

Un encaminador procesa cada PCO, comprobando cada una de sus interfaces para una dirección o prefijo que concuerda con el prefijo-plantilla.

Se aplica a cada interfaz en la que el prefijo-plantilla concuerda.

La operación puede ser: ADD, CHANGE, o SET-GLOBAL para respectivamente instar al encaminador a añadir un prefijo de uso, para configurar prefijos, quitar un prefijo y

[47] **Prefix Control Operation**, es la unidad más pequeña de operación en un router renumbering.

reemplazarlo con el prefijo de uso, o reemplazar todos los prefijos de ámbito global con los prefijos de uso.

5. SEGURIDAD IPV6

5.1. Introducción

Aunque el término Seguridad abarque gran cantidad de temas, en esta sección se abordaran solo los relacionados con IPv6.

En primer lugar se dará una descripción de IPsec debido a que es obligatoria su implementación en todas las pilas IPv6, proporcionando la posibilidad de su uso a todos los dispositivos IPv6.

A continuación se tratarán algunas soluciones de seguridad concretas desarrolladas en el contexto de IPv6: Extensiones de Privacidad y SEND.

Se compararán IPv6 e IPv4 desde el punto de vista de las amenazas a la seguridad.

Se expondrá un análisis general desde el punto de vista práctico, comparando elementos de seguridad IPv4 e IPv6.

Por último se introducirá el concepto de Seguridad Distribuida.

5.2. IPsec: la teoría

Seguridad IP (IPSec)

Objetivos:

- Proporcionar seguridad criptográfica, de calidad e interoperable para IPv4 e IPv6.
- No afectar negativamente a usuarios, hosts u otros componentes de Internet que no usen IPsec para la protección del tráfico.
- Los protocolos de seguridad (AH, ESP e IKE) se han diseñado para ser independientes de los algoritmos de cifrado usados. Se define un conjunto de algoritmos por defecto.

Conjunto de Servicios de Seguridad:

- Control de acceso.

- Integridad sin–conexión.
- Autenticación del origen de los datos.
- Protección contra reactuación (un tipo de integridad de secuencia parcial).
- Confidencialidad (cifrado).
- Confidencialidad de flujo de tráfico limitado.

IPsec: Elementos básicos

Elementos básicos:

- **Arquitectura base** para sistemas conformes con IPsec (RFC 4301[48]).
- **Protocolos de seguridad:** Authentication Header (RFC 4302[49]) y Encapsulating Security Payload (ESP) (RFC 4303[50]).
- **Asociaciones de seguridad:** qué son y cómo funcionan, cómo se gestionan (RFC 4301).
- **Gestión de claves:** Manual y Automática (La Internet Key Exchange IKE) (RFC4306[51]).
- **Algoritmos para autentificación y cifrado:** Se definen algoritmos obligatorios, por defecto, para su uso con AH y ESP (RFC4835[52]) y para IKEv2 (RFC4307[53]).

[48] RFC 4301: “Security Architecture for the Internet Protocol”.

[49] RFC 4302: “IP Authentication Header”.

[50] RFC 4303: “IP Encapsulating Security Payload (ESP)”.

[51] RFC 4306: “Internet Key Exchange (IKEv2) Protocol”.

[52] RFC 4835: “Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”.

[53] RFC 4307: “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)”.

Visión General

Una implementación IPsec opera en un host, como una pasarela de seguridad (SG) o como un dispositivo independiente.

La protección ofrecida por IPsec se basa en los requerimientos definidos en la Security Policy Database (SPD).

Los paquetes se clasifican basándose en información de las cabeceras IP y "next layer", para buscar coincidencias en la SPD.

Cada paquete puede ser DESCARTADO, PROTEGIDO usando los servicios IPsec o permitirse su PASO a través de la protección IPsec.

IPsec se puede usar para proteger uno o más "caminos":

- Entre un par de hosts.
- Entre un par de pasarelas de seguridad.
- Entre una pasarela de seguridad y un host.

Cuando se utiliza la autenticación Kerberos, durante la negociación de modo principal, cada interlocutor de IPSec envía al otro interlocutor la identidad de su equipo en formato no cifrado. La identidad del equipo no está cifrada hasta que la carga de identidad completa se cifra durante la fase de autenticación de la negociación del modo principal. Un intruso puede enviar un paquete de Intercambio de claves de Internet (IKE, Internet Key Exchange) para que el interlocutor IPSec que responde exponga la identidad de su equipo y su pertenencia a un dominio. En la ***Ilustración 57***, se muestran los dos escenarios a tomar en cuenta y que se describen a continuación:

- ***Tráfico protegido (mediante AH o ESP)*:**

A la hora de decidir entre usar AH o ESP para proteger el tráfico IP, hay que considerar lo siguiente:

  - AH proporciona servicios de autenticación y de integridad de datos mediante el cálculo e inclusión de una función hash basada en una clave para cada paquete.

Con AH, el cálculo de la función hash incluye todo el paquete IP y su encabezado. Se excluyen algunos campos que pueden cambiar en el trayecto. Para proporcionar servicios de protección de repetición de paquetes se incluye un número de secuencia para cada paquete.

- ESP proporciona servicios de autenticación y de integridad de datos mediante el cálculo e inclusión de una función hash basada en una clave para cada paquete. Con ESP, el cálculo de la función hash sólo incluye el encabezado ESP, el finalizador y la carga. El encabezado IP no se protege con la función hash. ESP proporciona servicios de confidencialidad de datos mediante el cifrado de la carga ESP con el algoritmo DES (Estándar de cifrado de datos) o 3DES (Triple DES). Para proporcionar servicios de protección de repetición de paquetes se incluye un número de secuencia para cada paquete.

Se consumen menos recursos de la CPU al calcular y comprobar la función hash de cada paquete que al cifrarlo y descifrarlo. Si el rendimiento es especialmente importante, puede utilizar AH para proteger la mayor parte del tráfico. Cuando se requiere confidencialidad, puede utilizar ESP en su lugar. Por ejemplo, puede utilizar AH para proteger el tráfico de la intranet y ESP para el tráfico que se envía a través de Internet.

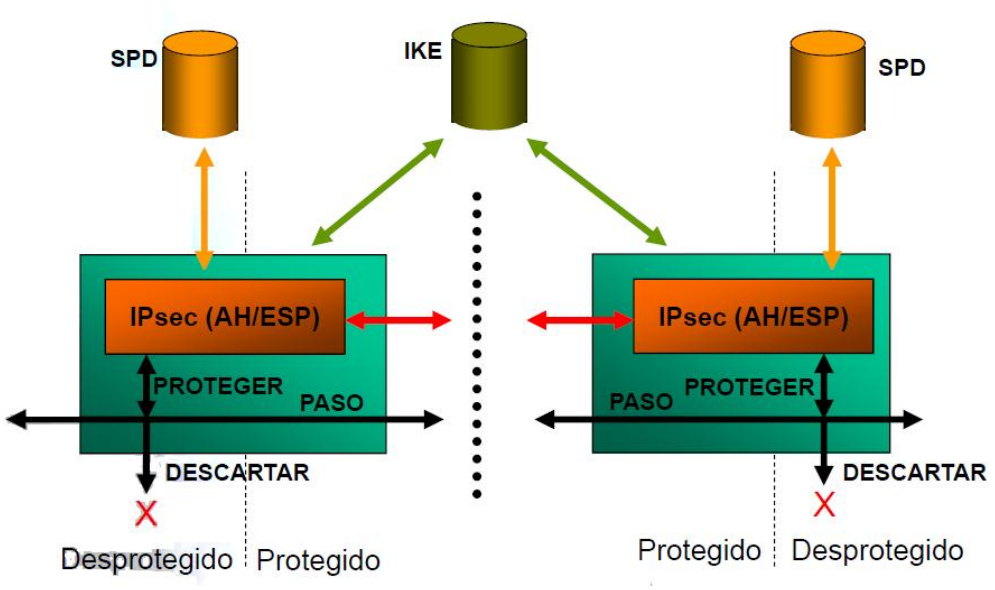


Ilustración 57. IPsec, visión general

- ***Tráfico no protegido (con la regla de respuesta predeterminada)***

Resulta sencillo establecer un escenario de implementación de IPSec que proteja el tráfico desde un conjunto específico de servidores, del modo siguiente:

1. Sitúar los servidores en una unidad organizativa y asigne una directiva IPSec a un objeto de directiva de grupos de esa unidad organizativa, con una regla que requiera tráfico protegido entre los servidores y cualquier otro equipo. Dentro de la acción de filtrado de la regla, permita a los servidores seguros aceptar comunicaciones no seguras, pero respondiendo siempre con IPSec.
2. Sitúe los equipos cliente en una unidad organizativa y asignar a un objeto de directiva de grupos de esa unidad organizativa una directiva IPSec que sólo aplique la regla de respuesta predeterminada.

En la ***Ilustración 57***, "Desprotegido" se refiere a una interfaz que también podría ser descrito como "negro" o "texto cifrado". Y "Protegido" se refiere a una interfaz que también podría ser descrita como "rojo" o "texto plano".

PAD (Peer Authorization Database)

La PAD proporciona un enlace entre la SPD y un protocolo de gestión de asociaciones de seguridad como IKE. Se encarga de varias funciones críticas:

- Identificar peers o grupos de peers que están autorizados a comunicarse con la entidad IPsec.
- Especifica el protocolo y el método usado para autentificar cada peer.
- Proporciona los datos de autentificación para cada peer.
- Limita los tipos y valores de IDs que puede usar un peer para crear una SA "hijo", asegurando así que no use identidades, que se busquen en la SPD, que no está autorizado a usar cuando se crea una SA hijo.

- Información de localización de pasarela de un peer, por ejemplo, dirección(es) IP o nombres DNS, PUEDEN incluirse para peers que se sabe están “detrás” de una pasarela de seguridad.

Protocolos de seguridad

Las implementaciones IPsec DEBEN soportar ESP y PUEDEN soportar AH. AH y ESP pueden aplicarse solas o en combinación con la otra.

AH proporciona:

- Integridad.
- Autenticación del origen de los datos.
- Opcionalmente (según criterio del receptor) servicio anti-reactuación.

ESP proporciona:

- Integridad.
- Autenticación del origen de los datos.
- Opcionalmente (según criterio del receptor) servicio anti-reactuación.
- Confidencialidad (no recomendada sin integridad).

Ambas ofrecen control de acceso, impuesta a través de la distribución de claves criptográficas y la gestión de flujos de tráfico según dicte la SPD.

Estos mecanismos están diseñados para ser independientes de los algoritmos.

SA: El concepto

La Asociación de Seguridad (Security Association - SA) es un concepto fundamental para IPsec: Una “conexión” simple que proporciona servicios de seguridad al tráfico que transporta.

AH y ESP usan SA, de forma que todas las implementaciones DEBEN soportar el concepto de Asociación de Seguridad.

Una de las principales funciones de IKE es el establecimiento y mantenimiento de SAs.

Para asegurar una comunicación bidireccional típica entre dos nodos con IPsec, se necesitan dos SAs (una para cada dirección). IKE crea pares de SAs.

Identificación de SA

Cada SA se identifica unívocamente por el tema:

- Índice de Parámetros de Seguridad (Security Parameter Index-SPI).
    - Cadena de bits asignada a la SA (significado local), como puntero a una base de datos de SAs (SPD o Security Policy Database).
- Dirección IP destino.
- Identificador de protocolo de seguridad (AH o ESP).

La dirección destino puede ser:

- Dirección Unicast.
- Dirección Broadcast.
- Direccion Grupo Multicast.

SA Database (SAD)

En cada implementación IPsec existe una base de datos de SAs (SAD, Security Association Database).

Cada entrada define los parámetros asociados con una SA.

Cada SA tiene una entrada en la SAD.

La SPD tiene punteros a entradas en la SAD, cuando se tiene que usar IPsec (Proteger).

Campos de la SAD

- ***Security Parameter Index (SPI)***: Un valor de 32 bits seleccionado por el extremo receptor de una SA para identificar unívocamente la SA.
- ***Sequence Number Counter***: Un contador de 64 bits usado para generar el número de secuencia transmitido en las cabeceras AH y ESP (los números de secuencia de 64 bits se usan por defecto, pero los de 32 bits también se soportan si se negocian previamente).
- ***Sequence Counter Overflow***: Un flag que indica si el desbordamiento del contador de número de secuencia debe generar un evento auditable y evitar el envío de más paquetes por la SA, o si se permite el reinicio del contador.
- ***Anti-Replay Window***: Un contador de 64 bits y un bit-map (o equivalente) usado para determinar si un paquete AH y ESP de entrada es un reenvío.
- ***AH Information***: Algoritmos de autentificación, claves, tiempos de vida, etc.
- ***ESP Information***: Algoritmos de autentificación y cifrado, claves, tiempos de vida, valores iniciales, etc.
- ***IPsec Protocol Mode***: Túnel o Transporte.
- ***SA Lifetime***: Intervalo de tiempo o bytes de una SA.
- ***Stateful fragment checking flag***: Indica si se aplica o no comprobación de fragmentado a la SA.
- ***DSCP values***: El conjunto de valores DSCP permitidos para los paquetes que van sobre esta SA. Si no se especifíca ningún valor no se aplica ningún filtro DSCP.
- ***Bypass DSCP (T/F)*** o mapear a valores DSCP no protegidos si es necesario para restringir el paso de valores DSCP, aplicable a SAs en modo túnel.
- ***Tunnel header IP source and destination address:*** ambas direcciones deben ser o IPv4 o IPv6.
- ***Path MTU:*** Tamaño máximo de paquete transmitido sin fragmentar.

Transmisión IPsec

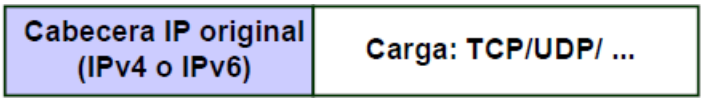


Ilustración 58. Cabecera IPsec

En la ***Ilustración 58*** se muestra la cabecera IPsec insertada entre la cabecera original y la carga.

Si se usa ESP, los datos se cifran y se añade una "coletilla" IPsec, a como se aprecia en la ***Ilustración 59***.

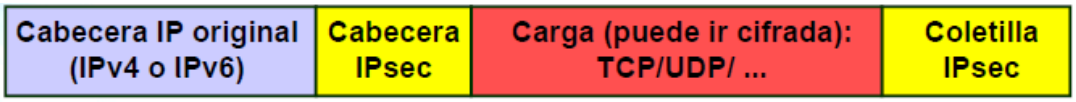


Ilustración 59. Cabecera IPsec con ESP

Valor de Next Header:

- ESP=50
- AH=51

Cabecera AH (RFC4302[54])

La cabecera AH, es un miembro de la suite del protocolo IPsec. AH garantiza la integridad sin conexión y la autenticación del origen de los datos de los paquetes IP. Además opcionalmente puede proteger contra los ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. A continuación en la ***Ilustración 60*** se muestra el formato de cabecera con los campos más importantes:

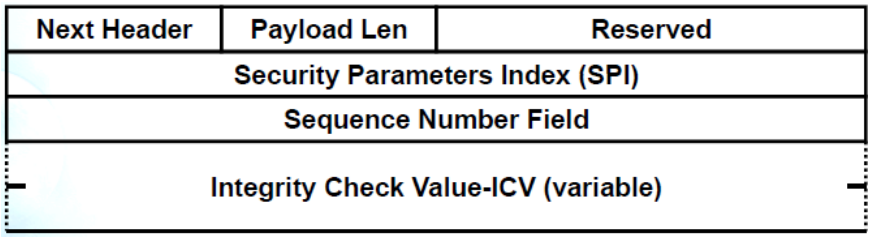


Ilustración 60. Cabecera AH

[54] RFC 4302: "IP Authentication Header".

- SPI: Valor arbitrario de 32 bits que usa el receptor para identificar la SA a la que pertenece un paquete que llega, el tipo de protocolo IPsec (AH) también puede ser necesario.
- Sequence Number: campo de 32 bits sin signo que contiene un contador que se incrementa en uno por cada paquete enviado, por ejemplo, un número de secuencia de paquete para cada SA.
- Integrity Check Value (ICV): Campo de longitud variable. El campo debe tener un tamaño múltiplo de 32 bits (para IPv4 e IPv6).

Cabecera ESP (RFC 4303[55])

ESP (Encapsulating Security Payload) es miembro de la suite del protocolo IPsec. IPsec proporciona autenticidad en el origen, integridad y protección de la confidencialidad de los paquetes. ESP también soporta configuraciones de solo encriptación y/o solo autenticación, pero el uso de cifrado sin autenticación esta totalmente desaconsejado porque es inseguro. A diferencia de la cabecera de autenticación (AH), ESP en modo de transporte no proporciona integridad y autenticación para todo el paquete IP.

Sin embargo, en modo túnel, donde se encapsula todo el paquete IP original con un encabezado de paquete nuevo añadido, ESP protege a todo el paquete IP interno (incluyendo el interior de la cabecera), mientras que la cabecera externa permanece sin protección. ESP opera directamente sobre IP, utilizando el protocolo IP numero 50.

En la siguiente ***Ilustración 61*** se muestra como esta construido un paquete ESP y sus principales campos:

[55] RFC 4303: “IP Encapsulating Security Payload (ESP)”.

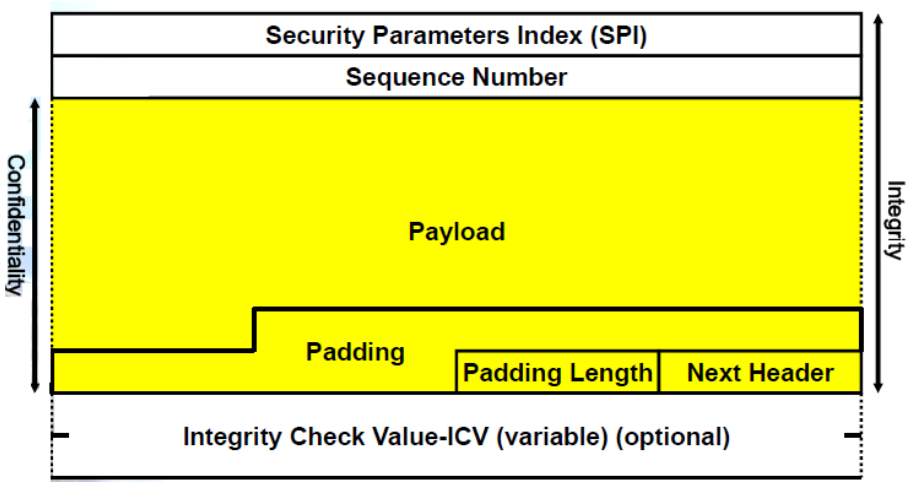


Ilustración 61. Cabecera ESP

Algoritmos ESP

Especificados en la SA.

Algoritmos de Cifrado ESP (RFC 4835[56]):

- ***MUST:*** NULL (RFC2410), AES-CBC con clave de 128-bit (RFC 3602[57]).
- ***MUST-:*** TipleDES-CBC (RFC 2451[58]).
- ***SHOULD:*** AES-CTR (RFC 3686[59]).
- ***SHOULD NOT:*** DES-CBC (RFC 2405[60]).

Algoritmos de Autentificación ESP (RFC 4835):

- ***MUST:*** HMAC-SHA1-96 (RFC 2404[61]).

[56] RFC 4835: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[57] RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".

[58] RFC 2451: "The ESP CBC-Mode Cipher Algorithms".

[59] RFC 3686: "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)".

[60] RFC 2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".

- ***SHOULD+:*** AES-XCBC-MAC-96 (RFC 3566[62]).
- ***MAY:*** NULL, HMAC-MD5-96 (RFC 2403[63]).

Algoritmos AH

Especificados en la SA.

Algoritmos de Autentificación AH (RFC 4835):

- ***MUST:*** HMAC-SHA1-96 (RFC 2404).
- ***SHOULD+:*** AES-XCBC-MAC-96 (RFC 3566).
- ***MAY:*** NULL, HMAC-MD5-96 (RFC 2403).

Modos de uso

Cada protocolo soporta dos modos de uso:

- Modo Transporte (protege principalmente protocolos de capa superior):
    a) Directo entre dos sistemas extremo-a-extremo.
    b) Los dos sistemas remotos deben soportar IPsec.

En la siguiente ***Ilustración 62***, se muestra el Encabezado de autenticación (AH) el cual proporciona autenticación, integridad y protección antirreproducción para todo el paquete (el encabezado IP y la carga de datos transportados en el paquete). No proporciona confidencialidad, ya que no cifra los datos. La información es legible, pero está protegida contra modificaciones. AH utiliza algoritmos hash con claves para firmar el paquete y asegurar su integridad.

Por ejemplo, si Alicia en el equipo A envía información a Benito en el equipo B. El encabezado IP, el encabezado AH y los datos tienen protegida su integridad. Esto

[61] RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[62] RFC 3566: "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec".

[63] RFC 2403: "The Use of HMAC-MD5-96 within ESP and AH".

significa que Benito puede estar seguro de que realmente fue Alicia quien envió la información y de que la información no ha sido modificada.

La integridad y la autenticación se consiguen al situar el encabezado AH entre el encabezado y la carga de IP, como se observa en la ***Ilustración 62***. AH firma todo el paquete para garantizar su integridad, a excepción de algunos campos del encabezado IP que pueden cambiar durante el trayecto (por ejemplo, los campos Tiempo de vida y Tipo de servicio). Si se utilizan otros encabezados de IPSec además de AH, el encabezado AH se inserta delante de todos ellos. La ***Ilustración 62*** siguiente muestra la firma AH del paquete.

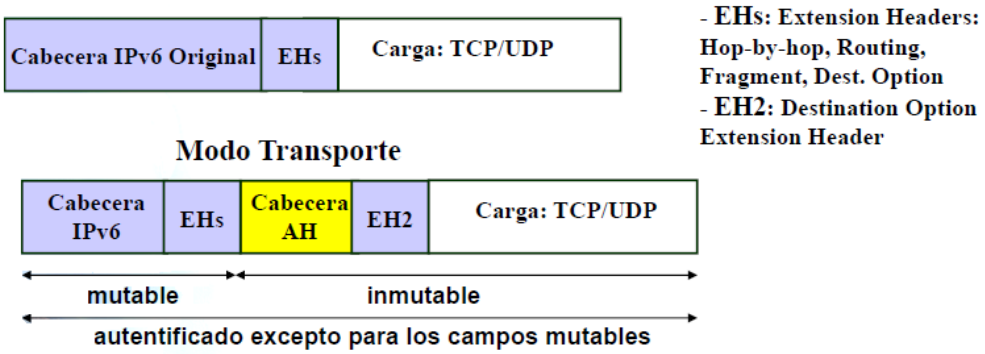


Ilustración 62. AH en modo Transporte

En la ***Ilustración 63*** se muestra, el encabezado ESP el cual se coloca delante de la carga IP, y tras ella se incluye un finalizador ESP y un finalizador de autenticación ESP.

La Carga de seguridad de encapsulación (ESP) ofrece confidencialidad (además de proporcionar autenticación, integridad y protección antirreproducción) para la carga IP. ESP en modo de transporte no firma todo el paquete. Sólo se protege la carga IP, no el encabezado IP. ESP puede utilizarse por sí solo o en combinación con AH.

Por ejemplo, si Alicia en el equipo A envía datos a Benito en el equipo B. La carga IP está cifrada y firmada para garantizar su integridad. Al recibirse, una vez completado el proceso de comprobación de la integridad, se descifra la carga de datos del paquete. Benito puede estar seguro de que fue Alicia quien le envió la información, de que la información no ha sufrido cambios y de que nadie más ha podido leerla.

Asi mismo, se puede apreciar en la ***Ilustración 63***, que ESP proporciona protección a las cargas IP. La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad.

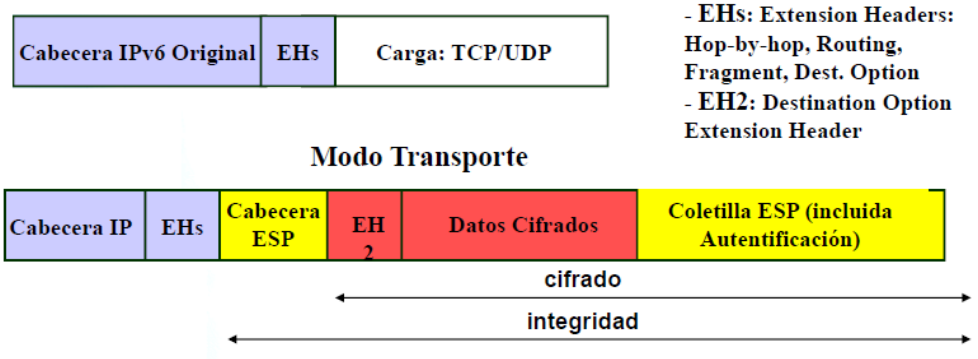


Ilustración 63. ESP en modo Transporte

- Modos Túnel (protocolos aplicados a paquetes IP encapsulados):

    a) Túnel seguro para encapsular paquetes IP inseguros.

    b) Entre sistemas intermedios (no extremo-a-extremo).

Cuando se utiliza modo de túnel de IPSec, IPSec cifra el encabezado IP y la carga, mientras que el modo de transporte sólo cifra la carga IP. El modo de túnel protege los paquetes IP completos, pues los trata como una carga AH o ESP. Con el modo de túnel, todo el paquete IP se encapsula con un encabezado AH o ESP y un encabezado IP adicional. Las direcciones IP del encabezado IP externo son los extremos del túnel, y las direcciones IP del encabezado IP encapsulado son las direcciones últimas de origen y de destino.

Como se muestra en la ***Ilustración 64***, el modo de túnel AH encapsula un paquete IP con un encabezado AH e IP y firma todo el paquete para asegurar su integridad y autenticación.

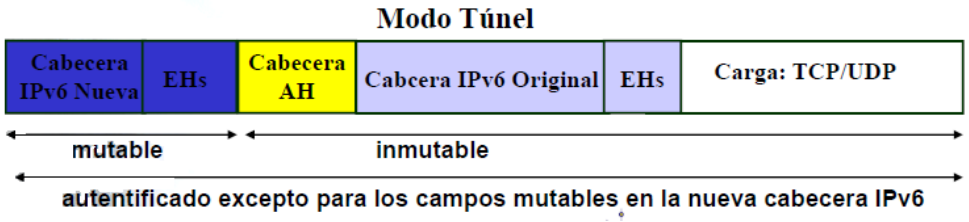


Ilustración 64. AH en modo Túnel

Como se muestra en la ***Ilustración 65*** siguiente, el modo de túnel ESP encapsula un paquete IP con un encabezado ESP e IP y un finalizador de autenticación ESP.

La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad.

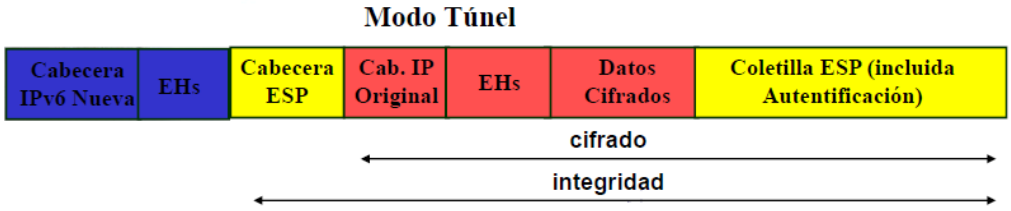


Ilustración 65. ESP en modo Túnel

Debido al nuevo encabezado agregado al paquete para el túnel, todo lo que sigue al encabezado ESP está firmado (excepto el finalizador de autenticación ESP), ya que ahora se encuentra encapsulado en el paquete enviado por el túnel. El encabezado original se coloca después del encabezado ESP. El paquete entero se anexará con un finalizador ESP antes del cifrado. Todo lo que sigue al encabezado ESP, salvo el finalizador de autenticación ESP, se cifra. Esto incluye el encabezado original, que ahora se considera parte de los datos del paquete.

En la ***Ilustración 66*** se aprecian los dos modos de operación de IPsec en que pueden ser implementados:

- En modo de transporte, sólo la carga útil (los datos se transfieren) del paquete IP suele ser cifrados y/o autenticado. El enrutamiento permanece intacto, ya que la cabecera IP no es modificada o cifrada, sin embargo, cuando la cabecera de autenticación se utiliza, las direcciones IP no pueden ser traducidas, ya que esto

anularía el valor hash. Las capas de transporte y aplicación están siempre aseguradas por hash, por lo que no pueden ser modificados de ninguna manera (por ejemplo traduciendo los números de puerto). El modo de transporte se utiliza para las comunicaciones de host a host.

- En modo túnel, todo el paquete IP es cifrado y/o autenticado. Es encapsulado en un paquete IP nuevo con una nueva cabecera IP. El modo túnel se utiliza para crear redes privadas virtuales para las comunicaciones de red a red (por ejemplo, entre los routers a los sitios de enlace), host-a-red de comunicaciones (por ejemplo, acceso de usuarios remotos), y el host a host de comunicación (chat privado, por ejemplo). El modo de túnel soporta NAT transversal.

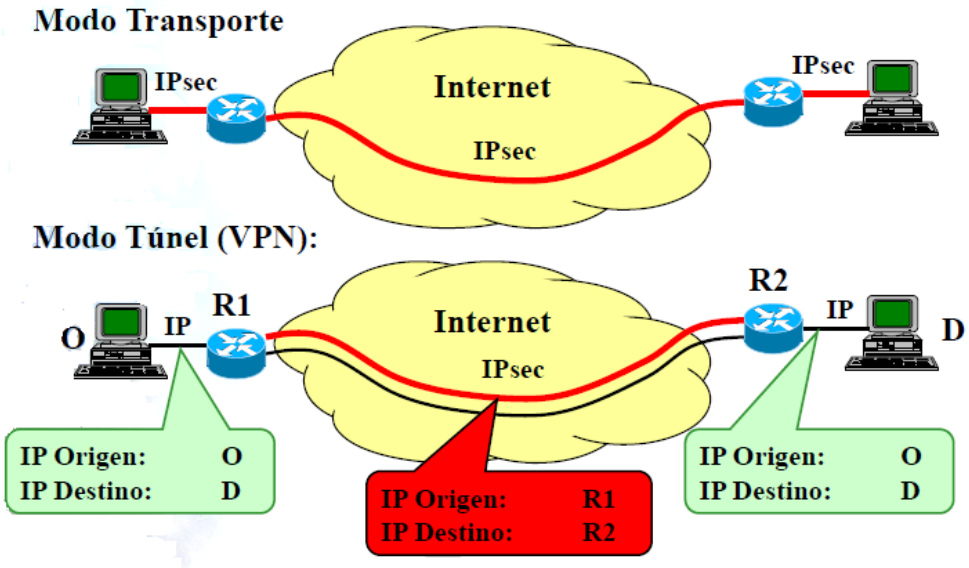


Ilustración 66. Modo Transporte vs Modo Túnel

El problema de la clave

AH y ESP necesitan usar las mismas claves con el fin de establecer la SA entro los nodos extremos:

- En algunos casos esa clave se configura manualmente, pero no es una solución escalable a decenas o cientos de nodos.
    - Gestión más sencilla.

- Cada sistema se configura con las claves propias y de los demás.

- En ciertos entornos se necesita una solución que sea automática, creando una SA de forma dinámica, pero eso requiere la existencia de un canal seguro entre los nodos con el fin de intercambiar las claves.
  - IKE es la solución propuesta para el establecimiento de SA de forma automática.

IKEv1 (RFC 4109[64]) es en realidad una combinación de otras piezas:

- ISAKMP (RFC 4109). Marco abstracto para la autenticación e intercambio de claves, diseñado para ser independiente del método particular de intercambio de claves que se vayan a usar.
  - "Internet IP Security Domain of Interpretation for ISAKMP" o Internet DOI (RFC 2407[65]). Define el uso de los campos de ISAKMP (números de protocolos algoritmos, modos, etc.).
- OAKLEY (RFC 2412[66]). Proporciona métodos seguros para la determinación de claves.
- SKEME. Proporciona un mecanismo versátil para el intercambio de claves.

Principios básicos de IKE

"IKE proporciona un mecanismo seguro para el intercambio de claves entre nodos IPsec con el fin de permitir el establecimiento y gestión de SA":

- Se trata de un protocolo extremo-a-extremo.
- El bloque fundamental de IKE es la Asociación de Seguridad del protocolo ISAKMP.
  - Una SA ISAKMP[67] es bidireccional, a diferencia de una SA IPsec.

[64] RFC 4109: "Algorithms for Internet Key Exchange versión 1 (IKEv1)".

[65] RFC 2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[66] RFC 2412: "The OAKLEY Key Determination Protocol".

IKE proporciona un canal seguro para el intercambio de información para el establecimiento de claves para IPsec.

Los nodos involucrados deben autenticarse mutuamente mediante:

- "pre-shared secrets" (PSK).
- Firmas digitales (DSS o RSA).
- Certificados X.509.
- Encriptación basada en claves públicas.

IKE usa datagramas UDP para el intercambio de mensajes, a través del puerto 500.

La configuración ISAKMP se compone de dos fases:

- La fase 1 es para la configuración de una SA ISAKMP entre los nodos (canal seguro).
    - Se ejecuta de forma infrecuente.
    - Existen tres métodos diferentes de funcionamiento de la fase 1 apropiados para diferentes escenarios/servicios.
- La fase 2 sirve para el establecimiento de la asociación IPsec:
    - Se ejecuta más a menudo para generar otras SAs.

Existen muchas variantes posibles debido a las posibles variantes de parámetros:

- Tipos de algoritmos de cifrado.
- Tipos de funciones hash.
- Tipos algoritmos intercambio de claves.
- Tipos de autenticación.

ISAKMP se basa en valores de jerarquía multinivel:

[67] **SA ISAKMP**, un SA es usado por los servidores de ISAKMP para proteger a su propio tráfico.

- Cada propuesta se compone de una transformada con diferentes atributos.
- Cada transformada define:
  - Método de cifrado.
  - Método de autenticación.

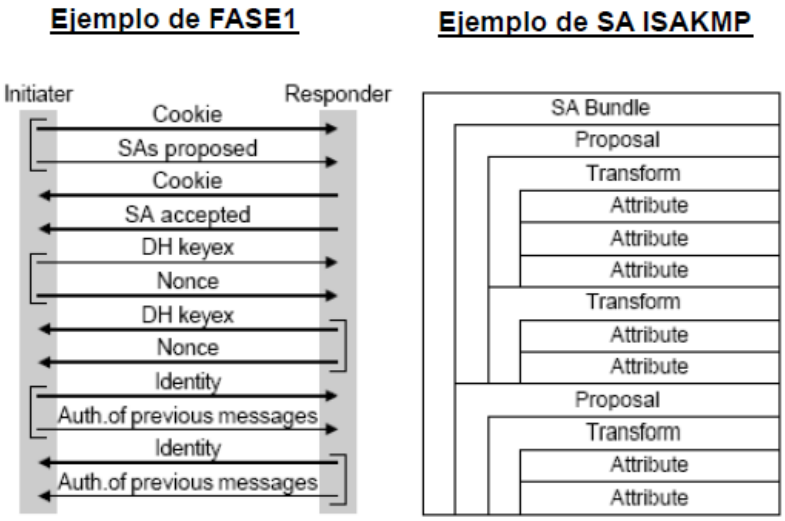


Ilustración 67. Ejemplo de Fase1 y SA ISAKMP

En la ***Ilustración 67*** se muestra el intercambio de mensajes de los nodos en el proceso de negociación. El término "SA bundle" se aplica a una secuencia de SAs a través de la cual el tráfico debe ser procesado para satisfacer una política de seguridad.

Objetivo de IKEv2

IKEv1 es demasiado difícil y extremadamente complicado de depurar en caso de problemas.

IKEv1 no es manejable en entornos de producción con muchos nodos.

La configuración de IKEv1 precisa de ingenieros de red con mucha experiencia. Se puede llegar a tardar más de una jornada de trabajo en la configuración de un enlace IPsec con IKEv1 en el caso de usar equipos de fabricantes diferentes.

Al final los usuarios tienden a configurar manualmente las SA IPsec debido a la complejidad de IKEv1.

Como consecuencia se ha definido IKEv2 (RFC 4306[68]) con el fin de hacer las cosas más sencillas:

- IKEv2 se define en un solo documento en vez de un conjunto de ellos como en IKEv1.
- Con IKEv2 se simplifica y se mejora IKEv1.
- IKEv2 ofrece un formato de cabeceras y un intercambio de mensajes más simples que IKEv1.
- Soluciona varios problemas de IKEv1.

Diferencias de IKEv2 respecto IKEv1

- La principal es que tiene muchas funcionalidades en común con IKEv1 pero de forma más simple:
  - Ocultación de la identidad.
  - "perfect forward secrecy" (PFS).
  - Dos fases para el establecimiento de la SA.
  - Negación de las claves.
  - IKEv2 usa también el puerto 500 UDP para el intercambio de mensajes, pero NO es compatible con los mensajes de IKEv1.
- IKEv2 pone más énfasis en VPN (modo túnel).
- Proporciona la posibilidad de atravesar NATs:
  - Permite el encapsulamiento de paquetes IKE y ESP en UDP para atravesar NATs.

[68] RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

- Su funcionamiento se basa en conocer el estado de la conexión con el fin de prevenir ataques de tipo DoS.
- Se añade soporte EAP (RFC 2284[69]) como método de autenticación.
- Se permite una asignación dinámica de dirección IP posibilitando la actualización de la SA.
- Se permite el uso de compresión IP.
- Buen soporte para la integración con infraestructuras AAA con el fin de que todo el material criptográfico del usuario resida en dicha infraestructura.

IKE	IKE v2
IKE SA+IPsec SA established in 8 messages	IKE SA+IPsec SA established in 4 messages
No Forward Compatibility	Forward Compatibility
No Reliability and State management	Reliability and State management
Complex cryptographic mechanisms	simple cryptographic mechanisms
No resilience for DOS attacks	Resilience for DOS attacks

Ilustración 68. IKEv1 vs IKEv2

En la ***Ilustración 68*** se plasman las principales diferencias entre ambos versiones.

5.3. Extensiones de privacidad

Introducción

En la autoconfiguración "stateless" de IPv6 en algunos casos el identificador de interfaz contiene un identificador único del IEEE, lo que permite identificar un nodo a partir de una dirección IP.

El RFC 4941[70] describe una extensión para la autoconfiguración "stateless" en IPv6 que hace que los nodos generen direcciones de ámbito global que cambian con el tiempo.

[69] RFC 2284: "PPP Extensible Authentication Protocol (EAP)".

El RFC 4941 se basa en generar identificadores de interfaz aleatorios con un tiempo de vida limitado.

¿Por qué Extensiones de Privacidad?

El problema (con identificadores IEEE):

- Las direcciones IPv6 en un interfaz dado y generada via "Stateless Autoconfiguration" contienen el mismo ID de interfaz, con independencia del lugar de Internet en el que el dispositivo se conecta. Esto puede facilitar la trazabilidad de dispositivos y/o individuos.

Posibles soluciones:

- Usar DHCPv6 para obtener direcciones. El servidor DHCP podría asignar "direcciones temporales" que nunca se renuevan y tienen la condición de temporalidad necesaria.
- Cambiar el ID de interfaz de una dirección IPv6 cada cierto tiempo y generar por tanto nuevas direcciones IPv6 para determinados ámbitos.

Extensiones de privacidad

Los nodos usan "IPv6 Stateless Autoconfiguration" para generar direcciones sin la necesidad de usar un servidor DHCPv6. Las direcciones se forman combinando el prefijo de red con un ID de interfaz:

- En interfaces que contienen ID de IEEE, se usa dicho ID para derivar el ID de interfaz de la dirección IPv6.
- En otros tipos de interfaces, el ID se crea por otros medios, por ejemplo generando números aleatorios.

[70] RFC 4941: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

El uso de extensiones de privacidad hace que los nodos generen direcciones IPv6 partiendo de ID de interfaz que cambian de vez en cuando, incluso si el interfaz contiene un ID de IEEE.

1. En realidad no provoca ningún cambio en el comportamiento básico de las direcciones generadas vía “Stateless Autoconfiguration”.
2. Se crean direcciones adicionales basadas en un ID de interfaz aleatorio con el propósito de iniciar sesiones:
    - Estas direcciones aleatorias se suelen emplear durante el período corto de tiempo (desde horas a días) y son deprecadas después de dicho período.
    - Las direcciones deprecadas se pueden seguir usando para sesiones abiertas, pero no para iniciar nuevas conexiones.
    - Periódicamente se generan nuevas direcciones temporales para reemplazar direcciones temporales que ya han expirado.
3. Se produce una secuencia de direcciones globales temporales a partir de una secuencia de IDs de interfaz que aparentemente son aleatorios en el sentido de que es difícil para un observador externo predecir la dirección/identificador futura basada en la actual e igualmente difícil determinar la dirección anterior conociendo la presente.
4. Por defecto, a partir del mismo ID de interfaz aleatorio, se generan tantas direcciones como prefijos se hayan usado para generar una dirección global mediante SAAC.

5.4. Amenazas a ND

Visión general

El protocolo Neighbor Discovery (ND) (RFC 4861[71]) es vulnerable a diversos ataques (RFC 3756[72]).

La especificación original del protocolo ND define el uso de IPsec para proteger los mensajes de ND. Por diversas razones en la práctica esta no es una solución.

SEcure Neighbor Disccovery (SEND) (RFC 3971[73]) explicado anteriormente, tiene como objetivo proteger ND.

Amenazas a ND

1. ***Neighbor Solicitation/Advertisement Spoofing:***
   - Se hace o bien mandando un NS con una opción de dirección de capa de enlace origen cambiada, o enviando un NA con una opción de dirección de capa de enlace destino cambiada.
   - Este es un ataque de redirección/DoS.

[71] RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[72] RFC 3756: "IPv6 Neighbor Discovery (ND) Trust Models and Threats".

[73] RFC 3971: "SEcure Neighbor Discovery (SEND)".

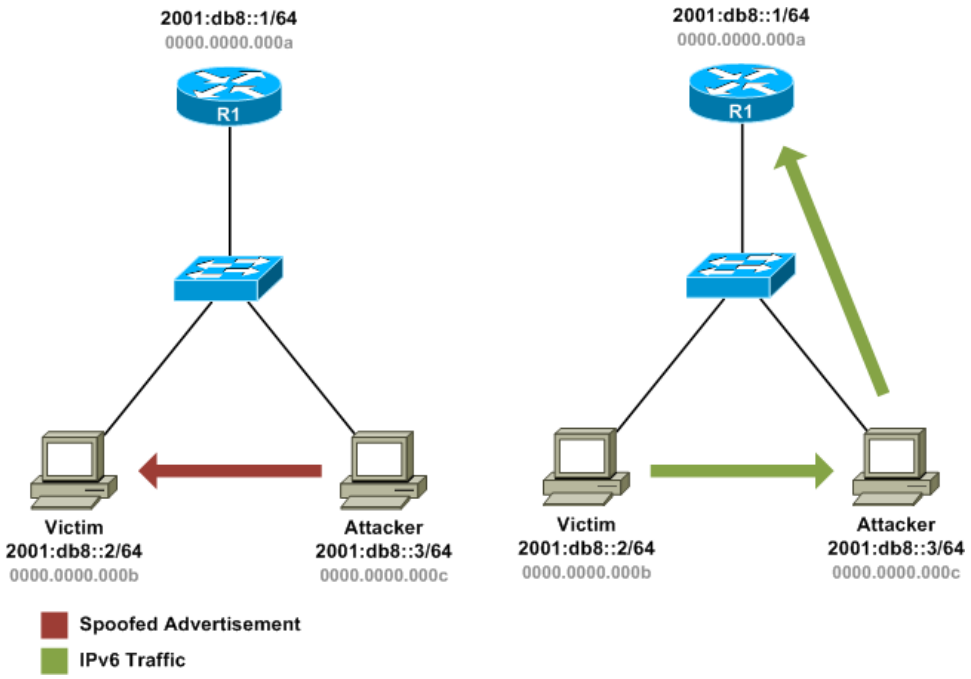


Ilustración 69. Neighbor solicitation/advertisement spoofing

En la ***Ilustración 69*** se muestra el ataque simplificado de advertisement spoofing. En IPv4 el ARP spoofing se logra cuando un atacante malintencionado a otras máquinas de la red, típicamente al Gateway por defecto. Haciéndose pasar por el Gateway prederminado de la subred, el atacante puede interceptar todo el tráfico desde los host víctimas. Aunque en la pila de protocolo de IPv6, no existe ARP, algo similar son las direcciones Neighbor Discovery que realizan la función de resolución cuando un host quiere transmitir a un prefijo de enlace pero no conoce la dirección de capa 2 del host destino, envía a los host por multicast neighbor solicitation, si es inalcanzable responden con un neighbor advertisement conteniendo la dirección de la capa 2.

Por lo tanto el intercambio de mensajes es totalmente garantizado, con lo cual los ataques se pueden producir.

2. ***Fallo de Neighbor Unreachability Detection (NUD):***

- Un nodo malicioso puede almacenar enviando NAs hechos “a medida” como respuesta a mensajes NS de NUD. Si los mensajes NA no se protegen de alguna

manera el atacante puede llevar a cabo el ataque por períodos muy largos de tiempo.

- Este es un ataque DoS (Denegación de Servicio).

3. Ataque DoS usando DAD:

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

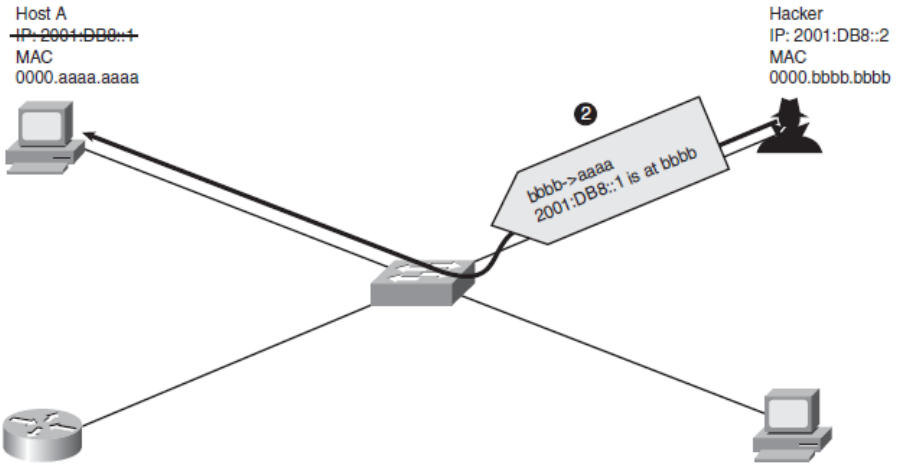


Ilustración 70. Denegación de servicio con Duplicate Address Detection

En la ***Ilustración 70*** se observa cuando el usuario malicioso envía mensajes Neighbor Discovery (mensaje etiquetado con 2) afirmando la propia dirección 2001:db8::1.

4. ***Encaminador de Último Salto Malicioso:***

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

5. ***"Muerte" del encaminador por defecto:***

- Un atacante "mata" el(los) encaminador(es) por defecto, haciendo que todos los nodos del enlace asuman que todos los nodos son locales.
- El atacante puede lanzar un ataque DoS clásico contra el encaminador de forma que parezca que no responde. Otra forma sería enviar un RA falso con tiempo de vida cero (zero Router Lifetime).

6. ***El "buen" encaminador se vuelve "malo":***

- Un router en el que previamente se confiaba queda comprometido.
- Se aplica el caso de "Encaminador de último salto malicioso".
- Este es un ataque de redirección/DoS.

7. ***Mensaje Redirect Falso:***

- El atacante usa la dirección en enlace-local del encaminador de primer salto actual para enviar un mensaje Redirect a un host legítimo.
- Debido a que el host identifica el mensaje como proveniente del encaminador por la dirección de enlace-local, acepta el Redirect.

- Siempre que el atacante responda a los mensajes NUD a la dirección de capa de enlace, el efecto de la redirección seguirá vigente.
- Este es un ataque de redirección/DoS.

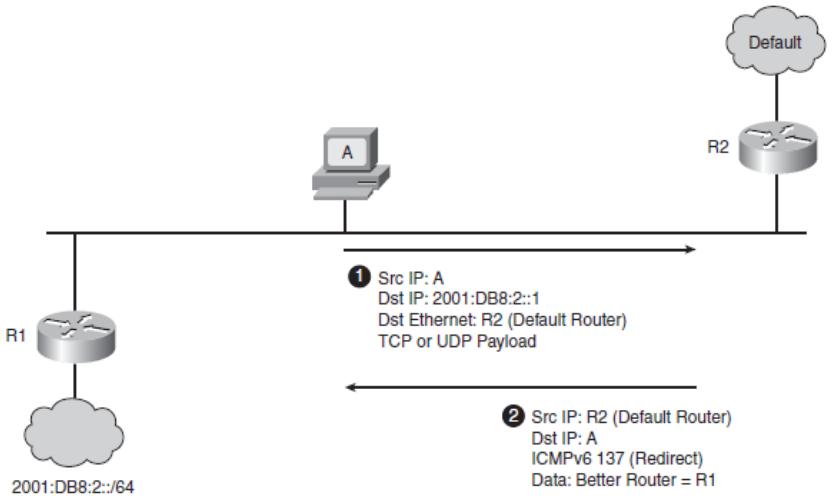


Ilustración 71. Redirigiendo trafico con Redirect ICMPv6

La redirección se muestra en la ***Ilustración 71*** y se basa en ICMPv6 tipo 137. En este ejemplo, el host A tiene una ruta por defecto del router a través de R2 y no es consciente de que router R1 tiene una ruta mejor y más específica para 2001:DB8:2::/64. Por lo tanto, cuando el host A quiere enviar un paquete a 2001:DB8:2::1, lo envía a la dirección MAC del router por defecto, que es R2. Cuando R2 recibe el paquete y, mediante la verificación de su propia base de la transmisión de información, detecta que R1 tiene una ruta mejor, R2 envía inmediatamente un redirect ICMPv6 al host A con la información que R1 tiene una mejor ruta a la red 2001: DB8:2::/64. El host A se instala esta ruta más específica en su tabla de enrutamiento y comienza a enviar todos los paquetes con un prefijo de destino de 2001:DB8:2::/64 para el router R1, consiguiendo una ruta más corta hacia el destino.

8. Prefijo falso en el enlace:

- Un nodo atacante puede enviar un RA especificando que un prefijo de longitud arbitraria pertenece al enlace.

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

9. Prefijo falso para configuración de dirección:

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

Debido a que no hay ningún mecanismo de autenticación integrado en SLAAC, un usuario malintencionado puede enviar mensajes de rogue RA y pretender ser el router por defecto. Este usuario malicioso inyecta información falsa en la tabla de enrutamiento de todos los demás nodos. Todos los demás nodos IPv6 en la subred envian sus paquetes que salen de la subred al host malicioso.

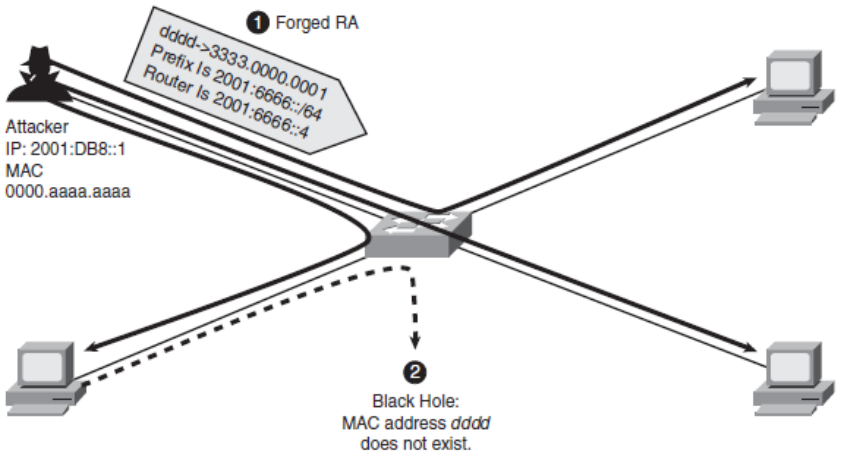


Ilustración 72. Router Advertisement que conduce a una denegacion de servicio

En lugar de simplemente capturar el tráfico, el atacante también podría descartar todos los paquetes, como lo muestra en la ***Ilustración 72***. Se trata de una denegación de servicio (DoS), ya que todos los paquetes enviados por los nodos IPv6 adyacentes se envían a la dirección MAC anunciado en el RA (en la ***Ilustración 72***, 0000.dddd.dddd), que no existe en la red local, por lo que todos los paquetes terminan en un agujero negro.

10. Parámetros falseados:

- Un nodo atacante puede enviar RAs con significado válido que dupliquen los RAs enviados por el encaminador por defecto válido, excepto en que los parámetros incluidos están pensados para interrumpir el tráfico legítimo.
- Algunos ataques específicos:
    - Incluir un "Current Hop Limit" de uno u otro número pequeño que el atacante sepa causará que los paquetes legítimos se descartarán antes de llegar a su destino.
    - El atacante implementa un servidor o "relay" DHCPv6 falso y los flags "M" y/o "O" están activados, indicando que la configuración "statefull" de direcciones y/o parámetros de realizarse. El atacante puede

responder a las peticiones de configuración "statefull" de un host legítimo con sus respuestas falsas.

- Este es un ataque DoS.

11. Ataques de Reactuación (Relay):

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

12. Ataques DoS a Neighbor Discovery:

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

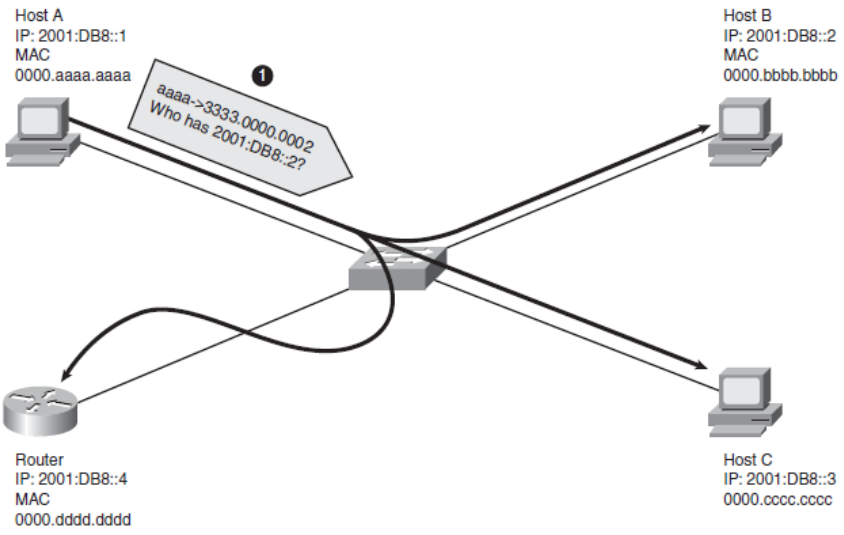


Ilustración 73. Neighbor Discovery: Solicitation

IPv6 no se basa en ARP, sino en el PND, que se ejecuta en la parte superior de ICMPv6. NDP esencialemente mantiene el mecanismo de ARP:

1. Un mensaje Neighbor Solicitation IPv6 multicast, utilizando ICMPv6 tipo 135, se envía a todos los nodos de la red de capa 2. La carga útil ICMPv6 contiene la dirección de destino IPv6, lo que es la dirección de B. Ver la ***Ilustración 73***.
2. Las respuestas pares correspondientes con los mensajes Neighbor Advertisement (NA), utilizando ICMPv6 tipo 136, conteniendo la dirección MAC en la carga de ICMPv6.Ver la ***Ilustración 74***.

