

FACULTAD: INFORMATICA Y CIENCIAS APLICADAS
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES.



TEMA: Configuración de Servidores DHCPv6. Laboratorio de Redes,
Universidad Tecnológica de El Salvador.

TRABAJO FINAL, PRESENTADO POR:

Chávez, Julio Cesar

Chavarría, Dennys Alexander

Figueroa Palacios, Samael

PARA OPTAR AL GRADO DE:

TECNICO EN INGENIERIA DE REDES
COMPUTACIONALES.

MARZO 2011.

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

INDICE

No. De Página

CAPITULO I SITUACION ACTUAL

1.1. Situación Problemática.....	1
1.2. Justificación.....	4
1.3. Objetivos.....	4
1.4. Alcances (Entregables).....	5
1.5. Estudio De Factibilidades.....	5
1.6. Carta de Autorización del Beneficiario.....	8

CAPITULO II DOCUMENTACION TECNICA

2.1. Marco Teórico De La Solución.....	10
2.1.1. Protocolo de Internet IPv4.....	58
2.1.2. Protocolo de Internet IPv6.....	61
2.1.3. Diseño de la solución.....	65

CAPITULO III

PROPUESTA DE SOLUCION

3.1.Propuesta de Solución.....	71
3.1.1.Planteamiento Del Proyecto Temático.....	71
3.1.2. Cronograma De Actividades.....	74
3.1.3.Tecnología y Recursos Seleccionado	75
3.1.4.Diseño De La Propuesta.....	77
3.1.5. Implementación De La Propuesta.....	81
3.1.6.Presentación De La Propuesta.....	99
3.2.Evidencias Del Proyecto.....	102
Conclusiones.....	114
Recomendaciones.....	115
Bibliografía.....	116
Anexos.....	117
Glosario.....	120

AUTORIDADES

LIC. JOSE MAURICIO LOUCEL
RECTOR

ING. NELSON ZARATE SANCHEZ
VICERRECTOR GENERAL

LIC. LISSETTE CANALES DE RAMIREZ
DECANO

JURADO EXAMINADOR
ING. JOSE MAURICIO RIVERA
PRESIDENTE

ING. OSCAR RODRIGUEZ
PRIMER VOCAL

LIC. WALTER NAVARRETE
SEGUNDO VOCAL

MARZO 2011.
SAN SALVADOR, EL SALVADOR, CENTROAMERICA

INTRODUCCION

El protocolo Internet versión 6 a(IPv6) es una nueva versión de IP (*Internet Protocol*), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso.

Se calcula que, actualmente, las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas

El reciente crecimiento exponencial de Internet y el agotamiento inminente del espacio de direcciones IPv4. Las direcciones IPv4 han empezado a escasear relativamente, lo que ha obligado a algunas organizaciones a utilizar un traductor de direcciones de red (NAT, Network Address Translator) para asignar múltiples direcciones privadas a una única dirección IP pública. Si bien los NAT fomentan la reutilización del espacio de direcciones privadas.

CAPITULO I.SITUACION ACTUAL.

1.1 SITUACION PROBLEMÁTICA

La Universidad Tecnológica de El Salvador se ha caracterizado por ofrece a la Sociedad Salvadoreña un conjunto de carreras en diversas áreas. Una de estas es la que está relacionada con las tecnologías de Información y Comunicación.

Es por eso que la Universidad, se ve obligada a estar a la vanguardia de la tecnología en cuanto a la educación de sus alumnos, para que de esta manera se pueda cumplir con el propósito de formar Profesionales que estén familiarizados con todas las novedades tecnológicas que son requeridas por el mercado laboral.

Las Tecnologías relacionadas a Informática y las Telecomunicaciones han sufrido diversos cambios, todo con el objetivo de hacer más efectivo, práctico y seguro el intercambio de información. Tecnologías como El Internet se vuelve esencial y necesaria en la vida cotidiana de cada Institución, Organización o Individuo.

Los encargados de crear, desarrollar, distribuir o mantener este recurso, se ven en la obligación constante de mejorar el servicio, ya que día a día son más y más los usuarios que requieren este tipo de medio para realizar sus labores diarias.

IPv4 es un recurso que permitió el crecimiento de este tipo de servicios. En la actualidad se han ocupado 2 de las terceras partes de las direcciones IPv4. Por esto fue necesario crear una nueva versión de direcciones (IPv6)

La Universidad Tecnológica de El Salvador, no es la excepción en cuanto a la necesidad de adoptar las nuevas tecnologías de Comunicación. IPv6 es parte de estos nuevos requerimientos. De acá surge la necesidad de Implementar IPv6 en la Universidad Tecnológica de El Salvador. El camino de IPv4 a IPv6, no es cuestión de Transición o de Migración, sino más bien Evolución e Integración, se trata de una evolución Necesaria y Real. IPv6 permitirá un crecimiento Escalable y Simple.

La Universidad Tecnológica de El Salvador debe de estar preparada para adoptar esta nueva tecnología y no debe de esperar que IPv4 deje de funcionar para hacer los cambios necesarios y de la noche a la mañana implementar IPv6, sin antes haber preparado sus recursos de Software y Hardware, personal docente y alumnos para trabajar con esta nueva versión de direcciones IP.

Se ha decidido plantear una propuesta que ayude a la Universidad a adoptar esto como parte de su proceso de mejoramiento en las tecnologías de Información. En este caso Laboratorio de Redes se vuelve el Sitio más adecuado para poner en funcionamiento IPv6 y hacer todas las pruebas de

efectividad y funcionalidad que se requieren para adoptar esta nueva versión en su totalidad, ya que cuenta con los medios necesarios para su Implementación.