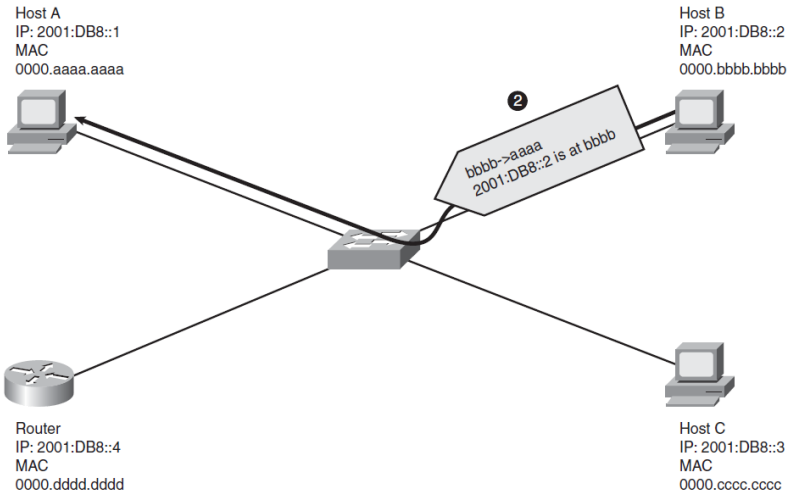


Ilustración 74. Neighbor Discovery: Advertisement

5.5. Comparativa IPv4 vs. IPv6

Visión general

Seguridad: incluye diversos procedimientos, mecanismo, prácticas recomendadas y herramientas.

Con ***IPv6*** hay muchos puntos que serán los mismos que con IPv4, por ejemplo, son "independientes de IP". Ejemplo, actualizaciones de firmware y software o riesgos de seguridad a nivel de aplicación.

IPv6 introduce nuevos temas a tener en cuenta. Veremos que estos puntos pueden significar una ventaja o desventaja desde el punto de vista de la seguridad.

Seguridad IPv6: Primer contacto

Las dos primeras ideas que vienen a la mente de un responsable de seguridad que despliega IPv6 son:

- Se utilizan direcciones globales (existe la excepción de las ULAs), por ejemplo, son alcanzables desde cualquier sitio de Internet, en otras palabras, ***no hay NAT***.
- Todas las pilas IPv6 deben soportar IPsec, como se ha visto.

La primera puede dar la falsa impresión de peligro y la segunda la falsa impresión de protección.

Clasificación de las Amenazas de Seguridad

Se establecen tres categorías para las amenazas de seguridad en IPv6:

1. ***Amenazas que ya existían con IPv4 y que tienen un comportamiento similar con IPv6.***
    - *Sniffing*: IPsec puede ayudar.
    - *Ataque a Nivel de Aplicación:* IPsec puede usarse para perseguir al atacante, aunque introduce problema con los ID. También puede usarse protección en el nivel de aplicación.
    - *Dispositivos no autorizados*: se hacen pasar por conmutadores, encaminadores, puntos de acceso o recursos como servidores DNS, DHCP o AAA.
    - *Ataques de "Hombre-en-el-medio"*: IPsec puede ayudar.
    - *Ataques por inundación*.
2. ***Amenazas que ya existían con IPv4 y que presentan novedades con IPv6.***
    - *Escaneo de red:* El escaneo de red típica (/64) en la práctica es más difícil. También los ataques automatizados, por ejemplo gusanos que seleccionan direcciones aleatorias para propagarse, se ven dificultados.
    - *Ataques de Amplificación Broadcast (Smurf)*: Ataques DoS. Un mensaje echo ICMP se envía a la dirección de broadcast de un prefijo de red con la dirección de origen falseada a la del host víctima. Todos los nodos del prefijo destino envían un echo reply a la víctima. En IPv6, no existe el concepto de broadcast.
    - *Ataques relaciones con Mecanismos de Transición*: No se utilizan nuevas tecnologías, el mismo tipo de vulnerabilidades que con IPv4:

- Redes doble-pila pueden ser atacadas usando ambos protocolos.
- Los túneles IPv6 necesitan nuevos puertos abiertos en los firewalls.

Recomendaciones:

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

3. Nuevas amenazas que aparecen con IPv6.

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

5.6. Aspectos de seguridad con IPv6

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

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

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

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

   Diversos escenarios:

   - *Usuarios DSL*: El tráfico debe alcanzar el CPE sin interferencias. El usuario tiene la responsabilidad de filtrar en el CPE.
   - *Centros de Datos*: Entornos controlando donde solo los servicios permitidos deben desplegarse.

3. El *esquema de direccionamiento* implica:

   - El número de direcciones es realmente grande. No tiene sentido el escaneo aleatorio o por fuerza bruta (RFC 5157[74]).
   - Cada nodo puede tener varias direcciones e incluso identificadores de interfaz aleatorios (RFC 4941[75]). Esto dificulta el control sobre un host por medio de su IP.
   - El uso de direcciones de enlace-local en una interfaz IPv6, proporciona conectividad IP en un segmento de LAN sin ayuda externa. Como guía, no debe confiarse en sesiones que vengan de direcciones de enlace-local y permitirlas solo para servicios básicos.
   - Se han definido direcciones multicast bien conocidas para facilitar la localización de servicios. Esto también facilita la localización de servicios para atacarlos (FF05::2 All routers, FF05::1:3 All DHCP Servers).

4. *Cabeceras de Extensión (EH)*: este potente y flexible mecanismo debe tenerse en cuenta por los dispositivos de seguridad, es decir, deben ser capaces de inspeccionar la "cadena" de cabeceras.

[74] RFC 5157: "IPv6 Implications for Network Scanning".

[75] RFC 4941: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

5. *Fragmentación*: En IPv6 solo los host finales pueden fragmentar paquetes. Esto reduce los ataques posibles utilizando solapamiento de fragmentos o fragmentos muy pequeños. Las consideraciones para fragmentos desordenados son las mismas que en IPv4 pero en los nodos finales. Los firewalls no deben filtrar fragmentos de paquetes.

6. *Autoconfiguración*: En IPv6 se definen distintos medios para la autoconfiguración. DHCP tiene las mismas consideraciones en IPv4 e IPv6. Neighbor Discovery Protocol tiene varias amenazas (como ARP en IPv4), e IPsec y SEND se pueden usar para añadir seguridad.

7. *Movilidad IPv6*: IPv6 facilita el despliegue de Movilidad IP aunque algunos elementos necesarios para un despliegue "en el mundo real" están siendo definidos, incluyendo temas de seguridad.

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

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

   La gravedad de esta amenaza se consideró suficiente para prohibir el uso de RH0 (RFC 5095[76]).

   Solo afecta a la cabecera de extensión Routing Type 0, de manera que las especificaciones para la Type 2 siguen siendo válidas, usada en MIPv6.

[76] RFC 5095: "Deprecation of Type 0 Routing Headers in IPv6".

5.7. Temas prácticos

- ICMPv6 es una parte fundamental de IPv6. Con IPv4 un filtrado de tipo "deny_all_ICMP" podría usarse, pero con IPv6 significaría que funcionalidades básicas dejasen de funcionar.
- Dependiendo del nivel de control y seguimiento que se requiera se deben usar distintos métodos de configuración de direcciones. De más o menos:
  - Direcciones estáticas.
  - Autoconfiguración "statefull": DHCPv6.
  - Autoconfiguración "stateless": Identificador de interfaz a partir de la dirección MAC.
  - Autoconfiguración "stateless": Identificador de interfaz utilizando las extensiones de privacidad.
- Se recomienda filtrar los prefijos no asignados. También el tráfico ULA no debe atravesar Internet. Si se despliega Multicast estos prefijos deben permitirse. IANA es la encargada de asignar los prefijos de direcciones:
  - Espacio de direcciones IPv6[77].
  - Asignaciones globales unicast IPv6[78].
- El filtrado puede ser "grueso" (permitir 2000::/3 Global Unicast) o fino (2600:0000::/12, 2400:0000::/12, etc).
- Utilizar direcciones difíciles de adivinar, por ejemplo no usar ::1 para encaminadores o servidores, para dificultar el trabajo del atacante.

[77] http://www.iana.org/assignments/ipv6-addresss-space

[78] http://www.iana.org/assignments/ipv6-unicast-address-assignments

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

- Desplegar Ingress Filtering (RFC 2827[79], RFC 3074[80]) de una manera similar a como se hace para IPv4.
- Si se utilizan Mecanismos de Transición, asegurarse de que el prefijo correspondiente se anuncia y que su tráfico no se filtra.

5.8. Firewalling

Introducción

Basado en todo lo anterior se darán algunas reglas para ser usadas en los firewalls.

Durante algún tiempo IPv4 e Ipv6 coexistirán, así que el escenario más probable será que las redes IPv6 sigan el diseño de las redes IPv4, compartiendo dispositivos de seguridad siempre que sea posible.

Consejos

- Ser cuidadoso con el filtrado de ICMPv6 (ver RFC 4890[81]).
- Desplegar Ingress filtering (igual que debe hacerse con IPv4).
- Las reglas IPv4 e IPv6 coexistirán, hacerlas coherentes (no permitir todo con IPv6/nada con IPv4).
- Asegurarse de que el firewall soporta:
  - Filtrado por dirección origen y destino.

[79] RFC 2827: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing".

[80] RFC 3074: "DHC Load Balancing Algorithm".

[81] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

- Procesado de cabeceras de extensión IPv6 (incluida RH0).
- Filtrado por información de protocolo de capa superior.
- Inspección de tráfico encapsulado.

- Considerar el filtrado en tres categorías: Plano de Datos, Plano de Gestión y Plano de Control de Encaminamiento.

5.9. Modelo de seguridad Distribuida

Visión general

En IPv4 la práctica común es utilizar el modelo perimetral, al desplegar seguridad en una red. Este modelo se basa en aislar redes por medio de dispositivos de seguridad a través de los cuales todo el tráfico debe pasar.

Hoy en día cada vez más herramientas de seguridad se están "moviendo" de la red a los host: firewalls, anti-virus, anti-spam, anti-malware, etc.

Esto conduce al modelo de seguridad distribuida o de host en el que la política de seguridad se impone en el host. Esto encaja a la perfección con el modelo extremo-a-extremo que IPv6 ha vuelto a traer.

También deben tenerse en cuenta los "nuevos" dispositivos IP que usarán las redes IP para conectarse: PDAs, portátiles, domótica, teléfonos móviles, etc. Necesitarán estar protegidos en todas partes.

Consideraciones del despliegue

El caso más común es añadir IPv6 a una red IPv4 existente, resultando una red de doble-pila.

De esta forma nos encontramos con el mismo modelo de seguridad perimetral y dispositivos de seguridad para ser usados en la seguridad IPv6. Esto puede tener algunas ventajas para el personal a cargo y desventajas en caso de falta de soporte IPv6.

Se espera que en el futuro (próximo) esto cambie debido al despliegue de redes solo IPv6.

Modelo se Seguridad Perimetral

La seguridad de un host depende del punto de la red donde se conecte.

Supuestos principales:

- Amenazas vienen de “fuera”.
- Los nodos protegidos no irán “fuera”.
- No hay puertas traseras (ADSL, WLAN, etc.)

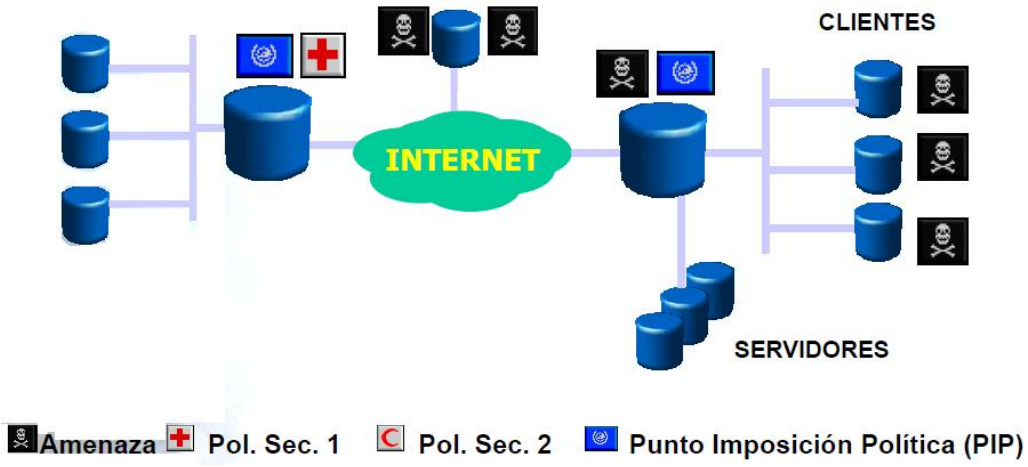


Ilustración 75. Modelo de seguridad perimetral

Desventajas principales:

- Modelo dependiente del Firewall.
- No cubre amenazas provenientes de “dentro”.
- Firewalls normalmente actúan como NAT/Proxy.
- Se necesitan soluciones especiales para comunicaciones seguras en modo transporte.

Modelo Seguridad Distribuida

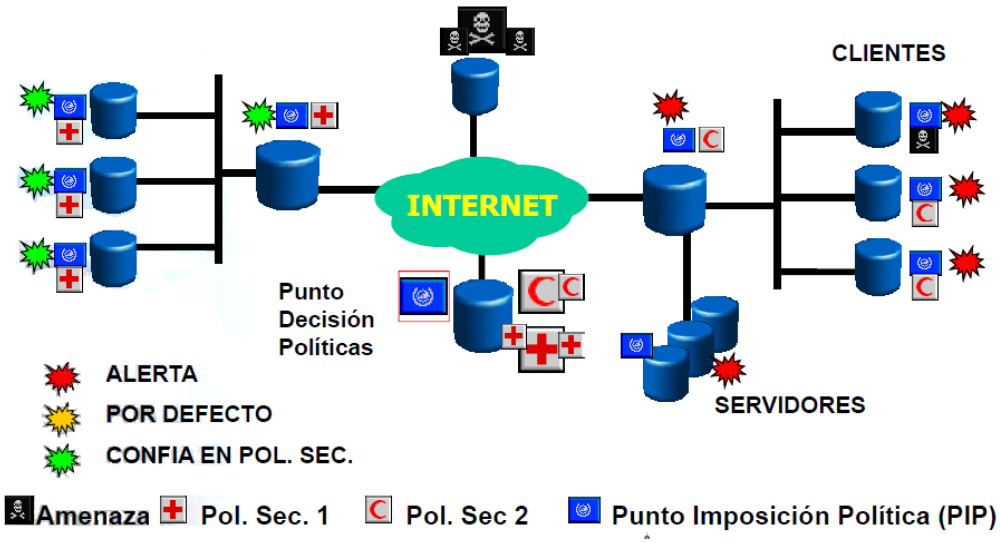


Ilustración 76. Modelo de seguridad distribuida

Idea básica: La política de seguridad se define centralmente y se distribuye a los RIPs. Las entidades de red autentifican para que confíen en ellas.

Tres elementos:

- Lenguaje de Especificación de Políticas.
- Protocolo de Intercambio de Políticas.
- Autentificación de Entidades.

Supuestos principales:

- Las amenazas vienen de cualquier parte en la red.
- Cada host puede ser identificado de forma unívoca y segura.
- La seguridad se puede aplicar en una o más de las siguientes capas: red, transporte y aplicación.

Desventajas principales:

- Complejidad.

- Identificación unívoca y segura de hosts no es algo trivial.
- La actualización de políticas debe llevarse a cabo de una manera eficiente y debe asegurarse que los hosts siguen las políticas.
- Un host "comprometido" sigue siendo un problema.
- Es dependiente del Punto de Decisión de Políticas: hay que añadir más complejidad para afrontar esto.

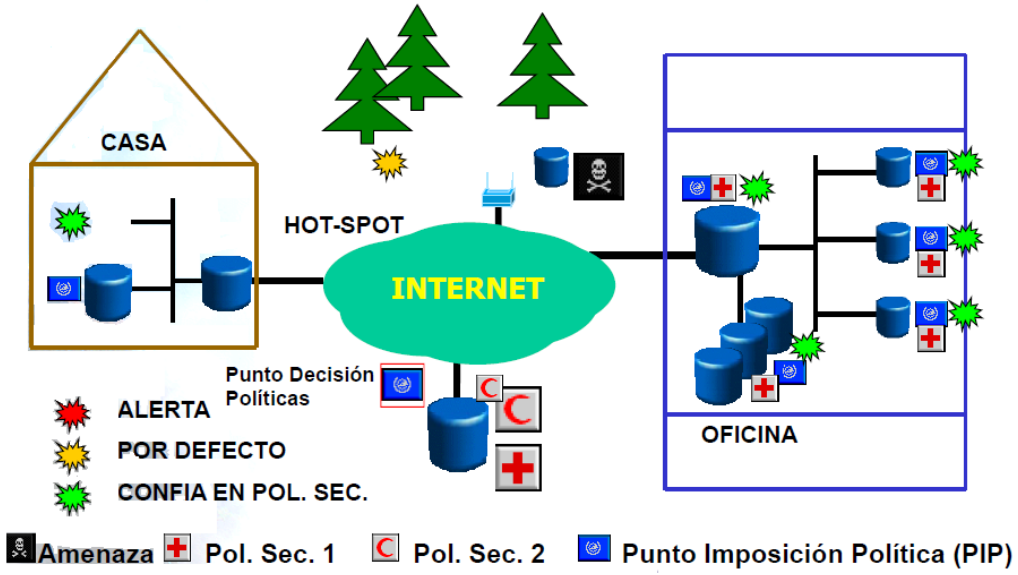


Ilustración 77. Modelo de seguridad distribuida

Ventajas principales:

- Flexibilidad en la definición de políticas de seguridad.
- Protege contra ataques internos.
- No depende de donde esté conectado el host.
- Sigue manteniendo un control centralizado.
- Habilita el modelo de comunicación extremo-a-extremo, tanto seguro como no.
- Se pueden tomar mejor decisiones basándose en información específica del host.
- Posibilita una mejor recopilación de información de auditoría.

- Puede controlar las comunicaciones de un host evitando comportamientos maliciosos en la red local o malas prácticas.
- Permite desarrollar soluciones de seguridad distribuidas y cooperativas.

Existe trabajo en curso que encaja con este modelo:

- Cisco NAC (Network Access Control): El host debe obtener acceso a la red cumpliendo con una política de seguridad.
- Microsoft NAP (Network Access Protection): crea políticas para validar la "salud" de un host antes de permitir acceso a la red, actualizar hosts conformes y opcionalmente confinar los host que no cumplan a una red restringida.
- Trusted Network Connect Work Group: Arquitectura abierta y un conjunto creciente de estándares para la integridad del nodo final.
- IWTF NSIS WG: Trabaja en la dirección de permitir al nodo final, previamente autentificado, a abrir puertos en los firewalls.
- IETF NEA WG: Revisa el estado de dispositivos finales para monitorizar el cumplimiento de la política de una organización y opcionalmente restringir el acceso hasta que en nodo final se haya actualizado para satisfacer los requisitos.
- IETF IDWG WG (OLD): Define formatos de datos y procedimientos para compartir información de interés a sistema de detección y respuesta de intrusiones, y para sistemas de gestión que pueden necesitar interactuar con ellos.

El mercado y los estándares parecen ir en la dirección de imponer la política de seguridad en el nodo final por medio del control de acceso a la red.

6. ENCAMINAMIENTO CON IPV6

6.1. Conceptos de encaminamiento

Visión General Encaminamiento

Los encaminadores deben saber cómo llegar al destino final de los paquetes que se le reenvían.

Las rutas estáticas no son adecuadas para redes medianas ni grandes. Tampoco para las pequeñas si se producen cambios en la topología de red.

Los protocolos de encaminamiento proporcionan un método automático de generar las tablas de encaminamiento. Tienen en cuenta cambio de la topología de red.

Tipos de protocolos de encaminamiento

Atendiendo al ámbito:

- IGP (Interior Border Gateway).
- EGP (Exterior Border Gateway).

En los de tipo IGP:

- Atendiendo a la metodología de propagación.
  - Vector Distancia.
  - Estado de Enlace.
- Atendiendo al tipo de rutas que propagan.
  - Classful.
  - Classless.

Criterios de selección IGP

La selección de uno u otro depende de varios factores[82]:

- Topología de la intrared.
- Tipos de rutas a propagar.
- Tiempo de convergencia.
- Criterio de cálculo de métricas de la ruta.
- Escalabilidad.
- Seguridad.

Encaminamiento IPv6

- Mismo mecanismo CIDR "longest-prefix match" que actualmente en IPv4.
- Cambios mínimos respecto de los protocolos existentes para encaminado en IPv4 (gestión de direcciones mayores).
  - Unicast: RIP, OSPF, IS-IS, BGP4+, …
  - Multicast: MOSPF[83], PIM, …
- Se puede utilizar la cabecera de routing con direcciones unicast para encaminar paquetes a través de regiones concretas.
  - Por ejemplo, para la selección de proveedores, políticas, prestaciones, etc.

El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de

[82] Guía Completa en: http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2003.htm

[83] **MOSPF** (Multicast Open Shortest Path First), es un protocol extensión para el OSPF, para apoyar el enrutamiento multicast, lo que permite a los routers compartar información sobre la pertenencia a grupos.

enrutamiento más utilizados. En la siguiente tabla se presentan las nuevas versiones desarrolladas para IPv6:

Tabla 4. Protocolos de enrutamiento en IPv6[84]

Protocolo de enrutamiento	Version IPv6
RIP	RIPng
EIGRP	EIGRP para IPv6
OSPF	OSPFv3
IS-IS	Integrated IS-IS
BG	BGP-MP

6.2. RIPng

RIP para IPv6 o RIPng está definido en el RFC2080[85]: RIPng for IPv6. Es similar a IPv4 (basado en RIPv2, vector distancia, 15 saltos máximo,…).

En la pila dual usando RIP, se necesita RIP (IPv4) y RIPng (IPv6). RIPng usa IPv6 para transporte.

Extiende RIPv1 y RIPv2 para proporcionar:

- Direcciones de 128 bits.
- Encaminamiento de prefijos IPv6.
- Uso de la dirección FF02::9, del grupo multicast all-RIP-routers, como la dirección destino de los mensajes de update de RIP.

6.3. EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) desarrollado por Cisco es una versión mejorada del IGRP[86].

[84] Fuente: Protocolos de enrutamiento en IPv6. www.6bone.net, pagina 25

[85] RFC 2080: “RIPng for IPv6”.

[86] **IGRP** (Interior Gateway Routing Protocol o Protocolo de enrutamiento de gateway interior), es un protocolo propietario patentado y desarrollado por CISCO que se emplea con el protocolo TCP/IP según el modelo (OSI) Internet.

EIGRP usa al igual que IGRP el algoritmo de vector de distancias e información de distancia, además de usar algunas características asociadas normalmente con los protocolos del estado de enlace.

Las propiedades de convergencia y la eficiencia operativa son mejores en EIGRP que en IGRP.

EIGRP para IPv4 se ejecuta sobre transporte IPv4, comunica solo peers IPv4 y anuncia solo rutas IPv4, mientras que EIGRP para IPv6 hace lo mismo pero para IPv6.

EIGRP para IPv4 y EIGRP para IPv6 se configuran y gestionan de manera separada, aunque la configuración es similar en ambos casos.

EIGRP para IPv6 esta soportado desde las versiones de IOS 12.4(6)T y 12.2(33)SRB.

6.4. OSPF

Visión General

OSPFv3 es igual a OSPF para IPv6. OSPFv3 esta basado en OSPFv2. Es un protocolo de encaminamiento IGP de tipo “link-state” que intenta dar solución a las necesidades más avanzadas de los Sistemas Autónomos más exigentes:

- Soporte VLSM[87] (Variable Length Subnet Masking).
- Autenticación.
- Rápida convergencia cuando se producen cambios en la topología de la red.
- Propagación de rutas por medio de multicast.
- Consideración del ancho de banda en la elección de la mejor ruta.

Se divide la red en varias áreas, todas conectadas al área de backbone, para una mejor escalabilidad.

OSPF utiliza el protocolo Hello para determinar:

[87] **VLSM** (Máscaras de subred de tamaño variable), son una de las tantas soluciones que se implementaron para el agotamiento de direcciones IP.

- Qué interfaces recibirán los LSAs.
- Qué otros encaminadores vecinos existen.
- Si los encaminadores vecinos siguen activos (keepalive).

Los encaminadores envían LSAs (Link-State Advertisements) a todos los encaminadores de la misma unidad jerárquica por medio de una dirección multicast e incluyen entre otros:

- Prefijo de red.
- Máscara de red.
- Tipo de red.
- Encaminadores conectados.
- Etc.

Todos construyen la misma base de datos topológica a partir de los LSAs recibidos. Se obtiene la nueva tabla de rutas a partir de la nueva topología.

OSPF IPv6

La versión 3 OSPF, para IPv6 (RFC2740[88]), extiende la versión 2 de OSPF (RFC2328[89]) para soportar el encaminamiento de prefijos IPv6 y las direcciones de 128 bits.

OSPFv3 es solo-IPv6, en un entorno doble-pila hará falta ejecutar dos instancias distintas para IPv4 (OSPFv2) e IPv6 (OSPFv3).

[88] RFC 2740: “OSPF for IPv6”

[89] RFC 2328: “OSPF Version 2”

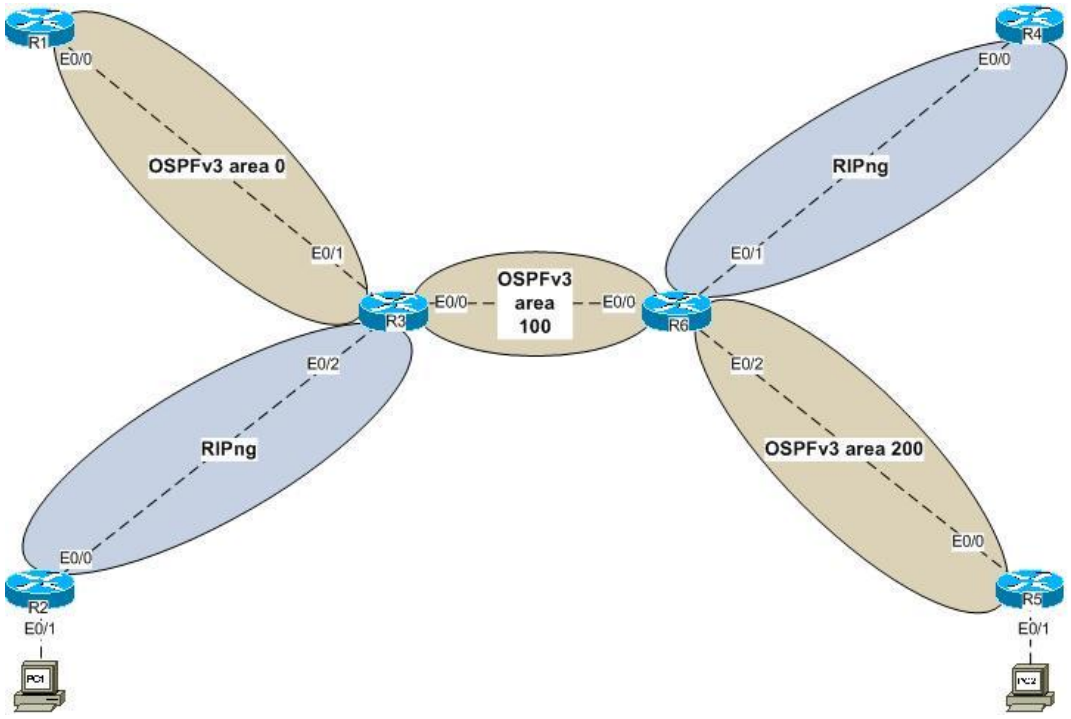


Ilustración 78. OSPFv3

En la ***Ilustración 78*** se pueden ver los protocolos de enrutamiento, donde, el Router1 esta corriendo OSPFv3 (area 0) con R3; R2 esta corriendo RIPng con R3; R3 esta corriendo OSPFv3 (area 100) con R6; R4 esta corriendo RIPng con R6; y R5 esta corriendo OSPFv3 (area 200) con R6.

Nuevas características:

- Se ejecuta directamente sobre IPv6.
- Se distribuyen prefijos IPv6.
- Nuevos tipos de LSA.
- Utiliza direcciones Multicast:
  - ALLSPFRouters (FF02::5).
  - ALLDRouters (FF02::6).

Puesto que en IPv6 una interfaz de red puede tener más de una dirección, los LSAs en OSPFv3 difieren de los de la versión para IPv4.

Tabla 5. LSAs en OSPFv3

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router. En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
2	Network LSA	Interface IP address of the DR En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
3	Interarea-prefix LSAs for ABRs	Destination network number. En IPv6 se expresa como prefijo, longitud de prefijo.
4	Interarea-router LSAs for ASBRs	Router ID of AS boundary router.
5	Autonomous system external LSAs	Redistributing routes from another AS. En IPv6 se expresa como prefijo, longitud de prefijo y la ruta por defecto, de longitud 0.
8	Link LSA	Local-link flooding scope. Informa de las direcciones link-local de todos los encaminadores del segmento de red
9	Intra-Area-Prefix LSA	Describes association to the router LSA.

6.5. IS-IS

Visión General IS-IS

IS-IS (Intermediate System–to–Intermediate System) es un protocolo de encaminamiento OSI. Diseñado para soportar el protocolo CLNP (Connectionless Network Protocol). CLNP es un protocolo de la capa de red similar a IP.

IS-IS se ha extendido para soportar también IPv4 e IPv6 (RFC5308[90]).

Características:

[90] RFC 5308: “Routing IPv6 with IS-IS”

- Encaminamiento jerárquico.
- Soporte “classless”.
- Uso de direcciones multicast.
- Autenticación mediante password.
- Soporte de múltiples métricas.
- Cálculo SPF local.

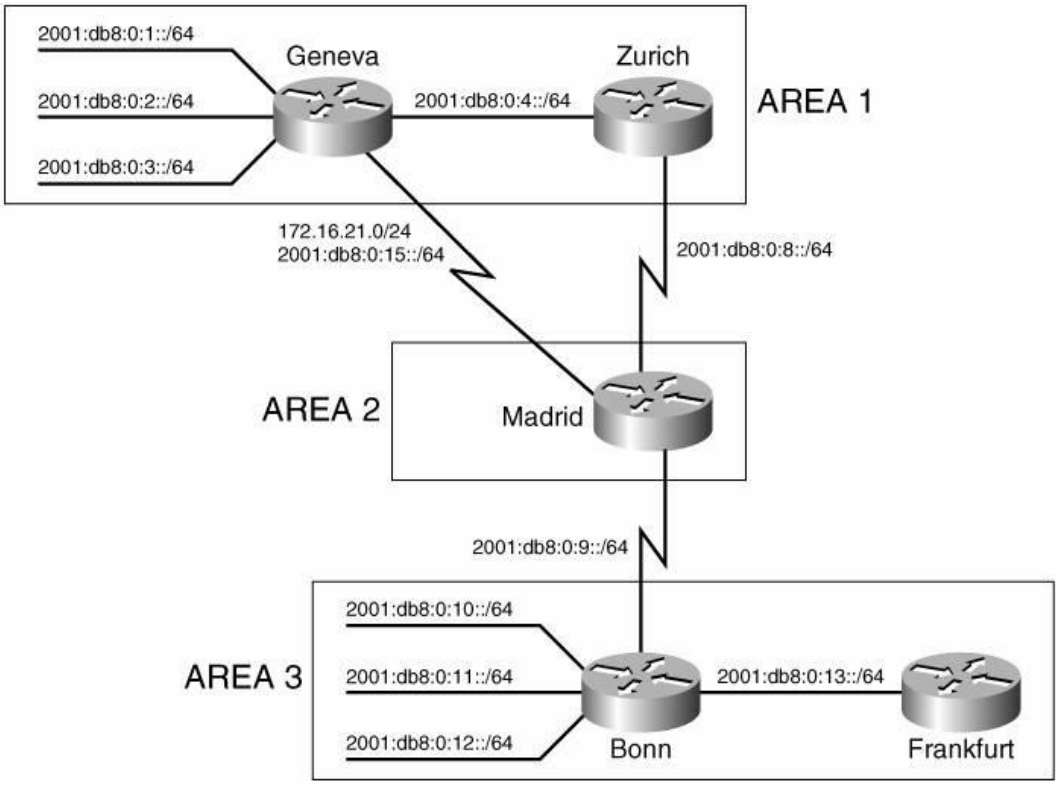


Ilustración 79. IS-IS para IPv6

IS-IS integrado calcula una sola SPF para crear una topología de IPv4 e IPv6 (y CLNS). Si los protocolos IPv4 e IPv6 son configurados en la red, todas las interfaces y todos los routers se deben configurar con ambos protocolos. En la ***Ilustración 79*** se muestra una red IS-IS con tres áreas. Para habilitar IS-IS para IPv6, se debe permitir el enrutamiento IPv6 a nivel global y luego habilitar IS-IS IPv6 en las interfaces de los routers.

Las direcciones IPv6 de la ***Ilustración 79*** de los routers Zurich, Geneva, y Bonn resumen las rutas a como ellas son anunciadas a los routers L2.

Se basa en dos niveles jerárquicos (backbone y stub). Se envían LSP (Link State Packets). La información se envía mediante TLVs (Tag / Lenght / Value).

Se definen dos nuevos TLVs para IPv6:

- Accesibilidad en IPv6.
- Dirección de la interfaz IPv6.

Se define un nuevo identificador de red para IPv6: IPv6 NLPID (Network Level Protocol ID).

6.6. BGP

Visión General de BGP

Border Gateway Protocol versión 4 (BGP4) es el protocolo de pasarela exterior (EGP) que se utiliza para intercambiar rutas entre sistemas autónomos en Internet. BGP fue diseñado con base en la experiencia adquirida con EGP, y ofrece soporte integrado para CIDR y agregación de ruta.

BGP conecta dominios de ruteo separados que tienen políticas de ruteo independientes (y ASNs).

BGP4 se especifica en el RFC 1771[91] y otros documentos relacionados con BGP: RFC 1772[92], RFC 1773[93] y RFC 1774[94].

El encaminamiento en Internet se hace a dos niveles:

[91] RFC 1771: "A Border Gateway Protocol 4 (BGP-4)".

[92] RFC 1772: "Application of the Border Gateway Protocol in the Internet".

[93] RFC 1773: "Experience with the BGP-4 Protocol".

[94] RFC 1774: "BGP-4 Protocol Analysis".

- Intra-AS → IGP:
  - La gestión de cada AS es local, lo cual incluye el tipo de protocolo de encaminamiento usado.
- Inter-AS → EGP:
  - Requiere una estandarización para que todos los ASs sean alcanzados por todos.
    - BGP estándar “de facto”.

En la ***Ilustración 80*** se puede apreciar las diferencias entre el enrutamiento Inter-AS e Intra-AS. Para mantener la nomenclatura, a los "router" entre ASs se les llama pasarelas. Todo el encaminamiento entre pasarelas se puede categorizar en intra-AS (o Interior) si las pasarelas pertenecen al mismo AS, o inter-AS(o Exterior) si pertenecen a distintos ASs.

El encaminamiento intra-AS usa un IGP ("Interior Gateway Protocol") y el inter-AS usa un EGP ("Exterior Gateway Protocol"). En lo que a políticas se refiere Inter-AS, el administrador controla como su tráfico es enrutado, asi como que rutas cruzan su red. En cambio Intra-AS, hay un único adminstrador, por tanto no es necesario tomar decisiones sobre políticas de enrutamiento. De forma escalar, el enrutamiento jerarquico ahorra tamaño en las tablas de enrutamiento y reduce el tráfico de actualización. A diferencia de Inter-AS, Intra-AS se centra en el rendimiento, en cambio en la primera las políticas pueden dominar sobre el desempeño.

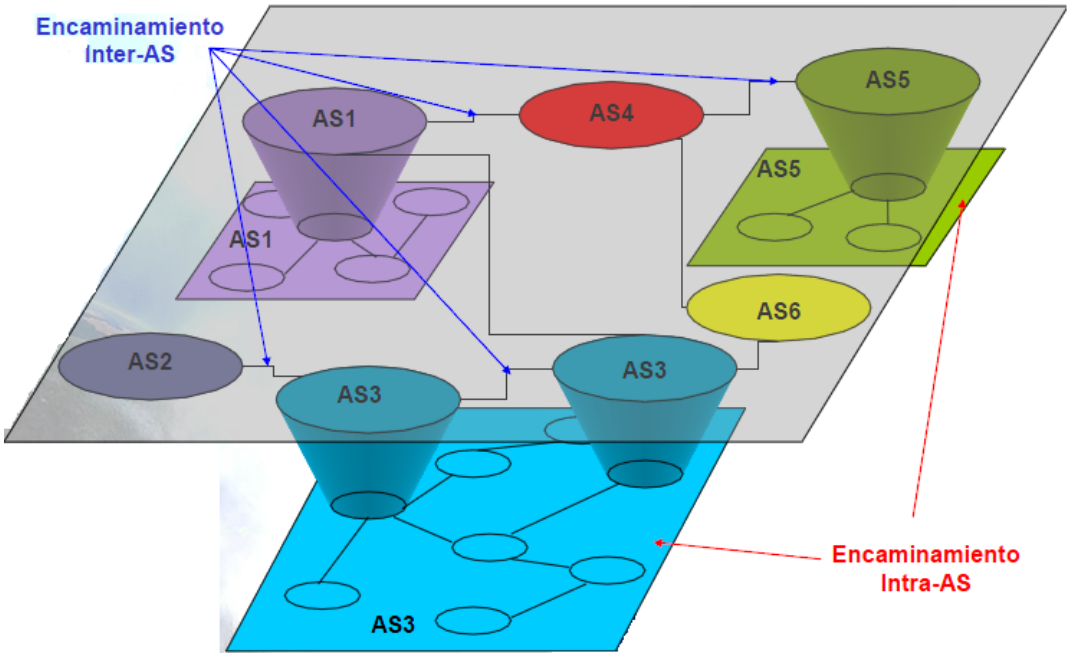


Ilustración 80. Visión general BGP

BGP "Border Gateway Protocol", estándar "de facto".

Se basa en el PVP (Path Vector Protocol):

- Similar al Distance Vector.
- Cada encaminador frontera envía a sus vecinos ("peerings") la ruta completa a un destino, no solo la distancia.
- El camino (path) es una secuencia de ASs hasta el destino.
    - Ejemplo: Path(X,Z)=X, Y1, Y2, Y3, Y5, Z

Se utiliza TCP para el intercambio de mensajes BGP:

- OPEN – abre una conexión TCP.
- UPDATE – anuncia o confirma un nuevo camino.
- KEEPALIVE – en ausencia de UPDATES sirve para mantener abierta la conexión TCP y como ACK de un mensaje OPEN.

- NOTIFICATION – informa de errores en mensajes precedentes y para cerrar conexiones.

BGP para IPv6 (BGP4+)

La versión actual de BGP es la versión 4, i.e. BGP4. BGP4 (BGP para IPv4) se describe en RFC4271.

Las Extensiones Multiprotocolo para BGP [RFC4760], i.e. BGP4+, permiten usar BGP4 con diferentes familias de direcciones (address family), tales como IPv6 y Multicast.

Las extensiones multiprotocolo para BGP para IPv6 soportan las mismas funcionalidades y características que BGP para IPv4. Las extensiones para IPv6 incluyen el soporte para:

- La familia de direcciones IPv6 (IPv6 address family) y la network layer reachability information (NLRI).
- El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6.

Las extensiones multiprotocolo para BGP para IPv6 Multicast soportan las mismas funcionalidades y características que BGP para IPv4 Multicast. Las extensiones para IPv6 Multicat incluyen el soporte para:

- La familia de direcciones IPv6 Multicast (IPv6 Multicast address family) y la network layer reachability information (NLRI).
- El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6 Multicast.

Características de BGP4+

Los únicos componentes de información de BGP que son específicos para IPv4 son los atributos:

- NEXT_HOP (expresado como una direcion IPv4).

- AGGREGATOR (contiene una direcion IPv4).
- NLRI (expresado como prefijos de direciones IPv4).

RFC4760[95] asume que cualquier router BGP (incluyendo los que soportan el mismo RFC4760) tiene una dirección IPv4 (la cual se usará, entre otras cosas en el atributo de AGGREGATOR).

Para proveer compatibilidad con versiones anteriores, así como para simplificar la introducción de las capacidades multiprotocolo en BGP4, el RFC4760 define dos nuevos atributos:

- Multiprotocol Reachable NLRI (MP_REACH_NLRI), contiene la información de los destinos alcanzables, asi como la información de next hop usada para hacer el reenvió (forwarding) hacia esos destinos.
- Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI), contiene la información de los destinos inalcanzables.

El atributo NEXT_HOP y NLRI es independiente del protocolo. Ambos atributos son opcionales y no-transitivos. Un router BGP que no soporta la extensiones multiprotocolo ignorara estos atributos y no la pasará a otros routers.

[95] RFC 4760: “Multiprotocol Extensions for BGP-4”

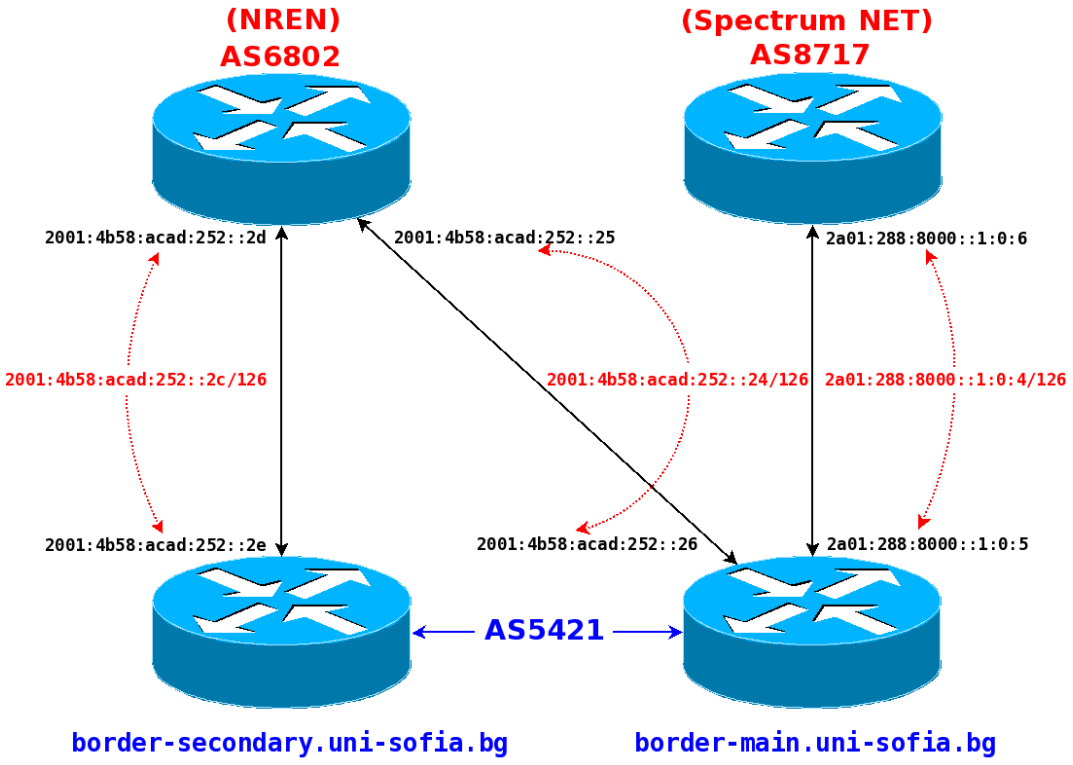


Ilustración 81. Establecimiento de sesión BGP4+ de tránsito de tráfico IPv6

En la ***Ilustración 81*** se muestra el establecimiento de sesión BGP4+ entre los routers de tránsito AS5421, AS6802 y AS8717. El tráfico de tránsito IPv6 desde y hacia los enrutadores de borde AS5421 se da tres sesiones BGP4+. Dos de estas sesiones es en el router de borde AS6802 (NREN) y la otra sesión se da en el router de borde AS8717 (Spectrum NET). El enrutador de borde border-secondary.uni-sofia.bg solo establece una sesión BGP4+ con el router de borde AS6802, mientras que border-main-uni-sofia.bg ha establecido dos sesiones BGP4+: uno con el router de borde AS6802 y la otra con el router AS8717.

MPLS 6PE

- Permite implementar IPv6 sin tocar el CORE.
- Solo se configuran los PE.

- Se pueden elegir los PE en los que se habilitará.
- Los PE serán dual stack y no perderán funcionalidad IPv6.
- No tiene problemas de performance o escalabilidad.
- Requiere tener MPLS en el backbone.

6PE en Cisco (Plano de Control)

Por cada prefijo 6PE recibido se realizan los siguientes pasos para determinar el next hop:

- Cada prefijo se envia por BGP usando "IPv6+etiqueta". La etiqueta será la nueva entrada creada en CEF al recibir los bloques.

6PE Packet forwarding

1. Forwarding IPv6 Normal (cuando tiene IPv6 Nativo para el destino).
2. Cuando recibe un paquete IPv6, busca el IP destino en el FIB[96] para saber que etiquetas colocar. Coloca primero la correspondiente al bloque IPv6 aprendido y luego la del LSP IPv4 para llegar al router 6PE de salida.
3. Se envía el paquete hasta el destino usando MPLS común (top label swaping).
4. En el 6PE de salida, la etiqueta del bloque IPv6 informa al router 6PE que debe buscar el destino en la table FIB IPv6.

6.7. Encaminamiento estático

Configuración de Rutas Estáticas

La forma de configurar rutas estáticas es similar a IPv4:

[96] **FIB** (Forward Information Base), es la tabla de encaminamiento que se consulta para hacer el reenvio de los paquetes generados por los usuarios (los PDU representan estos paquetes).

- Default Gateway
- Delegación de prefijos

7. MECANISMOS DE TRANSICIÓN

7.1. Conceptos de transición

Técnicas de Transición / Coexistencia

IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4. Sin embargo, pasar de IPv4 a IPv6 no es sencillo y los mecanismos que permiten la coexistencia y la transición entre las dos versiones han de estar estandarizados.

La migración al nuevo IP en tan corto período de tiempo requeriría la redefinición de un plan de direccionamiento IPv6 mundial, la instalación del protocolo en cada router y host, y la modificación de las aplicaciones actuales para que puedan soportarlo.

Un proceso caro, sin duda, y que podría causar interrupciones del servicio inaceptables.

Es por ello, que se han identificado e implementado un amplio abanico de técnicas, agrupadas básicamente dentro de tres categorías:

1) Doble-pila, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.
2) Técnicas de túneles, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más común.
3) Técnicas de traducción, para permitir la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4. Debe ser la última opción ya que tiene problemas.

Ilustración 82. Estrategias de transición a IPv6

Todos estos mecanismos suelen ser utilizados, incluso en combinación.

7.2. Doble pila

El método de doble pila es un método de integración en el que un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Es la opción recomendada y requiere que se ejecuten IPv4 e IPv6 simultáneamente. El router y los switches se configuran para admitir ambos protocolos; el protocolo preferido es IPv6.

Puesto que se debe soportar los dos protocolos en los enlaces y nodos seleccionados, se requiere soporte en:

- Host
- Routers
- Aplicaciones y servidores (por ejemplo, WEB, DNS, SMPT)

Cada nodo tiene dos pilas de protocolos con la configuración en la misma interfaz o en varias interfaces.

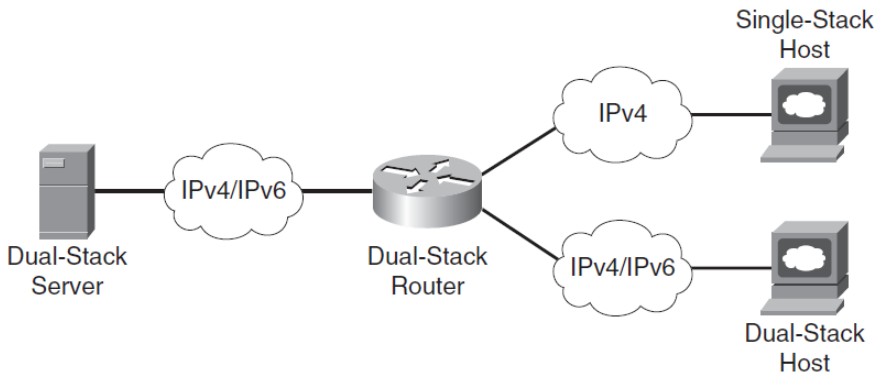


Ilustración 83. Topologia IPv6 de doble pila

La ***Ilustración 83*** muestra el modelo de doble pila. Los nodos y los dispositivos de red en en el modelo entienden y corren IPv4 e IPv6 de manera independiente.

Es la misma aproximación multi-protocolo que ha sido utilizada anteriormente y por tanto es bien conocida (AppleTalk, IPX, etc.)

Actualmente, IPv6 está incluido en todos los Sistemas Operativos modernos, lo que evita costes adicionales.

Las aplicaciones (o librerías) escogen la versión de IP a utilizar:

- En función de la respuesta DNS:
  - Si el destino tiene un registro AAAA, utilizan IPv6, en caso contrario IPv4.
- La respuesta depende del paquete que inició la transferencia.

Esto permite la coexistencia indefinida de IPv4 e IPv6, y la actualización gradual a IPv6, aplicación por aplicación.

En la ***Ilustración 84*** se muestra, el mecanimo que como su nombre lo sugiere, refiere al uso de dos pilas, de diferente protocolo, que trabajan paralelamente y permiten al dispositivo trabajar vía ambos protocolos. En el esquema de pila-dual (RFC 2893[97]) el nodo instala pilas IPv4 e IPv6 en paralelo (ver ***Ilustración 84***) y se conoce como nodos IPv4/IPv6.

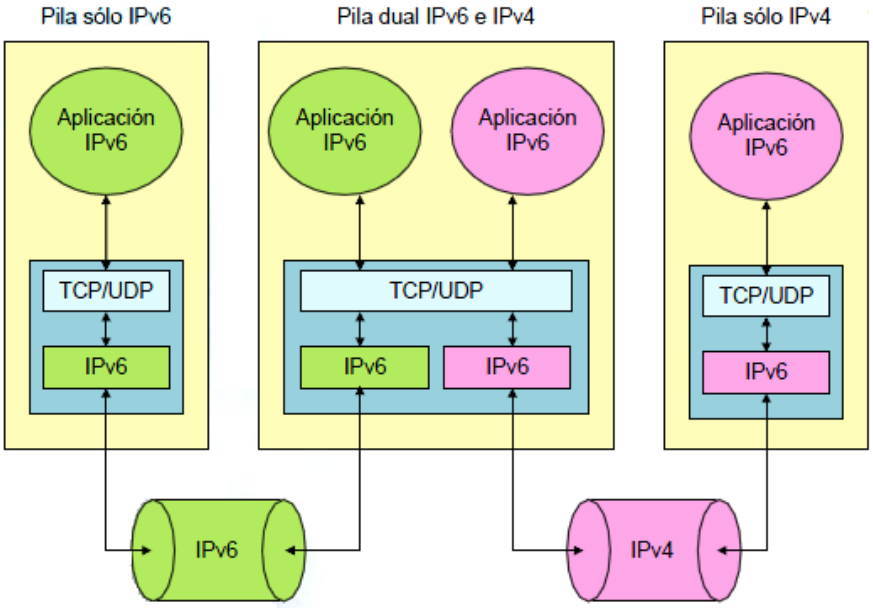


Ilustración 84. Mecanismo basado en doble pila

Los nodos tienen implementadas las pilas IPv4 e IPv6.

Comunicaciones con nodos solo IPv6 → Pila IPv6, asumiendo soporte IPv6 en la red.

[97] RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers

Comunicaciones con nodos solo IPv4 → Pila IPv4.

7.3. Túneles

Túneles para atravesar Routers que no Reenvían IPv6

Encapsulamos paquetes IPv6 en paquetes IPv4 para proporcionar conectividad IPv6 en redes que solo tiene soporte IPv4.

Muchos métodos para establecer dichos túneles:

Manuales:

- Configuración manual → 6in4.
- "tunnel brokers" (tipicamente con interfaces web) → 6in4.
- Site-a-site

Automáticos:

- "6-over-4" (intra-domain, usando IPv4 multicast como LAN virtual).
- "6-to-4" (inter-domain, usando la dirección IPv4 como el prefijo del sitio IPv6).

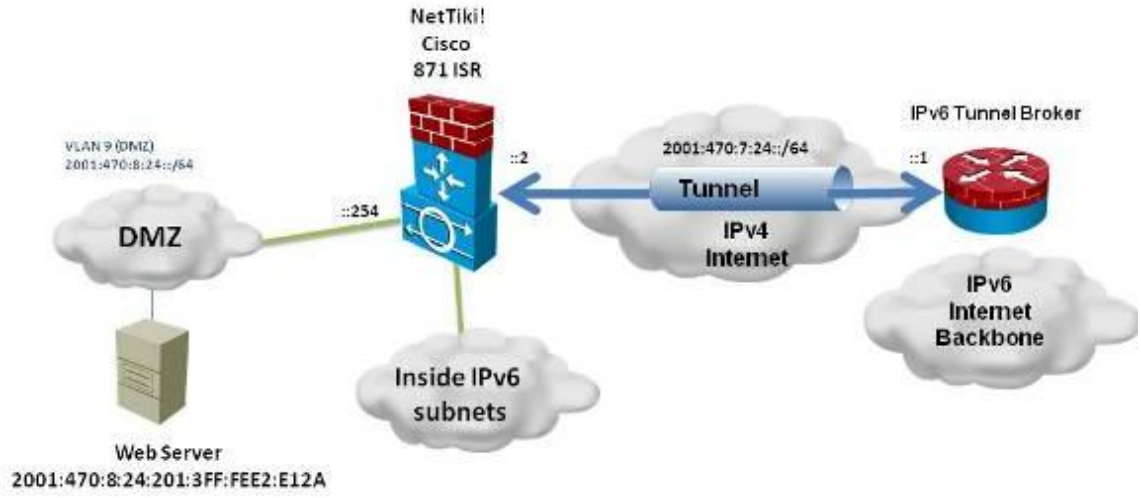


Ilustración 85. Túneles para atravesar routers

El RFC 2473[98] define el IPv6 Tunneling, como una técnica para establecer "enlaces virtuales" entre dos nodos IPv6 (ver ***Ilustración 85***). Desde el punto de vista de los nodos, este "enlace virtual" es lo que se conoce como túneles IPv6 y que actúan como un enlace punto a punto.

Los nodos mostrados en la ***Ilustración 85***, juegan un papel específico. Uno de ellos se dedica a encapsular los paquetes recibidos de otros nodos y los reenvia por el túnel. El otro nodo desencapsula el paquete que llega del túnel y reenvía el paquete original recién desencapsulado a su destino final. El nodo encapsulador es llamado nodo de entrada o entrada del túnel, mientras que el nodo desencapsulador, es llamado nodo de salida o destino del túnel.

Puede ser visto como:

- IPv6 utilizando IPv4 como capa de enlace virtual link-layer, o
- Una VPN IPv6 sobre la Internet IPv4.

Túneles IPv6 en IPv4 (6in4)

Usados para proporcionar conectividad IPv6 en redes que solo tiene soporte IPv4.

Se encapsulan paquetes IPv6 dentro de paquetes IPv4.

Los paquetes resultantes viajan por redes IPv4.

Este mecanimo esta definido en el RFC 2529[99]. Utiliza direcciones IPv4 empotradas en direcciones de capa de enlace IPv6 (ver ***Ilustración 87***). 6in4 realiza el tunneling dentro de una sola organización o sitio (se comporta efectivamente como una LAN virtual), esto lo logra tratando a una red como una funcional subred IPv6 y permitiendo la auto-configuración de direcciones. Desafortunadamente 6in4 requiere que la infraestructura IPv4 soporte ruteo multicast. De modo que la mayoría de la redes IPv4 no soportan este tipo de ruteo 6in4 no ha sido del todo desarrollado.

[98] RFC 2473: Generic Packet Tunneling in IPv6 Specification.

[99] RFC 2529: Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.

Un punto positivo acerca de este mecanismo es que conserva todas las características que ofrece IPv6, incluyendo la seguridad punto-a-punto y configuración estática.

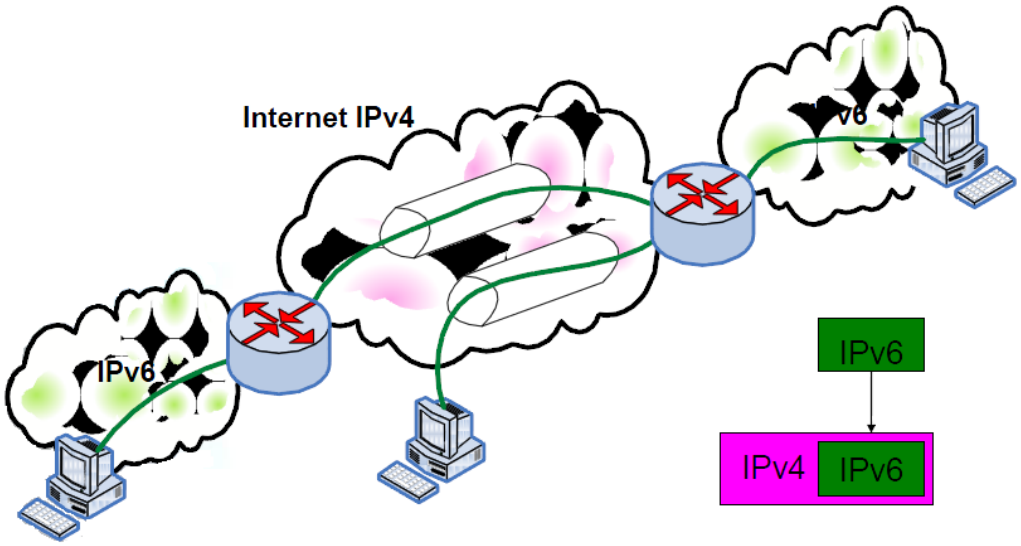


Ilustración 86. Mecanismo basado en Túneles 6in4

Existen diversas formas de encapsular los paquetes IPv6:

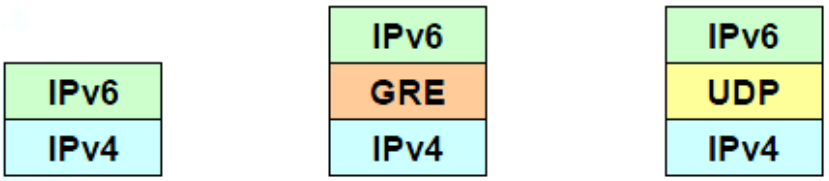


Ilustración 87. Diversas formas de encapsular paquetes IPv6

Lo mismo se aplica para IPv4 usado en redes solo IPv6.

Existen diversos mecanismos de transición basados en túneles, cada uno con una forma diferente de encapsulación. Algunos mecanismos de transición basados en túneles:

- 6in4 (*) [6in4]
- 6to4 (*) [6to4]
- TB (*) [TB]
- Teredo (*) [TEREDO], [TEREDOC]
- TSP [TSP]
- Túneles automáticos [TunAut]

- ISATAP [ISATAP]
- Silkroad [SILKROAD]
- 6over4 [6over4]
- DSTM [DSTM]
- –AYIYA [AYIYA]
- –Softwires (*) [SOFTWIRES]

(*) Más habituales y explicados en detalle a continuación

Detalles Túneles 6in4 (RFC 4213[100])

Encapsula directamente el paquete IPv6 dentro de un paquete IPv4.

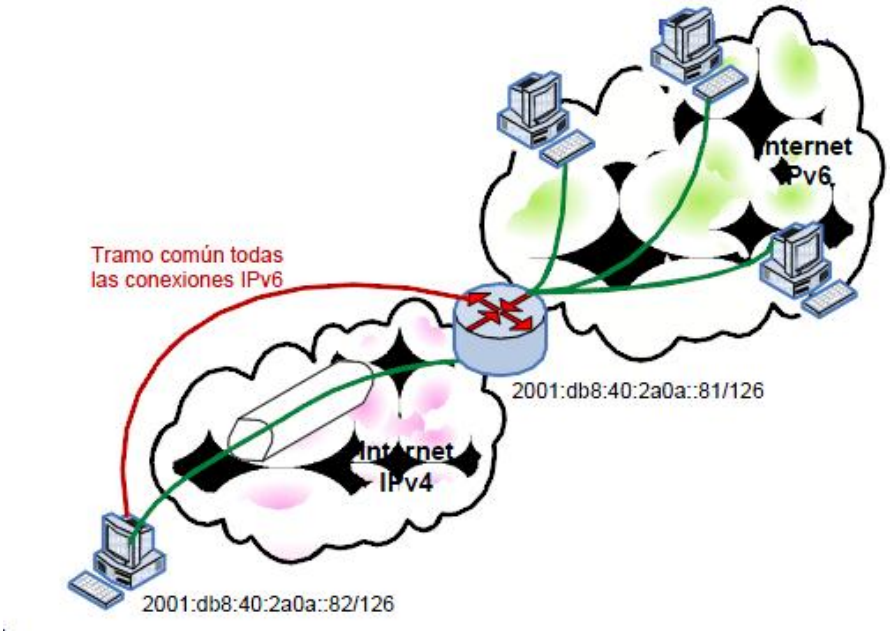


Ilustración 88. Detalle túneles 6in4

Se suele hacer entre:

- nodo final → router.
- router → router.

Aunque también es posible para: nodo final → nodo final.

[100] RFC 4313: Basic Transition Mechanisms for IPv6 Hosts and Routers

El túnel se considera como un enlace punto-a-punto desde el punto de vista de IPv6. Solo un salto IPv6 aunque existan varios IPv4.

Las direcciones IPv6 de ambos extremos del túnel son del mismo prefijo.

Todas las conexiones IPv6 del nodo final siempre pasan por el router que está en el extremo final del túnel.

Los túneles 6in4 pueden construirse desde nodo finales situados detrás de NAT. La implementación de NAT debe soportar "proto-41 forwarding" [PROTO41] para permitir que los paquetes IPv6 encapsulados atraviesen el NAT.

7.4. Tunnel Broker

Tunnel Broker (RFC 3053[101])

El tunnel broker, como se describe en el RFC 3053 "IPv6 Tunnel Broker", es un enfoque alternativo y utiliza los servidores dedicados para simplificar la creación de túneles, estos servidores se llaman proveedores de túneles. El túnel bróker es responsable de la gestión de las solicitudes del túnel procedentes de los extremos. Este método se ajusta a los escenarios con sitios pequeños, aislados o hosts IPv6.

La principal limitación del servicio de tunnel broker es que el router o el servicio de tunnel broker tiene que aceptar un cambio de configuración de un servidor remoto, lo que podría tener serias implicaciones de seguridad. Por ejemplo, una empresa puede registrar la dirección IPv4 del router con el proveedor de servicios en un sitio web. El proveedor de servicios ofrece un script que construye un túnel a la red IPv6, asigna una dirección IPv6 en el sistema final, y asigna un prefijo de red al router para permitir la conectividad para el resto del sitio. El túnel broker gestiona la creación y la supresión del túnel para el servidor del túnel. Errores o pérdida de esta información podría causar un riesgo de seguridad para el sitio.

[101] RFC 3053: IPv6 Tunnel Broker

Para facilitar la asignación de direcciones y creación de túneles IPv6, se ha desarrollado el concepto de Tunnel Broker (TB). TB es un intermediario al que el usuario final se conecta, normalmente con un interfaz web.

El usuario solicita al TB la creación de un túnel y este le asigna una dirección IPv6 y le proporciona instrucciones para crear el túnel en el lado del usuario.

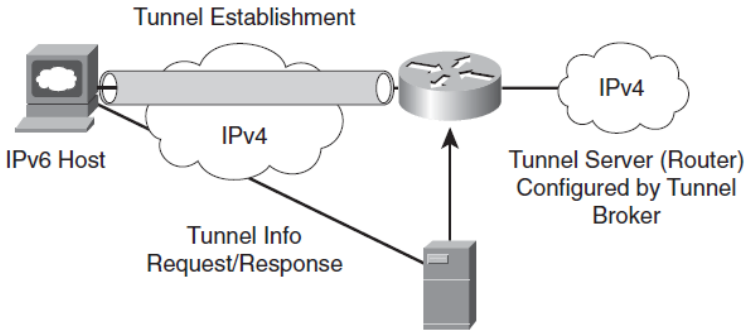


Ilustración 89. Establecimiento de túnel automático con Tunnel Broker

La ***Ilustración 89*** muestra el establecimiento de un túnel automático con tunnel broker.

El TB también configura el router que representa el extremo final del túnel para el usuario.

En http://www.ipv6tf.org/using/connectivity/test.php existe una lista de TB disponibles

TSP[102] es un caso especial de TB que no está basado en un interfaz web sino en una aplicación cliente que se instala el cliente y se conecta con un servidor, aunque el concepto es el mismo.

7.5. 6to4

Túneles 6to4: RFC 3056[103]

[102] **TSP** (Tunnel Setup Protocol o Configuración del protocolo de túnel), es un protocolo de red utilizado para negociar IP del túnel entre los parámetros de configuración a un cliente del túnel y un túnel corredor del servidor, el túnel de los puntos finales.

[103] RFC 3056: Connection of IPv6 Domains via IPv4 Clouds.

El túnel 6to4, especificado en el RFC 3056, "Conexión de dominios IPv6 a través de nubes IPv4", es un mecanismo automático de túnel, que es típicamente implementado en los routers de frontera.

El mecanismo de túnel 6to4 no requiere ninguna configuración explícita y utiliza la infraestructura IPv4 como un vínculo de difusión virtual. El destino del túnel es la dirección IPv4 integrado de la dirección IPv6 de destino en la cabecera IPv6. Las direcciones IPv6, que inician con el prefijo 2002::/16, se conocen como direcciones 6to4, por lo que para construir el prefijo 6to4 de 48 bits se antepone 2002 a los 32 bits de direcciones IPv4 para el uso de un host o una red detrás de él . Por ejemplo, usando una dirección IP global 192.168.10.1 se crea el prefijo 6to4 correspondiente 2002:C0A8:0A01::/48.

Mientras encapsula el paquete IPv6 en un paquete IPv4, el túnel 6to4 utiliza el protocolo número 41. El mecanismo de túnel 6to4 proporciona dos escenarios de implementación:

- Interconexión de dominios 6to4
- Interconexión 6to4 y dominios nativos IPv6 usando routers de reenvio.

La ***Ilustración 90*** muestra el despliegue 6to4 para interconectar dominios 6to4; este es un escenario de implementación simple para interconectar múltiples sitios IPv6. En este escenario de implementación, se asigna sólo una dirección 6to4 en la interfaz externa del router.

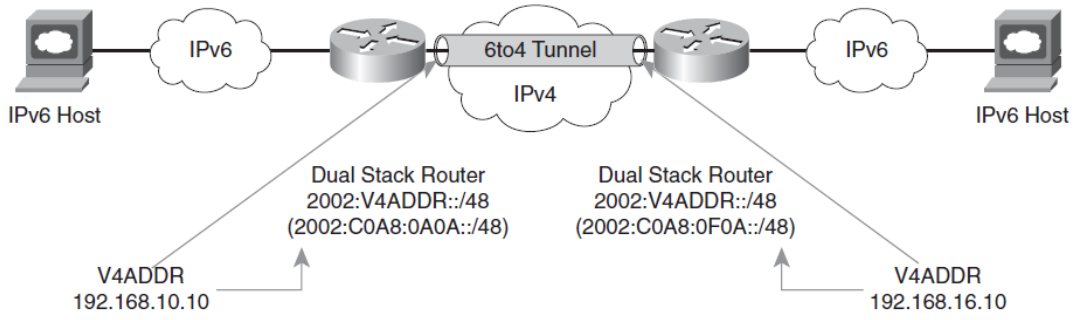


Ilustración 90. Interconectando dominios 6to4

El segundo escenario de implementación se vuelve más frecuente cuando hay una necesidad de comunicación entre el dominio 6to4 y un dominio IPv6 nativo. Esta

comunicación requiere los servicios de un enrutador de retransmisión (que es un router estándar de doble pila que utiliza ambas direcciones 6to4 y direcciones IPv6 nativas). El enrutador de retransmisión en la ***Ilustración 91*** se conecta a la red IPv4, a la red nativa IPv6 y la red del sitio IPv6 6to4.

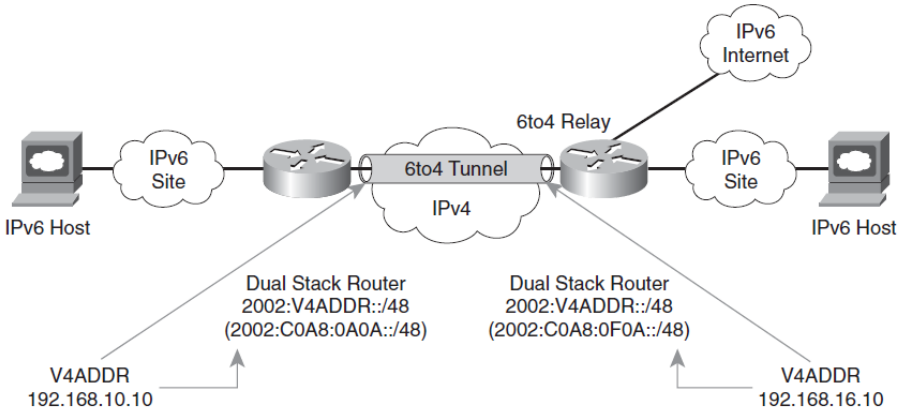


Ilustración 91. Interconección de dominios 6to4 a dominios IPv6 nativos

Para que funcione el enrutamiento cuando interconectan un dominio 6to4 a un dominio IPv6 nativo, un protocolo interno de enrutamiento como IGRP mejorado (EIGRP) para IPv6 puede ser utilizado para el encaminamiento de IPv6 dentro del sitio.

6to4 se trata de un encapsulado de paquetes IPv6 en paquetes IPv4, similar a 6in4.

Diferencias:

- La dirección IPv6 del cliente no depende del router al que se conecta sino de la dirección IPv4 pública. Rango 2002::/16
- Los paquetes IPv6 de salida del cliente siempre son enviados al mismo “6to4 relay”, sin embargo los paquetes IPv6 de entrada al cliente pueden provenir de otros “6to4 relay” diferentes.

Se utiliza un “truco” para proporcionar direcciones 6to4.

- Prefijo 6to4: 2002::/16
- Se usa la IPv4 pública (por ejemplo 192.0.1.1) para siguientes 32 bits.
- Se obtiene así un prefijo /48 (p.e. 2002:C000:0101::/48)

En la ***Ilustración 92*** se puede apreciar, que cuando un router 6to4 ve un paquete hacia el prefijo 2002::/16 lo encapsula en IPv4 hacia la IPv4 pública que va en la dirección.

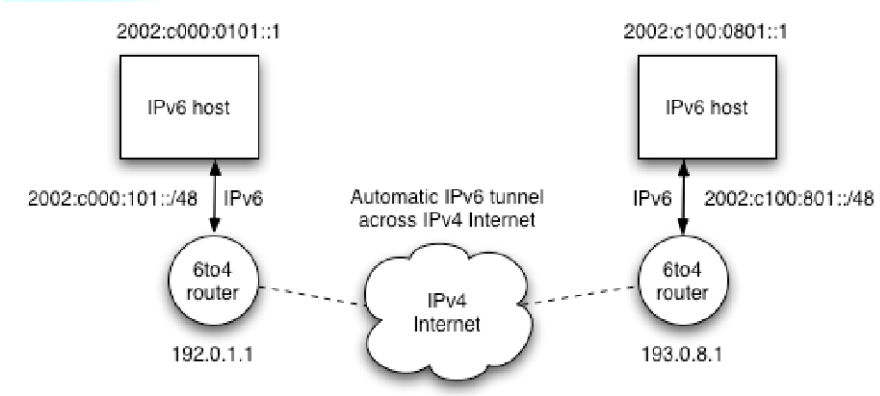


Ilustración 92. Túneles 6to4

Sigue faltando una cosa: ¿Cómo enviar paquetes hacia una IPv6 "normal"? Relay 6to4.

El Relay 6to4 se anuncia mediante:

- Dirección IPv4 anycast conocida: 192.88.99.1 (RFC3068[104]).
- Prefijo 6to4 (2002::/16).

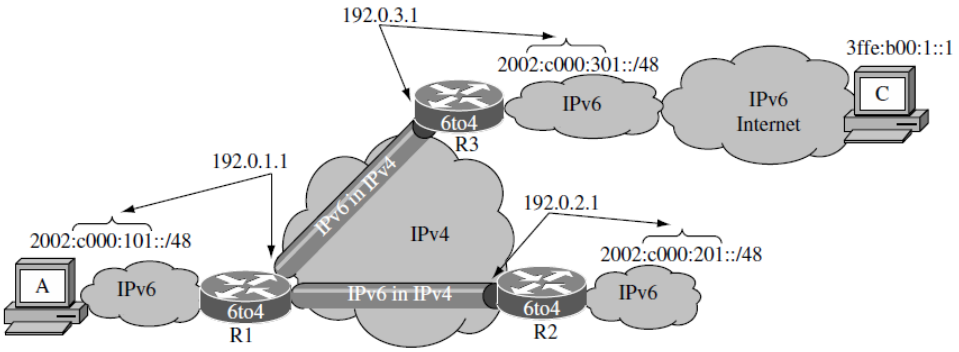


Ilustración 93. Relay 6to4

En la ***Ilustración 93,*** A envía un paquete a C. El router R3 es el 6to4 relay para el router R1 y está conectado a la Internet IPv6 que no es 6to4. Cuando R1 quiere reenviar el paquete a una dirección de destino que no es 6to4 (3ffe:b00:1::1), no se puede construir un túnel automático de algún enrutador 6to4 a otros, ya que no se puede extraer la

[104] RFC 3068: An Anycast Prefix for 6to4 Relay Routers

dirección IPv4 de la dirección IPv6 de destino. Si el R1 tiene una ruta predeterminada para llegar al R3 a través de un mecanismo 6to4, entonces R1 encapsula el paquete IPv6 para R3 y R3 lo desencapsula y lo envía a la red IPv6. R3 y los vínculos entre R3 y la Internet IPv6 que no es 6to4 se utilizan como una red de tránsito. En este contexto, debe haber algún tipo de acuerdo entre los sitios 6to4 para utilizar R3 de tránsito. Como contrapartida, cualquier router de borde de 6to4 debe estar bien configurado con el filtrado de entrada para evitar ser utilizado como lugar de tránsito para otros sitios 6to4.

Para activar el 6to4 relay, el enrutador de retransmisión 6to4 (router relay) es un enrutador 6to4 con una ruta predeterminada a Internet IPv6. El 6to4 relay debe contener algún tipo de filtrado de entrada. Un sitio 6to4 que está utilizando un 6to4 relay instala en el router de borde 6to4 una ruta por defecto IPv6 apuntando a la dirección 6to4 del router reley. Los routers 6to4 relay no requieren características específicas para actuar como 6to4 relay, sólo una entrada de ruta estática.

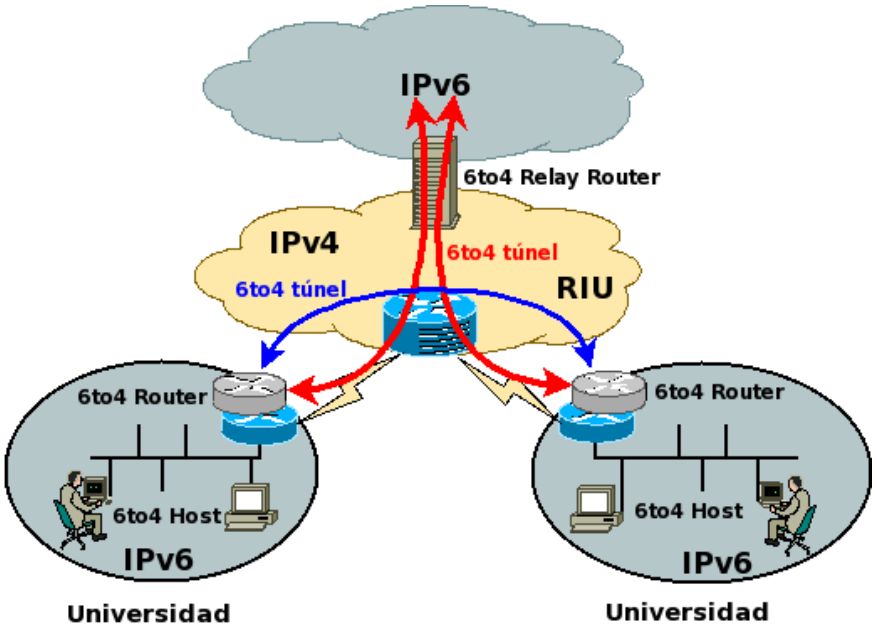


Ilustración 94. Elementos de arquitectura 6to4

En la siguiente ***Ilustración 94*** se muestran host y routers que implementan el mecanismo de transición 6to4.

El mecanismo de transición 6to4 presenta en su arquitectura los siguientes elementos:

- 6to4 Host: dispositivo que presenta por lo menos una dirección 6to4 y que además se comporta como un dispositivo IPv6 con soporte nativo.
- 6to4 Router (o 6to4 border router): router IPv6 que soporta pseudointerfaces 6to4. Normalmente es un router de borde entre un sitio IPv6 y una WAN IPv4.
- 6to4 Relay Router: router configurado para soportar transito de rutas entre direcciones 6to4 y direcciones IPv6 nativas.

7.6. 6RD

6RD: Un refinamiento de 6to4

6RD utiliza IPv4 para proporcionar acceso a Internet IPv6 e IPv4 con calidad de producción a los sitios de los usuarios. RFC 5969[105].

Cambios a 6to4:

- Formato dirección (de nuevo) => esfuerzo de implementación.
- Usa prefijo IPv6 “normal” (2000::/3), en vez de 2002::/16.
- Desde el punto de vista del usuario y de la Internet IPv6: se percibe como IPv6 nativo.
- Relay (o gateway) se encuentra solamente dentro del backbone del ISP, en el borde de la Internet IPv6.
- Múltiples instancias son posibles: anunciadas mediante una dirección anycast.
- Bajo estricto control del ISP.

[105] RFC 5969: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification

6RD: Formato direcciones

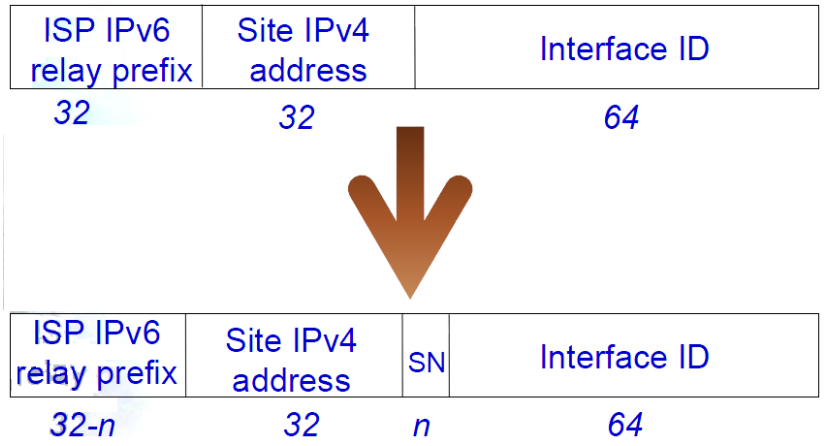


Ilustración 95. Formato de direcciones 6RD

En la ***Ilustración 95*** se muestra cómo el prefijo IPv6 de un cliente se deriva de la dirección IPv4. El formato de la dirección elegida utiliza 32 bits de direcciones IPv4 en direcciones IPv6 por razones de simplicidad y de compatibilidad con el código existente 6to4.

La comunicación IPv6 entre los sitios de los clientes de un mismo proveedor de Internet es directa a través de la infraestructura IPv4 del ISP: cuando un CPE ve que la dirección IPv6 de destino de un paquete de salida comienza con su propio prefijo IPSv6, se toman los 32 bits que siguen al prefijo como un paquete encapsulado con destino IPv4.

6RD: Pros & Contras

Pros:

- Parece fácil de implementar y desplegar si los dispositivos de red están “bajo control” (CPEs, …).
- Soluciona todos (?) los problemas de 6to4.
  - seguridad, routing asimétrico, …
  - Relay (o gateway) en la red del ISP bajo su control.

- Transparente para el cliente.
    - Configuración automática del CPE.
- Funciona con direcciones IPv4 públicas y privadas.
    - Asignadas al cliente.

Contras:

- Necesario cambiar software de todos los CPEs.
    - Actualmente solo hay un par de ellos.
- Añade una nueva "caja": 6RD relay/Gateway.
    - Hasta que otros fabricantes de routers soporten 6RD (Cisco ya lo hace).

6RD: Arquitectura

Sitios de Usuario (Dual-Stack):

- Asignado prefijo RD IPv6 => LAN(s) IPv6 Nativo.
- (+IPv4).

CPE (= 6RD CE = 6RD router):

- Proporciona conectividad IPv6 nativo (lado cliente).
- Ejecuta código 6RD (6to4 modificado).
- Tiene una interfaz multipunto virtual 6RD para soportar el en/desencapsulado de IPv6 en IPv4.
- Recibe un prefijo IPv6 6RD de un dispositivo del SP.
- y una dirección IPv4 (lado WAN = red del ISP).

6RD relay (= border relay):

- Gateway entre infraestructura IPv4 del ISP e Internet IPv6.
- Anuncia una dirección IPv4 a los CPEs.

- Dirección anycast puede ser usada para redundancia.

6RD: Escenario de Implementación

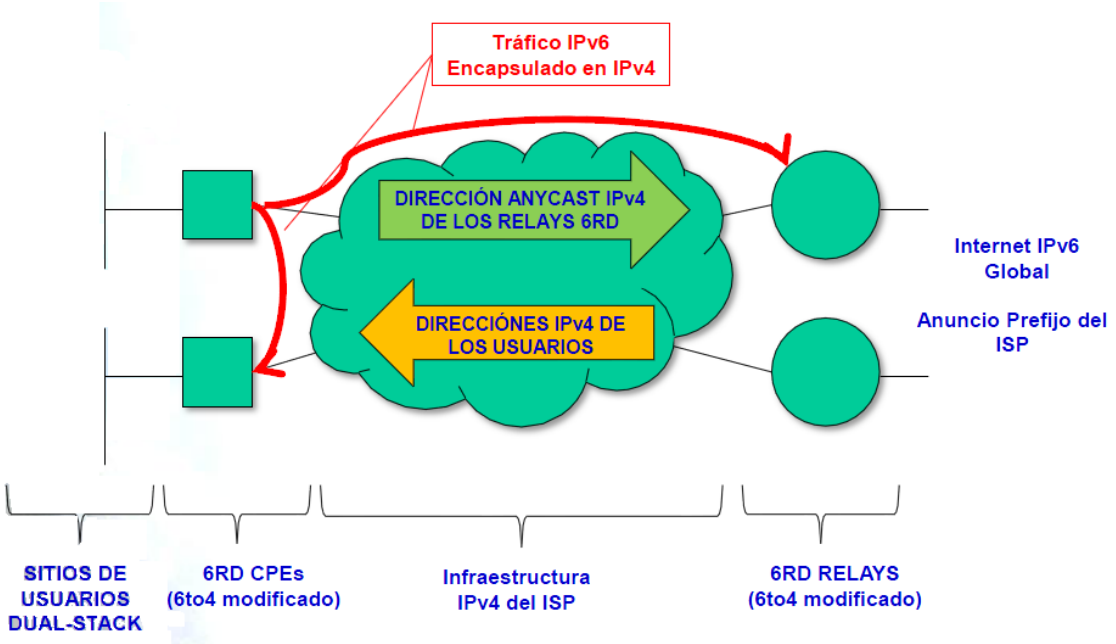


Ilustración 96. Arquitectura IPS para implementar IPv6 con 6RD

La ***Ilustración 96*** muestra cuales nodos tienen que ser actualizados de 6to4 a 6RD, y cuales direcciones o prefijos tienen que ser enrutados a ellos.

La comunicación IPv6 entre los sitios de los clientes de un mismo proveedor de Internet es directa a través de la infraestructura ISP IPv4: cuando un CPE ve que la dirección IPv6 de destino de un paquete de salida comienza con su propio prefijo IPv6 de 6RD relay, toma los 32 bits que siguen a este prefijo como destino IPv4 del paquete encapsulado.

La dirección IPv4 anycast de los 6RD relay puede ser elegido de forma independiente por cada ISP. La única restricción es que las rutas hacia el ISP que se anuncian no debe incluir esta dirección. Por ejemplo, Free tomó una dirección 192.88.99.201, enrutado con el mismo prefijo /24 como 6to4, pero con 201 en vez de 1 para evitar confusiones con 192.88.99.1, siendo esta la dirección anycast 6to4. Otra posibilidad, habría sido la

utilización de la dirección anycast 6to4 y agregar en el relay, un prefijo IPv6 de prueba a la dirección del lado del ISP. Si comienza con 2002::/16, el paquete es 6to4, no 6RD.

7.7. Teredo

Es una tecnología de transición a IPv6 que proporciona tunneling automático de host a host en lugar de tunneling de Gateway. Este enfoque transmite tráfico IPv6 unicast si hay host de doble pila (host que ejecutan tanto IPv6 como IPv4) detrás de una o varias NAT IPv4.

Funciona en NAT de tipo:

- Full Cone[106].
- Restricted Cone[107].

No funciona en NATs de tipo:

- Symmetric[108] (Solventado en Windows Vista).

El cliente configura un Teredo Server que le proporciona una dirección IPv6 del rango 2001:0000::/32 basada en la dirección IPv4 pública y el puerto usado:

- Si el Teredo Server configurado es además Teredo Relay, el cliente tiene conectividad IPv6 con cualquier nodo IPv6.
- De lo contrario solo tiene conectividad IPv6 con otros clientes de Teredo.

[106] **Full cone** NAT, es un tipo de NAT donde todas las peticiones de la misma direccion IP interna y Puerto se asignan a la misma dirección IP externa y puerto. Además, cualquier host externo puede enviar un paquete al host interno, enviando un paquete a la dirección externa asignada.

[107] **Restricted cone** NAT, es donde todas las peticiones de la misma dirección IP interna y puerto se asignan a la misma dirección IP externa ypuerto. A diferencia del full cone, un host externo (con dirección IP X) puede enviar un paquete al host interno si el host interno previamente había enviado un paquete a la dirección IP X.

[108] Un **NAT simétrico**, es uno donde todas las solicitudes de la misma dirección IP interna y puerto, a una dirección IP y puerto de destino específicos, se asignan a la misma dirección IP y puerto externa. Si el mismo host envía un paquete con la misma dirección y puerto de origen, pero a un destino diferente, se utiliza una asignación diferente. Además, solo el ost externo que recibe un paquete puede enviar un paquete UDP de vuelta al servidor interno.

Actualmente Microsoft proporciona Teredo Servers públicos y gratuitos, pero no Teredo Relays.

En la ***Ilustración 97*** se muestran los 4 agentes Teredo: Teredo client, Teredo server, Teredo relay, Teredo host-specific relay. El Teredo client es configurado por el usuario que desea conseguir conectividad IPv6. El Teredo server, asigna al cliente una dirección Teredo IPv6 y es también el encargado de descubrir el tipo de NAT que utiliza el cliente. Es importante porque el tipo de dirección IPv6 y la forma en que la conexión IPv6 se hace depende del tipo de NAT. Por lo tanto es la primera etapa handshake (Teredo setup) con el Teredo server cuando el cliente intenta obtener una dirección IPv6, como se muestra en la ***Ilustración 97***. El Teredo server solo se utiliza para asignar la dirección IPv6 y para ayudar en la comunicación IPv6, pero no hace reenvío de ningún paquete IPv6, ni IPv4. Esta tarea es realizada por el Teredo Relays.

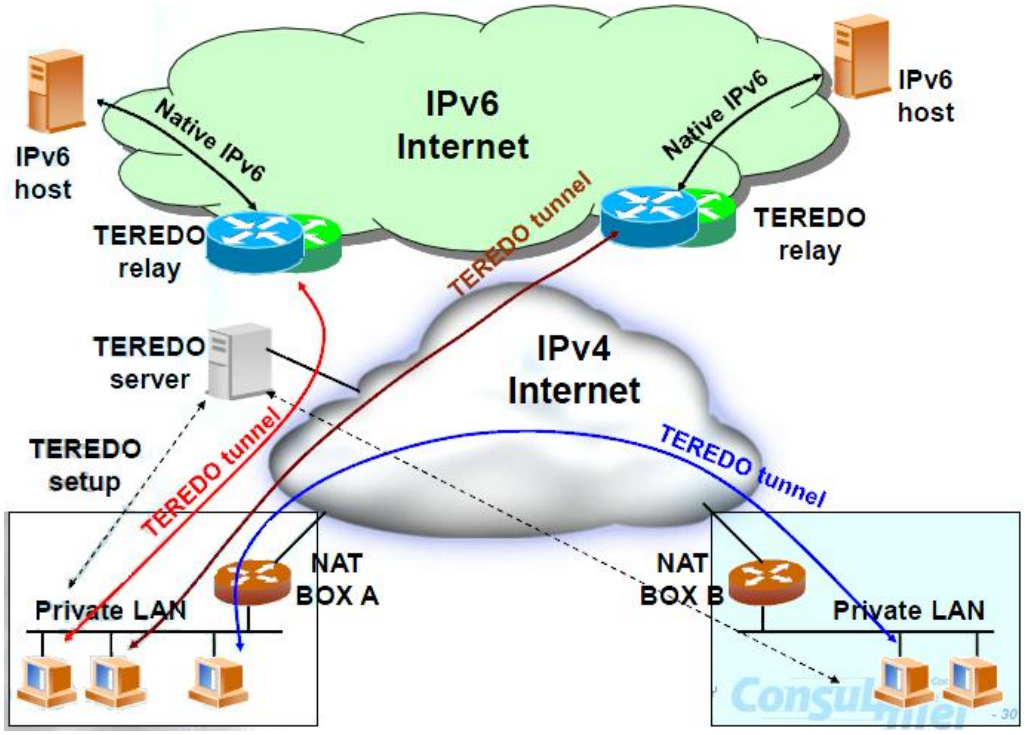


Ilustración 97. Teredo

Un nodo de aplicación del cliente Teredo, recibe una dirección IPv6 de un servidor Teredo y atraviesa NAT IPv4 utilizando IPv6 sobre UDP con encapsulación IPv4. Teredo se basa en los siguientes componentes, como muestra la ***Ilustración 98***:

- Cliente Teredo: el nodo A en la figura
- servidor Teredo;
- Teredo relay.

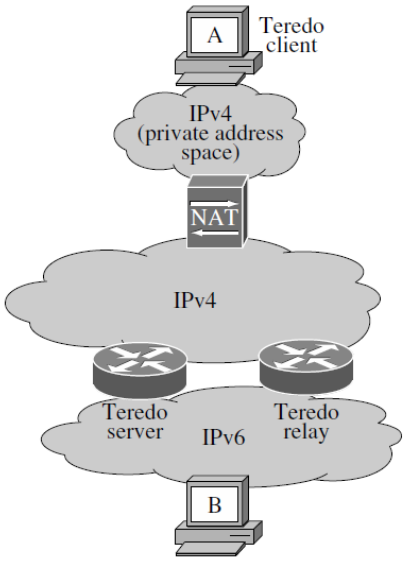


Ilustración 98. Componentes de arquitectura Teredo

7.8. Softwires

Protocolo que está siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:

- Mecanismo de transición "universal" basado en la creación de túneles:
  - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4.
  - Permite atravesar NATs en las redes de acceso.
  - Proporciona delegación de prefijos IPv6 (/48, /64, etc.).

- Autenticación de usuario para la creación de túneles mediante la interacción con infraestructura AAA.
- Posibilidad de túneles seguros.
- Baja sobrecarga en el transporte de paquetes IPv6 en los túneles.
- Fácil inclusión en dispositivos portátiles con escasos recursos hardware.

- Softwires posibilitará la provisión de conectividad IPv6 en dispositivos como routers ADSL, teléfonos móviles, PDAs, etc. cuando no exista conectividad IPv6 nativa en el acceso.
- También posibilita la provisión de conectividad IPv4 en dispositivos que solo tienen conectividad IPv6 nativa.

En realidad Softwires no es un nuevo protocolo, sino la definición de cómo usar de una forma diferente protocolos ya existentes con el fin de proporcionar conectividad IPv6 en redes IPv4 y viceversa.

Sofwires se basa en L2TPv2 (RFC 2661[109]) y L2TPv3 (RFC 3991[110]).

Encapsulamiento de Softwires basado en L2TPv2

El funcionamiento se especifica en draft-ietf-softwire-hs-framework-l2tpv2[111].

Existen dos entidades:

- Softwires Initiator (SI): agente encargado de solicitar el túnel.
- Softwires Concentrator (SC): agente encargado de crear el túnel (tunnel end point).

Se utiliza PPP para transportar paquetes IPx (x=4, 6) en paquetes IPy (y=4, 6).

[109] RFC 2661: Layer Two Tunneling Protocol "L2TP"

[110] RFC 3991: Media Gateway Control Protocol (MGCP) Redirect and Reset Packag

[111] Softwire Hub & Spoke Deployment Framework with L2TPv2 draft-ietf-softwire-hs-framework-l2tpv2-13, http://tools.ietf.org/html/draft-ietf-softwire-hs-framework-l2tpv2-13

- Opcionalmente se puede encapsular los paquetes PPP en UDP en caso de que haya que atravesar NATs.

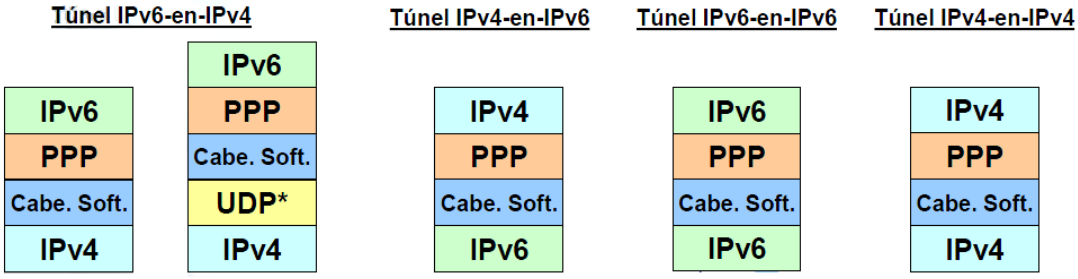


Ilustración 99. Encapsulamiento de Softwires basado en L2TPv2

En la ***Ilustración 99*** se muestran los encapsulados que apoya L2TPv2. Tener en cuenta que el by pass UDP no es compatible con L2TPv2 desde que L2TPv2 no apoyo la "detección" de NAT/NAPT.

Softwires basado en L2TPv2 L2TP header

Como se muestra en la ***Ilustración 100***, existe un plano de control y otro de datos. Se usa PPP como protocolo de encapsulamiento.

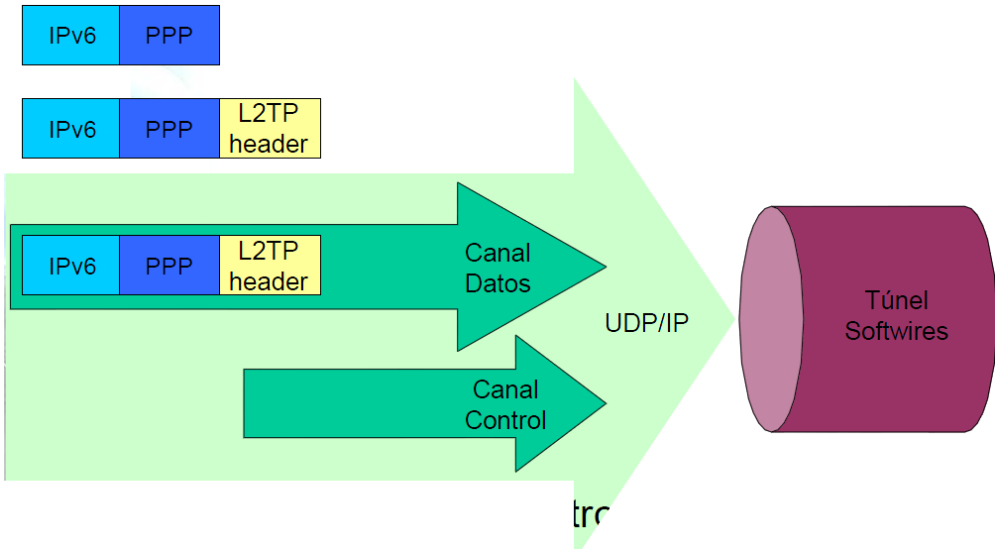


Ilustración 100. Softwires basado en L2TPv2

Ejemplo de uso de Softwires

Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4.

- El SC está instalado en la red del ISP (DSLAM[112], Router de agregación u otro dispositivo).
- El SI está instalado en la red del usuario:
  - CPE típicamente. También es posible otro dispositivo diferente en la red del usuario.
- El SC proporciona conectividad IPv6 al SI, y el SI hace de encaminador IPv6 para el resto de la red de usuario.
- Se usa delegación de prefijo IPv6 entre el SC y el SI para proporcionar un prefijo (típicamente /48) a la red del usuario.
  - DHCPv6 PD.

Otros usos son también posibles:

- VPNs sobre IPv6 o IPv4.
- Conectividad IPv4 en red de acceso solo IPv6, etc.

[112] **DSLAM** (Digital Subscriber Line Access Multiplexer, Línea de abonado digital de acceso multiplexor), es un dispositivo de red, situado en centrales telefonicas de los operadores de telecomunicaciones.

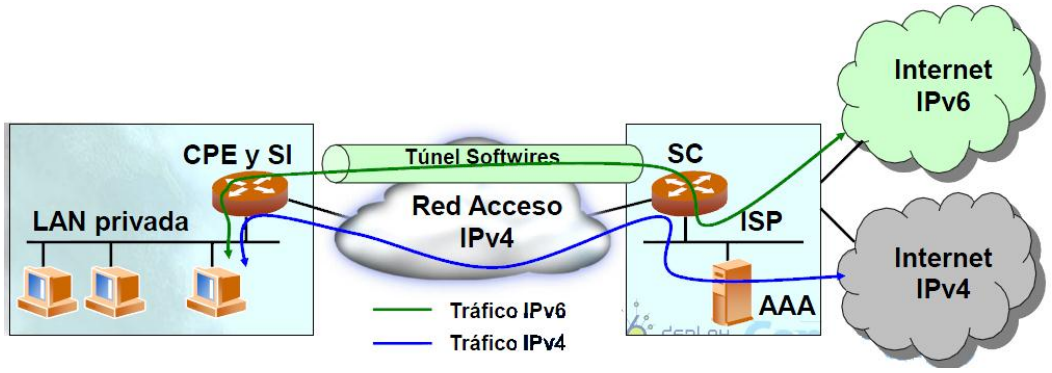


Ilustración 101. Ejemplo de uso de Softwires

En la ***Ilustración 101***, el Software Initiator (SI) es el host CPE (conectado directamente a un modem), que es de doble pila. No hay ningún dispositivo Gateway. El Softwire Concentrator (SC), es el nodo de terminación del Softwire en la red del proveedor de servicios. El tráfico IPv4 no debe atravesar el softwire. En este escenario, después que el canal de control L2TPv2, el establecimiento de sesión y negociación PPP LCP[113] (y opcionalmente autenticación PPP) son satisfactoria, IPv6CP negocia IPv6 sobre PPP, que también proporciona la capacidad de los ISP para asignar los 64 bits identificadores de interaz para el host CPE o realiza la validación de unicidad de los dos identificadores de interfaz en los dos extremos PPP.

Después que IPv6 sobre PPP ha terminado, la auconfiguración de direcciones IPv6 sin estado / Neighbor discovery se ejecuta sobre IPv6 a través de la conexión PPP, y el LNS puede informar al host CPE del prefijo a usar para la autoconfiguración de dirección sin estado a través de un anuncio de enrutador (RA).

Encapsulamiento de Softwires basado en L2TPv3

Misma filosofía y componentes que con L2TPv2, pero con las particularidades de L2TPv3:

- Transporte sobre IP/UDP de otros protocolos de capa 2 diferentes a PPP:

[113] **LCP** (Link Control Protocol o Control del Protocolo de Enlace), forma parte del protocolo punto a punto (PPP). En el establecimiento de comunicaciones PPP, tanto en el envio y recepción de los dispositivos que envían paquetes LCP para determinar las normas de la transición posterior de los datos.

- HDLC, PPP, FR, ATM, Ethernet, MPLS, IP.

- Formato de cabeceras mejorado para permitir un tratamiento más rápido en los SC:
  - Permite velocidades del rango de T1/E1, T3/E3, OC48.
- Mínimo overhead en los paquetes encapsulados (solo de 4 a 12 bytes extra).
- Otros mecanismos de autenticación diferentes a CHAP y PAP:
  - EAP.

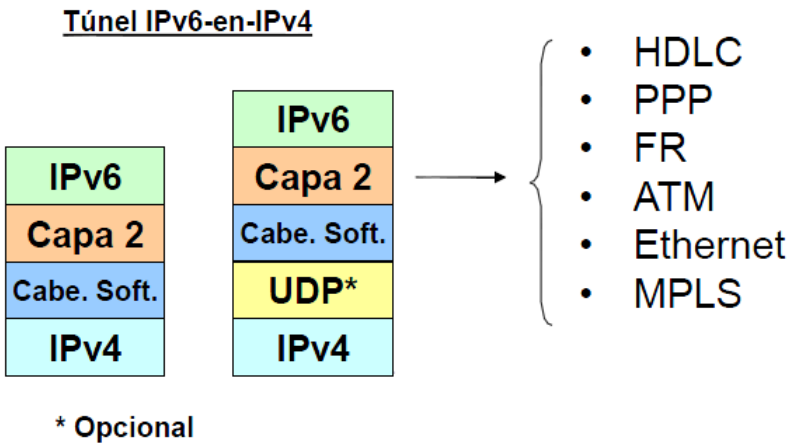


Ilustración 102. Encapsulamiento de Softwires basado en L2TPv3

7.9. DS-Lite

Dual Stack Lite Trata de solucionar el problema del agotamiento de IPv4. Esta enfocado a redes de banda ancha y agotamiento de direcciones IPv4. Comparte (las mismas) direcciones IPv4 entre usuarios combinando:

- Tuneling.
- NAT.

No hay necesidad de varios niveles de NAT. Dos elementos:

- DS-Lite Basic Bridging BroadBand (B4).

- DS-Lite Address Family Transition Router (AFTR) (También llamado CGN (Carrier Grade NAT) o LSN (Large Scale NAT)).

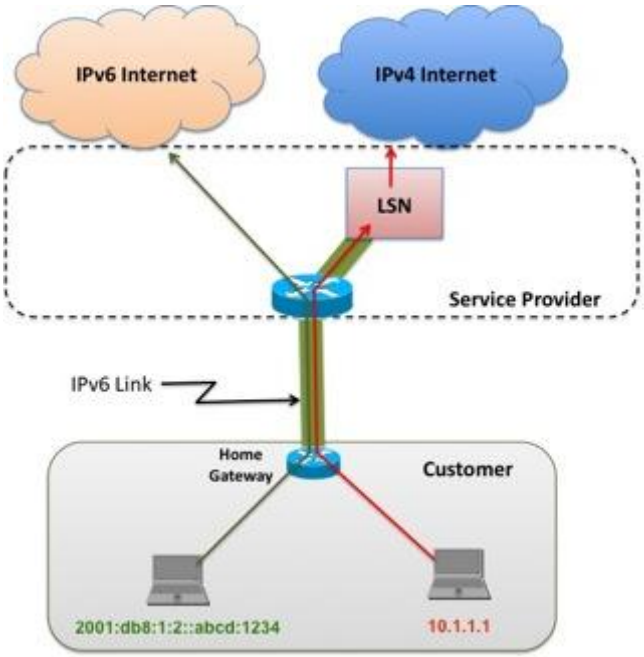


Ilustración 103. Dual Stack Lite

Asumiendo que hay multiples sistemas finales en la red del cliente, la función de DS-Lite ocurre en los dispositivos CPE como una puerta de entrada, a como se muestra en la ***Ilustración 103***. Si un dispositivo envía un paquete IPv6, el paquete se envía normalmente al destino IPv6. En caso que un dispositivo envie un paquete IPv4, el Gateway CPE lleva a cabo el encapsulamiento de IPv4 en IPv6, configurando la dirección de destino del paquete del paquete IPv6 a la dirección de DS-Lite activado en el LSN. En el LSN el paquete se desencapsula y se realiza NAT44. Este modelo permite el uso de doble pila, solo IPv4 y solo dispositivos IPv6 detrás delo Gateway.

7.10. Traducción

Se puede utilizar traducción de protocolos IPv6-IPv4 para:

- Nuevos tipos de dispositivos Internet (como teléfonos celulares, coches, dispositivos de consumo).

Es una extensión a las técnicas de NAT, convirtiendo no sólo direcciones sino también la cabecera:

- Los nodos IPv6 detrás de un traductor tienen la funcionalidad de IPv6 completa cuando hablan con otro nodo IPv6.
- Obtienen la funcionalidad habitual (degradada) de NAT cuando se comunican con dispositivos IPv4.
- Los métodos usados para mejorar el rendimiento de NAT (p.e. RISP) también se pueden usar para mejorar el rendimiento de la traducción IPv6-IPv4.

7.11. NAT64

Como el nombre sugiere, el mecanismo de transición NAT64 se refiere a la traducción de los paquetes IPv6 a un paquete IPv4. En el caso de NAT64, al iniciar el paquete esta siempre en el lado de IPv6. Aunque NAT64 comparte algunos de los mismos problemas que otros mecanismos de NAT, es la mejor opción, ya que se basa en los años de experiencia con NAT IPv4 y supera algunas de las cuestiones relacionadas con otros mecanismos como NAT-PT.

NAT64 ofrece funciones adicionales como la asignación de NAT y filtrado, que son necesarios para el medio peer-to-peer.

NAT64 también ofrece funciones tales como hairpinning, que permiten a los host IPv6 detrás de dispositivos NAT64 comunicarse unos con otros (ver ***Ilustración 104***).

La idea es similar al NAT-PT, pero funcionando mejor. Elemento opcional, pero desacoplado, DNS64.

Stateful NAT64 es un mecanismo para traducir paquetes IPv6 a IPv4 y viceversa:

- La traducción se lleva a cabo en las cabeceras de los paquetes siguiendo el Algoritmo de Traducción IP/ICMP.
- La dirección IPv4 de los host IPv4 se traducen algorítmicamente a/desde direcciones IPv6 usando un algoritmo específico.

- La especificación actual sólo define como NAT64 traduce paquetes unicast con tráfico TCP, UDP e ICMP.
- DNS64 es un mecanismo para sintetizar RRs tipo AAAA a partir de RRs tipo A. Las direcciones IPv6 contenidas en el AAAA sintetizado se genera mediante un algoritmo a partir de la dirección IPv4 y el prefijo IPv6 asignado al dispositivo NAT64.

NAT64 permite a múltiples nodos solo-IPv6 compartir una dirección IPv4 para acceder a internet.

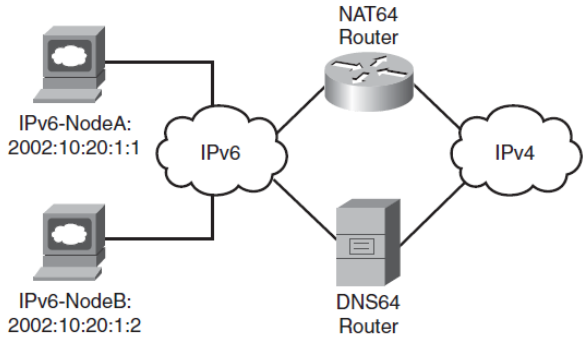


Ilustración 104. NAT64

La ***Ilustración 104*** se muestra un diseño de red con dispositivos NAT64, DNS64, clientes IPv6 y servidores IPv4.

Traducción IPv4/IPv6 (obsoleto)

Diferentes soluciones, pero tiene en común que tratan de traducir paquetes IPv4 a IPv6 y viceversa:

- [SIT[114]], [BIS[115]], [TRT[116]], [SOCKSv64[117]].

[114] **SIT**, permite a nodos que tienen soporte solo para IPv6 la comunicación con nodos que tienen soporte solo para IPv4, permite la comunicación a nodos pertenecientes a una red IPv6 con nodos que tienen soporte solamente para IPv4. Básicamente se basa en la traducción de la cabecera IP.

[115] **BIS** (Bump in the Stack), este mecanismo permite a un nodo que solo implementa IPv4 su comunicación con otros nodos que tienen soporte solo para IPv6 o solo par IPv4. Es útil debido a

La más conocida es NAT-PT [NATPT], [NATPTIMPL]:

- Un nodo intermedio (router) modifica las cabeceras IPv4 a cabeceras IPv6.
- El tratamiento de paquetes es complejo.

Es la peor solución puesto que la traducción no es perfecta y requiere soporte de ALGs, como en el caso de los NATs IPv4:

- DNS, FTP, VoIP, etc.

NAT-PT lleva a cabo la traducción de las direcciones de capa de red (Capa 3) entre IPv4 e IPv6. En este mecanismo, los nodos finales de la red IPv6 están tratando de comunicarse con los nodos de la red IPv4. Este método se utiliza principalmente para la comunicación entre los hosts que son solo IPv6 a los que son sólo IPv4.

NAT-PT utiliza un grupo de direcciones IPv4 y los asigna a los nodos/host IPv6 finales en los límites de IPv4-IPv6. Este mecanismo es similar a los mecanismos de NAT utilizado hoy en día en las redes IPv4.

Similar a NAT con IPv4, NAT-PT permite ambas traducciones estáticas y dinámicas (pools). En el caso de la traducción estática, una dirección IPv6 se asigna a una dirección IPv4. Utilizando la traducción de direcciones IPv6 de las direcciones IPv4 en el router NAT-PT, los nodos IPv6 son capaces de comunicarse. En la traducción dinámica, NAT-PT asigna las direcciones del pool para permitir múltiples asignaciones NAT-PT.

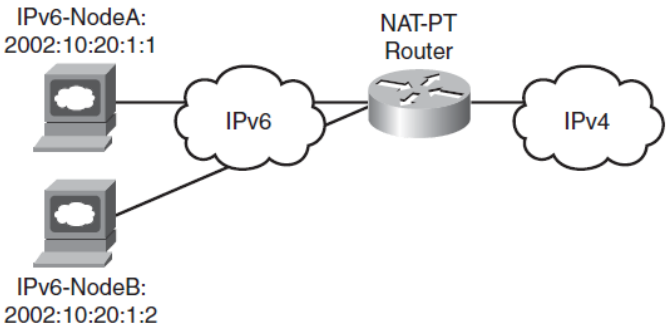
La ***Ilustración 105*** muestra un router NAT-PT con la tabla de traducción de direcciones.

---

que permite a aplicaciones IPv4, que de ninguna forma pueden ser actualizadas al protocolo IPv6, su comunicación con nodos IPv4 e IPv6.

[116] **TRT** (*Transport Relay Translation*), es el método más común de NAT-PT/NAPT-PT; se basa en la translación entre los registros DNS AAAA y A conocida como *DNS-ALG.*

[117] **SOCKSv64**, este mecanismo permite a un nodo IPv4 o IPv6 su comunicación con otros nodos IPv4 o IPv6 ubicados físicamente en redes distintas. Es de utilidad cuando un nodo solo implementa el protocolo IPv4 o existen aplicaciones en el que solo implementen el protocolo IPv4 y desea comunicarse con otro nodo que implementa IPv4 o IPv6.



Before Translation		After Translation	
Source Address	Destination Address	Source Address	Destination Address
2002:10:20:1:1	2002:CAFO:1:1	192.168.1.1	10.12.1.1
2002:10:20:1:2	2002:CAFO:1:2	192.168.1.2	10.12.1.2

Ilustración 105. Ejemplo de NAT-PT

7.12. Seguridad

Seguridad en los mecanismos de transición

La seguridad en las comunicaciones es un objetivo que debe garantizarse en un entorno hostil como es en la actualidad Internet.

Cada protocolo/mecanismo utilizado introduce nuevas amenazas y/o oportunidades que nodos malintencionados puedan aprovechar para comprometer la seguridad.

Los mecanismos de transición IPv6 no son una excepción y se han realizado análisis de posibles amenazas y recomendaciones de seguridad sobre los más empleados:

- Túneles 6in4.
- Túneles 6to4.
- Teredo.

8. CALIDAD DE SERVICIO (QOS)

8.1. Conceptos de QoS

Calidad de Servicio es una medida del comportamiento de la red con respecto a ciertas características de algunos servicios definidos.

Calidad: Entrega fiable de datos (“mejor de lo normal”)

- Pérdida de datos
- Latencia
- “Jittering”
- Ancho de banda

Servicio: Cualquier cosa ofrecida al usuario

- Comunicaciones
- Transporte
- Aplicaciones

Conceptos comunes a todas las definiciones de QoS:

- Diferenciación de Tráfico y Tipo de Servicio
- Los usuarios pueden ser capaces de tratar una o más clases de tráfico de forma diferente.

Aproximaciones a QoS en IP

Dos aproximaciones básicas desarrolladas en IETF:

- “Integrated Service” (int-serv)
  - “Ajuste fino” (por-flujo), especificaciones cuantitativas (p.ej., x bits por segundo), usa señalización RSVP.

- "Differentiated Service" (diff-serv)
  - "Ajuste basto" (por-clase), especificaciones cualitativas (p.ej., mayor prioridad), no hay señalización explícita.

8.2. Soporte QoS en IPv6

Soporte IPv6 para Int-Serv

Campo Flow Label de 20 bits para identificar flujos específicos que necesitan un tratamiento especial de QoS:

- Cada fuente especifica su propio valor de Flow Label; los encaminadores usan la Dirección Origen + Flow Label para identificar los distintos flujos.
- El valor 0 en el Flow Label se usa cuando no se requiere una QoS especial, lo cual es el caso más común de momento.
- Esta parte de IPv6 no está estandarizada aún y puede cambiar su semántica en el futuro.

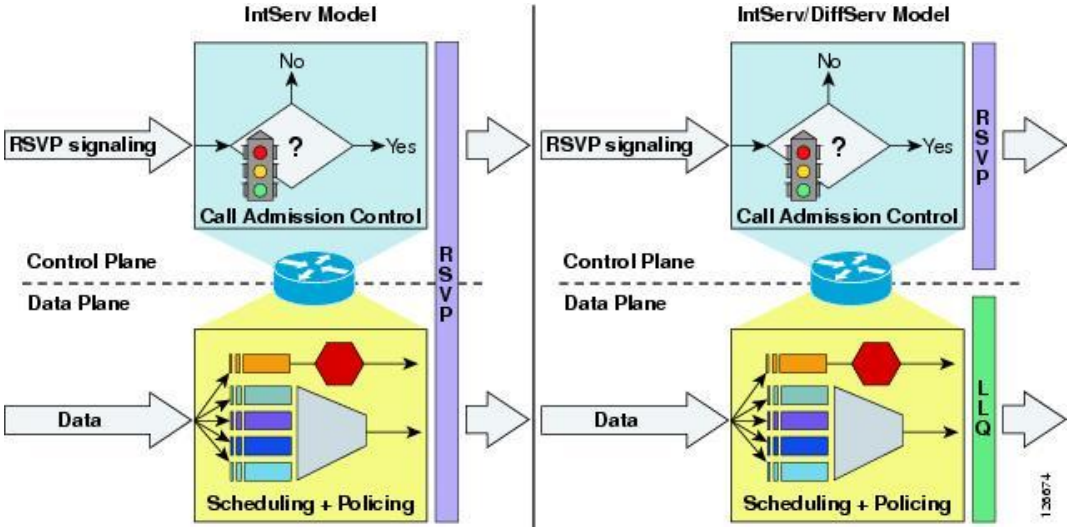


Ilustración 106. Modelo IntServ/DiffServ

En la ***Ilustración 106***, RSVP en el modelo IntServ involucra tanto el plano de control y el plano de datos. En el plano de control, RSVP admite o niega la solicitud de reserva. En el

plano de datos, clasifica los paquetes de datos, las políticas se basan en la descripción del tráfico contenido en los mensajes RSVP, y son encolados en las colas adecuadas.

La clasificación que realiza RSVP se basa en la 5-tupla formada por la dirección IP de origen, puerto de origen, dirección IP de destino, puerto de destino y numero de procolo. En este modelo, todos los paquetes de datos en transito a través del router deben ser interceptados por el RSVP para que RSVP pueda inspeccionar la 5-tupla y buscar una coincidencia entre las reservas establecidas. Si se encuentra una coindicencia, los paquetes son programados y vigilados por el RSVP de acuerdo a las especificaciones del trafico de reserva.

Soporte IPv6 para Diff-Serv

Campo Traffic Class de 8 bits para identificar clases de paquetes específicas que necesitan un tratamiento especial de QoS:

- Tiene el mismo significado que la definición nueva del octeto Type-of-Service en IPv4.
- Puede ser inicializada por un nodo o un encaminador en la ruta hacia el destino. También puede ser rescrito por cualquier encaminador en la ruta hacia el destino.
- El valor 0 en el campo Traffic Class se usa para especificar que no es necesario un tratamiento especial de QoS, lo cual es lo más común en la actualidad.

La figura siguiente (***Ilustración 107***) presenta un ejemplo de red desde el punto de vista de un despliegue DiffServ basado en QoS. Cada nodo implementa los mecanismos adecuados de espera y los mecanismos para evitar la congestión.

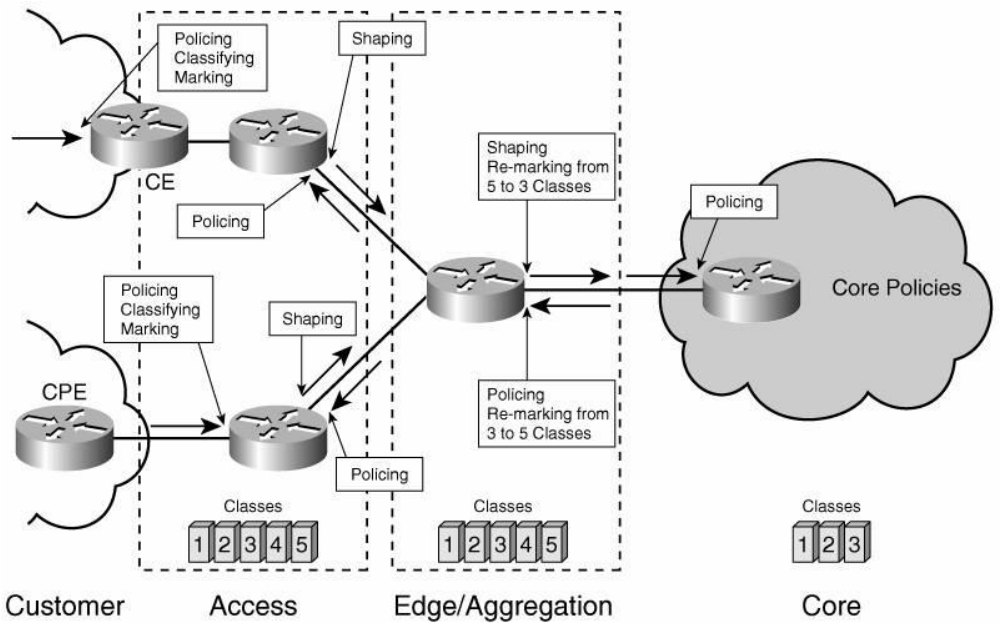


Ilustración 107. Una perspectiva de red de la operación DiffServ

IPv6 Flow Label

La ***Ilustración 108*** muestra el campo "Flow Label" de 20 bits, el cual habilita la clasificación eficiente de flujos IPv6 basados solo en los campos principales de la cabecera IPv6 que tienen posiciones fijas.

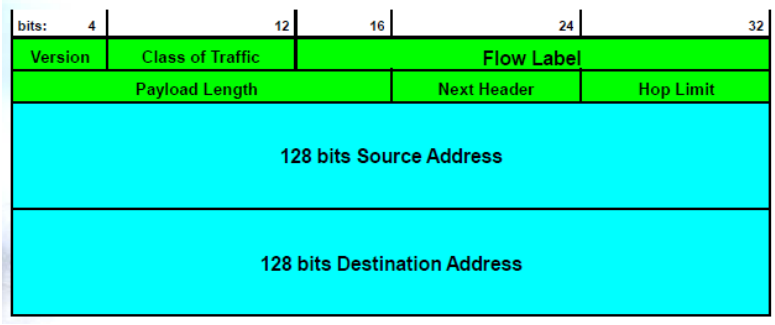


Ilustración 108. IPv6 Flow Label

El RFC 3697[118] específica:

- El campo "IPv6 Flow Label"

[118] RFC 3697: "IPv6 Flow Label Specification"

- Requisitos mínimos para:
    - Nodos IPv6 fuente que etiquetan flujos.
    - Nodos IPv6 que retransmiten paquetes ya etiquetados.
    - Métodos de establecimiento de estados de flujo.

Generalidades:

- Un flujo es una secuencia de paquetes enviados desde una fuente particular a un destino unicast, anycast o multicast particular, que la fuente desea etiquetar como un flujo.
    - Un flujo podría consistir en todos los paquetes de una conexión específica o "media stream".
    - Sin embargo, un flujo no es necesariamente un "mapeo" 1:1 a una conexión.
- Tradicionalmente, los clasificadores de flujo se han basado en tuplas de 5: dirección fuente, dirección destino, puerto origen, puerto destino y tipo de protocolo de transporte.
    - Pero alguno de estos campos puede no estar disponibles debido a la existencia de fragmentación, encriptación o aun estando disponibles, su localización detrás de una secuencia de cabeceras de extensión IPv6 puede resultar ineficiente.
    - Además, si los clasificadores son tales que solo se fijan en las cabeceras de la capa IP, la introducción de otros protocolos de transporte alternativos no será problemática.

IPv6 Flow Label:

- En IPv6 se usan tuplas de 3: campo Flow Label, dirección fuente y dirección destino.
- Esto permite la clasificación eficiente de flujos IPv6.
- Solo se usan campos de posiciones fijas en la cabecera IPv6.

El mínimo soporte de flujos IPv6 consiste en la etiquetación de los flujos:

- Los nodos IPv6 que soporten la etiquetación de flujos DEBEN ser capaces de etiquetar flujos conocidos (por ejemplo, conexiones TCP, aplicaciones de streaming, etc.)
- Incluso si el nodo por sí mismo no requiriera ningún tratamiento específico de flujos.

Especificación de Flow Label

- El campo "Flow Label" en la cabecera IPv6 es usado por una fuente para etiquetar los paquetes de un determinado flujo.
- Un "Flow Label" de valor cero se usa para indicar que el paquete no pertenece a ningún flujo determinado.
- Los clasificadores de paquetes usan la tupla de 3 campos para identificar el flujo al que pertenece un determinado paquete.
- Los paquetes se procesan de una determinada forma especificada en los nodos con capacidad de procesar flujos.
- El valor del "Flow Label" configurado por la fuente DEBE entregarse sin modificar en el nodo destino.
- Los nodos IPv6 NO DEBEN asumir ninguna matemática ni ninguna propiedad específica de los valores asignados al "Flow Label" por los nodos fuente.
- El rendimiento de los encaminadores NO DEBE depender de la distribución de los valores del "Flow Label".
- Los nodos que mantienen un estado de flujos dinámico NO DEBEN asumir que los paquetes que lleguen después de 120 sg o más de un paquete previo de un flujo, aún pertenece al mismo flujo, a no ser que el método de establecimiento de estados de flujo defina un tiempo de vida mayor o que el estado se haya refrescado dentro del tiempo de vida.

- El uso del campo “Flow Label” no implica necesariamente ningún requisito en la reordenación de paquetes.
    - Especialmente, el valor cero no implica que es aceptable la reordenación significativa de paquetes.
- Si un nodo IPv6 no proporciona un tratamiento específico para flujos DEBE ignorar el campo “Flow Label” cuando reciba o retransmita un paquete.

8.3. Aspectos prácticos

QoS para IPv6 en Cisco

Soporte Cisco de Quality of Service (QoS) en redes IPv6, basado en Differentiated Services (DiffServ).

Características disponibles:

- Clasificación de paquetes (Packet classification)
- Conformado de tráfico (Traffic shaping)
- Políticas en tráfico (Traffic policing)
- Marcado de paquetes (Packet marking)
- Encolado (Queueing)
- Weighted Random Early Detection (WRED)-based drop

CISCO proporciona un conjunto de herramientas de calidad de servicio que permite a los administradores de red para minizar los efectos de la perdida, retraso y la variación del retardo. Estas herramientas como se muestra en la ***Ilustración 109***, permiten la clasificación, programación, control y configuración de tráfico, siendo el objetivo de dar trato preferencial a tráfico de voz y video.

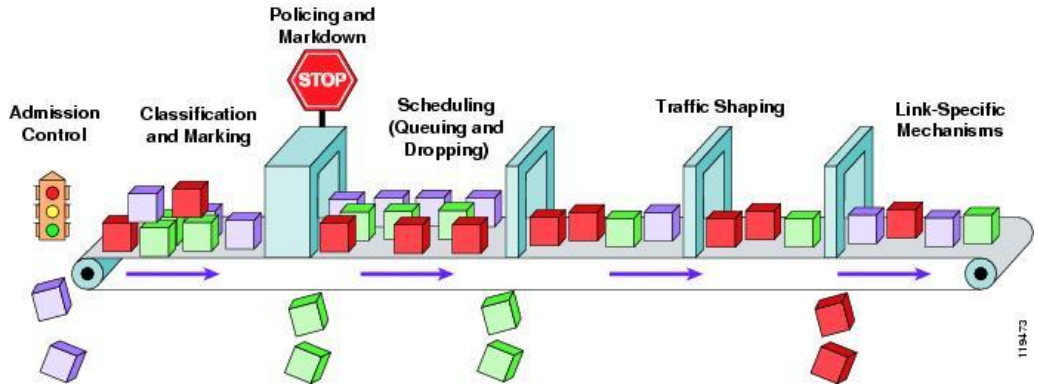


Ilustración 109. Conjunto de Herramientas de QoS

Características no disponibles:

- Compressed Real-Time Protocol (CRTP)
- Network-based application recognition (NBAR)
- Committed access rate (CAR)
- Priority queueing (PQ)
- Custom queueing (CQ)

Pasos generales para implementar QoS (IPv4 e IPv6)

1) Conocer que aplicaciones necesitan QoS.
2) Comprender las características de las aplicaciones para definir que herramientas de QoS les son apropiadas.
3) Crear clases basadas en criterios apropiados a la red. En particular, si la red transporta tráfico IPv4 e IPv6, decidir si ambos se tratan de la misma o distinta forma, y especificar criterios de coincidencia (match) apropiados:
   - Si se tratan ambos protocolos de la misma forma se pueden usar criterios de coincidencia como: match precedence, match dscp, set precedence, y set dscp
   - Si se tratan de forma separada se pueden usar criterios de coincidencia como match protocol ip and match protocol ipv6 en una match-all class map

4) Definir políticas para cada clase.

5) Configurar las políticas para tratar el tráfico.

6) Aplicar las políticas.

En resumen:

- Definir clases de tráfico (traffic classes).
- Definir y configurar políticas de tráfico (traffic policies - policy maps).
- Aplicar las políticas de tráfico a las interfaces.

Al aplicar herramientas de QoS, trabajar desde el extreme (Edge) hacia el centro (Core).

9. MULTICAST

9.1. Conceptos Multicast

¿Qué es Multicast?

Multidifusión (inglés multicast) es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen. En oposición a multicast, los envíos de un punto a otro en una red se denominan unidifusión (inglés unicast), y los envíos a todos los nodos en una red se denominan difusión amplia (inglés broadcast).

Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario establecer lo que se denomina "grupo multicast". Ese grupo multicast tiene asociado una dirección de internet. La versión actual del protocolo de internet, conocida como IPv4, reserva las direcciones de tipo D para la multidifusión. Las direcciones IP tienen 32 bits, y las de tipo D son aquellas en las cuales los 4 bits más significativos son '1110' (224.0.0.0 a 239.255.255.255).

La ***Ilustración 110*** muetra los conceptos mencionados anteriormente.

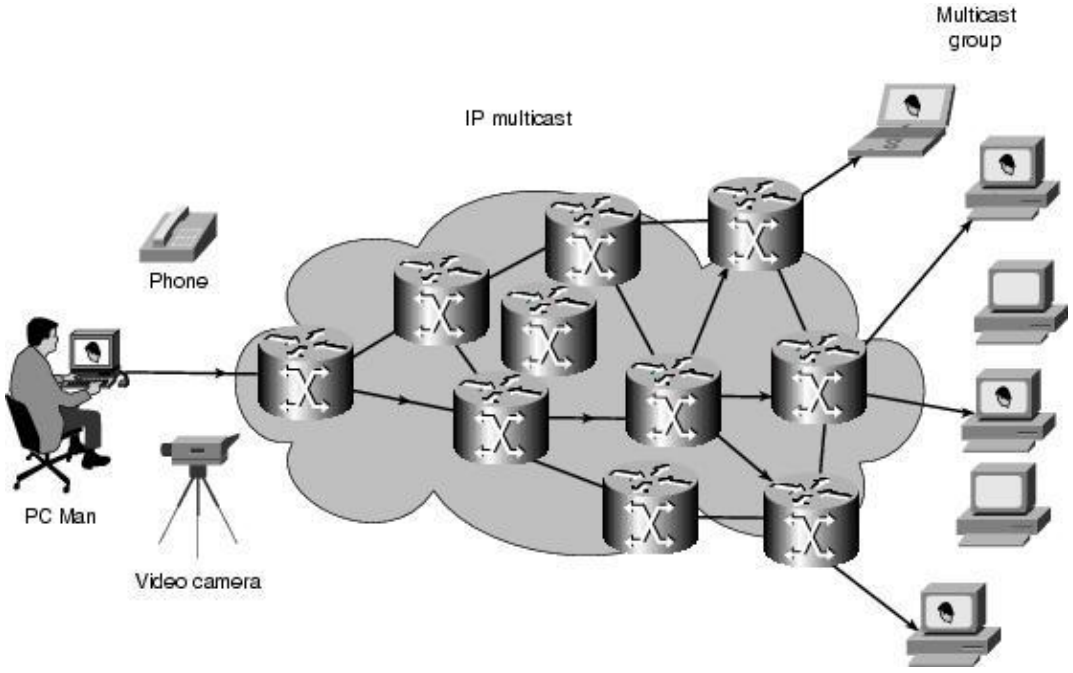


Ilustración 110. Multicast

Aplicaciones

- Sistemas Distribuidos
- Video bajo Demanda (VoD)
- Difusion Radio/TV
- Conferencias Multipunto (voice/video)
- Juegos en Red
- Funciones de nivel de Red

Conceptos Multicast

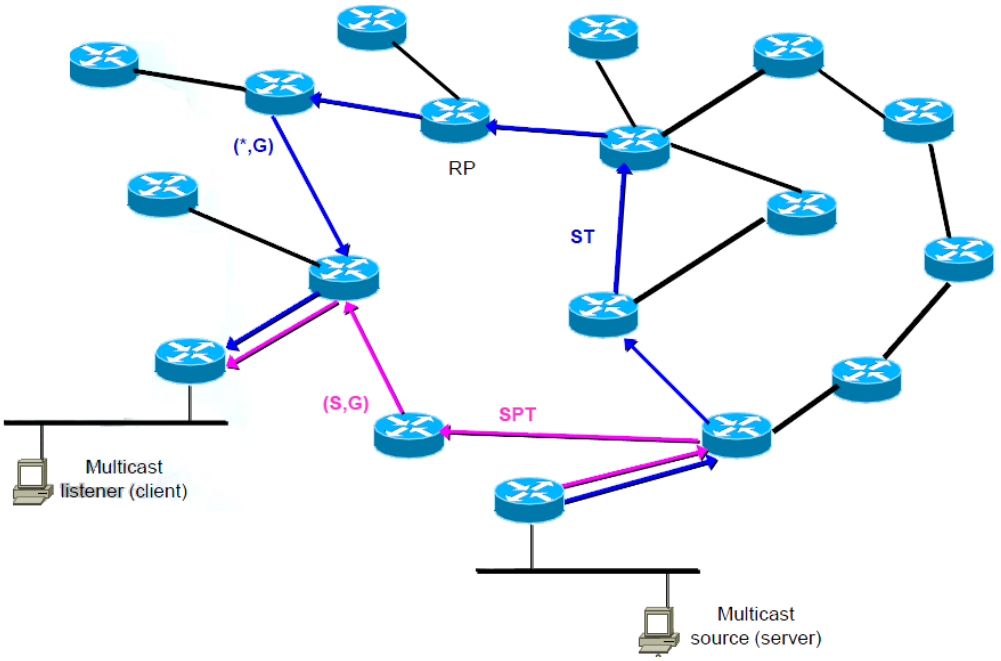


Ilustración 111. Multicast Client-Server

Multicast Distribution Tree (MDT)

- Es el camino de distribución multicast que se usa para entregar información multicast en las redes que tienen participantes multicast.
- Tiene forma de árbol con el fin de evitar bucles multicast cerrados en la red.
- La raíz del MDT es la fuente del grupo multicast.

Shortest Path Tree (SPT)

- Es el MDT que tiene la fuente del grupo multicast como raíz y a los participantes multicast como hojas del árbol.
- Se representa como (S,G).

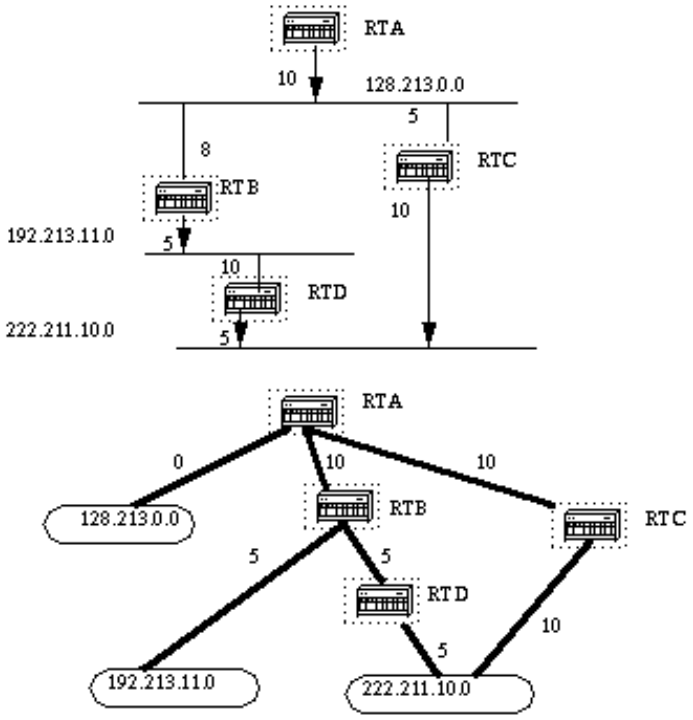


Ilustración 112. Shortest Path Tree

En la ***Ilustración 112*** se muestra la red desde el punto de vista del RTA. Tener en cuenta que la dirección de las flechas en el calculo de los costos. Por ejemplo, el costo de la interfaz RTB a la red 128.213.0.0 no es relevante cuando calculamos el costo para 192.213.11.0. RTA puede llegar a 192.213.11.0 a través de RTB con un costo de 15 (10+5). RTA también puede alcanzar 222.211.10.0 via RTC con un costo de 20 (10+10) o via RTB con un costo de 20 (10+10). En el caso que existan rutas con costos igual al mismo destino OSPF hara un seguimiento de hasta seis próximos saltos hacia el mismo destino.

Shared Tree (ST)

- Es el MDT resultante de tener una única raíz, denominada “Rendez-vous Point” cuando hay más de una fuente para el mismo grupo multicast.

¿Cómo funciona?

- El nodo se une/abandona un grupo multicast.
- No hay ninguna restricción acerca del número de grupos o del número de miembros por grupo.
- Enviar paquetes al grupo no significa que se pertenezca a él.
- La dirección de destino es una dirección multicast que representa a todo el grupo multicast.
- Los servicios multicast no están orientados a conexión por lo que no se puede emplear TCP.

9.2. Direcciones Multicast

IPv4 vs. IPv6

IPv4:

- Broadcast
  - Limitado: 255.255.255.255
  - Dirigido: <network>11..1

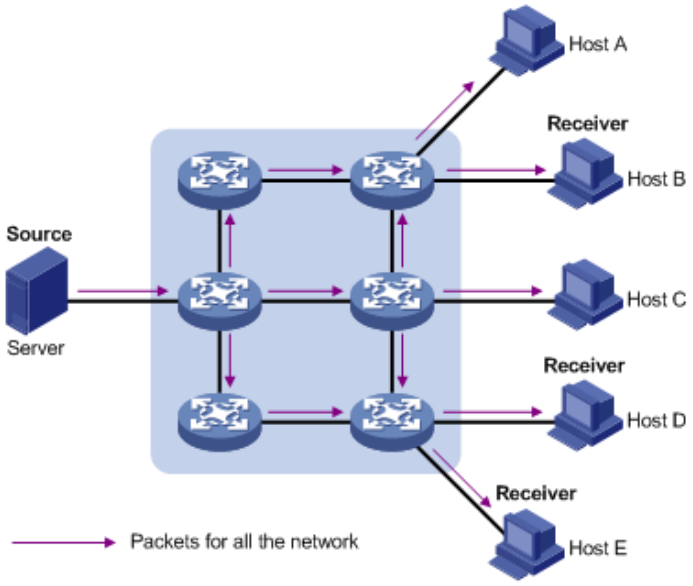


Ilustración 113. Transmisión de Informacion en modo Broadcast

Cuando se adopta broadcast, el sistema transmite la información a todos los usuarios en una red. Cualquier usuario de la red puede recibir la información, no importa que se necesite la información o no. La ***Ilustración 113*** muesta la transmisión de la información en modo de difusión (broadcast).

Supongamos que los host B, D y E necesitan la información. El servidor de origen emite esta información a través de routers y los hosts A y C en la red también reciben esta información.

Como podemos ver en el proceso de transmisión de la información, la seguridad y uso legal de servicio de pago no puede ser garantizada. Además, cuando sólo un pequeño número de usuarios en la misma red necesitan la información, la tasa de utilización de los recursos de la red es muy baja y los recursos de ancho de banda se desperdician mucho.

Por lo tanto, de difusión (broadcast) es una desventaja en la transmisión de datos a usuarios específicos y, además, ocupa gran ancho de banda de transmisión.

- Multicast
    - Clase D: 224.0.0.0 - 239.255.255.255

IPv6:

- Multicast
  - FF….

Multicast resuelve el problema de broadcast. Cuando algunos usuarios en una red requieren información especifica, el emisor de información de multidifusión (es decir, la fuente multicast) envía la información una sola vez. Con árboles de distribución multicast establecido para los paquetes de datos de multidifusión a través de protocolos de enrutamiento multicast, los paquetes se duplican y se distribuye a los nodos más cercanos, como se muestra en la ***Ilustración 114***:

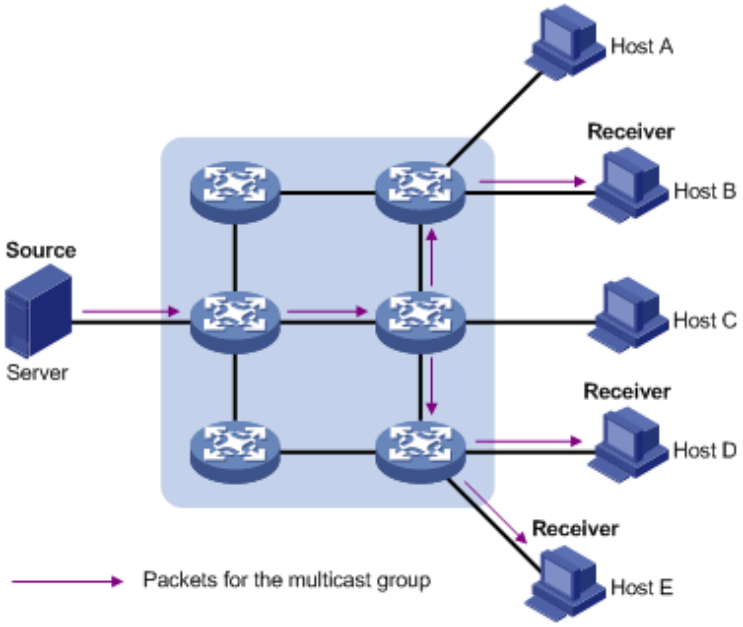


Ilustración 114. Transmisión de información en modo Multicast

Supongamos que los host B, D y E necesidad de la información. Para transmitir la información a los usuarios, es necesario agrupar los host B, D y E en un receptor. Los routers en la red duplican y distribuyen la información basandose en la distribución de los receptores de este conjunto. Finalmente, la información es correctamente entregada a los host B, D y E.

Las ventajas de multicast sobre unicast son las siguientes:

- No importa cuantos receptores existen, sólo hay una copia del mismo flujo de datos multicast en cada enlace.
- Con el modo de multidifusión utilizado para transmitir información, un aumento del número de usuarios no agrega carga de red notablemente.

Las ventajas de multicast sobre broadcast son los siguientes:

- Un flujo de datos multicast sólo se pueden enviar al receptor que requiere los datos.
- Multicast no trae ninguna pérdida de recursos de la red y hace buen uso de ancho de banda.

Direcciones Multicast IPv6

Una dirección IPv6 multicast es un identificador para un grupo de interfaces (por lo general en los diferentes nodos). Una interfaz puede pertenecer a cualquier número de grupos de multidifusión. Las direcciones de multidifusión tienen el siguiente formato mostrado en la ***Ilustración 115***:

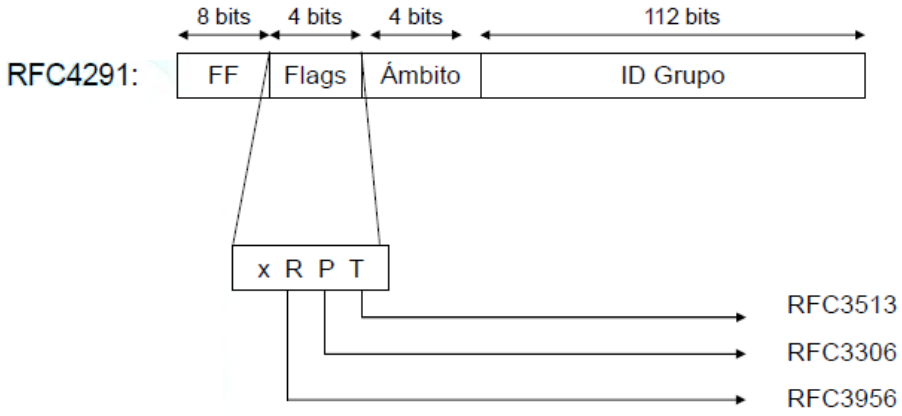


Ilustración 115. Direcciones Multicast IPv6

Los primeros 8 bits binarios al principio de la dirección puestos a FF (11111111), identifican la dirección como una dirección de multidifusión.

Los flags están establecidos a 4 banderas: 0 | R | P | T

Los flags de nivel alto están reservados y deben ser inicializados a 0. T=0, indica una dirección multicast de forma permanentemente asignado (“conocido”), asignado por la IANA; T=1, indica una asignación de dirección de multidifusión no permanente (“tránsitorio” o “dinámica”). En el caso de los flags P, la definición y uso se encuentra en el RFC3306[119]; así mismo, el la definición y uso del flag R se encuentra en el RFC3956[120].

El ámbito es un valor usado para delimitar el ámbito del grupo multicast; y el ID de grupo identifica el grupo multicast, ya sea permanente o transitoria, en el ámbito determinado.

Direcciones Multicast Reservadas

Node-Local Scope:

- FF01::1 Todos los nodos de la red
- FF01::2 Todos los encaminadores de la red

Link-Local Scope:

- FF02::1 Todos los nodos de la red
- FF02::2 Todos los encaminadores de la red
- FF02::4 Encaminadores DVMRP
- FF02::5 Encaminadores OSPFIGP
- FF02::6 Encaminadores designados OSPFIGP
- FF02::9 Encaminadores RIP
- FF02::B Mobile-Agents
- FF02::D Todos los encaminadores PIM

[119] RFC 3306: Unicast-Prefix-based IPv6 Multicast Addresses

[120] RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

- FF02::1:2 Todos los DHCP-agents
- FF02::1:FFXX:XXXX Solicited-Node Address

Site-Local Scope:

- FF05::2 Todos los encaminadores
- FF05::1:3 Todos los DHCP-servers
- FF05::1:4 Todos los DHCP-relays

Variable Scope Multicast Addresses:

- FF0X::101 Network Time Protocol (NTP)
- FF0X::129 Gatekeeper
- FF0X::2:0000-FF0X::2:7FFD Multimedia Conference Calls
- FF0X::2:7FFE SAPv1 Announcements
- FF0X::2:8000-FF0X::2:FFFF SAP Dynamic Assignments

Direcciones Multicast Importantes

- FF01::1, FF02::1 → Todos los nodos
- FF01::2, FF02::2, FF05::2 → Todos los encaminadores

Dirección (SN) multicast a partir de la unicast:

- Si la dirección acaba en “XY:ZTUV”
- La SN es: FF02::1:FFXY:ZTUV

Cada nodo IPv6 debe unir la dirección SN a todas sus direcciones unicast y anycast.

9.3. Multicast Listener Discovery

MLD (RFC 2710[121]) permite que cada encaminador IPv6 aprenda que direcciones multicast hay con nodos que escuchan por ellas, en cada uno de los links a los que el encaminador está unido.

MLD es el equivalente IPv6 del Internet Group Management Protocol versión 2 (IGMPv2) para IPv4. Permite que los routers descubran, por cada interfaz conectada, el conjunto de direcciones multicast para las cuales existen nodos escuchando.

Esta es una función obligatoria en los nodos IPv6. En IPv6 se usa MLD en vez de IGMP.

Versión actual MLDv2: RFC 3810[122] e interopera con MLDv1. Soporta source-filtering pero requiere PIM-SSM.

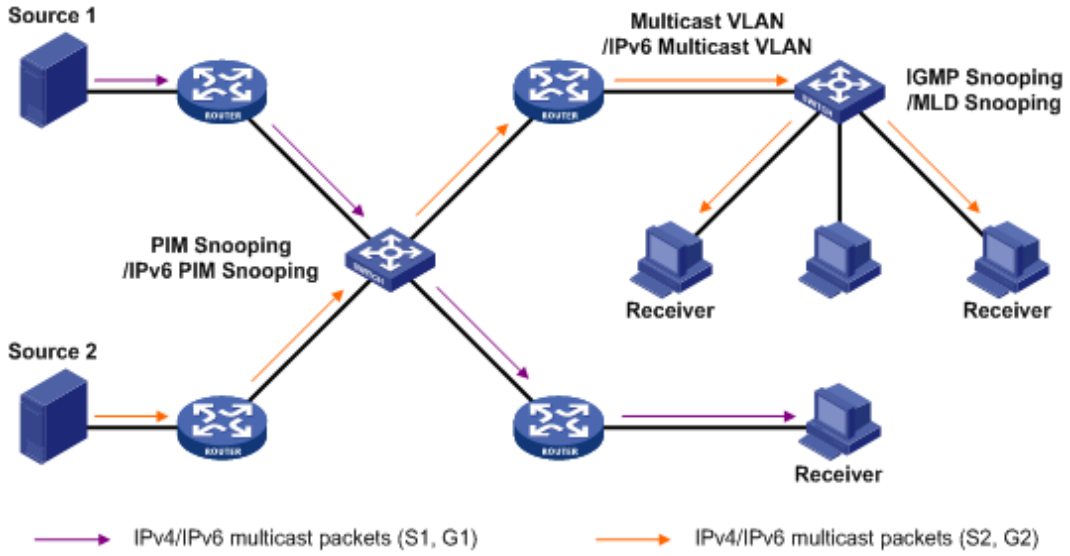


Ilustración 116. Protocolos Multicas de capa 2

La ***Ilustración 116***, muestra la posición de los protocolos de multidifusión de capa2. Los protocolos de multidifusión de capa 2 incluyen IGMP, MLD snooping, snooping PIM, spooping IPv6 PIM, VLAN multicast, IPv6 multicast y VLAN:

[121] RFC 2710: Multicast Listener Discovery (MLD) for IPv6
[122] RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IP

- IGMP snooping y MLD snooping. Son mecanismos multicast limitados que corren en dispositivos de capa 2. Gestionan y controlan los grupos de multidifusión por escucha y analizan mensajes IGMP o MLD intercambiados entre los host y los dispositivos de capa 3.
- PIM snooping IGMP y PIM IPv6. Corren en dispositivos de capa 2. Determinan qué puertos están interesados en los datos de multidifusión mediante el análisis de los mensajes recibidos IPV6 PIM, y añade los puertos a una entrada de reenvio de multidifusión para asegurar que los datos de multidifusión pueden ser enviados solo a los puertos que están interesados en los datos.
- Multicast VLAN y VLAN IPv6 multicast. Cuando la VLAN de multidifusión o multicast IPv6 VLAN esta habilitado en los dispositivos de capa 2, el dispositivo de capa 3 de multidifusión envía una sola copia de multicast a la VLAN de multidifusión o IPv6 multicast VLAN en el dispositivo de capa 2.

Internet Group Management Protocol Version 3 (IGMPv3) y Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source Specific Multicast: RFC 4604[123].

MLDv1 en IPv6 es equivalente a IGMPv2 en IPv4. MLDv2 en IPv6 es equivalente a IGMPv3 en IPv4, y funciona con PIM-SSM (PIM Source Specific Mode).

A diferencia de IGMP en IPv4, MLD usa ICMPv6 para enviar sus mensajes. Todos los mensajes MLD son locales al enlace con un hop-limit de 1.

[123] RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast

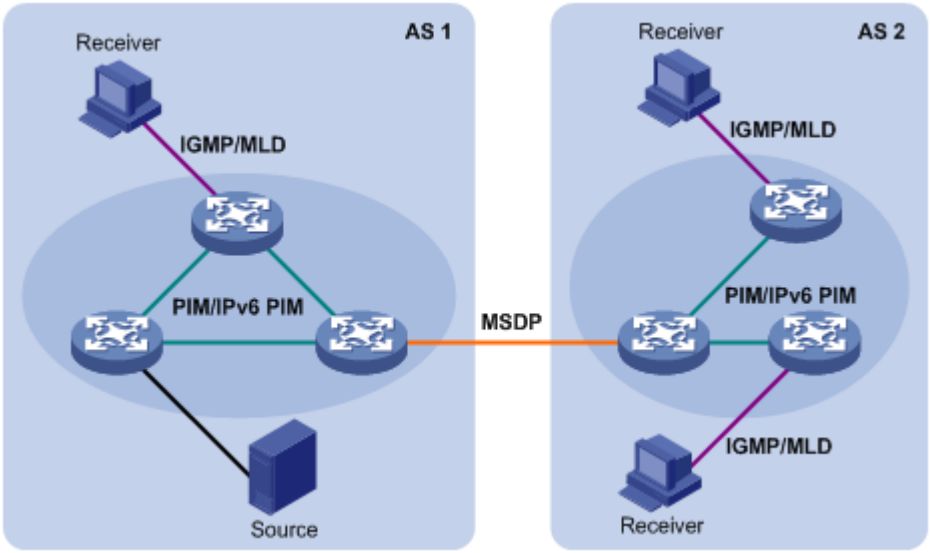


Ilustración 117. Protocolos Multicast de capa 3

En la ***Ilustración 117***, se muestra las posiciones de los protocolos muticast de capa3. Estos protocolos multicast de capa3 incluyen protocolos de manejo de grupos y protocolos de enrutamiento multicast.

La ***Ilustración 117*** describe estos protocolos de multidifusión en la red.

1. *Protocolo de gestión Multicast*

Por lo general, Internet Group Management Protocol (IGMP) se utiliza entre hosts y dispositivos de Capa 3 multicast conectado directamente con los host. Estos protocolos definen el mecanismo de establecimiento y mantenimiento de la pertenencia a grupos entre los hosts y dispositivos de Capa 3 de multidifusión.

2. *Protocolos de enrutamiento multicast*

Un protocolo de enrutamiento multicast se ejecuta en dispositivos de Capa 3 multicast para establecer y mantener las rutas de multidifusión y reenviar paquetes de multidifusión correcta y eficientemente. Las rutas de multidifusión constituyen un camino libre de bucles de transmisión de datos desde un origen de datos a múltiples receptores, es decir, un árbol de distribución multicast.

En el modelo ASM, las rutas de multidifusión vienen en rutas intra-dominio y rutas inter-dominio.

- En intra-dominio multicast el protocolo de enrutamiento se utiliza para descubrir las fuentes de multidifusión y construir árboles multicast de distribución dentro de un sistema autónomo (AS) con el fin de entregar los datos multicast a los receptores. Entre una variedad de protocolos de enrutamiento musticast intra-dominios, Protocol Independent Multicast (PIM) es muy popular. Basado en el mecanismo de reenvío, PIM se presenta en dos modos: modo denso (a menudo denominado como PIM-DM) y modo disperso (a menudo denominado como PIM-SM).
- Un protocolo de enrutamiento multicast inter-multicast, se utiliza para la entrega de información de multidifusión entre dos AS's. Hasta ahora, las soluciones incluyen al protocolo de descubrimiento de fuentes multicast (MSDP: multicast source discovery protocol).

Para el modelo de SSM, las rutas de multidifusión no se dividen en rutas inter-dominio y rutas intra-dominio. Dado que los receptores saben la posición de la fuente de multidifusión, los canales establecidos a través de PIM-SM son suficientes para el transporte de información de multidifusión.

Solo hay Tres tipos de mensajes ICMPv6:

- Query enviadas periódicamente por los encaminadores.
- Report, enviados por los nodos en respuesta a las peticiones de los encaminadores o cuando los nodos quieren unirse a un grupo multicast. Llevan información acerca de los grupos multicast que el nodo está interesado en recibir.
- Done para indicar que el nodo está interesado en abandonar un grupo multicast.

Mensajes MLD

1) Query (Type = decimal 130). El router consulta en la red para determinar los miembros en un grupo de host.

- General Query
  - El campo de la dirección multicast tiene el valor cero.
  - De esta forma el encaminador pregunta qué grupos multicast tienen participantes en la red local.
- Group Specific
  - El campo de la dirección multicast tiene la dirección multicast IPv6 específica.
  - De esta forma el encaminador pregunta si un grupo multicast específico tiene participantes en la red local.

2) Report (Type = decimal 131). Un host declara la membresía a un grupo de Host.

- El campo de la dirección multicast tiene la dirección multicast IPv6 específica en la que el nodo participante está interesado.

3) Done (Type = decimal 132). Un host declara que quizá no haya ningún otro miembro en un grupo de Host para una subred.

- El campo de la dirección multicast tiene la dirección multicast IPv6 específica en la que el nodo participante está interesado en abandonar.

9.4. Encaminamiento Multicast

Los protocolos de enrutamiento multicast hacer posible el intercambio de mensajes entre routers, el conjunto de árboles de distribución y la transmisión de paquetes de multidifusión. Enrutamiento multicast es diferente de enrutamiento IP estándar en varios aspectos. En primer lugar, la red se centra en el enrutamiento del tráfico desde el host de origen o hosts con el grupo receptor de los ejércitos. En segundo lugar, mientras que todos los hosts receptor comparten la misma dirección IP multicast grupo, que

puede ser arbitrariamente dispersos por toda la red. En tercer lugar, los receptores pueden unirse o dejar grupos multicast de forma arbitraria, también.

En la ***Ilustración 118***, se muestra una comparación de las transmisiones de unidifusión múltiples y las transmisioes de multidifusión. Con enrutamiento multicast, un router o switch envía paquetes a un gran grupo específico de host sin necesidad de utilizar emisiones de radio o multiples transmisiones unicast a como se muestra en la ***Ilustración 118***, y sin bucles de enrutamiento o transmisiones en exceso. Los destinos multicast pueden incluir host que residen en LAN locales, ordenadores que residen en diferentes sitios dentro de una red privada, o host que están dispersos por todo el internet.

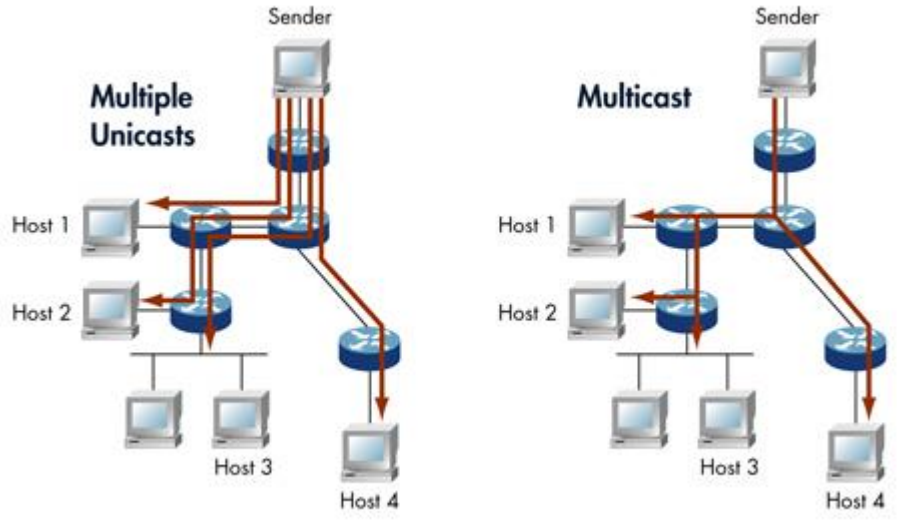


Ilustración 118. Comparación de las transmisiones de unidifusión múltiples y las transmisiones de multidifusión.

Los encaminadores escuchan todos los grupos. Los protocolos de construcción del árbol multicast son:

- Dense Mode: Adecuados para dominios densamente poblados.
  - DVMRP (Distance Vector Multicast Protocol)
  - PIM-DM (Protocol Independent Dense Mode)
  - MOSPF (Multicast Open Shortest Path First)

- Sparse Mode: Dominios no densamente poblados y dispersos.
    - CBT
    - PIM-SM
        - ASM, requiere un Rendez-vous Point (RP). Aplicaciones muchos-a-muchos. Multiples fuentes transmiten a múltiples participantes (mismo grupo (*,G)).
        - SSM, (PIM-SSM). Aplicaciones uno-a-muchos. Una única fuente transmite a muchos partipantes. (mismo grupo (S,G)). ASM y SSM peden usarse simultáneamente. Si se usa ASM, SSM va implícito puesto que es una sub-parte.
        - Bidir (PIM-Bidir). Aplicaciones muchos-a-muchos. Los miembros de un grupo pueden ser a la vez fuentes y receptores.

Se permiten túneles multicast sobre redes IPv6 unicast. En los protocolos de Encaminamiento Inter-Dominio Multicast, se usa MBGP cuando la topología de red unicast no es la misma que multicast:

- Construcción de túneles entre encaminadores separados por dominios no muliticast.

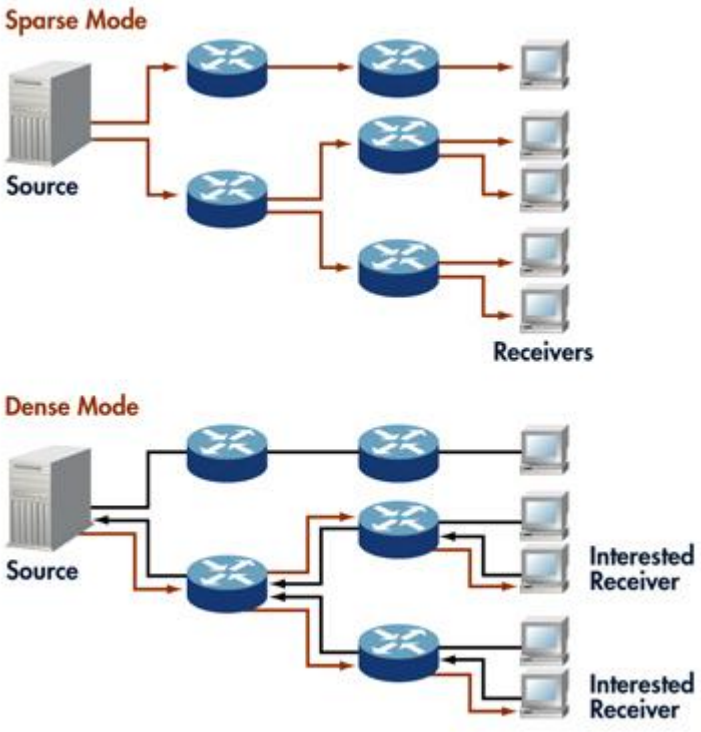


Ilustración 119. Diferencias entre los protocolos de multidifusión Dense Mode y Sparse Mode

En la ***Ilustración 119***, se muestra la diferencia en la transmisión de datos entre los procolos multicast Dense mode (modo denso) y Sparse mode (modo disperso). En el modo disperso, los paquetes de multidifusión se envían solo a los receptores que han manifestado su interes. En cambio, el modo denso funciona por inundación de paquetes de multidifusión en todas las direcciones, con base en el supuesto de que la red esta densamente poblada con receptores multicast que desean recibir estos paquetes.

Ámbitos Multicast y protocolos

- Ambito local
  - MLD en IPv6, equivalente a IGMP
- Intra-dominio
  - PIM-SM

- ASM
- SSM (PIM-SSM) (Requiere MLDv2)

- Inter-dominio
  - PIM-SM-ASM requiere Embedded RP (RFC3956[124]) para que todos los RP puedan contactar mutuamente
  - PIM-SSM no necesita nada especial para aplicaciones de una única fuente
  - MBGP necesario si la topología unicast difiere de la multicast.
    - Creación de túneles entre encaminadores separados por dominios sin soporte multicast

Escenario Básico Multicast IPv6

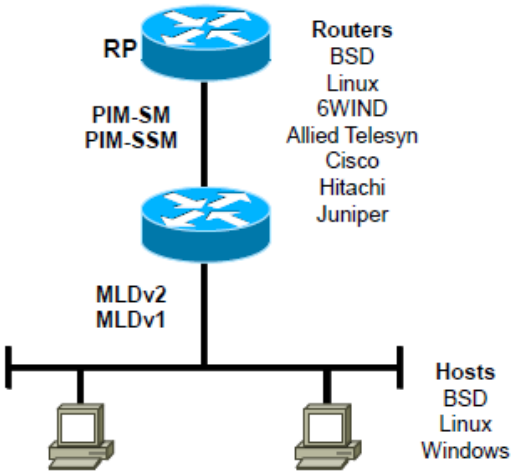


Ilustración 120. Escenario básico Multicast IPv6

En la ***Ilustración 120***, se muestran los elementos de una implementación punto a punto para la estructura SSM. Con el fin de utilizar el servicio de SSM, los host finales deben especificar una dirección de canal, que consiste en la dirección unicast de la fuente y una

[124] RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

dirección destino SSM. IGMPv2 y MLD versión 1 le permiten al host especificar sólo una dirección de multidifusión de destino.

La posibilidad de especificar una dirección de canal c de tipo SSM es proporcionada por IGMPv3 y MLD en su versión 2.

Escenarios Multicast IPv6

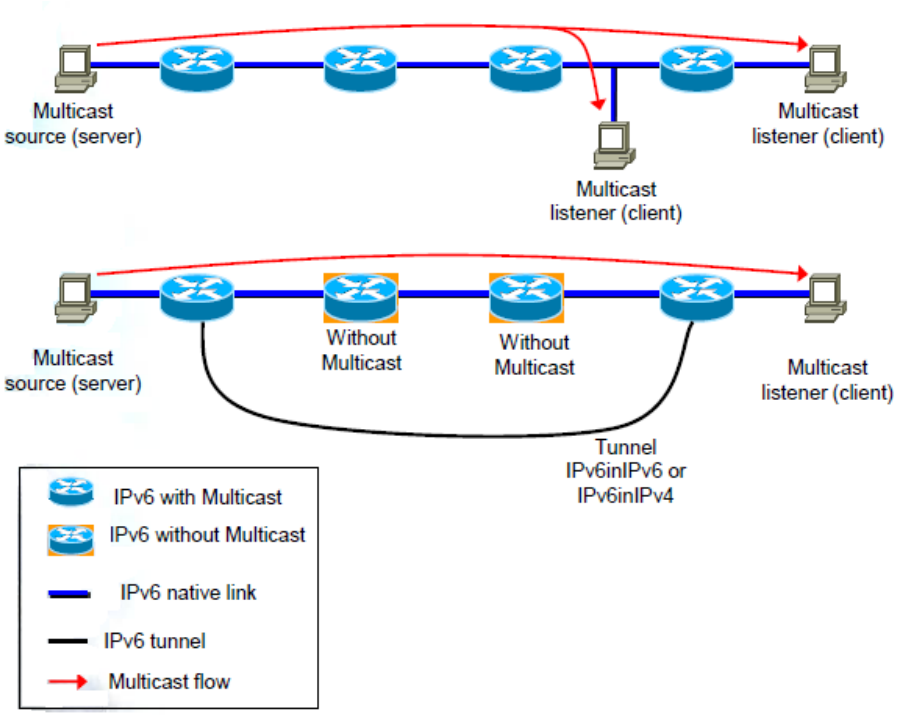


Ilustración 121. Escenario Multicast IPv6

9.5. PIM-ASM

Las acciones más importantes en PIM-ASM son:

- Registro de la fuente en el RP:
  - Es necesario registrar la fuente multicast en el RP antes de enviar paquetes multicast al grupo.

- El registro en el RP se hace a través de un túnel unidireccional entre el encaminador que alberga la fuente (Designated Router, DR) y el RP.
- El registro se hace encapsulando el trafico multicast y enviándolo por el túnel hasta el RP.
- El RP construye el (S,G) SPT enviando mensajes PIM Join.
- El RP avisa a la fuente del grupo (S,G), para detener la encapsulación del tráfico multicast, enviando mensajes de Register Stop.
- La fuente de (S,G) envía del trafico multicast hacia el RP vía el SPT entre ellos.

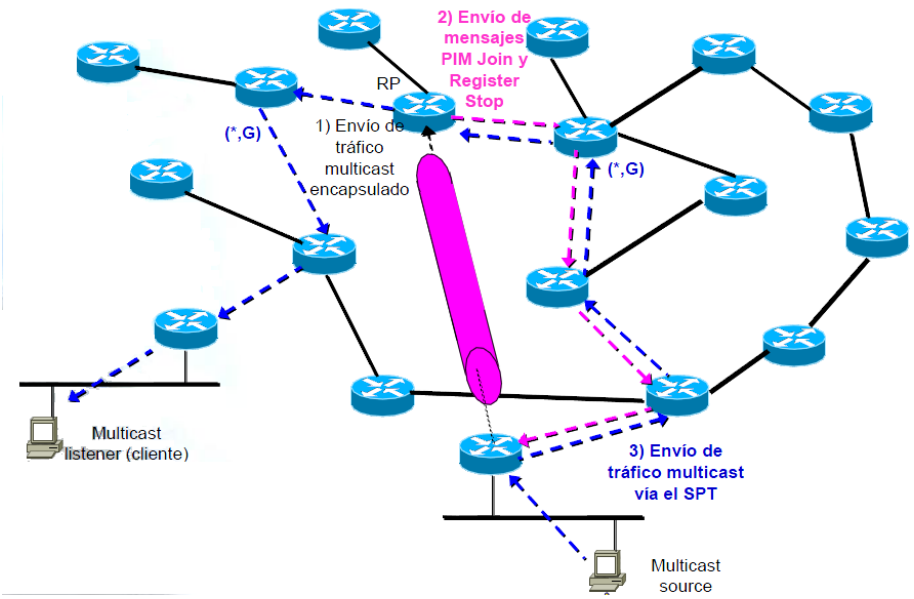


Ilustración 122. PIM-ASM: Registro de la fuente

- Unión del cliente (listener) al grupo multicast:
  - Una vez que el cliente expresa vía MLD su interés en unirse al grupo multicast (*,G), su DR envía mensajes PIM-SM Join al RP para construir el ST.
  - Una vez que los mensajes de PIM-SM llegan al RP, el tráfico multicast se envía por el ST recién construido.

- Cuando el tráfico multicast llega al DR, este extrae la fuente multicast y entonces puede enviar los mensajes PIM-SM join a la fuente para construir el SPT y recibir trafico vía el SPT más que por el ST.
    - Optimización de prestaciones.

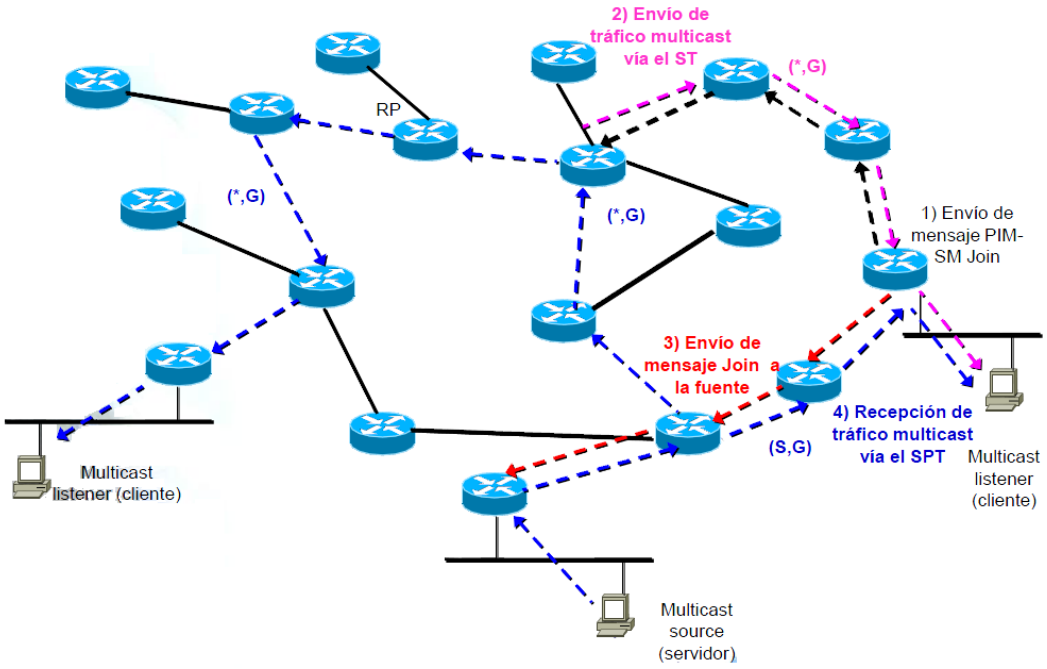


Ilustración 123. PIM-ASM: Unión del Cliente

La siguiente ***Ilustración 124*** es un ejemplo de distribución de un paquete multicast basado en el protocolo PIM-SM. En este ejemplo, cuando el origen multicast S envía un paquete multicast a un grupo particular, el primer salto del router R1 encapsula el paquete en un mensaje registrado PIM y lo reenvia al RP como un paquete unicast. El RP desencapsula el mensaje ***registrado*** (register) y reenvia el paquete multicast original a lo largo del arbol compartido a los host miembros que residen en la red..

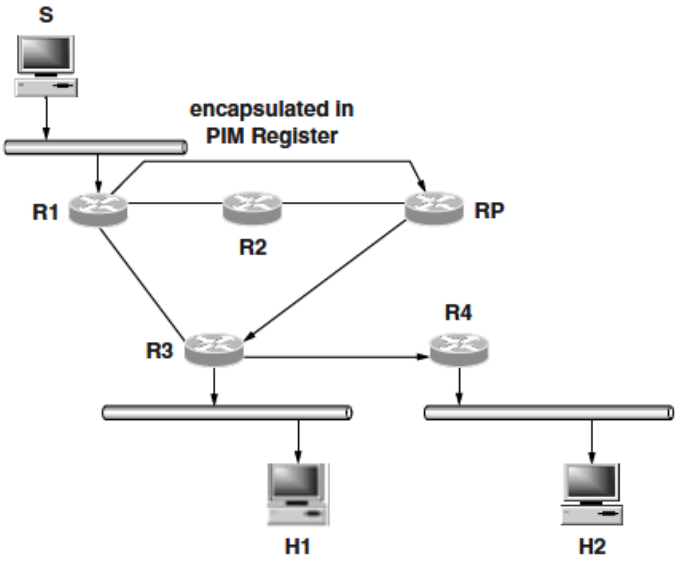


Ilustración 124. Esquema de distribución de paquetes PIM-SM

Por lo tanto: la forma escalable para hacer pim multicast es el modo Disperso (PIM-SM), y PIM-SM se requiere que haya al menos un RP.

RP Embebido

- RP en PIM-ASM se puede configurar manualmente.
- Embedded RP es otra opción en PIM-ASM para especificar el RP para un grupo multicast (*,G).
- Es un procedimiento para incluir la dirección IPv6 unicast del RP dentro de la dirección de un grupo multicast.
- Se basa en las direcciones del grupo multicast con un prefijo-unicast descrito en el RFC 3306[125].
    - Existen además algunas banderas que indican la presencia de la dirección del RP dentro de la dirección del grupo multicast.

[125] RFC 3306: "Unicast-Prefix-based IPv6 Multicast Addresses"

9.6. PIM-SSM

- Los clientes conocen información sobre el grupo y la fuente del grupo al que quieren unirse.
- El funcionamiento es similar al de PIM-SM cuando los clientes del DR envían mensajes de PIM-SM Join a la fuente para construir el SPT.
- No hay necesidad de un RP.
    - La implementación y la gestión es más sencilla.

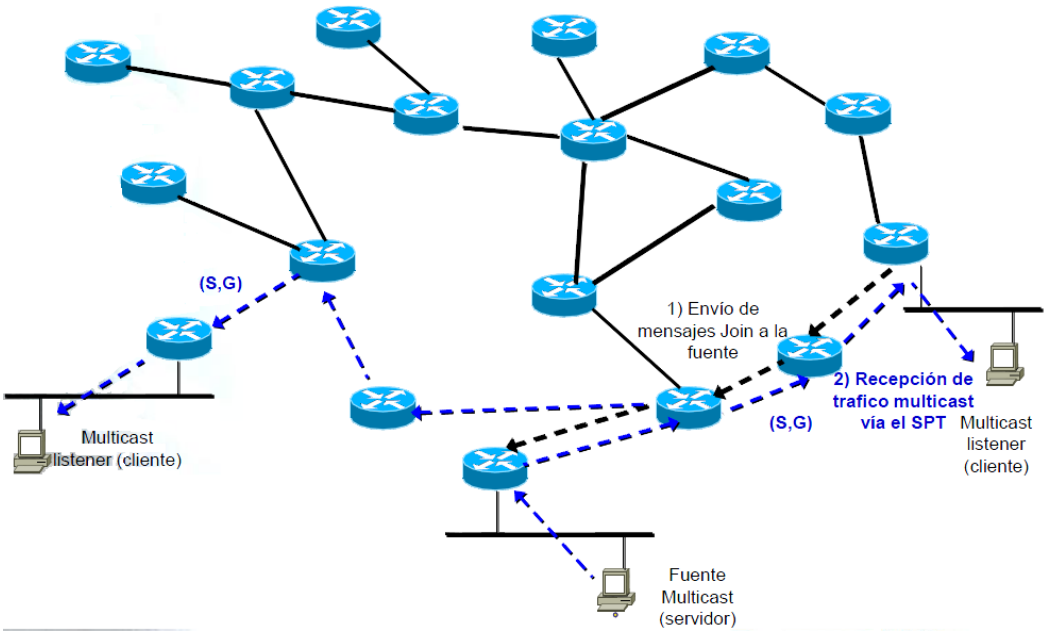


Ilustración 125. Funcionamiento de PIM-SSM

En el modelo de servicio SSM de la ***Ilustración 125***, un datagrama IP es transmitido por una fuente S a una dirección destino SSM llamada G, y los receptores pueden recibir este datagrama mediante la suscripción al canal (S, G). SSM proporciona a las aplicaciones host un "canal" de abstracción, en la que cada canal tiene exactamente una fuente y un numero de receptores.

9.7. Aspectos prácticos

Aplicaciones Multicast IPv6

- Beacon
- MAD FLUTE
- pcm6cast
- Freamp
- Windows Media Player
- VLC
- VIC, RAT, SDR, NTE, WBD
- VRVS (alfa)
- ISABEL
- Más Información http://www.m6bone.net
- Iperf

```
#./iperf -c ff16::2222 -u -V -T 5

------------------------------------------------------------

Client connecting to ff16::2222, UDP port 5001

Sending 1470 byte datagrams

Setting multicast TTL to 5

UDP buffer size: 110 KByte (default)

 ------------------------------------------------------------

[ 3] local 2001:db8::2115 port 32768 connected with ff16::2222 port 5001

[ ID] Interval Transfer Bandwidth

[ 3] 0.0-10.0 sec 1.25 MBytes 1.05 Mbits/sec

[ 3] Sent 893 datagrams (none):/usr/apps/iperf #

[pc2 iperf]# ./iperf -s -u -B ff16::2222 -V -T 5
```

```
------------------------------------------------------------

Server listening on UDP port 5001

Binding to local address ff16::2222

Joining multicast group ff16::2222

Receiving 1470 byte datagrams

UDP buffer size: 64.0 KByte (default)

------------------------------------------------------------
```

- ssmping/ssmpingd[126]
  - Verifica si hay conectividad SSM entre dos hosts IPv4/IPv6
  - Se ejecuta "ssmping <host>“, entonces ssmping se une a la dupla (S,G) donde (hosts,ff3e::4321:1234)

```
[consulintel@lacnic ssmping-0.6]$ ./ssmping -6 -I eth0 -c 50
2001:800:40:2b18:2b0:d0ff:fe16:76fc

ssmping joined (S,G) = (2001:800:40:2b18:2b0:d0ff:fe16:76fc,ff3e::4321:1234)

pinging S from 2001:1820:1a::2

unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=0 dist=10 time=164.701 ms

unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=1 dist=10 time=173.912 ms

multicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=1 dist=5 time=174.710 ms

unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=2 dist=10 time=193.795 ms
```

[126] http://www.venaas.no/multicast/ssmping/

```
multicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=2 dist=5 time=195.473 ms

[consulintel@lacnic ssmping-0.6]$ ./ssmping -6 -I eth0 -c 50
2001:800:40:2a0a:2c0:26ff:fe50:2115 ssmping joined (S,G) =
(2001:800:40:2a0a:2c0:26ff:fe50:2115,ff3e::4321:1234)

pinging S from 2001:1820:1a::2

unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=0 dist=9 time=163.997 ms

unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=1 dist=9 time=161.113 ms

multicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=1 dist=4 time=162.104 ms

unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=2 dist=9 time=161.357 ms

multicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=2 dist=4 time=161.898 ms
```

10. SERVICIOS IPV6

10.1. DNS

Introducción

Se definieron varios elementos para dar soporte IPv6 al DNS:

- Para resolución directa RRs: AAAA y A6
- Para resolución inversa: dominios IP6.INT e IP6.ARPA, DNAME y PTR RR, además de las notaciones nibble y bit-string

Nos centraremos en los elementos usados hoy en día (RFC 3596[127]):

- AAAA
- IP6.ARPA
- PTR
- Notación con nibbles (4 bits en hex)

DNS IPv6: Transporte vs. Contenido

[127] RFC 3596: DNS Extensions to Support IP Version 6

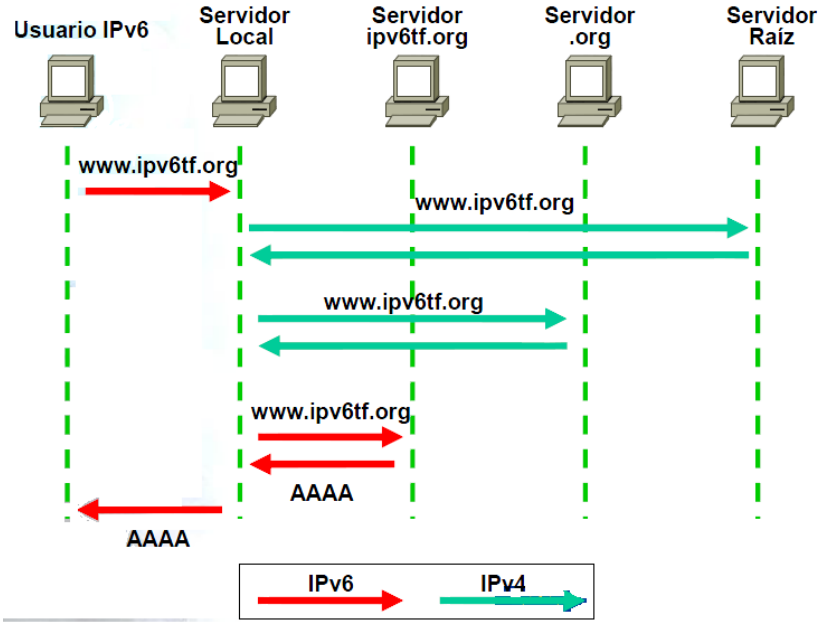


Ilustración 126. Diferencia entre DNSv6 modo transporte y contenido

DNS IPv6: Recomendaciones

- IPv4 e IPv6 coexistirán, 3 tipos de servidores:
  - Solo IPv4 -> alcanzable sólo por IPv4
  - Solo IPv6 -> alcanzable sólo por IPv6
  - Doble-pila -> alcanzable por ambos
- Evitar la fragmentación del espacio de nombres: el proceso de resolución recursiva se rompe (e.g. cuando solo un NS IPv6 es autoritativo para un dominio, resultando que un servidor DNS solo IPv4 no podrá seguir la cadena de resolución).
- IDEA: compatibilidad hacia atrás.
- Políticas administrativas (RFC 3901[128])
  - Todo servidor recursivo debe ser solo IPv4 o doble-pila.

[128] RFC 3901: DNS IPv6 Transport Operational Guidelines

- Toda zona DNS debe ser servida al menos por un servidor autoritativo alcanzable sobre IPv4.

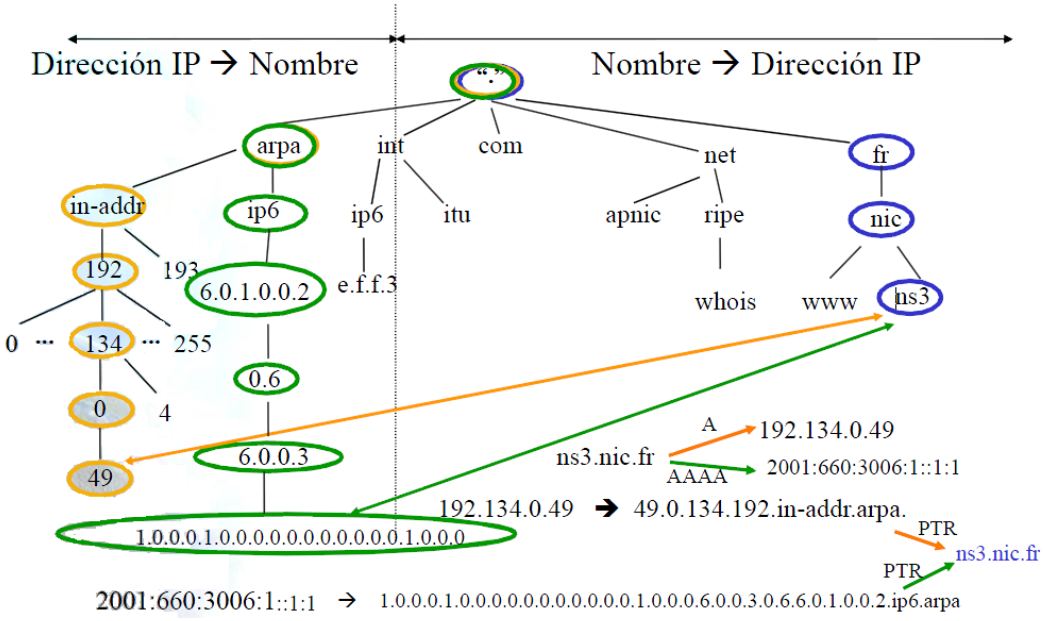


Ilustración 127. DNS IPv6: Ejemplo

DNS IPv6: Estado actual

- ***Clientes***: Buen soporte DNS IPv6
- ***Servidores***: Muy buen soporte: BIND, nsd, newbie, maradns and djbdns.
- Implantación extendida a nivel TLD (.fr, .uk, .jp, etc.), desde Julio 2004 con el anuncio de ICANN[129] sobre el soporte de direcciones IPv6 en los servidores raíz, muchos TLDs lo han añadido.
- ***Servidores Raíz*** (8/13)(root zone 2010061700) implantación actualmente en curso. Se hizo el anuncio y desde el 4 de Febrero de 2008 son alcanzables por IPv6.

[129] http://www.icann.org/

10.2. Configuracion de IPv6 en Servidores

Existen muchos servicios que se pueden ofrecer usando IPv6: FTP, SSH, NTP, Telnet, HTTP, DNS, Streaming, etc.

Aquí se abordara los más utilizados: HTTP y DNS.

Nos centraremos en la aplicación del servicio y su soporte IPv6 sobre Linux. Un paso previo será habilitar IPv6 en la plataforma del servidor.

Servidor Web

Los servidores web más utilizados y su plataforma de implementación natural son:

- Apache (http://httpd.apache.org) sobre Linux
- IIS (Internet Information Services) de Microsoft sobre Windows.

Apache

1. Para la instalacion se pueden utilizar los sistemas habituales de cada distribución (atp-get install apache2, yum, up2date, rmp, etc) o descargarse los fuentes desde: http://httpd.apache.org y compilarlo:

```
#>cd /usr/local/src
#>tar –xzvf httpd-2.2.21.tar.gz
#>cd httpd-2.2.21
#>./configure --prefix=/usr/local/apache2 --enable-module=so
#>make
#>make install
```

El parámetro --prefix indica la carpeta en la que se hará la instalación. El parámetro --enable-module=so habilita el soporte de Dynamic Shared Object (DSO) para poder cargar dinámicamente módulos, por ejemplo PHP.

Apache 2.0.X+ soporta IPv6 habilitado por defecto. Después de instalarlo solo hay que iniciarlo para que escuche por IPv6 (soporte IPv6 previamente configurado en el servidor).

2. La directiva que controla las IPs y puertos por los que escucha el servidor web es **Listen**, en **httpd.conf.** (en nuestros ejemplos /etc/apache2/**apache2.conf** que incluye /etc/apache2/ports.conf). Por defecto escucha por todas las IPs y el puerto 80 (http): Listen 80.

3. Ahora se procederá a configurar Apache (2.2.14) las direcciones IPv4 e IPv6 sobre Ubuntu 10.04 LTS (kernel 2.6.32). Para ello crear las carpetas necesarias:

```
#>cd /usr/local/apache2/htdocs
#>sudo mkdir example
#>sudo mkdir example/ipv6-web
#>sudo mkdir example/ipv4-ipv6-web
#>sudo cp index.html example/ipv6-web/
#>sudo cp index.html example/ipv4-ipv6-web/
```

4. Editar cada index.hmtl para que sean distintos

5. Para la resolución de los nombres se puede usar un servidor DNS local o /etc/hosts:

```
192.168.1.50  www.example.com
2001:db8:1::1000:1234  www.example.com
2001:db8:1::1000:1234  ipv6.example.com
```

6. En los ***Host virtuales IPv6*** se usan corchetes [] para "encerrar" la dirección IPv6 en httpd.conf. Crear /etc/apache2/sites-available/ipv4-ipv6-web con:

```
NameVirtualHost  [2001:db8:1::1000:1234]
NameVirtualHost  10.0.0.3
```

```
<VirtualHost  [2001:db8:1::1000:1234]>
   DocumentRoot  /var/www/example/ipv4-ipv6-web
   ServerName www.example.com
   ErrorLog /var/log/apache2/error.log
   CustomLog /var/log/apache2/access.log combined
</VirtualHost>
<VirtualHost 10.0.0.3>
   DocumentRoot  /var/www/example/ipv4-ipv6-web
   ServerName www.example.com
   ErrorLog /var/log/apache2/error.log
   CustomLog /var/log/apache2/access.log combined
</VirtualHost>
<VirtualHost  [2001:db8:1::1000:1234]>
   DocumentRoot  /var/www/example/ipv6-web
   ServerName ipv6.example.com
   ErrorLog /var/log/apache2/error.log
   CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

La configuración anterior permite al servidor:

- Atender peticiones sobre IPv4 a la dirección 10.0.0.3 y sobre IPv6 a la dirección `2001:db8:1::1000:1234`
- Las peticiones recibidas a esas direcciones se distinguen por la URL a la que van dirigida, por eso:
    - Las peticiones a www.example.com se atienden por IPv4 e IPv6, sirviendo el contenido de la carpeta /var/www/example/ipv4-ipv6-web
    - Las peticiones a ipv6.example.com se atienden por Ipv6 solamente, sirviendo el contenido de la carpeta /var/www/example/ipv6-web

7. Deshabilitar el sitio por defecto y habilitar el nuevo:

```
#>sudo a2ensite ipv4-ipv6-web
```

```
#>sudo a2dissite default

#>sudo /etc/init.d/apache2 reload
```

8. Para comprobar que todo funciona bien se puede utilizar lynx (sudo apt-get install lynx):

```
#sudo lynx ipv6.example.com

#sudo lynx www.example.com
```

9. Para comprobar como se accede al apache:

```
#sudo tail –f /var/log/apach2/access.log
```

10. Para comprobar que esta escuchando IPv6 en el puerto 80, ejecutar el siguiente comando desde una terminal linux:

```
[root]# netstat –tan
Active Internet connections (server and established)
Proto  Recv-Q  Send-Q  Local Address  Foreign Address  State
…
tcp      0        0      :::80             :::*        LISTEN
```

La salida anterior indica que esta eschando (LISTEN) en cualquier dirección (::) del servidor, ya sea IPv4 o IPv6, por el puerto 80(:80).

11. Para ***mostrar dirección IPv6/IPv4 del cliente***, introducir en la pagina inicial, por ejemplo index.php, el siguiente código:

```
<?php if(strpos($_SERVER['REMOTE_ADDR'], ".") == false)
{
   echo "<font color='#154983' size=2 face='verdana'>Esta usando IPv6
(".$_SERVER['REMOTE_ADDR']).</font><br><br>";
}else{
   $DIRv4=str_replace("::ffff:","",$REMOTE_ADDR);
```

```
   echo "<font color=='#FF0000' size=2 face='verdana'>Esta usando IPv4
("."$_SERVER['REMOTE_ADDR']."").</font><br><br>";
}
?>
```

12. **Desabilitar sendfile**: Apache 2 soporta un método llamado **sendfile** ofrecido por el sistema operativo que acelera el servir datos. Algunos controladores de tarjetas de red también soportan hacen TCP-checkums offline.

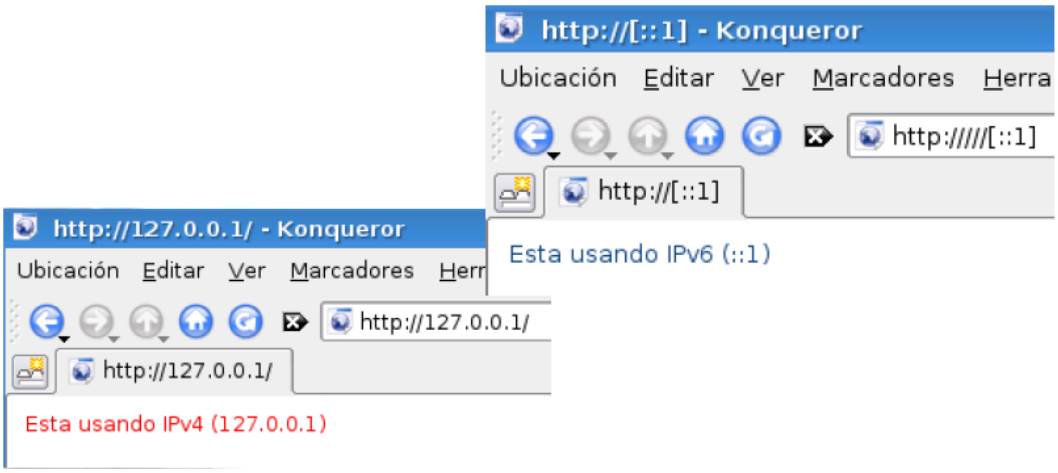
    Esto puede dar problemas de conexión y checksums TCP inválidos para tráfico IPv6.

    Para desahilitar sendfile hay que:

    - Recompilar el servidor usando la directiva: opción **–without-sendfile**
    - Usar **EnableSendfile off** en httpd.conf

    La directiva EnableSendfile off solo se soporta en versiones posteriores a la 2.0.44.

13. Finalmente se puede ***comprobar que todo esta bien*** desde un navegador en el propio servidor. Para ello se pueden utilizar las direcciones de localhost IPv4 (127.0.0.1) e IPv6 (::1) a como se muestra en las siguientes imágenes:



DHCP

- ***Instalación del servidor DHCP***

Para instalar los archivos necesarios de nuestro servidor DHCP podemos utilizar apt-get desde una consola de root:

// Instalación del servidor DHCP

 # apt-get install dhcp3-server

De esta forma instalaríamos los programas necesarios para disponer de nuestro propio servidor DHCP.

- ***Configuración del servidor DHCP***

Debido a que un servidor DHCP proporciona direcciones IP y otros parámetros a los clientes DHCP de forma que su configuración se puede determinar de manera automática sin tener que hacerlo manualmente lo cual es especialmente útil cuando el número de PCs de nuestra red local es grande.

El servidor DHCP deberá saber qué rangos de direcciones IP puede 'alquilar' y qué parámetros adicionales (puerta de enlace, servidores DNS, etc...) debe proporcionar a los clientes para que la configuración de los mismos sea completa y sea la deseada.

Una configuración TCP/IP mínima debe contener al menos la dirección IP y la máscara de subred, por lo tanto, esos son los dos mínimos datos que un servidor DHCP puede proporcionar a un cliente, no obstante, un servidor DHCP suele proporcionar muchos más parámetros:

- Dirección IP
- Máscara de subred
- Dirección de difusión o broadcast
- Puerta de enlace
- Servidores DNS, etc...

Además, existen una serie de parámetros que definen las condiciones del 'alquiler' o cesión de la configuración IP hacia un cliente como son:

- Tiempo de cesión por defecto

- Tiempo de cesión máximo, y algunos parametros más.

Esta información compone la configuración del servidor DHCP.

- ***Archivo de configuración del servidor DHCP***

Al igual que todas las aplicaciones en Linux, el servidor DHCP dispone de su propio archivo de configuración. Se trata del archivo:

```
// Archivo de configuración del servidor DHCP
/etc/dhcp3/dhcpd.conf
```

Este archivo de configuración consta de una primera parte principal donde se especifican los parámetros generales que definen el 'alquiler' y los parámetros adicionales que se proporcionarán al cliente.

El resto del archivo de configuración consta de una serie de secciones que especifican principalmente rangos de direcciones IPs que serán cedidas a los clientes que lo soliciten (sección subnet) y especificaciones concretas de equipos (sección host). Los parámetros de las secciones deberán ir entre llaves '{' y '}'.

Los valores de los parámetros especificados al principio del archivo se aplican como valores por defecto al resto de secciones aunque si dentro de una sección se redefine alguno de los parámetros, se aplicará éste ignorándose el valor por defecto.

Los rangos de direcciones IP se especifican en secciones que empiezan con la palabra clave 'subnet' seguido de la dirección de red de la subred, continua con la palabra 'netmask' seguido de la máscara de red.

A continuación estará la lista de parámetros para dicha sección encerrados entre llaves.

Ejemplo, supongamos que en nuestra red local disponemos de direcciones pertenecientes a la subred 192.168.1.0/24 (/24 significa máscara de subred 255.255.255.0 ó lo que serían 24 'unos' en binario) y deseamos que nuestro servidor DHCP alquile direcciones del rango comprendido entre la dirección 192.168.1.50 y 192.168.1.100. La sección subnet que debemos crear será:

```
// Rango de cesión
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.50 192.168.1.100;
}
```

Si además de proporcionar al cliente la dirección IP y la máscara deseamos que le proporcione también la dirección de la puerta de enlace y las direcciones de dos servidores DNS para que pueda navegar por Internet, la sección subnet que debemos crear será:

```
// Rango de cesión y parámetros adicionales
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.254;
option domain-name-servers 80.58.0.33, 80.58.32.97;
range 192.168.1.60 192.168.1.90;
}
```

Existe la posibilidad de establecer una configuración concreta a un cliente concreto identificándolo por la dirección MAC de su tarjeta de red. Recordemos que la dirección MAC (MAC address) es un número único, formado por 6 octetos, grabado en la memoria ROM de las tarjetas de red ethernet y viene fijado de fábrica.

Se suelen escribir los 6 octetos en hexadecimal separados por dos puntos ':'. Todas las tarjetas de red tienen una dirección MAC única en el mundo. Es como un número de serie. Los tres primeros octetos indican el fabricante y los tres siguientes el número de serie en fabricación.

Para establecer una configuración de equipo es necesario crear una sección host. Ejemplo, si deseamos que el cliente cuya dirección MAC sea 00:0c:29:c9:46:80 se configure siempre (reserva de dirección IP) con la dirección IP 192.168.1.40 y puerta de

enlace 192.168.1.254, que su nombre de dominio sea "maestria.com" y el servidor de nombres netbios sea "192.168.1.250" la sección host que debemos crear será:

```
// Crear una reserva de dirección IP
host Profesor5 {
hardware ethernet 00:0c:29:c9:46:80;
fixed-address 192.168.1.40;
option routers 192.168.1.254;
option domain.name "maestria.com";
option netbios-name-servers 192.168.1.250;
}
```

Cuando el PC cuya dirección MAC sea '00:0c:29:c9:46:80' solicite una dirección IP al servidor DHCP, recibirá la 192.168.1.40.

- ***Archivo dhcpd.conf comentado***

A continuación se muestra un sencillo archivo dhcpd.conf: (Todas las líneas que comienzan por almoadilla (#) son líneas de comentarios y son ignoradas por el servidor dhcp. Todas las líneas que especifican parámetros deben terminar en punto y coma ';')

```
// Ejemplo de archivo dhcp.conf
# Sample configuration file for ISC dhcpd for Debian
# $Id: dhcpd.conf,v 1.4.2.2 2002/07/10 03:50:33 peloy Exp $
# Opciones de cliente y de dhcp aplicables por defecto a todas las secciones
# Estas opciones pueden ser sobreescritas por otras en cada sección
option domain-name-servers 195.53.123.57; # DNS para los clientes (atenea)
option domain-name "maestria.com"; # Nombre de dominio para los clientes
```

```
option subnet-mask 255.255.255.0; # Máscara por defecto para los clientes
default-lease-time 600; # Tiempo en segundos del 'alquiler'
max-lease-time 7200; # Máximo tiempo en segundos que durará el 'alquiler'
# Especificación de un rango
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.50 192.168.1.100; # Rango de la 50 a la 100 inclusive
option broadcast-address 192.168.1.255; # Dirección de difusión
option routers 192.168.1.254; # Puerta de enlace
option domain-name-servers 80.58.0.33; # DNS (ej: el de telefónica)
default-lease-time 6000; # Tiempo
}
# Configuración particular para un equipo
host aula5pc6 {
hardware ethernet 00:0c:29:1e:88:1d; # Dirección MAC en cuestión
fixed-address 192.168.1.59; # IP a asignar (siempre la misma)
}
```

- ***Arranque y parada manual del servidor DHCP***

El servidor DHCP, al igual que todos los servicios en Debian, dispone de un script de arranque y parada en la carpeta /etc/init.d.

// Arrancar el servidor DHCP

root@maestria-desktop:/# /etc/init.d/dhcp3-server start

// Parar el servidor DHCP

root@maestria-desktop:/# /etc/init.d/dhcp3-server stop

// Reiniciar el servidor DHCP

root@maestria-desktop:/# /etc/init.d/dhcp3-server restart

Bind9

- ***Instalación del servidor DNS***

La aplicación que hace de servidor DNS en Linux se denomina **bind9**. Para instalarla, podemos hacerlo con apt-get desde una consola de root:

```
// Instalación del servidor DNS
# apt-get install bind9
```

De esta forma instalaríamos los programas necesarios para disponer de un servidor DNS. Tan solo será necesario configurarlo y ponerlo en marcha.

- ***Configuración del servidor DNS***

El servidor DNS admite tres modos de funcionamiento

- Servidor DNS maestro
- Servidor DNS esclavo
- Servidor caché DNS

Servidor DNS maestro

En este modo de funcionamiento, nuestro servidor se comporta como un auténtico servidor DNS para nuestra red local. Atenderá directamente a las peticiones de resolución de direcciones pertenecientes a la red local y reenviará a servidores DNS externos las peticiones del resto de direcciones de Internet.

Servidor DNS esclavo

Un servidor esclavo actuará como un servidor espejo de un servidor DNS maestro. Permanecerá sincronizado con el maestro. Se utilizan para repartir las peticiones entre varios servidores aunque las modificaciones solo se realicen en el maestro. En redes

locales salvo por razones de disponibilidad, es raro que exista la necesidad de tener dos servidores DNS ya que con uno será suficiente.

Servidor caché DNS

En este modo de funcionamiento, nuestro servidor se comporta como si fuera un auténtico servidor DNS para nuestra red local aunque realmente no sea un servidor DNS propiamente dicho. Cuando recibe una petición de DNS por parte de un cliente de nuestra red, la trasladará a un DNS maestro que puede estar en nuestra red o fuera, almacenará en una memoria caché la respuesta y a la vez la comunicará a quien hizo la petición. Si un segundo cliente vuelve a realizar la misma petición, como nuestro servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet.

Disponer de un servidor caché DNS en nuestra red local aumenta la velocidad de la conexión a Internet pues cuando navegamos por diferentes lugares, continuamente se están realizando peticiones DNS. Si nuestro caché DNS almacena la gran mayoría de peticiones que se realizan desde la red local, las respuestas de los clientes se satisfarán prácticamente de forma instantánea proporcionando al usuario una sensación de velocidad en la conexión.

Es un modo de funcionamiento de sencilla configuración ya que prácticamente lo único que hay que configurar son las direcciones IP de un DNS primario y de un DNS secundario. Muchos routers ADSL ofrecen ya este servicio de caché, tan solo hay que activarlo y configurar una o dos IPs de servidores DNS en Internet. En los PCs de nuestra red local podríamos poner como DNS primario la IP de nuestro router y como DNS secundario una IP de un DNS de Internet.

- ***Archivos de configuracion del DNS***

El archivo de configuración del DNS es el archivo **/etc/bind/named.conf**, pero este hace referencia a otros cuantos archivos como por ejemplo:

Archivo Descripción

named.conf Archivo principal de configuración

named.conf.options Opciones genéricas

named.conf.local Especificación particular de este servidor DNS

db.127 Especificación dirección de retorno

db.root DNSs de nivel superior

otros db.0, db.255, db.empty, db.local, rndc.conf, rndc.key, zones.rfc1918

- ***Configuración como caché DNS***

Por defecto, al instalar el paquete bind está preconfigurado como servidor caché DNS. Tan solo será necesario editar el archivo **/etc/bind/named.conf.options** y en la sección forwarders añadir las IPs de dos servidores DNS donde redirigir las peticiones DNS:

```
// Configuración como caché DNS
// Añadir IPs de los DNS de nuestro proveedor en /etc/bind/named.conf.options
forwarders {
        80.58.0.33; 80.58.32.97;
};
```

- ***Configuración DNS maestro***

Por razones de accesibilidad y organizativas, deseamos asignar un nombre a todos los equipos de nuestra red, para lo que instalaremos un servidor DNS privado con un **dominio ficticio**, por ejemplo 'maestria.com'. Todos los PCs de nuestra red pertenecerán a dicho dominio ficticio que funcionará solo en nuestra red interna, no en Internet. En tal caso el nombre completo de los PCs terminará con 'maestria.com', por ejemplo: aula5pc2.maestria.com. Lo ideal en una situación así es disponer de un servidor DNS que sea maestro de nuestro dominio, es decir, maestro del dominio interno 'maestria.com'.

Nuestro servidor DNS maestro para nuestro dominio ficticio interno 'maestria.com' será capaz de resolver peticiones internas de nombres de este dominio, tanto de forma directa como de forma inversa, es decir, si recibe una consulta acerca de quién es

aula5pc7.maestria.com deberá devolver su IP, pongamos por ejemplo 192.168.0.107. Si la consulta es una consulta DNS inversa acerca de quién es 192.168.0.107, deberá responder aula5pc7.maestria.com. Por ello deberemos añadir en el archivo **/etc/bind/named.conf.local** la especificación de maestro para el dominio y para la resolución inversa, por ejemplo:

```
// Añadir en /etc/bind/named.conf.local
// Archivo para búsquedas directas
zone "maestria.com" {
        type master;
        file "/etc/bind/maestria.db";
};
// Archivo para búsquedas inversas
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.rev";
};
```

Evidentemente será necesario crear los archivos maestria.db y 192.rev que especificarán la asociación entre nombres y direcciones IP de nuestra red en un sentido y en otro respectivamente.

- ***Archivo de zona de búsqueda directa***

Supongamos que en nuestra red local tenemos un aula llamada aula5 con 12 PCs con IPs que van desde la 192.168.0.101 hasta 112 y cuyos nombres van desde aula5pc1 hasta aula5pc10, luego un servidor web (pc11) y un servidor de correo electrónico que además es servidor DNS (pc12). El archivo de configuración DNS de nuestro dominio podría ser así:

```
// Archivo /etc/bind/maestria.db
;
; BIND data file for maestria.com
;
```

```
@ IN SOA maestria.com. root.maestria.com. (
                1 ; Serial
                604800 ; Refresh
                86400 ; Retry
                2419200 ; Expire
                604800 ) ; Default TTL
IN NS dns.maestria.com.
IN MX 10 mail.maestria.com.
aula5pc1 IN A 192.168.0.101
aula5pc2 IN A 192.168.0.102
aula5pc3 IN A 192.168.0.103
aula5pc4 IN A 192.168.0.104
aula5pc5 IN A 192.168.0.105
aula5pc6 IN A 192.168.0.106
aula5pc7 IN A 192.168.0.107
aula5pc8 IN A 192.168.0.108
aula5pc9 IN A 192.168.0.109
aula5pc10 IN A 192.168.0.110
www IN A 192.168.0.111
dns IN A 192.168.0.112
mail IN A 192.168.0.112
```

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y periodos de actuación). Las dos siguientes líneas indican quién es el servidor primario (NS = Name Server) y quien procesa el correo electrónico del dominio (MX = Mail eXchange). Las siguientes líneas especifican las IPs de los distintos PCs componentes del dominio (A = Address).

Si olvidamos algún punto y coma, dará errores y no funcionará correctamente. Para revisar los archivos disponemos de los comandos named-checkconf y named-checkzone que analizan que esté correcta la sintaxis de los mismos.

- ***Archivo de zona de búsqueda inversa***

Para poder realizar consultas inversas (de IP a nombre) será necesario crear el siguiente archivo:

```
// Archivo /etc/bind/192.rev
;
; BIND reverse data file for 192.168.0.0
;
@ IN SOA maestria.com. root.maestria.com. (
                        1 ; Serial
                        604800 ; Refresh
                        86400 ; Retry
                        2419200 ; Expire
                        604800 ) ; Default TTL
IN NS dns.maestria.com.
101 IN PTR  aula5pc1.maestria.com.
102 IN PTR  aula5pc2.maestria.com.
103 IN PTR  aula5pc3.maestria.com.
104 IN PTR  aula5pc4.maestria.com.
105 IN PTR  aula5pc5.maestria.com.
106 IN PTR  aula5pc6.maestria.com.
107 IN PTR  aula5pc7.maestria.com.
108 IN PTR  aula5pc8.maestria.com.
109 IN PTR  aula5pc9.maestria.com.
110 IN PTR  aula5pc10.maestria.com.
111 IN PTR  www.maestria.com.
112 IN PTR dns.maestria.com.
112 IN PTR mail.maestria.com.
```

Una vez configurado nuestro servidor DNS, debemos indicar a nuestro servidor Linux que el servidor DNS es él mismo, lo cual se especifica en el archivo **/etc/resolv.conf**.

```
// Indicamos que nosotros mismos somos servidores DNS
```

```
// y por defecto buscamos en nuestro dominio
// Editar /etc/resolv.conf del servidor DNS
nameserver 127.0.0.1
search maestria.com
```

En el resto de PCs de la red, indicaremos que el servidor DNS es 192.168.0.112

```
// En el resto de PCs de la red indicamos quién es el DNS
// Editar /etc/resolv.conf del resto de PCs de la red
nameserver 192.168.0.112
```

Tan solo nos faltará poner en marcha nuestro servidor de nombres ejecutando en el servidor el script de inicio correspondiente:

// Arranque del servidor DNS

 # /etc/init.d/bind9 restart

- ***Configuración DNS esclavo***

Si deseamos configurar nuestro servidor DNS para qué actúe como esclavo de un servidor DNS maestro, la configuración es mucho más sencilla que en el caso anterior ya que únicamente será necesario indicar en el DNS esclavo quién es el servidor DNS maestro, y en el DNS maestro, la IP del DNS esclavo.

Ejemplo, supongamos que el nombre del DNS maestro es dns.maestria.com (IP 192.168.0.112) y que el nombre del DNS esclavo es dns2.maestria.com. En el archivo 'maestria.db' de zona de búsqueda directa añadiremos la línea del segundo dns justo debajo de donde está la del primero:

```
// Añadir línea en /etc/bind/maestria.db del maestro
....
IN NS dns.maestria.com.
IN NS dns2.maestria.com. // Nueva Línea
....
```

De esta forma indicaremos que existen más servidores DNS para dicha zona. Lo mismo haremos en el archivo '192.rev' de la zona inversa:

```
// Añadir línea en /etc/bind/192.rev del maestro
....
IN NS dns.maestria.com.
IN NS dns2.maestria.com. // Nueva línea
....
```

En el archivo **/etc/bind/named.conf.local** del servidor DNS esclavo debemos indicar que se trata de un servidor esclavo y también debemos indicar quién es el maestro:

```
// Añadir en /etc/bind/named.conf.local del esclavo
zone "maestria.com" {
        type slave;
        file "/etc/bind/maestria.db";
        masters { 192.168.0.112; };
};
zone "0.168.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/192.rev";
        masters { 192.168.0.112; };
};
```

En el archivo **/etc/bind/named.conf.local** del servidor DNS maestro podemos utilizar also-notify para mantener los DNS sincronizados. Con also-notify pasamos los cambios de zonas en el maestro al esclavo:

```
// Archivo /etc/bind/named.conf.local del maestro
zone "maestria.com" {
        type master;
        file "/etc/bind/maestria.db";
        also-notify {ip_del_esclavo;}
};
```

```
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.rev";
        also-notify {ip_del_esclavo;}
};
```

De ésta forma dispondremos en la red de un servidor DNS esclavo que podrá satisfacer las peticiones DNS al igual que lo haría el maestro. Es interesante si el número de peticiones es muy elevado y se requiere distribuir la carga entre los dos servidores, o si deseamos disponer de servicio DNS de alta disponibilidad de forma que aunque el servidor maestro deje de funcionar, el servidor esclavo podrá seguir ofreciendo el servicio.

Cada vez que hagamos un cambio en los archivos /etc/bind/maestria.db y /etc/bind/192.rev del maestro, debemos acordarnos de actualizar el parámetro serial (incrementar en una unidad) para que los dns dependientes del maestro sepan que ha cambiado y actualicen su información para mantenerse perfectamente sincronizados.

- ***Arranque y parada manual del servidor DNS***

El servidor DNS, al igual que todos los servicios en Debian, dispone de un script de arranque y parada en la carpeta /etc/init.d.

// Arranque del servidor DNS

 # /etc/init.d/bind9 start

// Parada del servidor DNS

 # /etc/init.d/bind9 stop

// Reinicio del servidor DNS

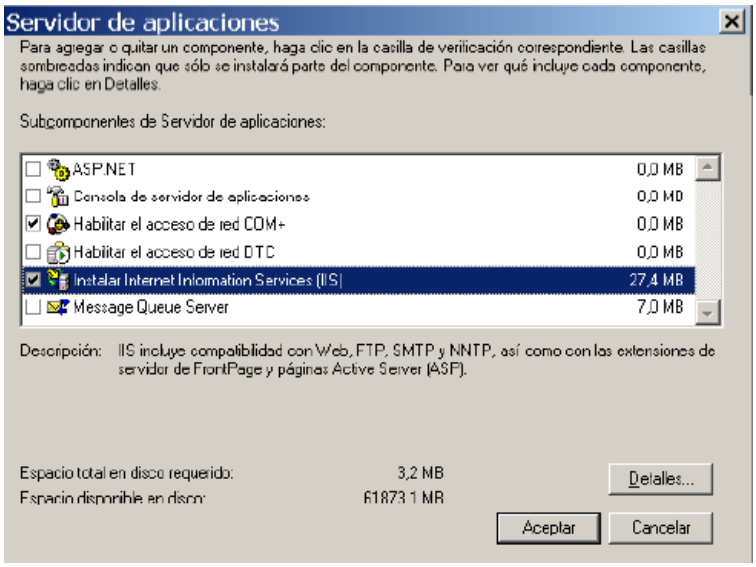
 # /etc/init.d/bind9 restart

IIS (Internet Information Services)

IIS soporta IPv6 desde la versión 6.0. La siguiente configuración de II 6.0 es sobre Windows 2008 Server SP1 Standard Edition.

1. La instalación/desintalación se hace desde Agregar o quitar programas en el **Panel de Control**.
2. Entrar en **Activar o Desactivar las Características de Windows** para acceder el **Iniciador del Complemento Administración de Equipos**.
3. En el asistente para componentes de Windows, seleccionar **Servidor de Aplicaciones** y hacer clic en Detalles…

4. Seleccionar **Instalar Internet Information Services (IIS)** y hacer clic en Detalles…



5. Para instalar correctamente el servidor web hay que activar **Administrador de Servicios de Internet Information Services**, **Archivos Comunes** y **Servicio World Wide Web**:
6. Instalar el IIS e IPv6 (C:\netsh interface ipv6 install), luego reiniciar el IIS para hacer que escuche por IPv6. Usar el **Administrador de IIS** (en Herramientas Administrativas), botón derecho sobre el servidor sobre el que se ejecuta el IIS, aparece la opción **Reiniciar IIS**… dentro de Todas las Tareas
7. Podemos comprobar que se esta escuchando por el puerto 80 (http) sobre IPv6:
8. La configuración de IIS para que devuelva páginas web sobre IPv6 se hace para cada web. Para ello hay que usar el Administrador de IIS (en Herramientas Adminstrativas). Clic con el botón derecho sobre la web a configurar y seleccionando Propiedades se entra a configurar las características de la web:
9. En la solapa Sitio Web debe configurarse en **Direccion IP** el valor **Ninguna Asignada**. De esta forma se escucha por el puerto 80 y por todas las direcciones IPv4 e IPv6. Se pueden añadir detalles entrando en Avanzadas…

Servidor DNS

Los servidores DNS más utilizados y su plataforma de implementacion natural son:

- BIND (http://www.isc.org) sobre Linux

- Windows DNS Server de Microsoft sobre Windows.

Nos centraremos en BIND.

Por un lado se configure la aplicacion servidor para que atienda peticiones IPv6 (transporte) y por otro se incluyen datos relacionados con IPv6 en los contenidos servidos (datos).

Una recomendación: servidores DNS de **doble-pila** (capaces de hacer peticiones DNS sobre IPv4 e IPv6). No toda la infraestructura de DNS soporta IPv6. Se asegura compatibilidad con servidores ya existentes.

Servidor **maestro/primario** vs servidor **secundario/esclavo**. El maestro es donde se crean y actualizan los datos, luego se propagan a los esclavos automáticamente.

- ✓ Para la instalación se pueden utilizar los sistemas habituales de cada distribución (apt-get install bind9, yum, up2date, rpm, etc.) o descargarse los fuentes desde http://www.isc.org y compilarlo:

```
#tar –xzvf bind-9.4.2-P2.tar.gz
#cd bind-9.4.2-P2
#./configure
#make
#make install
```

- ✓ El fichero de configuracion principal es: /etc/bind/named.conf, el cual incluye el fichero /etc/bind/named.conf.opttions.
- ✓ Para habilitar la escucha por IPv6 del servidor debe añadirse a la sección options la directiva **listen-on-v6{};**

```
options {
directory “/var/cache/bind”;
listen-on-v6 { any; };
};
```

Utilizaremos el subdominio **example.com**

- ✓ Configura en /etc/bind/named.conf que se cargue la zona que se encuentra en el fichero /var/cache/bind/example.com.zone. El servidor será el maestro o primario:

```
zone “example.com” {
type master;
file “example.com.zone”;
};
```

Una zona de resolución directa puede contener registros A y AAAA ala vez.

- ✓ Editamos /var/cache/bind/example.com.zone y anadimos lo siguiente:

```
$TTL 86400
@ IN SOA ns1.example.com  dnsadmin.example.com {
2010072201  ;  serial
29900 ;  refresh
7200  ;  retry
604800  ;  expire
86400  ;  ttk
}
IN NS ns1.example.com.
ns1    IN    A    10.7.8.xx
IN AAAA 2001:db8:a:b::xx
ipv4-ipv6  IN A  10.7.8.xx
IN AAAA 2001:db8:a:b::xx
ipv6  IN AAAA 2001:db8:a:b::xx
ipv4  IN  A  10.7.8.xx
```

Registros PTR: no es algo Nuevo, los mismo utilizados para IPv4.

La diferencia con IPv6 es la notación utilizada para las direcciones IPv6 (**nibbles**) y el nombre de dominio usado para ello (**IP6.ARPA**).

Los ficheros de zona para resolución inversa de direcciones IPv6 contendran solamente direcciones IPv6.

- ✓ En /etc/bind/named.conf declararemos la zona de resolución inversa correspondiente al prefijo 2001:db8:1::/48 que no han delegado:

```
zone “1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa” {
type master;
file “2001_0db8_0001.zone”;
};
```

Se divide el prefijo en nibbles y se concatenan en orden inverso al dominio ip6.arpa (Nota, en total deben sumar 32).

- ✓ El fichero 2001_0db8_0001.zone contendrá:

```
$TTL 86400
@ IN SOA ns1.example.com  dnsadmin.example.com {
2010072201  ;  serial
28800 ;  refresh
7200  ;  retry
604800  ;  expire
86400  ;  ttk
}
IN NS ns1.example.com.
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  www.example.com
8.7.6.5.4.3.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN PTR ipv6.example.com
```

- ✓ Reiniciamos el servidor DNS

```
#sudo /etc/initi.d/bind9 restart
```

- ✓ Para ver los log:

```
#tail –f /var/log/dameon
```

- ✓ Para ver como el servidor escucha:

```
#netstat –tan
Proto  Recv-Q  Send-Q   Local Address  Foreign Address    State
tcp6    0    0    :::53    :::*    LISTEN
```

```
tcp     0    0    10.7.8.xx:53      0.0.0.0:*    LISTEN
tcp     0    0    127.0.0.1:53      0.0.0.0:*    LISTEN

#dig any ipv6.example.com @::1
…
;; QUESTION SECTION:
; ipv6.example.com
IN       ANY

;; ANSWER SECTION:
ipv6.example.com.     172800   IN    AAAA   2001:db8:a:b::xx
…
;; Query time: 4 msec
;; SERVER:  ::1#53(::1)
;; MSG SIZE  rcvd: 296

#dig any ipv4-ipv6.example.com @::1
…
;; QUESTION SECTION:
; ipv4-ipv6.example.com.
IN       ANY

;; ANSWER SECTION:
ipv4-ipv6.example.com.     172800   IN    A   10.7.8.xx
ipv4-ipv6.example.com.     172800   IN    AAAA   2001:db8:a:b::xx

#dig -x 2001:db8:1::1000:1234  @::1
…
;; QUESTION SECTION:
; 4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. IN
PTR

;; ANSWER SECTION:
4.3.2.1.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
172800  IN PTR   www.example.com
```

Capítulo 3 Análisis de Red institucional y evaluación de alternativas

11. RED INSTITUCIONAL UNAN-LEÓN

La red de datos de la Universidad Nacional Autónoma de Nicaragua (UNAN-León) se compone de la interconexión del Edificio Central con los edificios de Ciencias Puras, Derecho, Anexo Derecho (Edificio Jorge Arguello), Hospital Oscar Danilo Rosales Arguello (HEODRA), Casa Salud Debayle, Campus Agropecuario, Asociación de trabajadores Docentes (ATD), Editorial Universitaria, Casa de Protocolo, Prepa y Campus Médico, los cuales están interconectados por fibra óptica, enlaces de radio y HDSL.

En la ***Ilustración 128*** se presenta la topología simplificada de la red institucional de la UNAN-León al momento de realizar el análisis. Así mismo el diagrama lógico simplificado de la UNAN-León.

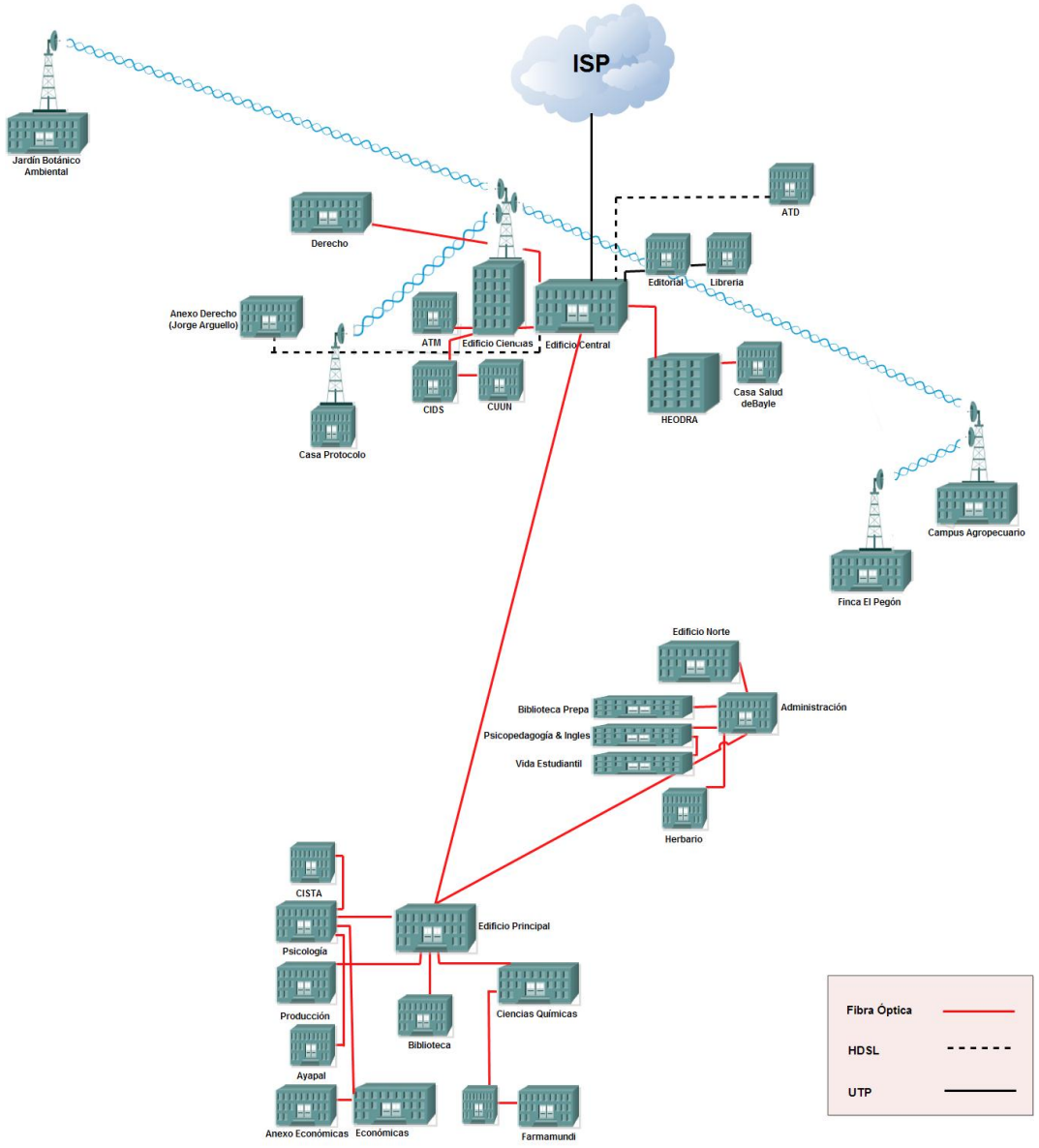
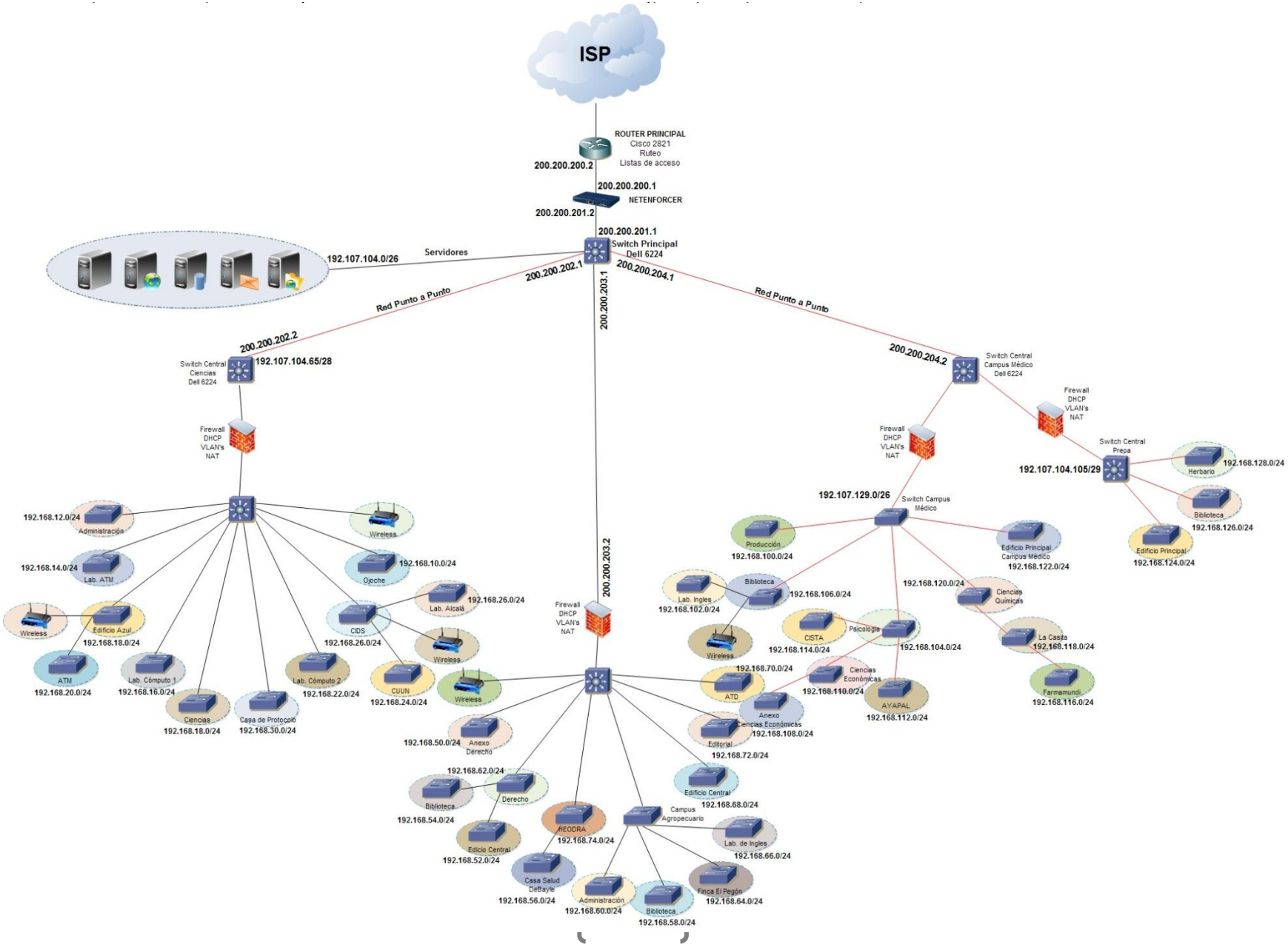


Ilustración 128. Diagrama Físico de edificios de la UNAN-León


ISP
ROUTER PRINCIPAL
Cisco 2821
Ruteo
Listas de acceso
200.200.200.2
200.200.200.1
NETENFORCER
200.200.201.2
200.200.201.1
Switch Principal
Dell 6224
192.107.104.0/26
Servidores
200.200.202.1
Red Punto a Punto
200.200.203.1
200.200.204.1
Red Punto a Punto
200.200.202.2
Switch Central
Ciencias
Dell 6224
192.107.104.65/28
Firewall
DHCP
VLAN's
NAT
200.200.204.2
Switch Central
Campus Médico
Dell 6224
Firewall
DHCP
VLAN's
NAT
Firewall
DHCP
VLAN's
NAT
Switch Central
Prepa
192.107.104.105/29
Herbario
192.168.128.0/24
Biblioteca
192.168.126.0/24
Edificio Principal
192.168.124.0/24
192.107.129.0/26
Switch Campus
Médico
Producción
192.168.100.0/24
Edificio Principal
Campus Médico
192.168.122.0/24
192.168.120.0/24
Ciencias
Químicas
La Casita
192.168.118.0/24
Farmamundi
192.168.116.0/24
Biblioteca
192.168.106.0/24
Lab. Ingles
192.168.102.0/24
Wireless
CISTA
192.168.114.0/24
Psicología
192.168.104.0/24
Ciencias
Económicas
192.168.110.0/24
AYAPAL
192.168.112.0/24
192.168.70.0/24
ATD
Anexo
Ciencias Económicas
192.168.108.0/24
Editorial
192.168.72.0/24
Edificio Central
192.168.68.0/24
Campus
Agropecuario
Lab. de Ingles
192.168.66.0/24
Finca El Pegón
192.168.64.0/24
Biblioteca
192.168.58.0/24
Administración
192.168.60.0/24
Casa Salud
DeBayle
192.168.56.0/24
Edicio Central
192.168.52.0/24
HEODRA
192.168.74.0/24
Biblioteca
192.168.54.0/24
192.168.62.0/24
Derecho
192.168.50.0/24
Anexo
Derecho
200.200.203.2
Firewall
DHCP
VLAN's
NAT
192.168.12.0/24
Administración
Wireless
192.168.14.0/24
Lab. ATM
Ojoche
192.168.10.0/24
Wireless
Edificio Azul
192.168.18.0/24
Lab. Alcalá
192.168.26.0/24
CIDS
192.168.26.0/24
Wireless
ATM
192.168.20.0/24
Lab. Cómputo 1
192.168.16.0/24
Lab. Cómputo 2
192.168.22.0/24
CUUN
192.168.24.0/24
Wireless
Ciencias
192.168.18.0/24
Casa de Protocolo
192.168.30.0/24

Dado que IPv6 es un protocolo de capa 3, su uso es transparente para todos los dispositivos de capa 2. Por ello, en este análisis no se consideran los "switches" de acceso que se encuentran a lo largo de las dependencias de la UNAN-León.

El objetivo de este análisis es diseñar una propuesta de implementación de red IPv6 que permita conectar a la UNAN-León con acceso IPv6 a Internet.

La implementación de la red IPv6 debe estar enmarcada dentro del proyecto de actualización de la red institucional de la UNAN-León. Dicha actualización se debe al aumento de tráfico y usuarios en la red en los últimos años. Los cambios aquí propuestos buscan mejorar el rendimiento de la red institucional en general, junto con proveer soporte IPv6.

Requerimientos para la migración de red IPv4 a IPv6

Para migrar servicios de una red IPv4 a IPv6 lo primero que se debe hacer es migrar la infraestructura de la red IPv4 a IPv6 y luego ofrecer los servicios en esta como se muestra en la ***Ilustración 129***.

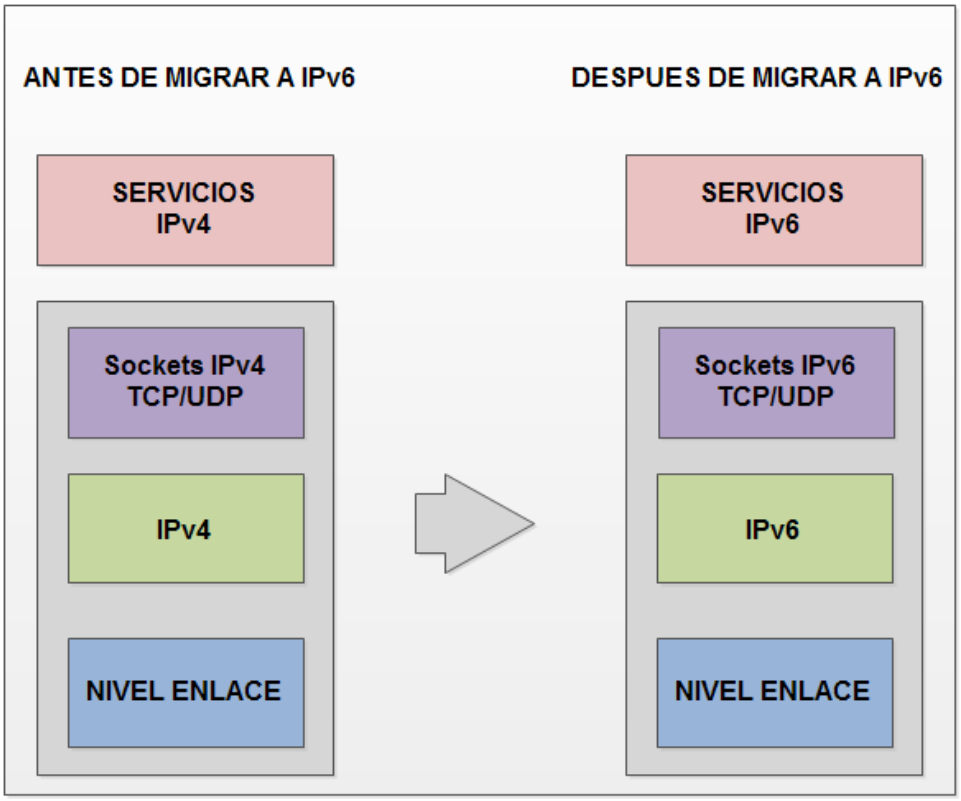


Ilustración 129. Migración IPv4 a IPv6

Si se migrara toda la red de IPv4 a IPv6 una de las ventajas es que el espacio de direcciones es mayor, sin embargo algo que también permite este protocolo es que las direcciones de IPv6 globales usadas en una porción de IPv6 del Internet sean diseñadas para crear una eficiente, jerárquica y extensible infraestructura de ruteo la cual se basa en la común ocurrencia de múltiples niveles de ISP.

Respecto a la configuración de direcciones IPv6 se puede utilizar: stateful (con la configuración de las direcciones si se tiene un servidor DHCPv6) y stateless (con la configuración de las direcciones en ausencia de un servidor DHCPv6).

IPv6 tiene la seguridad incorporada ya que presenta soporte para IPSec, el cual provee estándares base para la solución de problemas de seguridad que la red necesita y provee la interoperabilidad entre diferentes implementaciones IPv6.

El soporte para QoS se encuentra mejorado ya que los nuevos campos en la cabecera IPv6 definen cómo el tráfico es manipulado e identificado. El tráfico es priorizado usando una etiqueta de flujo en la cabecera IPv6 que permita a los routers identificar y mantener un tratamiento especial para los paquetes que pertenecen a un sólo envío entre el origen y el destino, debido a que el tráfico es identificado en la cabecera IPv6 el soporte para la QoS incluso puede lograrse cuando el paquete es encriptado con IPSec y ESP.

Dentro de las desventajas que presenta migrar a IPv6 en este momento, está el riesgo de que los equipos en la institución no soporten IPv6 y adquirir unos nuevos requiere una gran inversión por lo que tendrá que pasar mucho tiempo antes que esto suceda.

Otra de las desventajas es que casi todas las instituciones y/o organizaciones dependen del Internet u otro tipo de enlaces de gran cobertura prestados por empresas comerciales y no pueden tolerar tiempos fuera de estos servicios hasta que IPv6 sea implantado por las redes comerciales, así mismo actualmente nuestro proveedor de Internet no cuenta con soporte de IPv6 nativo.

En cuanto a las proyecciones de tiempo estimado para el cual las redes mundiales estarán para el cual las redes mundiales estarán usando sólo IPv6 se tienen los siguientes criterios:

Según Tony Hain[130] para los años 2009-2016, IPv6 debe reemplazar a IPv4, ante el acelerado desarrollo de dispositivos, tecnología móvil y una demanda masiva de nuevas direcciones IPv6.

Mientras que en un artículo de CISCO[131] se espera que para los años 2025-2050 IPv6 ya se haya adoptado como protocolo de comunicación mundial.

[130] UNDERSANTINDG IPV6, Joseph Davis. Copyright ©2003 by Microsoft Corporation. Chapter 11. Coexistence and Migration.

[131] http://www.cisco.com/en/US/about/acl23/archived_issues/ipj_8-3/IPv4.html

Ante estas proyecciones, en lo que coinciden los diseñadores de IPv6 es que la migración de IPv4 a IPv6 tomará algunos años más que pueden existir organizaciones o nodos dentro de ellas que continuarán usando IPv4 indefinidamente.

A continuación se propone dos fases que deben ser parte del proceso de migración:

a) Actualizar la infraestructura de red
b) Actualizar las aplicaciones y servicios

Este proceso propone que la red debe pasar por una etapa de coexistencia IPv4/IPv6 y luego usar solo IPv6, esto se muestra en la ***Ilustración 130***.

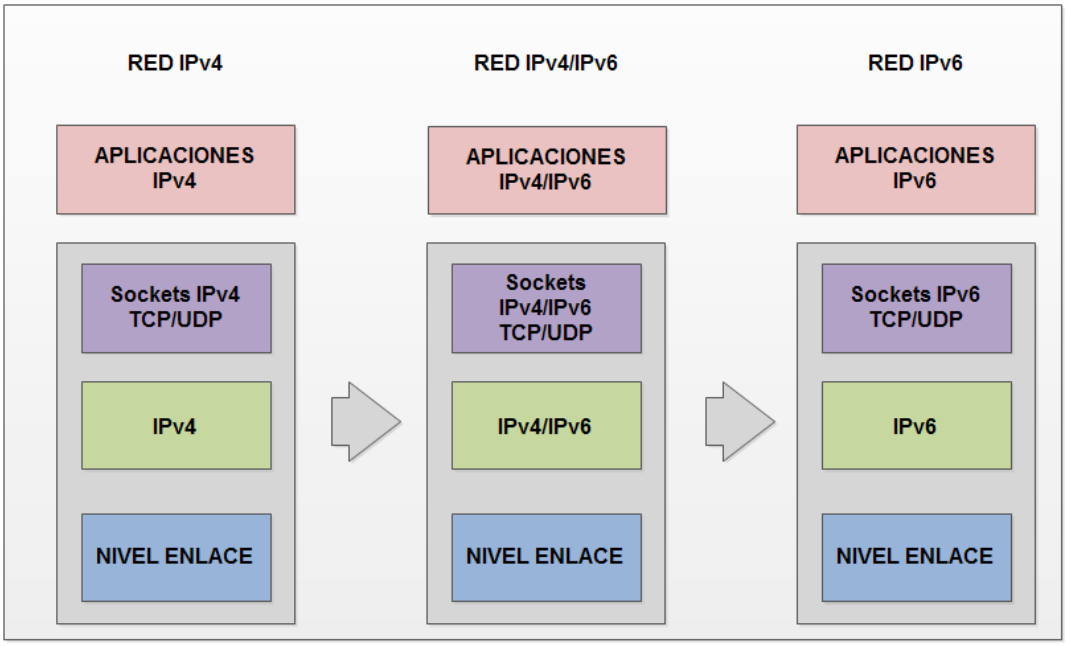


Ilustración 130. Proceso de migración: Pasar por una etapa de coexistencia IPv4/IPv6 y luego usar sólo IPv6

a) Actualizar la infraestructura de red

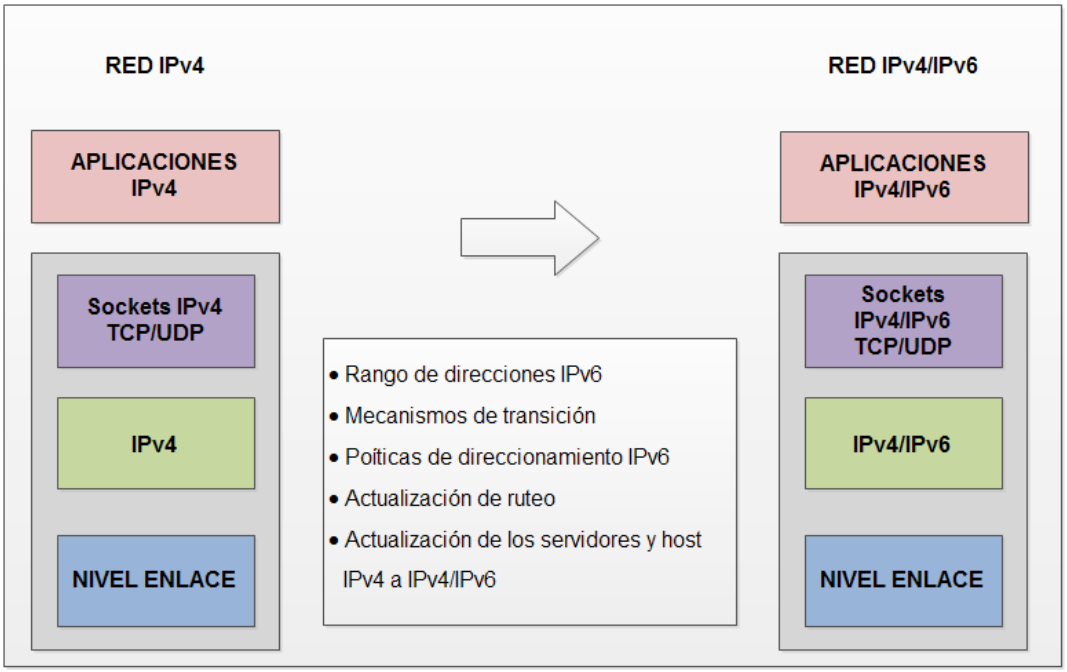


Ilustración 131. Red IPv4 a red IPv4/IPv6

Como se indica en la ***Ilustración 131***, dentro de la actualización de la infraestructura de red se debe considerar los siguientes puntos:

- Obtener un rango de direcciones IPv6 para poder comunicarse con otras redes IPv6.

  La UNAN-León tiene asignado un segmento IPv6 el cual es **2800:10:13::/48**.

- Seleccionar los mecanismos de transición que se implantarán en la Intranet y con otras redes.

  Se debe escoger primero el mecanismo de transición que se implantará al interior de la red de la UNAN-León.

- Definir un esquema de direccionamiento IPv6 en la Internet.

Para definir un esquema de direccionamiento IPv6 se tiene como base los RFC que lo norman, estos son: RFC 2928[132], RFC 3513[133].

- Actualizar los routers para que soporten protocolos de ruteo IPv6, esto supondrá la adquisición de nuevos equipos en algunos casos, a fin de poder rutear tráfico IPv6 con la proyección de rutear tráfico sólo IPv6 en un futuro.

- Actualizar la pila IP de los host IPv4 a IPv4/IPv6.

  Los equipos deben ser actualizados para usar doble pila, para esto lo primero será verificar si el sistema operativo tiene el soporte IPv6 (***Ver Anexos***) y luego confirmar los parámetros de red. La mayoría de sistemas operativos incluyen el protocolo IPv6. En cuanto a la configuración de los parámetros de la red se puede realizar una configuración manual y automática. Respecto de la configuración automática existen dos posibilidades, utilizar *Autoconfiguración Stateless* o descubrimiento automático – sin intervención, o *Auconfiguración Statefull* o configuración predeterminada – DHCPv6 (Para mayor información ***Autoconfiguración*** y ***DHCPv6***).

  En caso de redes o sitios grandes con múltiples subredes y routers, no se requiere un servidor DHCPv6, ya que los hosts para generar sus direcciones determinan los prefijos que identifican las subredes a las que se conectan, por esto la autoconfiguración stateless tiene como característica implícita facilitar la renumeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios y se actualiza la configuración de los routers. La renumeración se logra al permitir que una misma interfaz pueda tener varias direcciones por un tiempo (cuando cambia el prefijo de la subred), permitiendo que varias direcciones, una dirección anterior y una nueva dirección, den continuidad a la comunicación (Para mayor información, ***Router Renumbering***).

[132] RFC 2928: "Initial IPv6 Sub-TLA ID Assignments".

[133] RFC 3513: "Internet Protocol Version 6 (IPv6) Addressing Architecture".

Posteriormente una vez que el protocolo sea implantado definitivamente en la institución y todo el proceso de prueba sea satisfactorio únicamente será necesario eliminar toda la configuración IPv4, a como muestra la ***Ilustración 132***.

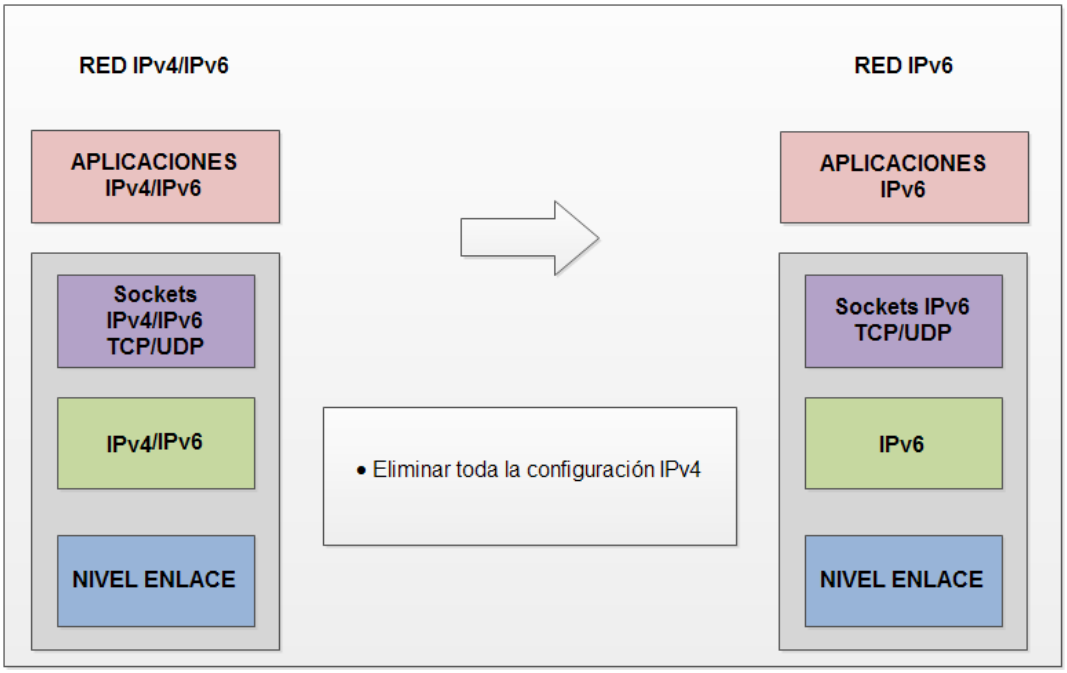


Ilustración 132. Red IPv4/IPv6 a red IPv6

b) Actualizar las aplicaciones y servicios

Las aplicaciones deben estar en la capacidad de utilizar cualquier versión IP de forma independiente para esto deben tener programados los sockets tanto IPv4 como IPv6 de acuerdo a los RFC: 2292[134], 2553[135].

Existen dos alternativas principalmente para tener aplicaciones IPv6, la primera es añadir el soporte IPv6 a las aplicaciones IPv4, de tal manera que se tendrá una sola aplicación para atender peticiones en ambos protocolos, como se muestra en la ***Ilustración 133***.

[134] RFC 2292: "Advanced Sockets API for IPv6".

[135] RFC 2553: "Basic Socket Interface Extensions for IPv6".

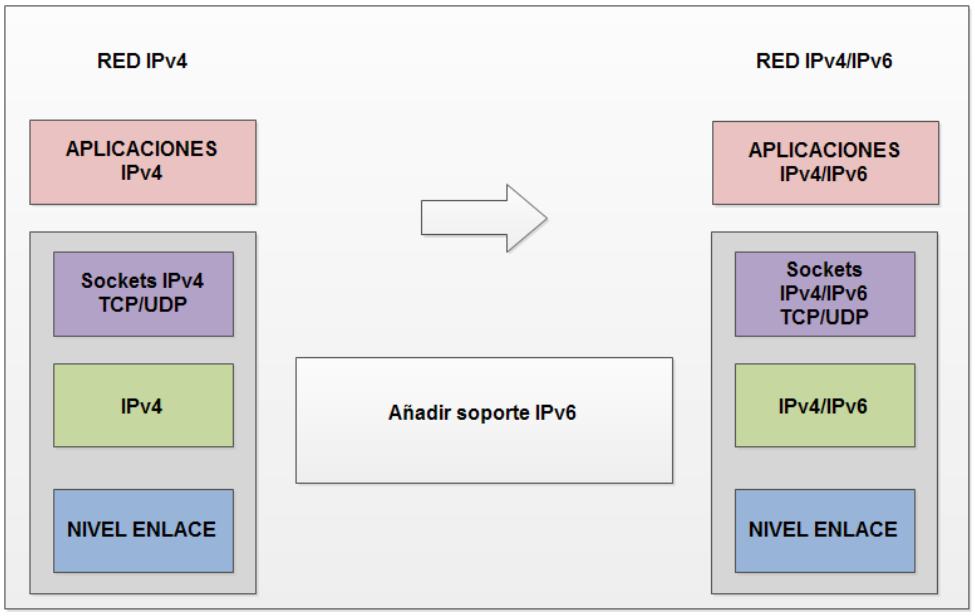


Ilustración 133. Aplicaciones IPv4 a aplicaciones IPv4/IPv6

La segunda alternativa es tomar el código de la aplicación IPv4 reemplazar las llamadas y estructuras IPv4 por la de IPv6 y crear una nueva aplicación para IPv6, como se muestra en la ***Ilustración 134***.

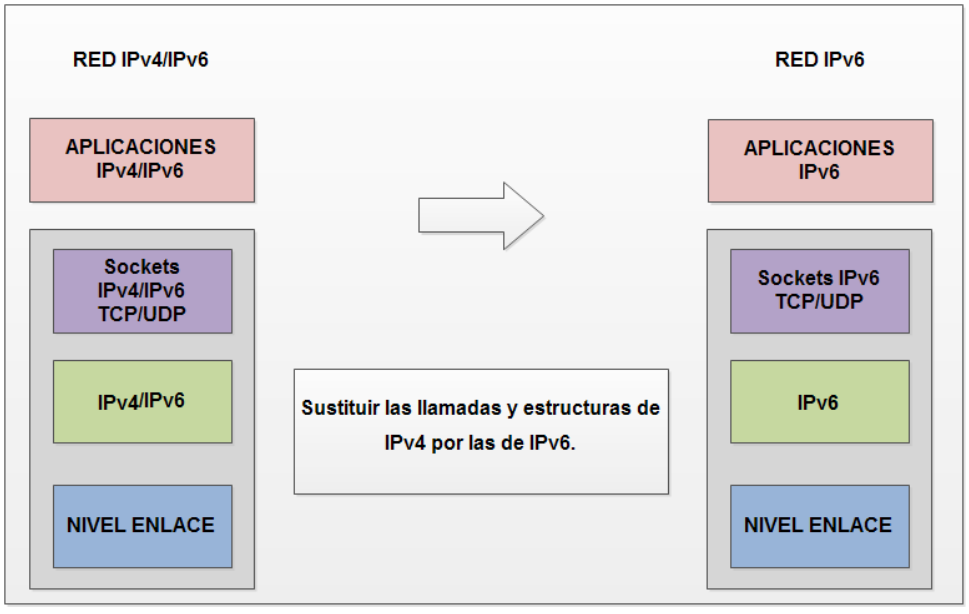


Ilustración 134. Aplicaciones IPv4/IPv6 a aplicaciones IPv6

Si se sigue la primera alternativa, es decir, trabajar con una aplicación dual, se tiene como ventajas: el uso de una única aplicación, mantenimiento de un único código fuente, sin embargo se requieren muchos cambios y más tiempo.

Si se sigue la segunda alternativa, es decir, crear una nueva aplicación para IPv6, las ventajas que presenta son: facilidad de codificación, requiere un período corto de tiempo, los problemas que presenta es que el usuario debe seleccionar entre la aplicación IPv4 ó la aplicación IPv6, y que se debe realizar el mantenimiento del código fuente de dos aplicaciones.

Sin embargo, las principales empresas comerciales y comunidades Open Source ya han agregado a sus aplicaciones el soporte IPv6.

Tecnologías y filosofía de diseño

CISCO utiliza en sus productos el sistema operativo IOS. Este es un sistema operativo monolítico, lo que significa que correo como una sola instancia y que todos los procesos comparten el mismo espacio de memoria. Por este hecho, errores en una operación pueden alterar o corromper otros procesos del sistema. Junto a esto, si un usuario desea agregar nuevas funciones o complementos al sistema operativo, se debe detener el equipo y reemplazar el sistema operativo completamente.

Por otra parte, JUNOS fue construido como un sistema operativo modular. El núcleo del sistema esta basado en el sistema operativo FreeBSD y los procesos corren como módulos sobre el núcleo, con su propio espacio de memoria separado y protegido del resto. De esta forma los usuarios pueden agregar características y funciones al sistema operativo sin tener que reemplazarlo completamente, una característica llamada actualizaciones en línea, la que permite obtener una mejor disponibilidad del servicio.

CISCO consciente de estas limitaciones en sus sistemas operativos, ha desarrollado nuevas versiones del IOS (IOS XR, IOS XE y NS-OS), que buscan superar las limitaciones del esquema monolítico del IOS original. Estos 3 sistemas operativos son de arquitectura modular: los servicios de IOS corren como módulos sobre un núcleo Linux (NX-OS y IOS

XE) o un núcleo POSSIX (IOS XR). En la ***Tabla 6*** se presenta un cuadro resumen de las principales diferencias entre ambos sistemas operativos:

Tabla 6. Comparación entre IOS y JUNOS

Juniper JUNOS	CISCO IOS
Creado en 1996	Creado en 1987
Ultima versión principal: 9.0	Ultima versión principal: 12.4
Arquitectura modular	Arquitectura monolítica (en proceso de cambio a arquitectura modular)
Misma versión corre en todos los equipos. (Excepto en "firewalls")	Distintas versiones disponibles para cada equipo CISCO.

Cabe destacar que ambas empresas han anunciado planes para permitir que aplicaciones desarrolladas por terceros tengan acceso a los servicios otorgados por sus sistemas operativos.

Si bien ambos sistemas implementan el mismo conjunto de protocolos y estándares utilizando en redes IP, CISCO destaca por estar constantemente actualizando sus sistemas operativos con herramientas y protocolos propios, que facilitan la configuración y administración de sus dispositivos. Dentro de dichos protocolos destacan "NetFlow", "Hot Standby Router Protocol" (HSRP) y "VLAN Trunking Protocol" (VTP).

Análisis del soporte IPv6 en la red institucional

El uso de la técnica "dual-stack" requieren que todos los equipos involucrados en conectar la red institucional a internet cuenten con soporte para IPv6. En la ***Tabla 7*** siguiente se presenta un resumen de los resultados obtenidos al revisar los equipos existentes:

Tabla 7. Equipos switch y routers existentes en la UNAN-León

Marca	Modelo
D-Link	Des-1024D[136]

[136] ftp://ftp10.dlink.com/pdfs/products/DES-1024D/DES-1024D_ds.pdf

D-Link	DSS-24[137]
Dell	PowerConnect 2724[138]
Allied Telesyn	AT-FS724L[139]
Encore	ENH924-AUT[140]
Netgear	FSM726[141]
Dell	PowerConnect 3424[142]
Dell	PowerConnect 2724[143]
Dell	PowerConnect 5424[144]
Dell	PowerConnect 6424[145]
Dell	PowerConnect 2716[146]
Lynksys	EF4124[147]
Cisco	2821

Alternativas de equipamiento

El análisis de los equipos demostró que para la implementación de IPv6 satisfactoriamente en la UNAN-Léon será necesario realizar cambios hardware de los equipos que proporcionaran la conectividad, entre ellos:

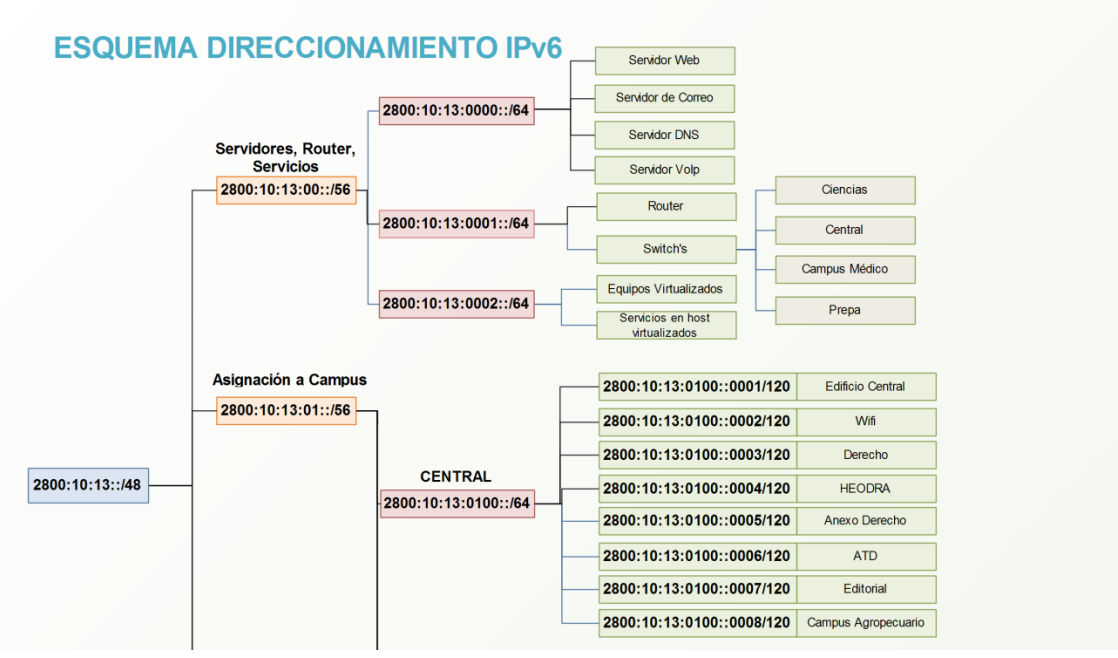
- Si bien no es estrictamente necesario desde el punto de vista de soporte IPv6, los equipos cortafuegos que actualmente implementa la UNAN-León (Monowall), deben ser considerados en la lista de dispositivos a reemplazar por una solución que tenga soporte IPv6 estable, puesto que Monowall (versión beta 1.33) no tiene el nivel de madurez en IPv6 requerido para implementar sobre él la migración.

[137] ftp://ftp10.dlink.com/pdfs/products/DSS-24+/DSS-24+_ds.pdf
[138] http://www.andovercg.com/datasheets/dell-powerconnect-2708.pdf
[139] http://www.alliedtelesis.es/media/datasheets/guides/fs724l_ig_a.pdf
[140] http://www.encore-usa.com/pl/sites/default/files/product_file_datasheet/ENH924-AUT%28USENV4%29_Spec_%28EN%29_100313.pdf
[141] http://kbserver.netgear.com/datasheets/FSM726_datasheet_061603.pdf
[142] http://www.dell.com/downloads/global/products/pwcnt/en/tolly_ts206135_3424.pdf
[143] http://www.dell.com/downloads/global/corporate/environ/comply/pwcnt_2724.pdf
[144] http://www.dell.com/downloads/global/corporate/environ/comply/pwcnt_5424.pdf
[145] http://www.dell.com/downloads/global/corporate/environ/comply/pwcnt_6224.pdf
[146] http://www.dell.com/downloads/global/corporate/environ/comply/pwcnt_2716.pdf
[147] http://www.startechtel.com/docs/linksys24.pdf

- Además se requiere realizar cambio en al menos los equipos de capa 3 que proporcionan conectividad en los principales puntos de distribución (Edificio central, Edicicio Ciencias Puras, Edificio de Campus médico, Edificio de Humanidades) y dotarlos de routers CISCO, con sus respectivos firmware actualizados con soporte IPv6.
- Así mismo se requerirá agregar soporte IPv6 a los tres switches capa 3 para implementar ruteo entre VLANs (router-on-a-stick), es decir, conectar a través de una interfaz en el router y en el switch de cada edificio y a través de ella rutear las VLANs, optimizando así la utilización de recursos.

Asignación de direcciones IPv6

El rango IPv6 que tiene asignado la UNAN-León es: 2800:10:13::/48, en base a ello se ha elaborado una propuesta de asignación de direcciones:



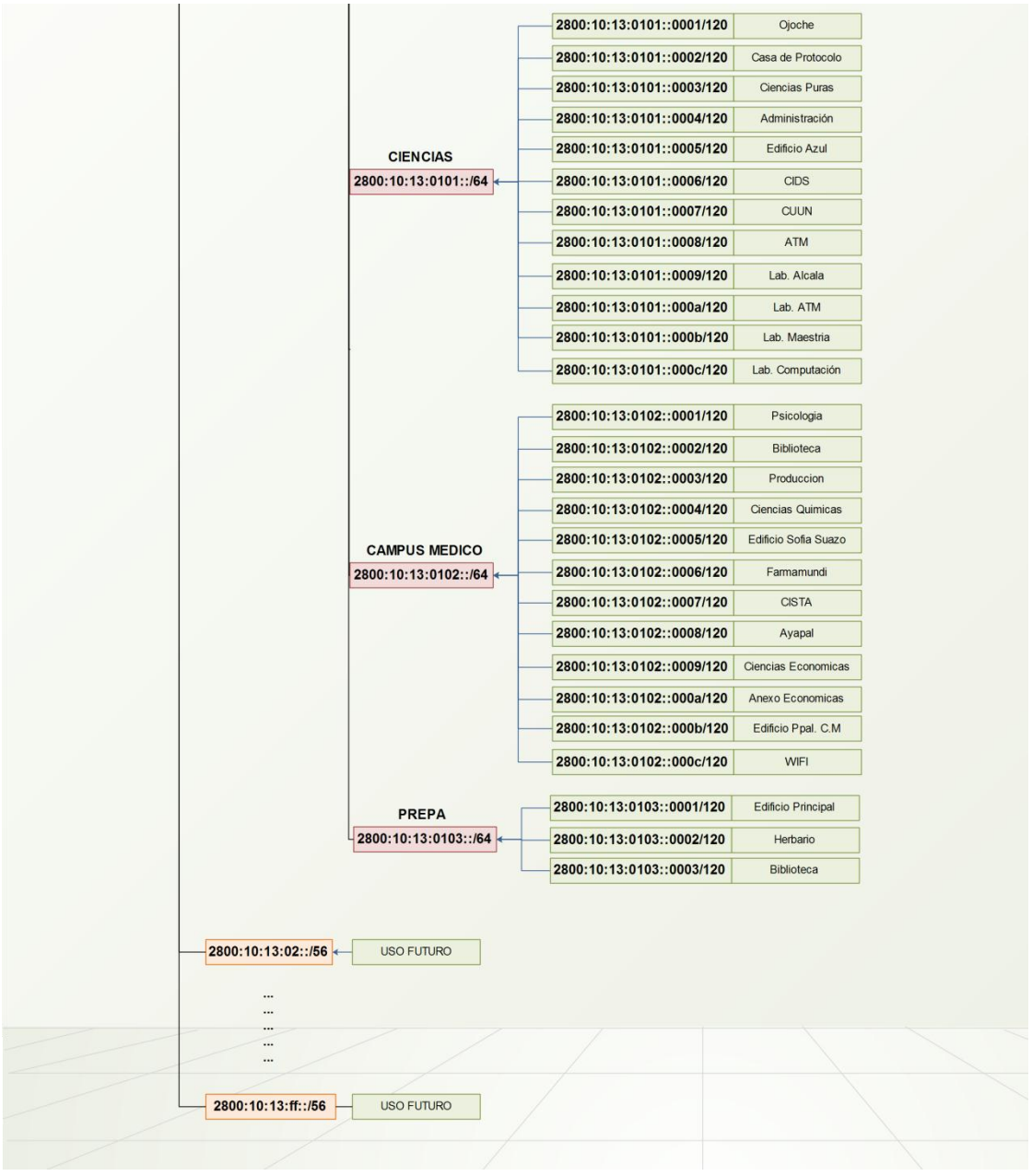


Ilustración 135.Propuesta Esquema de direccionamiento IPv6

En la ***Ilustración 136.*** Propuesta de diagrama de Red IPv6 UNAN-León se muestra la propuesta de diagrama IPv6 manteniendo la lógica de red igual que IPv4.

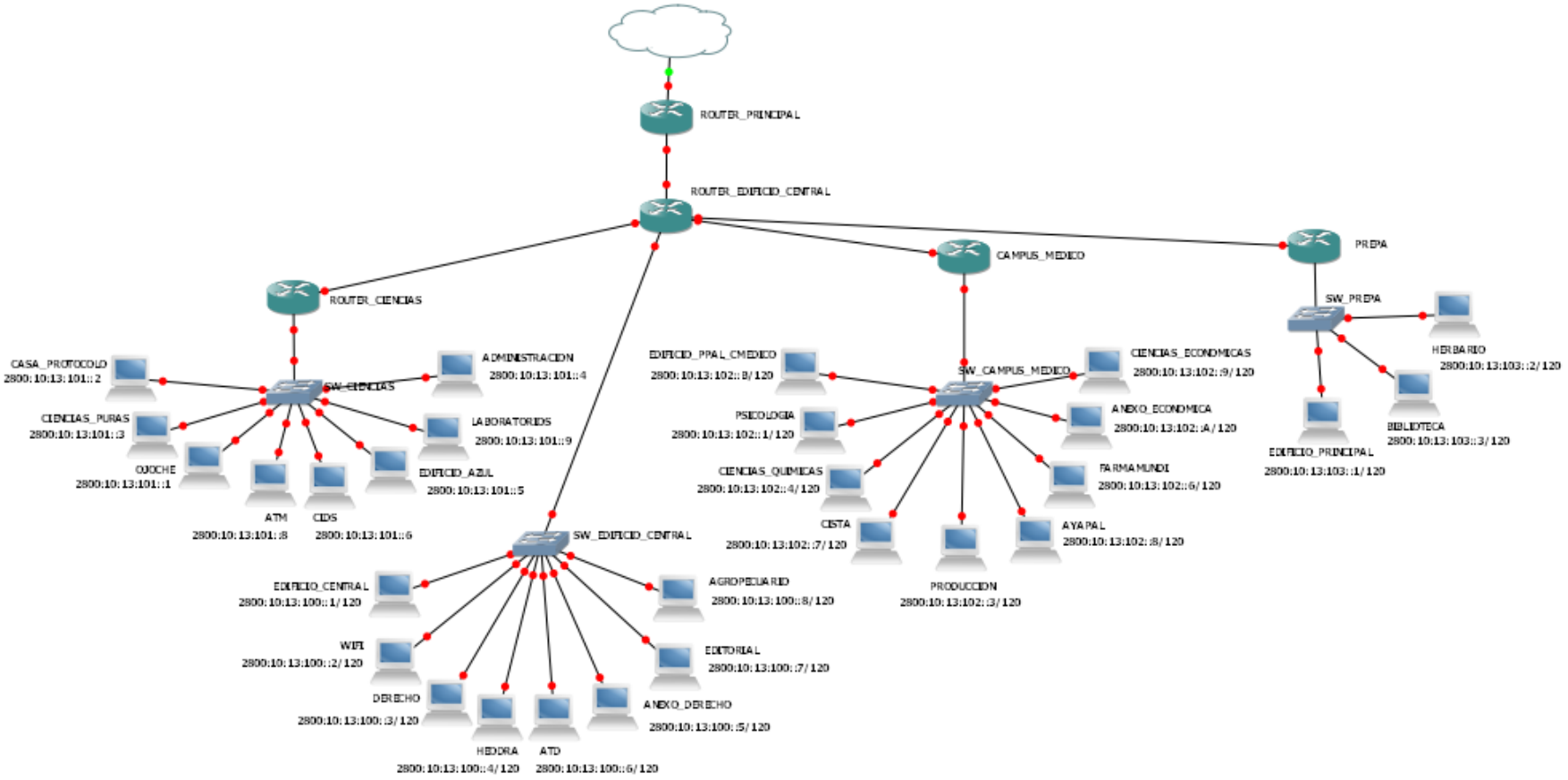


Ilustración 136. Propuesta de diagrama de Red IPv6 UNAN-León

Seguridad perimetral IPv6 en la UNAN-León en los routers

El modelo de seguridad perimetral es la arquitectura de seguridad de TI que la mayoría de las organizaciones utilizan.

La filosofía es crear una fortaleza impenetrable en torno a la empresa que intenta evitar todos los ataques. El perímetro es la primera línea de defensa frente a amenazas externas. El interior del perímetro podría o no podría ser fortalecida, mientras que las aplicaciones internas suelen ser libre para comunicarse sin ningún tipo de protecciones de seguridad interna. Sin embargo, el modelo del perímetro no es la única estrategia de seguridad que se debe utilizar para prevenir la explotación de un ataque si tiene éxito. El modelo de perímetro es sólo uno de varios componentes esenciales que se requieren en una diversidad de diseño de la defensa.

El modelo perimetral comienza a romperse cuando una organización pone toda su fe en ella y no utiliza una arquitectura de seguridad en capas que protege contra las amenazas que se originan desde el interior. En los últimos años, las organizaciones que únicamente se basan en sus perímetros de seguridad han sido víctimas de ataques de malware que se dirigen a los equipos de usuario final. Si el perímetro es el único mecanismo de seguridad utilizado, estas amenazas internas completaran la explotación de sistemas de la red interna.

En el caso de migración de IPv6 de la UNAN-León, al actual perímetro IPv4 se tendrá que añadir soporte IPv6. El hecho de que la UNAN-León migre a un entorno de doble pila no significa que se va a sustituir sus actuales defensas del perímetro, sino que simplemente se deberá añadir capacidades de IPv6 a sus puntos de salida existentes.

A muchas de las mismas arquitecturas de seguridad y dispositivos de protección que existen para IPv4 se le han añadido funciones de IPv6. Las políticas de seguridad IPv4 implementadas actualmente por la UNAN-León se pueden utilizar para determinar qué tipos de tráfico IPv6 es aceptable y lo que debería estar prohibido. La política de permitir tráfico de aplicaciones en la parte superior de IPv6 será similar a la actual política de

IPv4. Esto es porque las capas de transporte TCP y UDP funcionan de manera similar en la parte superior de cualquiera de las versiones IP Capa 3.

Por ejemplo, actualmente la UNAN-León tiene una norma que permite responder las solicitudes IPv4 de su servidor web, para las conexiones IPv6 en su política de seguridad habría que agregar una norma similar para salida del puerto TCP 80 (HTTP).

- ***Filtrando direcciones IPv6 sin asignar***

Actualmente se utilizan los firewall IPv4 para bloquear direcciones ilegales e intentos de spoofing. Es una buena práctica filtrar el tráfico de entrada y salida. Por lo tanto, si tenemos en cuenta la migración a IPv6, el mismo tipo de filtrado antispoofing será necesario. Además se debe tener en cuenta los rangos válidos de direcciones IPv6 y filtrar los paquetes que utilizan las direcciones no asignadas.

A continuación se detallarán las actuales direcciones globales IPv6 (públicas), y cómo filtrar las direcciones falsas en el firewall.

Los firewalls deben bloquear los paquetes que provienen o con destino al espacio no asignado de direcciones IPv6. El hecho es que la mayor parte del espacio de direcciones IPv4 ya se ha asignado. Es más fácil para llegar a una lista de direcciones IPv4 privadas de una lista de todas las direcciones IPv4 públicas. Sin embargo, con IPv6, sólo una pequeña fracción del espacio de direcciones IPv6 total ha sido asignada. En este caso, la seguridad se puede mejorar, porque la política de seguridad sólo permitiría los paquetes provenientes de los prefijos del espacio de direcciones IPv6 asignado y todas las otras direcciones IPv6 serían bloqueadas. Este tipo de políticas de seguridad es más sencillo de configurar que una política de IPv4, y la posición por defecto es denegar el paquete si la dirección de origen o de destino no es legítima.

La lista de las direcciones IPv6 que son legítimas y deben ser permitidas es pequeña y fácil de mantener debido a la jerarquía de direcciones IPv6.

Los siguientes son los grandes bloques de direcciones que han sido asignados por la Internet Assigned Numbers Authority (IANA) en 2008 y la organización a la que han sido delegadas:

Bloques IPv6	Asignado a:
2001::/16	Direcciones unicast IPv6
2002::/16	Túnel 6to4
2003::/18	RIPE NCC
2400::/12	APNIC
2600::/12	ARIN (US DoD)
2610::/23	ARIN
2620::/23	ARIN
2800::/12	LACNIC
2A00::/12	RIPE NCC
2C00::/12	AfriNIC

La lista anterior es una visión general del espacio de direcciones IPv6 asignado[148].

Hay muchos tipos de direcciones IPv6 no asignados que no deben atrevesar el firewall. Estos deben ser bloqueados desde y hacia cualquier dirección IPv6.

La ***Tabla 8*** enumera las direcciones que deben ser denegadas por el firewall:

Tabla 8. Direcciones IPv6 a Denegar

Paquetes a bloquear	Direcciones
Denegar direcciones sin especificar	::
Denegar direcciones loopback	::1
Denegar direcciones IPv4 compatibles	::/96
Denegar direcciones IPv4-mapeadas (obsoleto)	::ffff:0.0.0.0/96 ::/8
Denegar automáticamente paquetes tuneleados usando direcciones compatibles (obsoleta RFC 4291)	::0.0.0.0/96
Denegar otras direcciones compatibles	::224.0.0.0/100 ::127.0.0.0/104 ::0.0.0.0/104 ::255.0.0.0/104
Denegar paquetes falsos 6to4	2002:e000::/20 2002:7f00::/24 2002:0000::/24 2002:ff00::/24 2002:0a00::/24 2002:ac10::/28 2002:c0a8::/32

[148] Para mayor información: http://www.iana.org/assignments/ipv6-unicast-address-assignments

Denegar direcciones de enlace local (link-local)	fe80::/10
Denegar direcciones locales al sitio (site-local) [obsoleta]	fec0::/10
Denegar paquetes unique-local	fc00::/7
Denegar paquetes multicast (solo como dirección origen)	ff00::/8
Denegar direcciones de prueba	2001:db8::/32
Denegar direcciones 6Bone (obsoleto)	3ffe::/16

Propuesta de ACL a implementar en routers CISCO UNAN-León

Teniendo en mente que los usuarios de Internet deben ser capaces de llegar al servidor web de la UNAN-León, y los usuarios internos tienen que ser capaces de acceder a Internet, el firewall de la UNAN-León debe ser configurado de forma tal que, bloquee direcciones no válidas, pero permita protocolos de enrutamiento y tipos de mensajes ICMPv6 legítimos.

Se debe encontrar un equilibrio entre la seguridad y los gastos administrativos asociados a la gestión de una política compleja.

- ***Listas de acceso de entrada con acceso a internet***

Tomaremos como referencia la ***Ilustración 136.*** Propuesta de diagrama de Red IPv6 UNAN-León En la interfaz de entrada las ACLs de cara a Internet se inician mediante el bloqueo de los paquetes provenientes de direcciones de origen falsos. Luego, los mensajes ICMPv6 legítimos están permitidos. EBGP se permite entre los dos routers (router principal y router central), y el tráfico web entrante se permite, para que a los paquetes DNS de respuesta se les permita volver a la red. Asi mismo, muchos tipos de direcciones están bloqueados. En la ***Tabla 9*** se muestra una propuesta de política de tráfico entrante:

Tabla 9. ACLs entrantes con acceso a internet

```
ipv6 access-list Internet-Inbound
-- Comentario: Denegar direcciones loopback
deny ipv6 ::1/128 any

-- Comentario: Denegar direcciones IPv4-compatibles
deny ipv6 0::/96 any
```

```
-- Comentario: Denegar direcciones IPv4-mapeadas (obsoleta)
deny ipv6 ::ffff:0.0.0.0/96 any

-- Comentario: Denegar direcciones de paquetes de túnel automático/compatibles
deny ipv6 ::0.0.0.0/96 any

-- Comentario: Denegar otras direcciones compatibles
deny ipv6 ::224.0.0.0/100 any log
deny ipv6 ::127.0.0.0/104 any log
deny ipv6 ::0.0.0.0/104 any log
deny ipv6 ::255.0.0.0/104 any log

-- Comentario: Denegar paquetes 6to4 falsos
deny ipv6 2002:e000::/20 any log
deny ipv6 2002:7f00::/24 any log
deny ipv6 2002:0000::/24 any log
deny ipv6 2002:ff00::/24 any log
deny ipv6 2002:0a00::/24 any log
deny ipv6 2002:ac10::/28 any log
deny ipv6 2002:c0a8::/32 any log

-- Comentario: Permitir mensajes NDP debido a que deniegan y registran (log)
permit icmp fe80::/10 any nd-na
permit icmp fe80::/10 any nd-ns

-- Comentario: Denegar comunicaciones de enlace local (Link-Local)
deny ipv6 fe80::/10 any

-- Comentario: Denegar sitios locales (Site-Local) [obsoleto]
deny ipv6 fec0::/10 any

-- Comentario: Denegar paquetes Unique-Local
deny ipv6 fc00::/7 any

-- Comentario: Denegar paquetes multicast
deny ipv6 ff00::/8 any

-- Comentario: Denegar direcciones de prueba
deny ipv6 2001:db8::/32 any

-- Comentario: Denegar direcciones 6Bone (obsoleto)
```

```
deny ipv6 3ffe::/16 any

-- Comentario: Denegar paquetes RH0
deny ipv6 any any routing-type 0 log

-- Comentario: Denegar nuestra propia red como tráfico entrante
deny ipv6 2800:10:13::/48 any log

-- Comentario: Permitir BGP desde y hacia nuestra red (EBGP)
permit tcp host 2800:10:13::1 host 2800:10:13::2 eq bgp
permit tcp host 2800:10:13::1 eq bgp host 2800:10:13::2

-- Comentario: Permitir tráfico a nuestro servidor web
permit tcp any host 2800:10:13::100 eq www

-- Comentario: Permitir que nuestro tráfico regrese a los clientes internos
permit tcp any 2800:10:13::/48 range 1024 65535
permit udp any 2800:10:13::/48 range 1024 65535

-- Comentario: Permitir que tráfico entrante al DNS se responda a lo interno
permit udp any eq domain host 2800:10:13:30:20c:29ff:fe5d:982a

-- Comentario: Permitir mensajes buenos de tipo ICMPv6
permit icmp any 2800:10:13::/48 destination-unreachable
permit icmp any 2800:10:13::/48 packet-too-big
permit icmp any 2800:10:13::/48 parameter-problem
permit icmp any 2800:10:13::/48 echo-reply

-- Comentario: Permitir que nuestro ISP haga ping a nuestra interfaz externa
permit icmp host 2800:10:4::1 host 2800:10:4::2 echo-request

-- Comentario: Denegar todo lo demás y almacenalo (logs)
deny ipv6 any any log
```

- ***Listas de acceso de salida con acceso a internet***

La salida de ACL en la interfaz de cara a Internet se inicia por los paquetes de bloqueo que van a direcciones ilegales de destino. Por tanto, están permitidos mensajes legítimos ICMPv6, se permite EBGP entre los dos routers (principal y central), y los paquetes de consulta DNS se dejan fuera de la red.

En la ***Tabla 10*** se muestra una propuesta de política de tráfico de salida. Notar que hay sutiles diferencias entre las ACL entrantes y salientes.

Tabla 10. ACLs salientes con acceso a internet

```
ipv6 access-list Internet-Outbound
-- Comentario: Denegar direcciones loopback
deny ipv6 any ::1/128

-- Comentario: Denegar direcciones IPv4-compatibles
deny ipv6 any 0::/96

-- Comentario: Denegar direcciones IPv4-mapeadas (obsoleta)
deny ipv6 any ::ffff:0.0.0.0/96

-- Comentario: Denegar direcciones de paquetes de túnel automático/compatibles)
deny ipv6 any ::0.0.0.0/96

-- Comentario: Denegar otras direcciones compatibles
deny ipv6 any ::224.0.0.0/100 log
deny ipv6 any ::127.0.0.0/104 log
deny ipv6 any ::0.0.0.0/104 log
deny ipv6 any ::255.0.0.0/104 log

-- Comentario: Denegar paquetes 6to4 falsos
deny ipv6 any 2002:e000::/20 log
deny ipv6 any 2002:7f00::/24 log
deny ipv6 any 2002:0000::/24 log
deny ipv6 any 2002:ff00::/24 log
deny ipv6 any 2002:0a00::/24 log
deny ipv6 any 2002:ac10::/28 log
deny ipv6 any 2002:c0a8::/32 log

-- Comentario: Permitir mensajes NDP debido a que deniegan y registran (log)permit
icmp fe80::/10 any nd-na
permit icmp fe80::/10 any nd-ns

-- Comentario: Denegar comunicaciones de enlace local (Link-Local)
deny ipv6 any fe80::/10

-- Comentario: Denegar sitios locales (Site-Local) [obsoleto]
deny ipv6 any fec0::/10
```

```
-- Comentario: Denegar paquetes Unique-Local
deny ipv6 any fc00::/7

-- Comentario: Denegar paquetes multicast
deny ipv6 any ff00::/8

-- Comentario: Denegar direcciones de prueba
deny ipv6 any 2001:db8::/32

-- Comentario: Denegar direcciones 6Bone (obsoleto)
deny ipv6 any 3ffe::/16

-- Comentario: Denegar paquetes RH0
deny ipv6 any any routing-type 0 log

-- Comentario: Permitir salida a las peticiones DNS de nuestro servidor cache DNS interno
permit udp host 2800:10:13:30:20c:29ff:fe5d:982a any eq domain

-- Comentario: Permitir mensajes buenos de tipo ICMPv6
permit icmp 2800:10:13::/48 any destination-unreachable
permit icmp 2800:10:13::/48 any packet-too-big
permit icmp 2800:10:13::/48 any parameter-problem
permit icmp 2800:10:13::/48 any echo-reply
-- Comentario: Permitir a nuestras direcciones salir a la internet
permit ipv6 2800:10:13::/48 any

-- Comentario: Denegar todo lo demás y almacenalo (logs)
deny ipv6 any any log
```

Costos de implementación y soporte

Para llevar a cabo una migración sin sorpresas desagradables, habría que sopesar en costes al menos las siguientes tareas administrativas fundamentales:

- Formación del personal técnico para la gestión de IPv6 en las redes de la organización.

- Actualización del software necesario, incluyendo el sistema operativo (en caso de ser requerido).
- Configuración de los dispositivos a nivel de sistema operativo para utilizar direcciones IPv6.
- Configuración software de los dispositivos que tengan que manejar varias VLANs.
- Configuración de los diferentes sistemas operativos para gestionar las preferencias entre IPv4 e IPv6 en caso que el host destino tenga ambas direcciones.
- Configuración de las aplicaciones de red para que soporten ambos tipos de direccionamiento.
- Administración de VLANs.
- Administración de direcciones IPv4 e IPv6.
- Administración de rutas IPv4 e IPv6 y anunciamiento de prefijos IPv6 (gestión de routers).
- Administración de reglas de filtrado IPv6 e IPv6.
- Administración y mantenimiento de cortafuegos IPv4 e IPv6.
- Actualización de los script de backup y mantenimiento del sistema.

Así mismo, aún cuando el sistema operativo JUNOS ha sido diseñado para operar de forma similar al sistema IOS de CISCO, posee importantes diferencias en su estructura y metodología para llevar a cabos ciertas tareas. Esto implica que de seleccionarse la alternativa presentada por Juniper, seria necesario invertir tiempo y recursos en capacitación de los administradores de dichos equipos.

Relacionado con lo anterior, un aspecto negativo de la alternativa de Juniper es la escasa documentación y base de usuarios que posee en comparación con CISCO. El sitio web de CISCO pone a disposición de los usuarios una serie de documentos técnicos (“whitepapers”) que buscan resolver problemas y dudas que los usuarios tienen comúnmente. Ademas, los equipos presentados por CISCO son utilizados en un gran

número de redes a lo largo del mundo, permitiendo constar con una gran base de usuarios que comentan y publican sus experiencias en sitios web y grupos de discusión.

- ***Otras consideraciones***

Si queremos que los dos protocolos de red compartan una infraestructura común, habremos de tener en cuenta los diversos aspectos que las caracterizan y las diferencian, y que principalmente son:

1. *Configuración cero*. Mientras que en IPv6 se resuelve de forma más sencilla la autoconfiguración sin estado del dispositivo de red en tiempo de arranque, sigue sin resolverse a nivel práctico la configuración automática con estado de los hosts (también llamada proceso Zero-config) para lo que se prevé utilizar protocolos como DHCP modificados para IPv6 y que a día de hoy están aún en desarrollo.

2. *Ancho de Banda*: El protocolo IPv4 hace uso de las capacidades de broadcast (protocolo ARP) para obtener la dirección física de cada host en la red (también llamada dirección MAC), para así poder componer la trama de nivel de enlace.

   La propia definición de broadcast implica que todos los paquetes de este tipo lleguen a todos los dispositivos conectados a un mismo dominio de broadcast. Dado que en IPv6, el broadcast podría no ser necesario, este efecto actuará disminuyendo el ancho de banda disponible en aquellos segmentos de red que sean compartidos entre clientes IPv4 y clientes IPv6. Este efecto, sin embargo, dadas las capacidades actuales de redes locales y procesadores se prevé que provoque una interferencia prácticamente despreciable entre ambas re redes.

3. *Seguridad:* Mientras que los mecanismos de seguridad de protocolo (IPsec) para IPv4 son opcionales, en IPv6 todos los dispositivos que pretendan pertenecer a la red deberían ser capaces de manejarlos, lo que de por si, ya introduce un grado de complejidad en la red que hasta ahora no era de obligado cumplimiento.

Además, hay que tener en cuenta que los nodos IPv6, al utilizar el protocolo Neighbour Discovery (ND) para diversas funciones de red, son susceptibles de varios ataques si no se utiliza la arquitectura de seguridad ofrecida por IPsec Authentication Header (AH).

Además, como los métodos automáticos de gestión de claves (p.ej. el Internet Key Exchange, IKE) actualmente están en fase de desarrollo, es obligatorio llevar a cabo la gestión manual de las claves de autenticación de los nodos en caso de ser necesario, lo cual puede introducir una gran carga de trabajo de administración si el número de dispositivos a configurar es grande.

Por todo ello, en la actualidad se está desarrollando soluciones basadas en IPsec (SEcure Neighbour Discovery, SEND) y en direcciones generadas criptográficamente Criptographically generated addresses, CGA) que permiten identificar el nodo origen de un paquete y saber si el paquete ha sido modificado en tránsito.

Este tipo de problemas es previsible que se solucionarán en un futuro próximo, dada la gran cantidad de gente que está desarrollando la tecnología de este campo.

4. *Rendimiento*: Los balanceadores de carga comerciales son dependientes del nivel de red, estando los actualmente disponibles diseñados para utilizar IPv4. Esto puede ser un problema a la hora de desplegar en la actualidad servicios en producción con el nuevo protocolo de red.

Desventajas de migración de IPv6 en la UNAN-León

Aunque IPv6 proporciona muchas bondades, la implementación de este proyecto en la UNAN-León debe ser analizado con cautela puesto que las desventajas que esto supondría están:

1. Falta de capacitación del personal técnico de informática.
2. Verificación de la compatibilidad de las aplicaciones usadas en la UNAN-León.

3. Tiempo de interrupción mientras se realiza migración y pruebas.
    a. Creación de ACLs en routers.
    b. Creación de reglas en firewall.
    c. Reingeniería en proceso de enrutamiento.
4. Compra de equipos (enrutadores) que soporten el protocolo.
5. Actualmente el proveedor de la Internet de la universidad no tiene soporte de IPv6 nativo.

12. CONCLUSIONES

La migración al nuevo protocolo en las redes actuales es un trabajo no exento de riesgos y costes. Algunos estarán ocultos hasta el momento de llevar a cabo la puesta en escena, pero la planificación y la discusión son las únicas herramientas que nos pueden ayudar a conseguir una migración lo mas suave posible. Los riesgos están relacionados con la posible pérdida de eficiencia en las redes en las que se implante IPv6 en los períodos de transición, los costes dependerán de la densidad de cambios, la velocidad del depligue y el esfuerzo (tanto económico como humano) que vayamos a dedicar a la tarea de migración.

Es más, hemos de ser concientes que la migración a nivel de red y de servicios solo será una parte de la migración a IPv6, puesto que si queremos aprovechar las nuevas caracterisiticas del protocolo, habremos de emplear nuevos esfuerzos en extender con aplicaciones que soporten calidad de servicio, sistemas preparados para la gestión de claves de seguridad y encaminadores capaces de proveer entornos de movilidad a los usuarios, entre otras cosas.

También es importante remarcar que el éxito de la migración dependerá, además, en gran medida de la disponibilidad de software adecuado a la nueva tecnología, que no solo permita estar a la altura del servicio proporcionado por la tecnología basada en IPv4, sino que nos permita sacar partido de sus características positivas y que nos permita obviar, en mayor o menor medida, sus posibles desventajas.

Así mismo es importante destacar que las implementaciones de IPv6 todavía no tienen el mismo nivel de madurez que las de IPv4. Esto no es un argumento en contra del despliegue de IPv6 sino un llamado sobre el trabajo que aún falta por hacer.

13. BIBLIOGRAFÍA

- IPv6 Security. Scott Hogg, Eric Vyncke. 2009. Cisco Press.
- [RFC 1891] K. Moore, “SMTP Service Extension for Delivery Status Notifications”, RFC 1891, Enero 1996, http://www.ietf.org/rfc/rfc1891.txt
- [RFC 2373] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture”, RFC 2373, Julio 1998, http://www.ietf.org/rfc/rfc2373.txt
- [RFC 2460] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Diciembre 1998, http://www.ietf.org/rfc/rfc2460.txt
- [RFC 2461] T. Narten, E. Nordmark, W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6)”, RFC 2461. Diciembre 1998. http://www.ietf.org/rfc/rfc2461.txt
- [RFC 2463] A. Conta, S. Deering. “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”. RFC 2463. Diciembre 1998. http://www.ietf.org/rfc/rfc2463.txt
- [RFC 2461] T. Narten, E. Nordmark, W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6”, RFC 2461. Diciembre 1998. http://www.ietf.org/rfc/rfc2461.txt
- [RFC 2710] S. Deering, W. Fenner, B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710. Octubre 1999. http://www.ietf.org/rfc/rfc2710.txt
- [RFC 2740] R. Coltun, D. Ferguson, J. Moy. “OSPF for IPv6”. RFC 2740. Diciembre 1999. http://www.ietf.org/rfc/rfc2740.txt
- [RFC 3041] T. Narten, R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”. RFC 3041, Enero 2001, http://tools.ietf.org/html/rfc3041
- [RFC 3053] A. Durand, P. Fasano, I. Guardini, D. Lento. "IPv6 Tunnel Broker". RFC 3053, Enero 2001. http://www.ietf.org/rfc/rfc3053.txt
- [RFC 3056] B. Carpenter, K. Moore. "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, Febrero 2001. http://www.ietf.org/rfc/rfc3056.txt
- [RFC 3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC3315, Julio 2003, http://www.ietf.org/rfc/rfc3315.txt

- [RFC 3513] R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC 3513, Abril 2003, http://www.ietf.org/rfc/rfc3513.txt
- [RFC 3587] R. Hinder, S. Deering, E. Nordmark, “IPv6 Global Unicast Address Format”, RFC 3597, Agosto 2003, http://www.ietf.org/rfc/rfc3587.txt
- [RFC 3596] S. Thomson, C. Huitema, V. Ksinant, M. Souissi. "DNS Extensions to Support IP Version 6", RFC 3596, Octubre 2003. http://www.ietf.org/rfc/rfc3596.txt
- [RFC 3633] O. Troan, R. Droms, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6”, RFC3633, Diciembre 2003, http://www.ietf.org/rfc/rfc3633.txt
- [RFC 3756] P. Nikander, J. Kempf, E. Nordmark, “IPv6 Neighbor Discovery (ND) Trust Models and Threats”. RFC 3756. Mayo 2004. http://www.ietf.org/rfc/rfc3756.txt
- [RFC 3810] R. Vida, L. Costa. "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810. Junio 2004. http://www.ietf.org/rfc/rfc3810.txt
- [RFC 4214] F. Templin, T. Gleeson, M. Talwar, D. Thaler, “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP”, RFC 4214, Octubre 2005, http://www.ietf.org/rfc/rfc4214.txt
- [RFC 4291] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture”, RFC4291, Febrero 2006, http://tools.ietf.org/html/rfc4291
- [RFC 4301] S. Kent, K. Seo. “Security Architecture for the Internet Protocol”, RFC 4301. Diciembre 2005. http://www.ietf.org/rfc/rfc4301.txt
- [RFC 4302] S. Kent. “IP Authentication Header”, RFC 4302. Diciembre 2005. http://tools.ietf.org/html/rfc4302
- [RFC 4303] S. Kent, “IP Encapsulating Security Payload (ESP)”, RFC 4303, Diciembre 2005, http://www.ietf.org/rfc/rfc4303.txt
- [RFC 4861] T. Narten, E. Nordmark, W. Simpson, H. Soliman. “Neighbor Discovery for IP version 6 (IPv6)”. RFC 4861. Septiembre 2007. http://www.ietf.org/rfc/rfc4861.txt
- [RFC 4862] S. Thomson, T. Narten, T. Jinmei, “IPv6 Stateless Address Autoconfiguration”, RFC 4862. Septiembre 2007. http://www.ietf.org/rfc/rfc4862.txt

- [RFC 4941] T. Narten, R. Draves, S. Krishnan. "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941. Septiembre 2007. http://www.ietf.org/rfc/rfc4941.txt
- [RFC 5006] J. Jeong, S. Park, L. Beloeil, S. Madanapalli. "IPv6 Router Advertisement Option for DNS Configuration". RFC5006. Septiembre 2007. http://www.ietf.org/rfc/rfc5006.txt
- [RFC 5157] T. Chown. "IPv6 Implications for Network Scanning", RFC 5157. Marzo 2008. http://www.ietf.org/rfc/rfc5157.txt
- [RFC 5308] C. Hopps. "Routing IPv6 with IS-IS", RFC 5308. Octubre 2008. http://www.ietf.org/rfc/rfc5308.txt
- [RFC 5569] R. Despres, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC5569, Enero 2010, http://tools.ietf.org/html/rfc5569
- [RFC 5571] B. Storer, C. Pignataro, B. Stevant, L. Toutain, J. Tremblay, "Softwire Hub and Spoke Deployment Framework with Layer Two Tunneling Protocol Version 2 (L2TPv2)", RFC5571, Junio 2009, http://www.rfc-editor.org/rfc/rfc5571.txt
- DeepSpace6 - Current Status of IPv6 Support for Networking Applications http://www.deepspace6.net/docs/ipv6_status_page_apps.html
- Firewalls Distribuidos , http://www.textoscientificos.com/redes/firewalls-distribuidos
- http://portalipv6.lacnic.net
- IANA Administrative Procedure for Root Zone Name Server Delegation and Glue Data: http://www.iana.org/procedures/delegation-data.html
- Internet Systems Consortium http://www.isc.org
- IPv6 Address Added for Root Servers in the Root Zone: http://www.icann.org/announcements/announcement-04feb08.htm
- IPv6 Address Autoconfiguration, http://msdn.microsoft.com/en-us/library/aa917171.aspx

- IPv6 mobile home-agent (global configuration) through ipv6 ospf database-filter all out, http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_07.html#wp2360073
- IPv6 neighbor spoofing , http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/
- IPv6 Stateless Autoconfiguration, http://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ipv6-stateless-autoconfiguration
- IPv6 with dynamic routing and redistribution – RIPng and OSPFv3, http://www.i-1.nl/blog/?p=193
- Multicast Configuration Guide, http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Routers/H3C_SR8800_Series_Routers/Configuration/Operation_Manual/H3C_SR8800_CG-Release3342-6W102/07/
- Multicast: Conformance and Peformance Testing, http://www.ixiacom.com/library/white_papers/display?skey=multicast
- Next-generation IPv6 Address Added to the Internet's Root DNS Zone: http://www.icann.org/announcements/announcement-20jul04.htm
- Root Zone Hints File in IANA Popular Links: http://www.iana.org/popular.htm
- Seguridad del protocolo Internet (IPSec) , http://technet.microsoft.com/es-es/library/cc783420(WS.10).aspx
- Softwire Hub & Spoke Deployment Framework with L2TPv2 draft-ietf-softwire-hs-framework-l2tpv2-13, http://tools.ietf.org/html/draft-ietf-softwire-hs-framework-l2tpv2-13
- Tutorial y descripción técnica de TCP/IP, http://www.cicei.com/ocon/gsi/tut_tcpip/index.html
- Compilación e instalación Versión 2.2 del Servidor HTTP Apache, http://httpd.apache.org/docs/2.2/install.html

Capítulo 4 Anexos

1. CONFIGURACIÓN DE HOST EN WINDOWS XP

Para habilitar IPv6 en Windows XP (SP2), hay métodos alternativos de hacerlo:

- Usando la interfaz gráfica WinXp

A través del entorno gráfico o panel de control, llegar hasta “Conexiones de red”, seleccionar la “red de área local” o “red inalámbrica”, clic derecho y seleccionar “Propiedades”, en la ventana que se muestra seleccionar “Protocolo Internet (TCP/IP)”, dar clic al botón “Instalar”, “Protocolo” y dar clic a “Agregar” y seleccionar “Microsoft TCP/IP versión 6”, finalmente dar clic en “Aceptar”.

El resultado será similar al mostrado en la siguiente captura de pantalla:

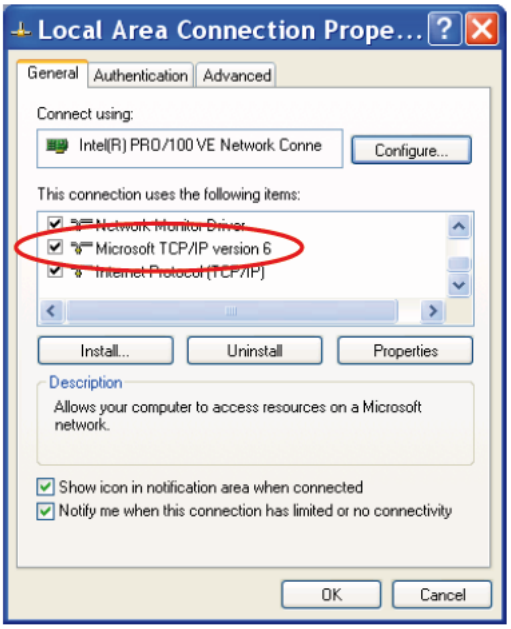


Ilustración 137. Instalación de IPv6 en XP/2003

- O desde la interfaz de línea de comandos (cmd.exe) correr ***ipv6 install***

Tras unos segundo, un mensaje de confirmación indicra la correcta instalación. También se podría utilizar, dependiendo de la versión: **netsh interface ipv6 install**.

2. CONFIGURACIÓN DE HOST EN WINDOWS VISTA/2008

Desde el lanzamiento de Windows Vista, este sistema operativo incluye soporte de IPv6 instalado y habilitado por defecto.

Por lo tanto, no es necesario hacer ninguna configuración adicional. En caso de que se hubiese desactivado, se podría utilizar el procedimiento con netsh o entorno gráfico indicado para Windows XP/2003.

Téngase en cuenta que para usar netsh, se requiere una ventana de DOS explícitamente abierta con permisos de administración.

En comparación con XP/2003, IPv6 en Vista tiene funcionalidades adicionales, como por ejemplo:

- Soporte completo IPsec.
- MLDv2.
- Link-Local Multicast Name Resolution (LLMNR).
- Soporte de direcciones IPv6 en URLs.
- IPv6 Control Protocol (IPv6CP - RFC5072).
- IPv6 sobre PPP.
- DHCPv6, en el cliente y el servidor.
- Identificador de intefaz aleatorio por defecto (RFC3041).
- Teredo soporta NATs simétricos.

Se puede comprobar que esta instalado, por medio de comandos o con el entorno gráfico, de forma similar a lo indicado para el caso de XP:

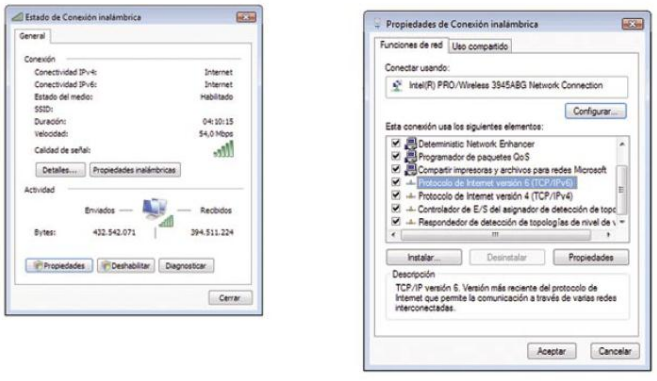


Ilustración 138. Propiedades de Conexión de red e instalación de IPv6 en Vista

3. CONFIGURACIÓN DE HOST EN WINDOWS 2000

El método mas fiable para la instalación de la pila IPv6 para Windows 2000, requiere primero descargar el código correspondiente a la pila IPv6, dado que a diferencia de los sistemas operativos hasta ahora mencionados, no esta preinstalado por el fabricante.

Windows 2000 IPv6 no está soportado por Microsoft, dado que se trataba de una versión de desarrollo. Por lo tanto, en primer lugar, descargar "Microsoft IPv6 Technology Preview for Windows 2000":

- tpipv6-001205-SP2-IE6 para SP1 y SP2
- tpipv6-001205-SP3-IE6 para SP3
- tpipv-001205-SP4-IE6 para SP4

Todos están disponibles en:

http://www.sixxs.net/faq/connectivity/?faq=ossetup&os=windows

Una vez descargado, el procedimiento de instalación es el siguiente:

- Entrar en el sistema como usuario con privilegios locales de administrador.
- Extraer los ficheros de IPv6 Technology Preview, por ejemplo en C:\IPv6Kit
- Seguir el procedimiento de SPn & IE6 fixed.txt para cambiar el fichero /setup/hotfix.ini
- Ejecutar Setup.exe o hotfix.exe
- Desde el escritorio de Windows 2000, clic Inicio, luego Configuración, y luego Conexiones de red, luego clic en Propiedades.
- Hacer clic con el botón derecho en conexión basadas en Ethernet para las que se desea añadir el protocolo IPv6 y luego clic en Propiedades. Normalmente, esta conexión se denomina Conexión de Área Local.
- Clic Install.
- En el cuadro de diálogo Seleccionar Tipo de Componentes de Red, hacer clic en Protocolo, y luego clic Añadir.
- En el cuadro de diálogo Seleccionar Protocolo de Red, hacer clic en Microsoft IPv6 Protocol y luego clic en Aceptar.

4. INSTALACION DE IPV6 EN LINUX

IPv6 esta soportado a partir de la versión del kernel 2.4.x.

Para comprobar si esta instalado:

 # test –f /proc/net/if_inet6 && echo “Kernel actual soporta IPv6”

Para instalar el modulo IPv6:

 # modprobe ipv6

Se puede comprobar el módulo con:

 # lsmod | grep –w ‘ipv6’ && echo “modulo IPv6 cargado”

También se puede configurar la carga/descarga automática del modulo (/etc/modules.conf o /etc/conf.modules)

alias net-pf-10 ipv6 # habilita carga bajo demanda

alias net-pf-10 off # deshabilita carga bajo demanda

Se puede realizar la configuración permamente, en función de la versión de Linux.

5. CONFIGURACION PERMANENTE EN RED HAT

Esta configuración es valida desde la versión 7.1 y similares.

Añadir a /etc/sysconfig/network:

NETWORKING_IPV6=yes

Reiniciar la interfaz de red:

 # service network restart

O

 # /etc/init.d/network restart

6. CONFIGURACION PERMANENTE EN SUSE

Añadir en /etc/sysconfig/network/ifcfg-<Interface-Name>:

SUSE 8.0: IP6ADDR='"<ipv6-address>/<prefix>"

SUSE 8.1: IPADDR='"<ipv6-address>/<prefix>"

7. CONFIGURACION PERMANENTE EN DEBIAN

Con el módulo IPv6 cargado se edita /etc/network/interfaces, por ejemplo:

iface eth0 inet6 static

pre-up modprobe ipv6

address 2001:DB8:1234:6::1:1

 # Elimina completamente la autoconfiguracion

 # up echo 0 > /proc/sys/net/ipv6/conf/all/autoconf netmask 64

 # el encaminador esta autoconfigurado y no tiene dirección fija

 # se encuentra gracias a

 # (/proc/sys/net/ipv6/conf/all/accept_ra).

 # Si no habrá que configurar el GW:

 # Gateway 2001:DB8:1234::1

Se reinicia la interfaz de red:

 # ifup –force eth0

8. INSTALACION DE IPV6 EN BSD

El soporte de IPv6 en BSD esta disponible a partir de la versión 4.5.

Se trata de un soporte muy bueno y la pila se halla preinstalada, por lo que no se requiere ningún paso adicional.

9. CONFIGURACION AVANZADA IPV6 EN WINDOWS

Por diversos motivos, puede requerirse configurar manualmente una dirección IPv6.
Para ello se usa el comando netsh con el formato siguiente:

netsh interface ipv6 add addresss [interface=]<cadena(nombre de interfaz o índice)>[address=] <dirección IPv6> [/<entero>] [[type=] unicast|anycast] [[validlifetime=] <entero>|infinite] [[preferredlifetime=] <entero>|infinite] [[store=] active|persistent]

Ejemplo:

netsh interface ipv6 add address 5 2001:db8::2 type=unicast validlifetime=infinite preferredlifetime=10m store=active

Igualmente, se puede revisar la configuración con netsh (asumiendo que es la interfaz número 5):

netsh interface ipv6 show address 5

Una vez configurada una dirección manualmente, se puede modificar con:

netsh interface ipv6 set address [interface=]<cadena> [address=] <dirección IPv6> [[type=] unicast|anycast] [[validlifetime=] <entero>|infinite] [[preferredlifetime=] <entero>|infinite] [[store=] active|presistent]

Ejemplo:

netsh interface ipv6 set address 5 2001:db8::2 preferredlifetime=infinite

Y finalmente, dicha dirección puede ser eliminada con:

netsh interface ipv6 delete address [interface=] <cadena> [address=] <dirección IPv6> [[store=] active|persistent]

Ejemplo:

netsh interface ipv6 delete address 5 2001:db8::2 store=persistent

Igualmente se puede dar el caso en que necesitemos agregar una ruta estática, y de forma similar, utilizaríamos:

netsh interface ipv6 add route [prefix=] <dirección IPv6>/<entero> [interface=] <cadena> [[nexthop=] <dirección IPv6>] [[siteprefixlength=] <entero>] [[metric=] <entero>] [[publish=] no|yes|immortal] [[validlifetime=] <entero>|infinite] [[preferredlifetime=] <entero>|infinite] [[store=] active|persistent]

Ejemplo:

netsh interface ipv6 add route 2002::/16 5 fe80::200:87ff:fe28:a0e0 store=persistent

Donde, fe80::200:87ff:fe28:a0e0 es la puerta de enlace que se desea configurar para la ruta 2002::/16.

Para borrar dicha ruta:

netsh interface ipv6 delete route [prefix=] <dirección IPv6>/<entero> [interface=] <cadena> [[nexthop=] <dirección IPv6>] [[store=] active|persistent]

Ejemplo:

netsh interface ipv6 delete route 2002::/16 5 fe80::200:87ff:fe28:a0e0 store=persistent

Y se pueden visualizer las rutas con:

netsh interface ipv6 show route [[level=] normal|verbose] [[store=] active|persistent]

Ejemplo:

Netsh interface ipv6 show route

Publicar	Tipo	Mét	Prefijo	Índ	Puerta enl./Nombre interfaz
No	Manual	8	::/0	13	Conexión de area local*7
No	Manual	0	2002::/16	5	fe80::200:87ff:fe28:a0e0
No	Autoconf	8	2001:db8::/64	5	Local Area Connection
No	Autoconf	256	::/0	5	fe80::200:87ff:fe28:a0e0

Finalmente, se puede agregar un servidor DNS con:

Netsh interface ipv6 add dnsserver [name=]<cadena> [address=]<dirección IPv6> [[index=]<entero>]

En XP SP1/2003 SP1 se usa dns en lugar de dnsserver.

Ejemplo:

netsh inteface ipv6 add dnsserver “Local área network” 2001:7f9:1000:1::947c 1

El “index” representa la posición (preferencia) del servidor DNS que se configura en la lista de servidores DNS.

Y se puede mostrar los servidores DNS configurados manualmente con:

netsh interface ipv6 show dnsservers [[name=]cadena]

Ejemplo:

```
Netsh interface ipv6 show dnsservers
DNS servers in LAN interface
Index   DNS server
-------  ------------------------------------------------------
1        2001:7f9:1000:1::947c
2        2001:7f9:1000:1::947c
```

Y por ultimo, borrarlos con:

netsh interface ipv6 delete dnsserver [name=]<cadena> [[address]=]<dirección IPv6>|all

Ejemplo:

netsh interface ipv6 delete densserver “Local área network” all

10. CONFIGURACION AVANZADA IPV6 EN LINUX

Añadir una dirección IPv6:

/sbin/ip -6 addr add <ipv6address>/ <prefixlength> dev <interface>

/sbin/ifconfig <interface> inet6 add <ipv6address> / <prefixlength>

Eliminar una dirección IPv6:

/sbin/ip -6 addr del <ipv6address>/ <prefixlength> dev <interface>

/sbin/ifconfig <interface> inet6 del <ipv6address> / <prefixlength>

Añadir ruta a través de una puerta de enlace:

/sbin/ip -6 route add <ipv6network>/ <prefixlength> via <ipv6address> [dev <device>]

/sbin/route -A inet6 add <ipv6network> / <prefixlength> gw <ipv6address> [dev <device>]

Ver rutas IPv6:

/sbin/ip -6 route show [dev <device>]

/sbin/route –A inet6

Eliminar ruta a través de una puerta de enlace:

/sbin/ip -6 route del <ipv6network>/ <prefixlength> via <ipv6address> [dev <device>]

/sbin/route -A inet6 del <ipv6network> / <prefixlength> gw <ipv6address> [dev <device>]

Añadir ruta a través de una interfaz:

/sbin/ip -6 route add <ipv6network>/ <prefixlength> dev <device> metric 1

/sbin/route -A inet6 add <network> / <prefixlength> dev <device>

Eliminar ruta a través de una interfaz:

/sbin/ip -6 route del <ipv6network>/ <prefixlength> dev <device>

/sbin/route -A inet6 del <network> / <prefixlength> dev <device>

11. CONFIGURACIÓN AVANZADA IPV6 EN BSD

Añadir una dirección IPv6:

#>ifconfig <interface> inet6 add <dir.IPv6>

Eliminar una dirección IPv6:

#>ifconfig <interface> inet6 del <dir.IPv6>

Si se desea hacer la configuración de forma permanente, se emplea el fichero /etc/rc.conf:

ipv6_enable="YES"

ipv6_ifconfig_rl0="2001:618:10:4::4 prefixlen 64"

En /etc/defaults/rc.conf se pueden consultar las posibles opciones existentes y las que se usan por defecto.

Para aplicar cambios en rc.conf habrá que reiniciar.

Añadir ruta por defecto:

#>route –n add –inet6 default <dir.IPv6>

Eliminar ruta por defecto:

#>route –n del –inet6 default

12. CONFIGURACIÓN IPV6 EN ROUTER'S CISCO

Habilitando y configurando IPv6 en un router Cisco

Comprobar la capacidad de IPv6

Hasta el momento, todos los routers sólo tienen direcciones IPv4. Igualmente se puede configurar IPv6 en las interfaces de los routers.

Una vez haya ingresado al prompt del router debería aparecer así:

```
routerX#
```

Luego comprobar la configuración del router, específicamente el soporte IPv6, con lo cual deberán aparecer las siguientes líneas estando en la configuración de alguna de las interfaces FastEthernet:

- ipv6 enable
- ipv6 unicast-routing

Un tip es verificar la versión del IOS del router que está corriendo, para ello escribir:

```
routerX> show running-config
```

El comando ***ipv6 enable*** configura una dirección IPv6 de enlace local en la interfaz a la vez que permite el procesamiento IPv6 en la interfaz. El ***ipv6 unicast-routing*** permite el enrutamiento en los routers Cisco. Si esta línea no está configurada el router no enviará todos los paquetes IPv6.

Habilitando IPv6 en una interfaz

Entrar en modo configuración:

```
routerX# configure terminal
routerX(config)#
```

Ingresar en modo de configuración de interfaz para la interfaz:

```
routerX(config)# interface fastEthernet 0/0
routerX(config-if)#
```

Habilitar IPv6 en la interfaz

```
routerX(config-if)# ipv6 enable
```

Configurar una dirección IPv6 haciendo:

```
routerX(config-if)# ipv6 2001:db8:cafe:28::2/64
```

Modificar algunos parámetros en los mensajes Router Advertisement

1. Suprimir el mensaje Router Advertisement

En los routers Cisco, después de configurar una dirección IPv6 en una interfaz, el router empieza a enviar mensajes "Router advertisement". Estos mensajes llevarán un prefijo de red igual al prefijo de la red configurado en la interfaz del router. Si no se desea que el router envíe mensajes "Router advertisement" en un enlace, se puede desactivar en la interfaz del router.

Para ello ingresar en modo de configuración de la interfaz y deshabilitar los mensajes RA:

```
routerX# configure terminal
routerX(config)# fastEthernet 0/0
routerX(config-if)# ipv6 nd ra suppress       or
routerX(config-if)# ipv6 nd suppress-ra
```

Ejemplo de salida de un switch Ethernet con capacidades de IPv6:

```
switch# show ipv6 interface vlan 28
Router2#sh ipv6 interface vlan 28
Vlan33 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::217:E0FF:FED6:A12
No Virtual link-local address(es):
```

```
Global unicast address(es):
2001:DB8:CAFE:28::2, subnet is 2001:DB8:CAFE:28::/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:3
FF02::1:FFD6:A12
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.
```

Puede comprobar que los mensajes RA están desactivadas mediante:

```
switch# show running-config | beg interface VlanX
interface Vlan28
ip address 192.168.28.2 255.255.255.0
ipv6 address 2001:DB8:CAFE:28::2/64
ipv6 enable
ipv6 nd suppress-ra
```

Para permitir los mensajes de anuncio de enrutador (RA) en la interfaz:

```
Router2# configure terminal
Router2(config)#
Router2(config)# interface interface 28
Router2(config-if)# no ipv6 nd suppress-ra
```

Salida de ejemplo:

```
Router2# show ipv6 interface vlan 28
Vlan28 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::217:E0FF:FED6:A12
…
```

```
(Output omitted)
…
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
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

2. Cambiar el intervalo de tiempo entre los mensajes Router Advertisement

Por defecto en los routers Cisco, el mensaje Router Advertisement es enviado cada 200 segundos.

Si se tienen un switch Ethernet se puede verificar el intervalo. Para cambiar el intervalo de tiempo de los mensajes RA a 30 segundos:

```
RouterX# configure terminal
RouterX(config)#
RouterX(config)# interface interface 28
routerX(config-if)# ipv6 nd ra-interval 30
```

Para ver la información IPv6 en la vlan de un switch, usar el siguiente comando:

```
switch# show ipv6 interface vlan X
```

Para verificar el intervalo de tiempo actual (solo en los switch):

```
switch# show ipv6 interface vlan 28
Vlan28 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::216:C8FF:FE30:5E4A
No Virtual link-local address(es):
Global unicast address(es):
2001:DB8:CAFE:28::2, subnet is 2001:DB8:CAFE:28::/64
Joined group address(es):
```

```
        FF02::1
        FF02::2
        FF02::1:FF00:1
        FF02::1:FF30:5E4A
        MTU is 1500 bytes
        …
        ND router advertisements are sent every 30 seconds
        ND router advertisements live for 1800 seconds
        ND advertised default router preference is Medium
        Hosts use stateless autoconfig for addresses.
```

Ó hace lo siguiente:

```
        switch# show running-config | beg interface Vlan28
        interface Vlan28
        ip address 192.168.28.2 255.255.255.0
        ipv6 address 2001:DB8:CAFE:28::2/64
        ipv6 enable
        ipv6 nd ra interval 30
```

Los grupos de multidifusión son:

FF02::1 → Todos los equipos de enlace local

FF02::2 → Todos los routers de enlace local

FF02::1:FFxx:xxxx → Dirección de nodo solicitado. Un nodo debe configurar esta dirección multicast para cada dirección IPv6 unicast y anycast. La dirección está formada por el prefijo FF02:0000:0000:0000:0000:0001:FF concatenando al final los 24 bits de la dirección unicast o anycast.

Ejemplo de salida para una breve información sobre las interfaces de IPv6:

```
        routerX# show ipv6 interface brief
        FastEthernet0 [up/up]
        FastEthernet1 [up/up]
        … (Output omitted) …
        FastEthernet2 [up/down]
```

```
        FastEthernet3 [up/up]
        …
        Vlan1 [administratively down/down]
        Vlan22 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:22::2
        Vlan23 [up/up]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:23::2
        Vlan24 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:24::2
        Vlan25 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:25::2
        Vlan26 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:26::2
        Vlan27 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:27::2
        Vlan28 [up/down]
        FE80::217:E0FF:FED6:A12
        2001:DB8:CAFE:28::2
        …
```

13. AUTOCONFIGURACIÓN STATELESS IPV6

IPv6 de forma automática puede configurarse sin el uso de un protocolo que configura las direcciones con estado, como el Protocolo de configuración dinámica de host para IPv6 (Dynamic Host Configuration Protocol-DHCPv6). La configuración automática de direcciones sólo se puede realizar en interfaces multidifusión. De manera predeterminada, un host IPv6 configura una dirección de enlace local para cada interfaz.

Mediante el uso de descubrimiento de encaminadores (router discovery), un host puede determinar las direcciones de los routers, direcciones adicionales, y otros parámetros. Una indicación de si una dirección de protocolo de configuración de estado se debe utilizar está incluido en el mensaje de anuncio de router (Router Advertisement).

Las direcciones configuradas automáticamente en uno o más de los estados se muestra en la siguiente ***Ilustración 139***. La relación entre los estados de una dirección auto-configurada, el tiempo de vida preferido y válido también se muestran.

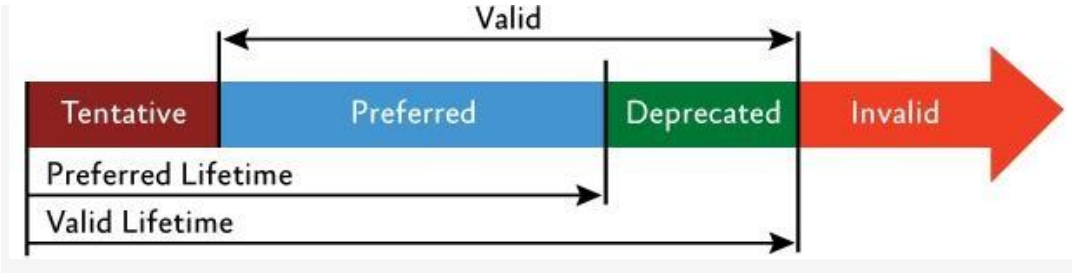


Ilustración 139. Estados de dirección de autoconfiguración

La siguiente tabla muestra los estados y sus descripciones:

Tabla 11. Estados del proceso autoconfiguración stateless

Estado	Descripción
Tentative	La dirección está en el proceso de verificación como única. La verificación ocurre a través de la detección de direcciones duplicadas. El mensaje de anuncio (Router Advertisement) del router especifica el período de tiempo que una dirección puede permanecer en este estado.
Preferred	La dirección ha sido verificada como única. Un nodo puede enviar y recibir

	tráfico unicast y de una dirección preferida. El mensaje de anuncio de router (Router Advertisement) especifica el período de tiempo que una dirección puede permanecer en este estado.
Deprecated	La dirección sigue siendo válida, pero su uso para la comunicación de nuevo no se recomienda. Las sesiones de comunicación existentes pueden continuar utilizando una dirección obsoleta. Un nodo puede enviar y recibir tráfico unicast hacia y desde una dirección obsoleta.
Valid	La dirección puede enviar y recibir tráfico unicast. Este estado se refiere tanto a los Estados preferido y obsoleto. El mensaje de anuncio del router especifica el período de tiempo que una dirección puede permanecer en este estado. La duración válida debe ser mayor o igual a la duración preferida.
Invalid	La dirección ya no puede enviar tráfico unicast o recibirlo de un nodo. Una dirección entra en este estado después de que el periodo de vida válido expira.

Siendo el proceso de auto-configuración de direcciones ipv6 de un nodo el siguiente:

- Una dirección local de vínculo tentativa se deriva, basado en el prefijo local de vínculo FE80:: / 64 y el identificador de interfaz de 64 bits.
- La detección de direcciones duplicadas se realiza para comprobar la exclusividad de la tentativa dirección local de vínculo.
- En caso de detección de direcciones duplicadas falle, se debe configurar manualmente el nodo. O, si la detección de direcciones duplicadas tiene éxito, la dirección provisional se supone que es válido y única. La dirección de enlace local se inicializa para la interfaz.

Para un host IPv6, configuración automática de direcciones continúa como se muestra en la siguiente lista:

- El host envía un mensaje de solicitud de enrutador.

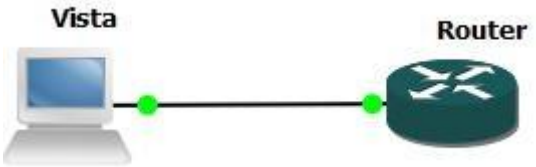
- Si el mensaje de anuncio (Router Advertisement) del router es recibido, la información de enrutamiento se configura en el host.

- Para cada prefijo de direcciones de configuración automática sin estado (stateless) que se incluye, ocurre el siguiente proceso:

    - El prefijo de la dirección y la de 64 bits de identificador de interfaz se utilizan para derivar una dirección tentativa.

    - La detección de direcciones duplicadas se utiliza para comprobar la exclusividad de la dirección provisional. Si la dirección tentativa está en uso, la dirección no se inicializa para la interfaz. Si la dirección tentativa no está en uso, la dirección se ha inicializado. Esto incluye el establecimiento de la duración válida y preferida sobre la base de información contenida en el mensaje de anuncio de router.

El escenario a implementar será el mostrado en la siguiente ilustración. Para ello se ha utilizado un pc con Windows Vista con IPv6 (por defecto) el cual se encuentra conectado al router Cisco 2811 a través de la Interfaz Ethernet.



El router Fa0 / 1 se configura de la siguiente manera:

```
maestria(config)# ipv6 unicast-routing
maestria(config)# interface fastEthernet 0/1
maestria(config-if)# ipv6 enable
maestria(config-if)# ipv6 nd prefix 2001:ABAB::/48 2000 2000    <--- Optional
maestria(config-if)# ipv6 nd managed-config-flag                <--- Optional
maestria(config-if)# ipv6 nd other-config-flag                  <--- Optional
```

```
maestria(config-if)# no shutdown
```

El comando ***debug ipv6 nd*** muestra la siguiente salida. Cuando el router recibe un mensaje de RS desde el host antes de que su dirección local sea asignada, se crea una entrada para el host en su Neighbor Cache con el estado “incompleto” e inmediatamente pone al Estado de “no fresco o viejo” y lleva a cabo el mecanismo de DAD.

Cuando la interfaz Fa0/1 levanta, el primer router realiza DAD enviando un mensaje NS con una dirección "tentativa" como la dirección de destino. Una vez el mecanismo DAD comprueba es único, el vínculo de la dirección local se asigna a la interfaz. Windows Vista está configurado para enviar mensajes RS por defecto y el router los recibe en Fa0/1. Así el router envía un mensaje RA con la información configurada como, información de prefijo, flags “M” o “O” y tiempos de vida válida y recomendados.

```
maestria(config-if)#

*Nov 19 02:32:31.971: ICMPv6-ND: Received NS for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1 from FE80::58E6:E63C:730D:B8B

*Nov 19 02:32:31.971: ICMPv6-ND: NS target is not ready

*Nov 19 02:32:32.831: ICMPv6-ND: Sending NS for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1

*Nov 19 02:32:32.971: ICMPv6-ND: Received NS for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1 from FE80::58E6:E63C:730D:B8B

*Nov 19 02:32:32.971: ICMPv6-ND: NS target is not ready

*Nov 19 02:32:33.831: ICMPv6-ND: DAD: FE80::21B:2AFF:FEEC:47C1 is unique.

*Nov 19 02:32:33.831: ICMPv6-ND: Sending NA for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1

*Nov 19 02:32:33.831: ICMPv6-ND: Address FE80::21B:2AFF:FEEC:47C1/10 is up on
```

```
FastEthernet0/1

*Nov 19 02:32:34.971: ICMPv6-ND: Received RS on FastEthernet0/1 from
FE80::58E6:E63C:730D:B8B

*Nov 19 02:32:34.971: ICMPv6-ND: Sending RA to FF02::1 on FastEthernet0/1

*Nov 19 02:32:34.971: ICMPv6-ND:     MTU = 1500

*Nov 19 02:32:38.471: ICMPv6-ND: Received NS for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1 from FE80::58E6:E63C:730D:B8B

*Nov 19 02:32:38.471: ICMPv6-ND: Sending NA for FE80::21B:2AFF:FEEC:47C1 on
FastEthernet0/1
```

Análisis de trama Router Advertisements

A continuación se hará uso del analizador de red “wireshark” para ver de cerca lo que sucede cuando una interfaz se configura con auto-configuración de direcciones sin estado y analizar otros mecanismos de IPv6 fundamental.

Para ello iniciar la captura de la primera interfaz ethernet (que debería ser "eth0"). Se visualizaran anuncios de enrutamiento (Routing Advertisements) ICMPv6 al conectar un extremo del patchcord en la interfaz fe0/1 del router y el otro extremo a la PC.

Detener la captura cuando se tengas por lo menos 10 mensajes. Utilizando el menú Ver, se puede desmarcar “Bytes del paquete” para tener mayor espacio en la pantalla.

Hacer clic en cualquiera de los paquetes ICMPv6 Router Advertisement. En el área de Detalles del paquete de la ventana de Wireshark, haga clic en el revelar (+) situado de forma recursiva para abrir el paquete y así ver todos los campos y subcampos del "Protocolo de Internet versión 6" y "Internet Control Message Protocol v6".

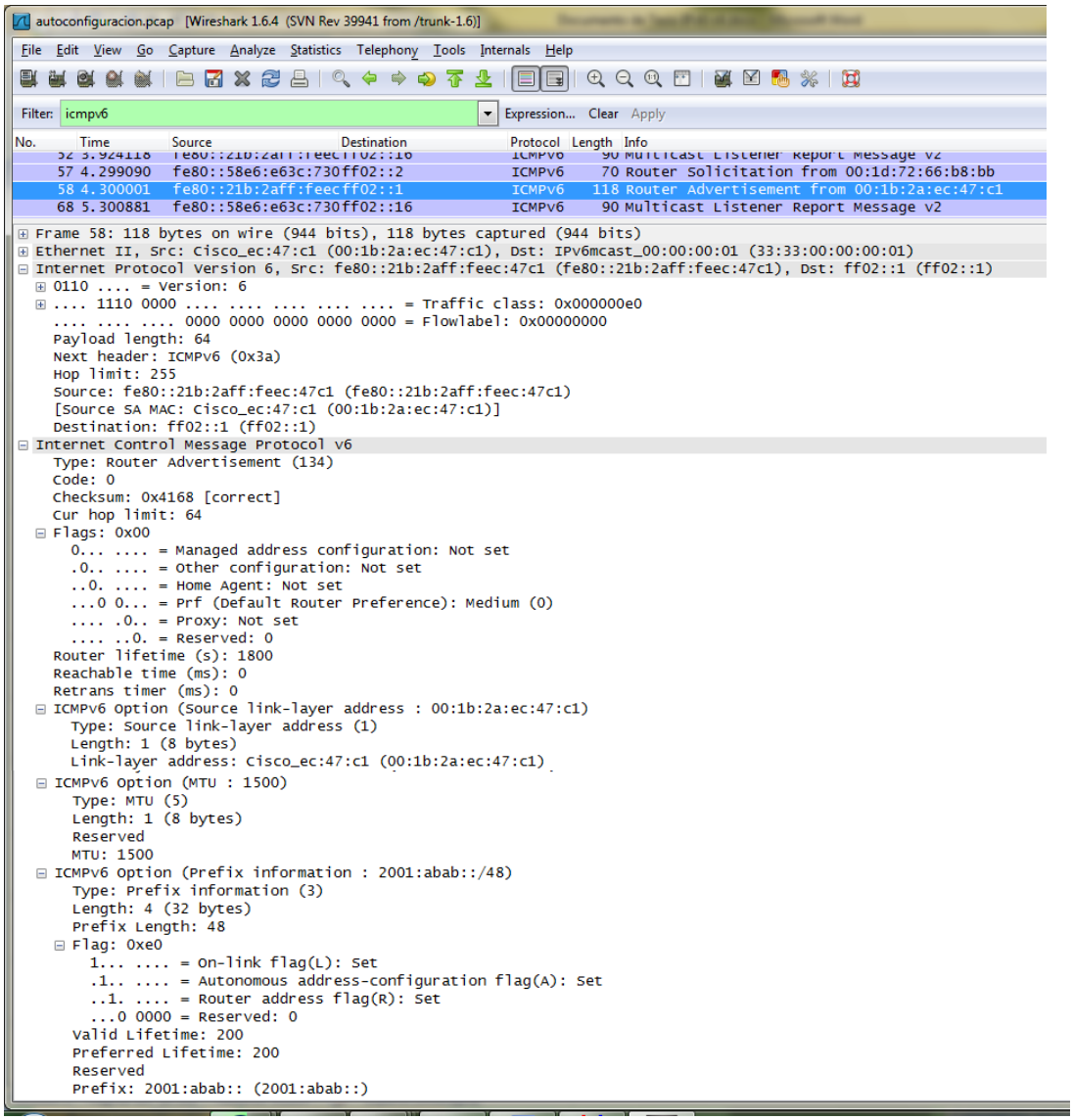


Ilustración 140. Detalle de un mensaje Router Advertisement IPv6

Aquí hay una breve explicación de las partes más importantes del Router Advertisement, de arriba a abajo en la vista de Detalles del paquete.

- IPv6 Source. En este paquete se muestra la dirección unicast de vínculo local.
- IPv6 Destination. ff02::1 es una dirección bien conocida comúnmente llamada "dirección multicast de vínculo local a todos los hosts". Cada host en la red local escuchara todo el tráfico enviado a esta dirección.

Internet Control Message Protocol v6 (ICMPv6)

- Type. ICMPv6 es un protocolo de gestión que es muy importante para el funcionamiento de IPv6. Como tal, hay muchos tipos diferentes de mensajes que se pueden transmitir. Para identificar el tipo de mensaje que se transmite, el campo type es utilizado. Aquí, el type 134 identifica este mensaje como un Router Advertisement (anuncio de router).

- Banderas ICMPv6. La bandera de configuración "Managed" especifica si la dirección "de configuración de estado" se va a utilizar. La configuración con estado general, se entiende por DHCPv6. En la mayoría de las redes, este indicador no se establece, lo que significa que el sistema debe utilizar "Configuración automática de direcciones sin estado" (StateLess Address AutoConfiguration -SLAAC).

  La bandera de estado de configuración " Other" significa que los nodos en este enlace (red local) deben utilizar la configuración de estado (DHCPv6) para otras cosas adicionales a la asignación de direcciones. Por lo tanto, si usted no utiliza la configuración de estado para la asignación de direcciones, se puede utilizar para anunciar otro tipo de información (tales como información sobre los servicios de DNS).

  Por ejemplo, en la captura anterior, vimos M=0 y S=0, que significa "Not managed" y "Not other". Por lo que no utilizan la configuración de estado (como DHCPv6) para tratar de obtener una dirección (en lugar de eso sólo tiene que utilizar SLAAC), no hay direcciones de información sobre la red (por ejemplo, configuración DNS, a cuál host enviar los mensajes de log y una amplia gama de posibilidades).

  Estos "M" y "O" bits (Managed y Other) son importantes para entender cómo la asignación de direcciones IPv6 funciona.

- Opción ICMPv6 (información de prefijo). Puede haber una serie de componentes opcionales para un Router advertisement. La más común sería una opción de publicidad lo que se utiliza "como prefijo(s)" en este enlace. Un prefijo es muy

parecido a una dirección de red: en SLAAC, un conjunto de direcciones se forma tomando cada prefijo y la adición de la interfaz EUI-64 ID de host (normalmente formado por la dirección MAC).

Tener en cuenta que puede haber varias opciones de "Prefijo de información" incluidas en un router advertisement. Una interfaz puede usar varios prefijos para generar varias direcciones IPv6.

- Longitud de prefijo ICMPv6. ICMPv6 Prefix length, nos dice que este prefijo en particular es un /48 (recordar que las direcciones IPv6 son de 128 bits). Con SLAAC, todos los prefijos anunciados son /48**,** lo que hace esta entrada en particular y no menos interesante.

- ICMPv6 Banderas. La única bandera que queremos llamar su atención aquí es la bandera de configuración autónoma (que se muestra como "Autonomous address-configuration flag(A): Set" en la imagen). Hay que recordar que puede haber varios prefijos incluidos en un anuncio de enrutador: sólo los marcados con la bandera "auto" obtienen direcciones SLAAC. Esto es por defecto.

- Prefijo de ICMPv6. Esta es la pieza clave de los datos de este anuncio. Junto con la longitud del prefijo hemos visto anteriormente, vemos que esta el prefijo que se anuncia es 2001:abab::/48. Visto sin comprimir, así que usted puede ver exactamente qué tan largo es el prefijo en relación con la dirección completa:

  2001:abab:0000:0000:0000:0000:0000:0000

  bits de red ↤ ↦ bits de host

- ICMPv6 Source link-layer address option. Esta opción sólo comunica la dirección MAC del router a los host en el enlace, para que puedan pre-almacenar de la "caché de sus vecino" (esto es como ARP, a pesar de que IPv6 no utiliza ARP, pero es algo similar). Estando incluido significa que no se da un mensaje extra de ida y vuelta en la red para averiguar la capa de enlace (MAC) del router, lo que reduce el plazo.

Todo lo anterior es un router advertisement, visto en el estado donde un nuevo host aparece en el enlace. Ahora vamos a repetir la captura y esta vez vamos veremos todo lo que sucede cuando una interfaz levanta.

Para ello cambiar el tamaño de la pantalla de Wireshark para que el área de la lista de paquetes ocupe la mayor parte de la pantalla. Iniciar una nueva captura en vivo en Wireshark, es posible descartar la captura anterior. Cuando se ha empezado a capturar, desde una terminal de linux ejecute el comando ***ifconfig eth0 down***, como usuario root, lo cual "apagara" la interfaz "eth0", básicamente desactivar y eliminar cualquier información que se relaciona con ella, tales como entradas de la tabla de enrutamiento [18].

Ahora recordar cual fue el último paquete que se muestra actualmente en el área de lista de paquetes Wireshark. Para levantar la interfaz hacerlo con "***ifconfig eth0 up***", con lo cual se verán varios paquetes llegan a la ventana.

No.	Time	Source	Destination	Protocol	Info
8	*REF*	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
9	0.143968	::	ff02::1:ff99:c27d	ICMPv6	Neighbor solicitation
10	1.143983	fe80::a00:27ff:fe99:c27d	ff02::2	ICMPv6	Router solicitation
11	1.145709	fe80::a00:27ff:fe5c:cced	ff02::1	ICMPv6	Router advertisement
12	1.715971	::	ff02::1:ff99:c27d	ICMPv6	Neighbor solicitation
13	5.383968	fe80::a00:27ff:fe99:c27d	ff02::16	ICMPv6	Multicast Listener Report Message v2
14	7.828503	fe80::a00:27ff:fe5c:cced	ff02::1	ICMPv6	Router advertisement
15	13.170226	fe80::a00:27ff:fe5c:cced	ff02::1	ICMPv6	Router advertisement
16	19.628712	fe80::a00:27ff:fe5c:cced	ff02::1	ICMPv6	Router advertisement

En la ilustración anterior Wireshark muestra los paquetes cuando la interfaz levanta. Los paquetes marcados como *REF* es el primer paquete en llegar al sistema después que se levanta la interfaz.

Comandos netsh para la interfaz IPv6

Por defecto, un PC con Windows Vista genera un identificador de interfaz aleatorio. Sin embargo, este comportamiento se puede desactivar mediante el siguiente comando desde la consola del prompt:

C:\> netsh interface ipv6 set global randomizeidentifiers=disabled

La siguiente salida es tomada desde una PC con Windows Vista con la opción desactivada. Las direcciones IPv6 son de la forma ***ipv6address%ZoneID*** indicando que es una dirección de enlace local fe80::21b:2aff:feec:47c1 (las direcciones de enlace local inician con **FE80::**) y el ZoneID de la interfaz a la cual la dirección esta asignada **%11**(el índice de la interfaz LAN):

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : unanleon.edu.ni
   Vínculo: dirección IPv6 local. . . : fe80::58e6:e63c:730d:b8b%11
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.100.10
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::21b:2aff:feec:47c1%11
                                               192.168.100.1
```

A menos que se configuren manualmente, el ZoneID es el índice de interfaz de direcciones locales de vínculo. Para direcciones de sitios locales, el ZoneID es el número del sitio. El ZoneID no es necesario para direcciones globales.

Cuando esta deshabilitado, IPv6 utiliza el formato identificador de interfaz EUI-64. Dos octetos ***0xFF*** y ***0xFE*** indican EUI-64 el formato identificador de interfaz EUI-64.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . :   fe80::222:19ff:fedf:9252%11
   Autoconfiguration IPv4 Address. . : 169.254.41.115
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::211:92ff:feec:b255%11
```

El comando "***netsh interface ipv6 show interface***" muestra la lista de las interfaces IPv6, el índice de la interfaz, métrica de la interfaz, vínculo MTU, estado y nombre de la interfaz.

```
C:\Windows\System32>netsh interface ipv6 show interface

Índ     Mét         MTU         Estado              Nombre
---  ----------  ----------  ------------  ---------------------------
  1          50  4294967295  connected     Loopback Pseudo-Interface 1
 13          25        1500  disconnected  Conexión de red inalámbrica
 12          30        1280  disconnected  isatap.{9B3534A3-5DE6-40F7-B298-
21E47
2CF3394}
 19           5        1500  disconnected  Conexión de red inalámbrica 2
 14          30        1280  disconnected  isatap.{BE6645EA-C859-4AC4-9013-
8C6E7
941D5F2}
 11          20        1500  connected     Conexión de área local
 20          30        1280  disconnected  isatap.unanleon.edu.ni
 21          30        1280  disconnected  isatap.{D29B4575-0350-42A8-9EDA-
979AB
B9ECEC7}
 17          30        1280  disconnected  Teredo Tunneling Pseudo-Interface
 15          20        1500  connected     VMware Network Adapter VMnet1
 23          30        1280  disconnected  isatap.{BDD54A50-CDDE-4C93-992E-
07ADB
78CA001}
 16          20        1500  connected     VMware Network Adapter VMnet8
```

El comando "***netsh interface ipv6 show address***" muestra las direcciones IPv6 asignadas por la interfaz, los tipos de direcciones, estado DAD (de preferencia o en desuso), y tiempos de vida preferido y válido.

```
C:\Windows\System32>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 13: Conexión de red inalámbrica

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- -------------- -----------------------
-
```

```
Otros      Obsoleto      infinite   infinite fe80::6c14:8e35:9d3a:128f%13

Interfaz 12: isatap.{9B3534A3-5DE6-40F7-B298-21E472CF3394}

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Obsoleto      infinite   infinite fe80::5efe:192.168.22.1%12

Interfaz 19: Conexión de red inalámbrica 2

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Obsoleto      infinite   infinite fe80::cc36:e33c:ec7c:38ac%19

Interfaz 14: isatap.{BE6645EA-C859-4AC4-9013-8C6E7941D5F2}

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Obsoleto      infinite   infinite fe80::5efe:169.254.11.139%14

Interfaz 11: Conexión de área local

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Preferido     infinite   infinite fe80::58e6:e63c:730d:b8b%11

Interfaz 17: Teredo Tunneling Pseudo-Interface

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Obsoleto      infinite   infinite fe80::e0:0:0:0%17

Interfaz 15: VMware Network Adapter VMnet1

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
-

Otros      Preferido     infinite   infinite fe80::3c90:cf03:450f:336d%15

Interfaz 16: VMware Network Adapter VMnet8

Tipo direc.  Estado DAD  Vigencia válida Vigencia pref. Dirección
-----------  ----------- --------------- ------------- -----------------------
```

```
-

Otros      Preferido     infinite   infinite fe80::24f4:fde6:588d:df29%16


C:\Windows\System32>
```

La siguiente salida muestra la dirección MAC de la interfaz Fa0/1 del router que se utiliza para crear el formato identificador de interfaz EUI-64 para la dirección de vinculo local.

```
maestria>show interface fastEthernet 0/1 | include Hardware
  Hardware is MV96340 Ethernet, address is 001b.2aec.47c1 (bia 001b.2aec.47c1)
maestria>
*Nov 19 03:16:40.243: ICMPv6-ND: Sending RA to FF02::1 on FastEthernet0/1
*Nov 19 03:16:40.243: ICMPv6-ND:     MTU = 1500
```

```
maestria#show interface fastEthernet 0/1 | include Hardware
  Hardware is MV96340 Ethernet, address is 001b.2aec.47c1 (bia 001b.2aec.47c1)
maestria#show ipv6 interface
FastEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21B:2AFF:FEEC:47C1
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FFEC:47C1
  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.
maestria#
```

El siguiente comando muestra el Neighbor Cache y su estado. Muestra a los vecinos conectados al enlace. En este caso el equipo con Windows esta conectado a la intefaz FastEthernet 0/1. La direccion de vínculo local es la dirección MAC del PC con Windows.

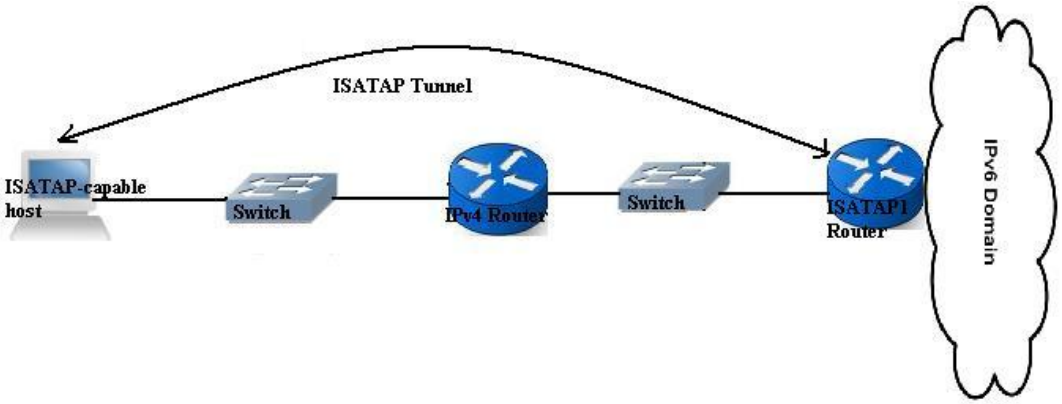
```
maestria#show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::58E6:E63C:730D:B8B                    0 001d.7266.b8bb  REACH Fa0/1
```

Cuando el router intenta hacer ping al enlace local de la PC de Windows Vista FE80::58E6:E63C:730D:B8B, el router consulta su caché de vecinos (Neighbor Cache). El estado de la entrada es obsoleta. Dado que el paquete se envía sobre la base de la entrada obsoleta, se cambia el estado a RETRASADO. Desde entonces, no puede verificar la "progreso de envio" usando paquetes ICMP (como PING/ICMP se ejecuta directamente sobre IP), el estado cambia a PROBE (exploración) y se envía un mensaje de NS al vecino. Una vez que el mensaje NA se recibe, se cambia el estado de REACH (alcanzado).

```
maestria#ping FE80::58E6:E63C:730D:B8B
Output Interface: fastethernet0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::58E6:E63C:730D:B8B, timeout is 2
seconds
:
Packet sent with a source address of FE80::21B:2AFF:FEEC:47C1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
maestria#
```

```
maestria#show ipv6 neighbor
IPv6 Address                              Age Link-layer Addr State Interface
FE80::62EB:69FF:FEF8:63A4                  41 60eb.69f8.63a4  STALE Fa0/1
FE80::58E6:E63C:730D:B8B                    0 001d.7266.b8bb  REACH Fa0/1

maestria#
```

14. CONFIGURAR ISATAP



En este caso, los siguientes pasos se toman en un host con Windows XP para la conexión ISATAP:

1. IPv6 está desactivado por defecto en Windows XP. Para activar, utilizar el comando "**ipv6 install**" desde la línea de comandos.
2. El host tiene que resolver la dirección IPv4 para el nombre "ISATAP". Esto se puede hacer de las siguientes maneras:
    a. Manualmente proporcionar la dirección IPv4 del router ISATAP usando el comando"**netsh interface ipv6 isatap set router 192.16.1.1**" desde el símbolo del sistema.
    b. Editar el archivo **hosts** el cual se encuentra localizado en la carpeta "**C:\Windows\System32\drivers\etc**" con la entrada "**192.16.1.1 isatap**".
    c. Utilizar el servidor de DNS.

Si un host desea utilizar varios enrutadores ISATAP para la redundancia, la configuración manual no funcionará. En este caso será necesaria una búsqueda de DNS utilizando los métodos anteriores.

Cuando el host es el primero habilitado para IPv6, el comando "**ipconfig /all**" muestra lo siguiente para el adaptador ISATAP. El host genera una dirección de enlace local de la forma "**FE80::0:5EFE:d.d.d.d**" por sí mismo, donde **d.d.d.d** es la dirección IPv4 del host.

No tiene ninguna información sobre su puerta de enlace predeterminada, que será la dirección local de enlace del router ISATAP.

```
Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Automatic Tunneling Pseudo-
Interface

        Physical Address. . . . . . . . . : 0A-01-01-02
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : fe80::5efe:10.1.1.2%2
        Default Gateway . . . . . . . . . :
        DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%2
                                            fec0:0:0:ffff::2%2
                                            fec0:0:0:ffff::3%2
        NetBIOS over Tcpip. . . . . . . . : Disabled
```

El router ISATAP es configurado a como se muestra a continuación:

```
               -------  configuración el router ISATAP1  -------
ipv6 unicast-routing
ipv6 cef
!
interface fastethernet 0/0
 ip address 192.16.1.1 255.255.255.0
!
interface Tunnel 0
 ipv6 address 2001:ABAB::/64 eui-64
 tunnel source fastethernet 0/0
 tunnel mode ipv6ip isatap
 no ipv6 nd ra suppress
!
interface Loopback 0
 ipv6 address CAFE::1/128
!
```

NOTA. El comando "***no ipv6 nd ra suppress***" es necesario para que el router no envíe mensajes RA en la interfaz de túnel (esta desactivado por defecto).

Esta configuración resulta en una dirección IPv6 asignada a la interfaz de túnel correspondiente a la interfaz FastEthernet 0/0 (C010:0101 = 192.16.1.1).

```
ISATAP1# show ipv6 interface brief
FastEthernet0/0            [up/up]
FastEthernet0/1            [administratively down/down]
Loopback0                  [up/up]
    FE80::CE02:14FF:FEE4:0
```

```
    CAFE::1
Tunnel0                   [up/up]
    FE80::5EFE:C010:101
    2001:ABAB::5EFE:C010:101
```

Cuando el host envía un mensaje de solicitud al router (RS) encapsulado en un paquete IPv4 sobre el túnel ISATAP, el router ISATAP envía un mensaje de anuncio de enrutador (RA) al host con la información de prefijo y MTU. También anuncia la ruta por defecto y el siguiente salto como su dirección local de vínculo.

```
   -------  "debug ipv6 nd" y "debug ipv6 icmp" en el router ISATAP1  -------

*Mar  1 00:54:17.719: ICMPv6: Received ICMPv6 packet from FE80::5EFE:A01:102,
type 133
*Mar  1 00:54:17.723: ICMPv6-ND: Received RS on Tunnel0 from FE80::5EFE:A01:102
*Mar  1 00:54:17.727: ICMPv6-ND: Sending solicited RA on Tunnel0
*Mar  1 00:54:17.727: ICMPv6-ND: Sending RA from FE80::5EFE:C010:101 to
FE80::5EFE:A01:102 on Tunnel0
*Mar  1 00:54:17.731: ICMPv6-ND:     MTU = 1480
*Mar  1 00:54:17.735: ICMPv6-ND:     prefix = 2001:ABAB::/64 onlink autoconfig
*Mar  1 00:54:17.735: ICMPv6-ND:              2592000/604800 (valid/preferred)
```

El host genera una dirección IPv6 por sí mismo basado en el prefijo anunciado por el router ISATAP en los mensajes RA.

A veces, en Windows XP, el host no aceptar el mensajes RA desde el router ISATAP. En este caso, desinstalar IPv6 usando el comando "***IPv6 uninstall***" desde el símbolo del sistema y "*install IPv6*" nuevamente.

```
  -------  adaptador ISATAP en el host después de recibir mensaje RA  -------

Tunnel adapter Automatic Tunneling Pseudo-Interface:

       Connection-specific DNS Suffix  . :
       Description . . . . . . . . . . . : Automatic Tunneling Pseudo-
Interface

       Physical Address. . . . . . . . . : 0A-01-01-02
       Dhcp Enabled. . . . . . . . . . . : No
       IP Address. . . . . . . . . . . . : 2001:abab::5efe:10.1.1.2
       IP Address. . . . . . . . . . . . : fe80::5efe:10.1.1.2%2
       Default Gateway . . . . . . . . . : fe80::5efe:192.16.1.1%2
       DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%2
                                           fec0:0:0:ffff::2%2
```

```
                                                    fec0:0:0:ffff::3%2
       NetBIOS over Tcpip. . . . . . . . : Disabled
```

La table de enrutamiento en el host quedara así:

```
C:\> netsh interface ipv6 show route
Querying active state...

Publish  Type       Met  Prefix                    Idx   Gateway/Interface
Name
-------  --------  ----  ------------------------  ---  ----------------------
no       Autoconf     9     2001:abab::/64         2     Automatic Tunneling
Pseudo-Interface
no       Autoconf   257    ::/0                       2     fe80::5efe:192.16.1
.1
```

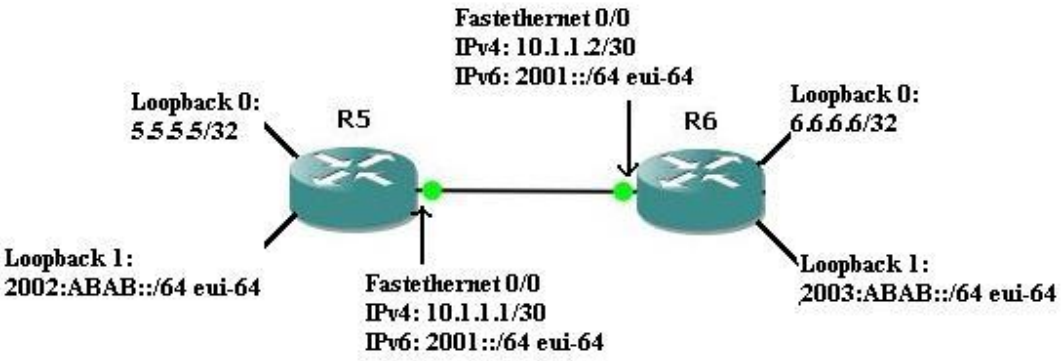
Al hacer PING a un dominio IPv6, por ejemplo a la interfaz Loopback 0 del router ISATAP desde el host, da resultados satisfactorios, como se muestra a continuación:

```
C:\> ping6 cafe::1

Pinging cafe::1
from 2001:abab::5efe:10.1.1.2 with 32 bytes of data:

Reply from cafe::1: bytes=32 time=129ms
Reply from cafe::1: bytes=32 time=197ms
Reply from cafe::1: bytes=32 time=177ms
Reply from cafe::1: bytes=32 time=206ms

Ping statistics for cafe::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 129ms, Maximum = 206ms, Average = 177ms
```

15. PILA DUAL

La pila dual es una forma de implementar IPv6, y seguir siendo compatibles con IPv4. Un nodo que corre IPv6 y la pila de protocolos IPv6 se llama un nodo IPv6/IPv6. Un nodo IPv6/IPv4 se comunica usando paquetes IPv6 con nodos IPv6 y usando paquetes IPv4 con nodos IPv4.

Considere lo siguiente. Dos nodos IPv6/IPv4, R5 y R6, están conectados entre sí a través de una interfaz FastEthernet. La interfaz FastEthernet está configurada con una dirección IPv4, así como una dirección IPv6, a como se muestra en la siguiente ilustración:



La configuracion de ambos routers se muestra a continuación:

------- Router R5 -------	------- Router R6 -------
ipv6 unicast-routing ipv6 cef ! interface Loopback 0 ip address 5.5.5.5 255.255.255.255 ! interface Loopback 1 ipv6 address 2002:ABAB::/64 eui-64 ipv6 rip TEST enable ! interface fastethernet 0/0 ip address 10.1.1.1 255.255.255.252 ipv6 address 2001::/64 eui-64 ipv6 rip TEST enable ! router ospf 1 network 5.5.5.5 0.0.0.0 area 0	ipv6 unicast-routing ipv6 cef ! interface Loopback 0 ip address 6.6.6.6 255.255.255.255 ! interface Loopback 1 ipv6 address 2003:ABAB::/64 eui-64 ipv6 rip TEST enable ! interface fastethernet 0/0 ip address 10.1.1.2 255.255.255.252 ipv6 address 2001::/64 eui-64 ipv6 rip TEST enable ! router ospf 1 network 6.6.6.6 0.0.0.0 area 0

network 10.1.1.0 0.0.0.3 area 0 ! ipv6 router rip TEST !	network 10.1.1.0 0.0.0.3 area 0 ! ipv6 router rip TEST !

El comando "***show ip interface brief***" muestra las interfaces configuradas con las direcciones IPv4 en el router R5.

```
R5#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            10.1.1.1        YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Loopback0                  5.5.5.5         YES manual up                    up
Loopback1                  unassigned      YES unset  up                    up
```

El commando "***show ipv6 interface brief***" muestra las interfaces configuradas con direcciones IPv6 en el router R5:

```
R5# show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::C200:EFF:FE24:0
    2001::C200:EFF:FE24:0
FastEthernet0/1            [administratively down/down]
Loopback0                  [up/up]
Loopback1                  [up/up]
    FE80::C200:EFF:FE24:0
    2002:ABAB::C200:EFF:FE24:0
```

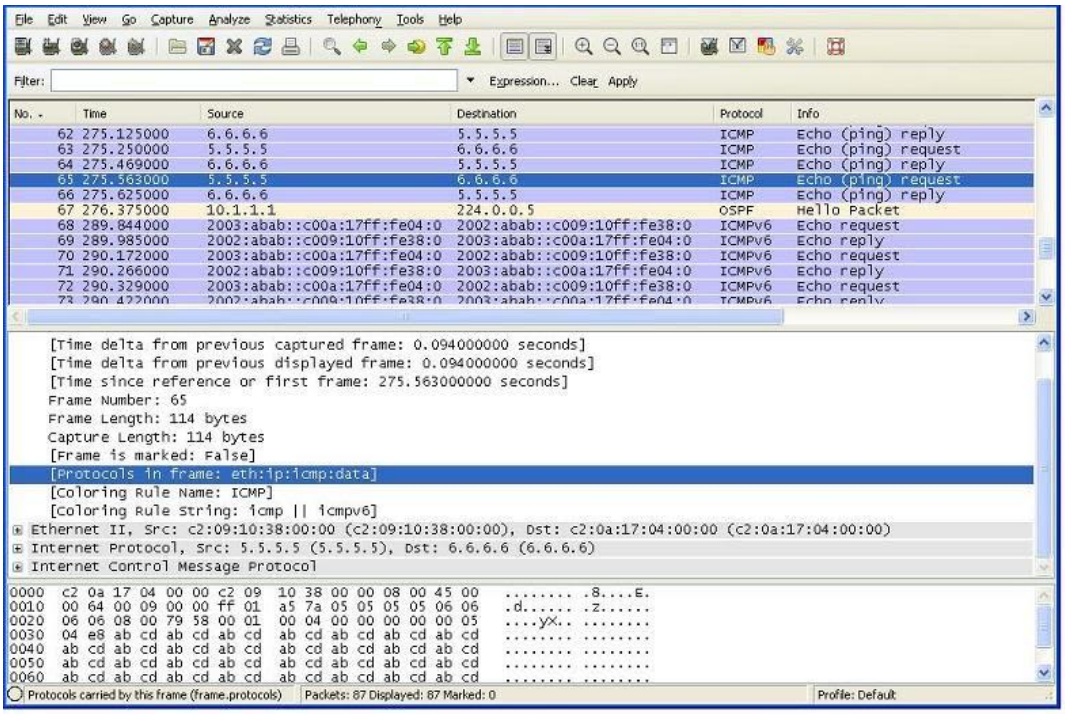
El comando "***show ip route***" muestra la tabla de enrutamiento IPv4 en el router R5. Esto demuestra que la interfaz loopback0 del router R6 es accesible a través de Fa 0/0.

```
R5# show ip route | begin Gateway
Gateway of last resort is not set

     5.0.0.0/32 is subnetted, 1 subnets
C       5.5.5.5 is directly connected, Loopback0
     6.0.0.0/32 is subnetted, 1 subnets
O       6.6.6.6 [110/11] via 10.1.1.2, 00:07:26, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
```

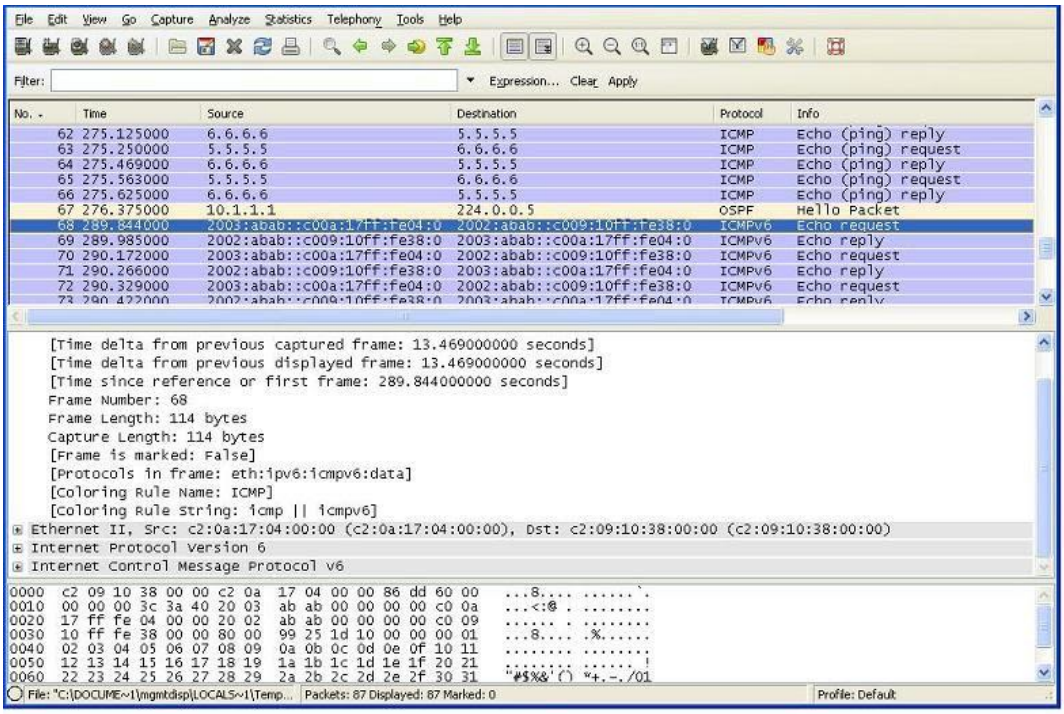
El comando "**show ipv6 route**" muestra la tabla de enrutamiento IPv6 del router R5. Esto demuestra que la interfaz de Loopback1 del router R6 también es alcanzable a través de la interfaz FastEthernet 0/0.

```
R5# show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001::/64 [0/0]
     via ::, FastEthernet0/0
L   2001::C200:EFF:FE24:0/128 [0/0]
     via ::, FastEthernet0/0
C   2002:ABAB::/64 [0/0]
     via ::, Loopback1
L   2002:ABAB::C200:EFF:FE24:0/128 [0/0]
     via ::, Loopback1
R   2003:ABAB::/64 [120/2]
     via FE80::C201:EFF:FE24:0, FastEthernet0/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

La salida siguiente muestra el flujo de tráfico IPv4 del router R5 al router R6 a través de la interfaz de salida FastEthernet 0/0.



La siguiente salida muestra el tráfico IPv6 que fluye del router R6 al router R5 a través de salida FastEthernet 0/0.



16. AUTOMATIC 6TO4 TUNNEL

Túnel 6to4 automático es un método para conectar dominio IPv6 a través de nubes IPv4. Se asigna un único prefijo IPv6 a cualquier sitio que actualmente cuenta con al menos un dirección IPv6 única a nivel mundial. Se proporcionan mecanismos para la transmisión de paquetes IPv6 utilizando un prefijo en la red IPv4 global.

La IANA ha asignado un agregador de nivel superior de 13 bits (TLA) en formato de prefijo IPv6 (FP) 001 para el esquema de 6to4. Su valor numérico es 0x0002 es decir, es de 2002::/16 cuando se expresa como un prefijo de dirección IPv6.

El sitio de suscriptores que tiene al menos una dirección IPv4 unica globalmente, es considerada para tener una dirección IPv6 con información de prefijo:

Prefix Length: 48
Format Prefix: 001
TLA Value: 0002
NLA Value: IPv4 address

Este prefijo puede ser abreviado como: **2002:V4ADDR::/48**.

Encapsulacion en IPv4:

Los paquetes IPv6 son encapsulados en paquetes IPv4 con un protocolo IPv4 de tipo 41 (0x29). La cabecera de IPv4 contiene las direcciones origen y destino IPv4. El cuerpo del paquete IPv4 contiene la cabecera IPv6 y la carga útil.

------- Router SiteA -------	------- Router SiteB -------
ipv6 unicast-routing ipv6 cef ! interface fastethernet 0/0 ipv6 address 2001:1:1:1::2/124 ipv6 rip TEST enable no shutdown ! ipv6 router rip TEST	ipv6 unicast-routing ipv6 cef ! interface fastethernet 0/0 ipv6 address 2001:2:2:2::2/124 ipv6 rip TEST enable no shutdown ! ipv6 router rip TEST

!	!

```
   -------  Router SiteA_6to4 -------

ipv6 unicast-routing
ipv6 cef
!
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
 ipv6 address 2002:0101:0101::1/64
!
interface Tunnel 0
 ipv6 address 2002:0101:0101:FFFF::1/64
 tunnel source Loopback 0
 tunnel mode ipv6ip 6to4
!
interface serial 0/0
 ip address 192.16.1.1 255.255.255.252
 no shutdown
!
interface fastethernet 0/0
 ipv6 address 2001:1:1:1::1/124
 ipv6 rip TEST enable
 no shutdown
!
router ospf 1
 network 192.16.1.0 0.0.0.3 area 0
 network 1.1.1.1 0.0.0.0 area 0
!
ipv6 router rip TEST
 redistribute static metric 5
!
ipv6 route 2002::/16 Tunnel 0
ipv6 route 2001:2:2:2::/64
2002:0303:0303::1
!
```

```
   -------  Router SiteB_6to4 -------

ipv6 unicast-routing
ipv6 cef
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
 ipv6 address 2002:0303:0303::1/64
!
interface Tunnel 0
 ipv6 address 2002:0303:0303:FFFF::1/64
 tunnel source Loopback 0
 tunnel mode ipv6ip 6to4
!
interface serial 0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface fastethernet 0/0
 ipv6 address 2001:2:2:2::1/124
 ipv6 rip TEST enable
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 3.3.3.3 0.0.0.0 area 0
!
ipv6 router rip TEST
 redistribute static metric 5
!
ipv6 route 2002::/16 Tunnel 0
ipv6 route 2001:1:1:1::/64
2002:0101:0101::1
!
```

Las direcciones IPv4 en la interfaz loopback0 de los router SiteA_6to4 y SiteB_6to4 se convierten en números hexadecimales y se convierten en direcciones IPv6 de la forma 2002:V4ADDR::/64.

Un túnel 6to4 es un túnel de punto a multipunto. La interfaz de túnel sólo tiene una dirección de origen y la dirección destino se deriva del destino del paquete.

```
                        -------  Tunnel interface -------
SiteA_6to4# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
```

```
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 1.1.1.1 (Loopback0), destination UNKNOWN
  Tunnel protocol/transport IPv6 6to4
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:02:03, output 00:02:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     36 packets input, 4064 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     42 packets output, 4680 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Los routers SiteA_6to4 y SiteB_6to4 son routers de doble pila. A continuación, el router SiteA_6to4 está configurado con direcciones IPv6:

```
                  -------  show ipv6 interface brief  -------
SiteA_6to4# show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::CE08:13FF:FEEC:0
    2001:1:1:1::1
FastEthernet0/1            [administratively down/down]
Serial1/0                  [up/up]
Serial1/1                  [administratively down/down]
Serial1/2                  [administratively down/down]
Serial1/3                  [administratively down/down]
Loopback0                  [up/up]
    FE80::CE08:13FF:FEEC:0
    2002:101:101::1
Tunnel0                    [up/up]
    FE80::101:101
    2002:101:101:FFFF::1
```

La tabla de enrutamiento en el router SiteA es como sigue:

```
                          -------  rutas IPv6  -------
SiteA# show ipv6 route
```

```
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
LC  2001::1/128 [0/0]
     via ::, Loopback0
C   2001:1:1:1::/124 [0/0]
     via ::, FastEthernet0/0
L   2001:1:1:1::2/128 [0/0]
     via ::, FastEthernet0/0
R   2001:2:2:2::/64 [120/6]
     via FE80::CE08:13FF:FEEC:0, FastEthernet0/0
R   2002::/16 [120/6]
     via FE80::CE08:13FF:FEEC:0, FastEthernet0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

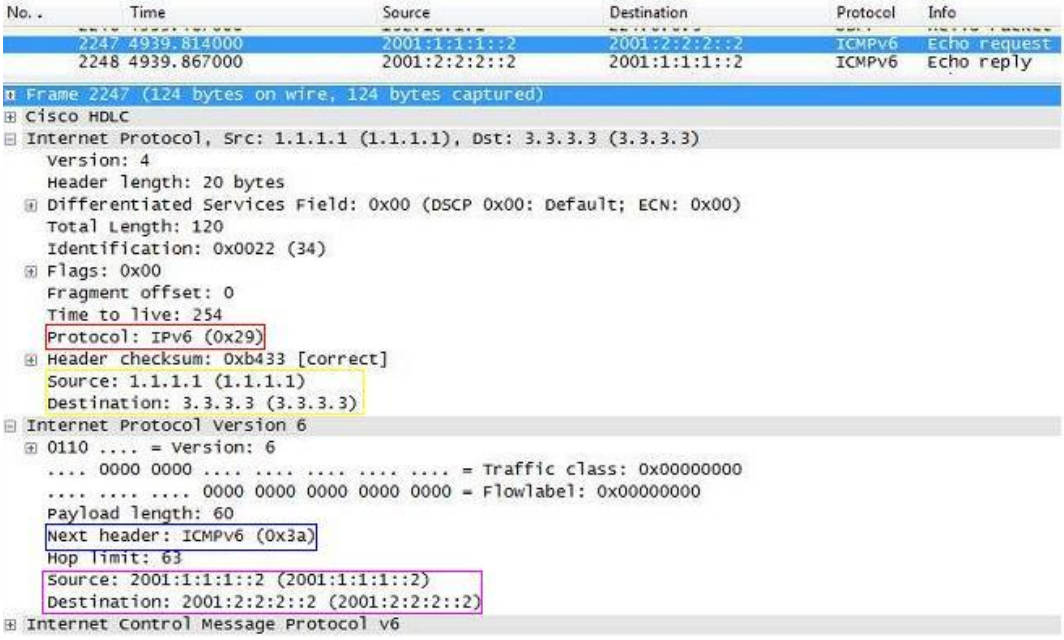
Cuando se hace PING desde el router SiteA al router SitioB (la interfaz Fa0/0 *2001:2:2:2::2*), busca en su tabla de enrutamiento y coincide con la ruta por defecto RIPng anunciada por el router SiteA_6to4. Cuando el paquete llega al router de SiteA_6to4, busca su tabla de enrutamiento para el prefijo de destino.

```
                        -------  Rutas IPv6  -------

SiteA_6to4# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:1:1:1::/124 [0/0]
     via ::, FastEthernet0/0
L   2001:1:1:1::1/128 [0/0]
     via ::, FastEthernet0/0
S   2001:2:2:2::/64 [1/0]
     via 2002:303:303::1
S   2002::/16 [1/0]
     via ::, Tunnel0
C   2002:101:101::/64 [0/0]
     via ::, Loopback0
L   2002:101:101::1/128 [0/0]
     via ::, Loopback0
C   2002:101:101:FFFF::/64 [0/0]
     via ::, Tunnel0
```

```
L   2002:101:101:FFFF::1/128 [0/0]
     via ::, Tunnel0
L   FF00::/8 [0/0]
     via ::, Null0
```

El prefijo de destino coincide con la ruta estática que es la dirección del Tunel IP del router SiteB_6to4 como siguiente salto. Después de una búsqueda recursiva, el router SiteA_6to4 encuentra que la interfaz de salida es el Tunel 0. El router SiteA_6to4 encapsula el paquete IPv6 en un paquete IPv4 con dirección de origen IPv4 de la interfaz Loopback0 del router SiteA_6to4 (1.1.1.1) y dirección de destino IPv4 de la interfaz Loopback0 del router SiteB_6to4 (3.3.3.3).

El campo de protocolo en la cabecera IPv4 se establece en 0x29 (valor decimal 41) que indica IPv6. La siguiente captura de paquetes es realizada en el enlace entre el router SiteA_6to4 y Router2.



Cuando el router SiteB_6to4 recibe el paquete, desencapsula el paquete IPv4 y mantiene el paquete IPv6 dentro de un paquete IPv4. A continuación, se comprueba su tabla de

enrutamiento IPv6 para saber si se puede llegar al destino del paquete. Encuentra la interfaz de salida y envía el paquete al destino.

```
                          -------  rutas IPv6  -------
SiteB_6to4# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S   2001:1:1:1::/64 [1/0]
     via 2002:101:101::1
C   2001:2:2:2::/124 [0/0]
     via ::, FastEthernet0/0
L   2001:2:2:2::1/128 [0/0]
     via ::, FastEthernet0/0
S   2002::/16 [1/0]
     via ::, Tunnel0
C   2002:303:303::/64 [0/0]
     via ::, Loopback0
L   2002:303:303::1/128 [0/0]
     via ::, Loopback0
C   2002:303:303:FFFF::/64 [0/0]
     via ::, Tunnel0
L   2002:303:303:FFFF::1/128 [0/0]
     via ::, Tunnel0
L   FF00::/8 [0/0]
     via ::, Null0
```

17. CONFIGURACIÓN DEL CLIENTE 6TO4 EN LINUX

1. Verificar la conectividad a la dirección IP anycast 192.88.99.1. Esto es importante para que el túnel se establezca de forma automática, sin necesidad de indicar la dirección IPv4 del relay 6to4
2. Ejecutar el siguiente script indicando la dirección IPv4 del cliente como parámetro de entrada

```
#!/bin/sh

IPV4=$1
PARTS=`echo $IPV4 | tr . ' '`
PREFIX=`printf "2002:%02x%02x:%02x%02x" $PARTS`

ip tunnel add tun6to4 mode sit ttl 80 remote any local $IPV4
ip link set dev tun6to4 up
ip -6 addr add $PREFIX::1/64 dev tun6to4
ip -6 route add 2000::/3 via ::192.88.99.1 dev tun6to4 metric 1
```

3. Verificar que la interfaz tun6to4 se encuentre activa y las direcciones inet6 sean las correctas

```
# ifconfig tun6to4
tun6to4   Link encap:IPv6-in-IPv4
          inet6 addr: 2002:aad2:0313::1/64 Scope:Global
          inet6 addr: ::170.210.3.19/128 Scope:Compat
          UP RUNNING NOARP  MTU:1480  Metric:1
          RX packets:823426 errors:0 dropped:0 overruns:0 frame:0
          TX packets:924373 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:123913520 (118.1 MiB)  TX bytes:114622252 (109.3 MiB)
```

4. Comprobar la conectividad a algún sitio IPv6 mediante el uso de herramientas como traceroute6 o mtr. Podemos utilizar como destino la máquina data2.riu.edu.ar que tiene asignada la dirección IPv6: 2800:110:2::3

```
# mtr -6 -r data2.riu.edu.ar
                                Snt: 10    Loss%  Last   Avg  Best  Wrst StDev
2002:c058:6301::1                           0.0%  11.2  11.2  10.7  11.6   0.3
data2.riu.edu.ar                            0.0% 253.1 253.0 249.1 255.6   2.4

# mtr -6 -r -n data2.riu.edu.ar
                                Snt: 10    Loss%  Last   Avg  Best  Wrst StDev
2002:c058:6301::1                           0.0%  11.3  11.2  10.7  11.6   0.3
2800:110:2::3                               0.0% 254.4 253.6 250.8 255.2   1.5
```

5. Comprobar la conectividad a sitios IPv6 fuera de RIU

```
traceroute6 www.kame.net

traceroute to www.kame.net (2001:200:0:8002:203:47ff:fea5:3085), 30 hops max, 40
byte packets

 1  2002:c058:6301::1 (2002:c058:6301::1)  11.182 ms  11.126 ms  11.107 ms

 2  data2.riu.edu.ar (2800:110:2::3)  253.406 ms  253.371 ms  253.341 ms

 3  rgda1.riu.edu.ar (2800:110:2::1)  251.787 ms  251.778 ms  251.933 ms

 4  host1.2001.13d0.ipv6.telecom.net.ar (2001:13d0::1)  255.190 ms  255.504 ms
255.628 ms

 5  2001:41a8:5000:2::1 (2001:41a8:5000:2::1)  253.483 ms  253.596 ms  253.657
ms

 6  ge-9-4.r02.miamfl02.us.bb.gin.ntt.net (2001:418:1000:5000::5)  189.136 ms
185.957 ms  185.996 ms

 7  ae-1.r21.miamfl02.us.bb.gin.ntt.net (2001:418:0:2000::299)  189.625 ms
186.348 ms  187.111 ms

 8  as-3.r20.dllstx09.us.bb.gin.ntt.net (2001:418:0:2000::33d)  204.887 ms
205.063 ms  205.361 ms

 9  as-2.r20.lsanca03.us.bb.gin.ntt.net (2001:418:0:2000::295)  240.345 ms
242.626 ms  241.264 ms

10  as-2.r20.osakjp01.jp.bb.gin.ntt.net (2001:218:0:2000::ae)  438.083 ms as-
5.r20.tokyjp01.jp.bb.gin.ntt.net  (2001:218:0:2000::112)  395.345 ms  as-
2.r20.osakjp01.jp.bb.gin.ntt.net (2001:218:0:2000::ae)  432.062 ms

11  po-1.a15.tokyjp01.jp.ra.gin.ntt.net (2001:218:0:6000::10e)  397.504 ms
393.121 ms  393.117 ms

12  ge-8-2.a15.tokyjp01.jp.ra.gin.ntt.net (2001:218:2000:5000::82)  394.562 ms
po-1.a15.tokyjp01.jp.ra.gin.ntt.net (2001:218:0:6000::10e)  399.234 ms  418.085
ms
```

```
13  ve44.foundry6.otemachi.wide.ad.jp (2001:200:0:10::141)  396.200 ms  401.513
ms  393.497 ms

14  ve44.foundry6.otemachi.wide.ad.jp (2001:200:0:10::141)  398.319 ms  399.797
ms  406.467 ms

15       ve42.foundry4.nezu.wide.ad.jp    (2001:200:0:11::66)       407.349    ms
ve45.foundry2.yagami.wide.ad.jp (2001:200:0:12::74)  401.855 ms  401.754 ms

16  * * 2001:200:0:4803:212:e2ff:fe28:1ca2 (2001:200:0:4803:212:e2ff:fe28:1ca2)
394.521 ms

17  orange.kame.net (2001:200:0:8002:203:47ff:fea5:3085)  398.514 ms  402.442 ms
403.267 ms
```

18. CONFIGURACIÓN DEL CLIENTE TEREDO EN LINUX

1. Instalar el software miredo[149] en la máquina cliente. Miredo se encuentran disponible en formato de paquete (.deb, .rpm) para diferentes distribuciones de linux, bajo los nombres miredo y miredo-server. Es necesario instalar solo miredo, que es el cliente a utilizar.

2. Editar el archivo miredo.conf (generalmente se encuentra en /etc) y definir los siquientes parámetros:

```
RelayType client
ServerAddress teredo.riu.edu.ar
```

3. Ejecutar el servicio miredo como superusuario

```
# /etc/init.d/miredo start
o
# /service miredo start
```

4. Verificar la conectividad a sitios IPv6 en RIU

```
# mtr -6 -r data2.riu.edu.ar
                                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. 6to4.ash1.he.net            0.0%    10  155.1 152.1 151.1 155.1   1.2
  2. gige-g3-7.core1.ash1.he.net  0.0%    10  154.3 154.4 151.3 163.5   4.0
  3. ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  4. 2001:41a8:5000:2::2         10.0%    10  343.8 341.7 336.6 348.9   4.0
  5. host2.2001.13d0.ipv6.telecom 20.0%    10  340.3 340.7 335.3 354.1   5.9
  6. data2.riu.edu.ar            20.0%    10  344.0 343.1 336.6 362.5   8.5
```

5. Verificar la conectividad a sitios IPv6 fuera de RIU

```
# traceroute6 www.kame.net
traceroute to www.kame.net (2001:200:0:8002:203:47ff:fea5:3085), 30 hops max, 40
byte packets
```

[149] http://www.remlab.net/miredo/

```
 1  2001:200:0:b003::2 (2001:200:0:b003::2)  376.730 ms  376.637 ms  376.830 ms

 2  2001:200:0:b004::1 (2001:200:0:b004::1)  383.565 ms  384.115 ms  384.455 ms

 3  2001:200:0:b002::1 (2001:200:0:b002::1)  389.250 ms  389.253 ms  389.259 ms

 4  2001:200:0:b001::1 (2001:200:0:b001::1)  453.946 ms  455.170 ms  455.167 ms

 5  ve44.foundry6.otemachi.wide.ad.jp (2001:200:0:10::141)  390.069 ms  390.101
ms  390.102 ms

 6  ve42.foundry4.nezu.wide.ad.jp (2001:200:0:11::66)  390.163 ms  368.015 ms
368.352 ms

 7  ve45.foundry2.yagami.wide.ad.jp (2001:200:0:12::74)  368.284 ms  377.259 ms
377.171 ms

 8     2001:200:0:4803:212:e2ff:fe28:1ca2  (2001:200:0:4803:212:e2ff:fe28:1ca2)
770.098 ms * *

 9  orange.kame.net (2001:200:0:8002:203:47ff:fea5:3085)  376.266 ms  376.253 ms
376.255 ms
```

19. CONFIGURACIÓN DEL CLIENTE TEREDO EN WINDOWS

- Windows XP SP2
  - Instalar el stack IPv6

```
netsh interface ipv6 install
```

  - Habilitar Teredo y utilizar el servidor Teredo de RIU

```
netsh interface ipv6 set teredo teredo.riu.edu.ar
```

- Windows Vista
  - Implementa IPv6 de forma completa (ya viene instalado)
  - Utiliza el servidor Teredo *teredo.ipv6.microsoft.com*. Para utilizar el servidor Teredo de RIU ejecutar:

```
netsh interface teredo set state servername=170.210.2.36
```