Un servidor DHCPv6 con Plataforma de Windows Server 2008, ofrece un excelente sistema automático de asignación de direcciones IP, que ayudara a poner a prueba las novedades y bondades que tiene IPv6 con relación a IPv4.

Los alumnos serán los más beneficiados, ya que contarán con un Servicio que les permita realizar prácticas más efectivas, además de una guía que les indique detalladamente la manera correcta de cómo manejar este recurso.

Esto les ofrecerá la oportunidad de adquirir los conocimientos y destrezas necesarias para ser más competitivos en el mercado laboral.

Es necesario contar con un Servidor DHCPv6 para garantiza un método eficaz de asignación de direcciones IP, requeridas por cada uno de los clientes del Laboratorio de Redes. Y este a su vez pondría a la Universidad Tecnológica de El Salvador como una de las Instituciones Educativas Pioneras en cuanto a la resolución de Problemas de Asignación de Direcciones IP.

1.2 JUSTIFICACION

Estos son los beneficios que obtendría el laboratorio de red de la universidad tecnológica de el salvador:

Disminución de problemas técnicos (NAT) y complejidad en la red.

Generación de nuevos servicios y aplicaciones

Disminución de costos.

Mejoramiento en seguridad, autoconfiguración, multicast y multimedia.

1.3 OBJETIVOS.

➤ OBJETIVO GENERAL.

Realizar un Trabajo de investigación sobre la nueva tecnología de direccionamiento IPV6, la forma en cómo funcionada el servicio de DHCP con esta Versión y hacer la configurar del servicio con Windows Server 2008 en el Laboratorio de Redes de la Universidad Tecnológica de El Salvador.

➤ OBJETIVOS ESPECIFICOS.

- Investigar sobre los cambios y nuevas características que ofrece IPv6.
- Instalar y configurar el servicio de red de DHCP bajo el nuevo protocolo de IPv6.
- Realizar una comparación entre las diferencias para el servicio de DHCP que se ofrecen en las versiones de IPv4 e IPv6.

1.4 ALCANCES.

- Presentar una documentación que detalle el nuevo esquema de direccionamiento de IPv6 y su forma de operación.
- Configurar un servidor con Microsoft Windows 2008 para que trabaje con el servicio de DHCP en formato del protocolo IPv6.
- Elaborar una tabla comparativa respecto a la implementación de DHCP en IPv4 e IPv6.

1.5 ESTUDIO DE FACTIBILIDAD

Es evidente que el mundo de los servidores de informática, ha cambiado y el cambio ha sido radical, no solo en hardware y software, sino también. En forma de asignación de direcciones IP, de versiones anteriores (IPv4), como también en las actuales. (IPv6)

Esto indica claramente la necesidad de cambios en la forma de asignación de direcciones (IP), así como también, en las consolas de administración como: DHCP.

Una forma centralizada, y de fácil administración, donde podemos crear ámbitos, reservas, y exclusiones. Al igual que crear rangos de direcciones.

(Pero esto se trato, de una era ya pasada.)

Puesto que en la anterior versión se trato de formato decimal y dividido en octetos, los cuales mantenían 8 bits de encriptación, haciendo un total de 32 bits en la sumatoria, lo cual delimito mucho el total de direcciones mundiales; por lo cual hoy en día es necesario, un cambio urgente de formato decimal a hexadecimal, lo cual nos diera un margen mayor de direcciones totales... Y nos abrirá a una nueva era. La necesidad es clara la implementación de IPv6, en la Universidad Tecnológica de El Salvador.

De acuerdo a la naturaleza el estudio está enmarcado dentro de la modalidad de un proyecto factible, debido a que está orientado a proporcionar solución o respuesta a problemas planteados en una determinada realidad

El estudio se fundamenta en una investigación de campo, ya que los datos se recogen de manera directa de la realidad en su ambiente natural. De igual manera se considera una investigación de campo, ya que los datos fueron recabados con distintas técnicas e instrumentos en la propia institución donde se desarrolló la investigación.

Se considera la investigación de carácter descriptivo ya que los datos obtenidos en las distintas situaciones planteadas en la investigación, son descritos e interpretados según la realidad planteada en la organización.

Las técnicas de recolección de datos aplicadas en la investigación fueron; la observación directa. Además debe mencionarse que la observación fue de tipo participante debido a que la investigación forma parte de la comunidad objeto de estudio. Y a modo de complemento en la aplicación de esta técnica se utilizó como instrumento una lista de chequeo en el cual se plasmaron todos los datos recopilados. La observación aplicada en este trabajo de grado permitió la búsqueda de los datos necesarios que conllevaron a resolver la situación planteada.

➤ **FACTIBILIDAD ECONOMICA**

Es importante y cabe mencionar, la inversión económica. Pues es necesario la compra de software nativo, con respectivas licencias de uso para ipv6. Como lo es Windows Vista (cualquier modalidad) y/o Windows 7. En todos los laboratorios Informáticos de la cátedra de REDES. De la Universidad Tecnológica de El Salvador. Pues así ayudaran a la mejor comprensión del protocolo Ipv6. Para todos los alumnos que allí acudan.

Al mismo tiempo vale recalcar la necesidad de actualización de hardware, en cuanto a sus procesadores, y memorias RAM.

➤ **FACTIBILIDAD OPERACIONAL**

De los recursos, es necesario contar. De al menos 8 personas capacitadas y un grado académico de cómo mínimo Técnico en cualquiera de las ramas de la informática y con experiencia comprobable. Al mismo tiempo tomando muy en cuenta el resultado económico, en la descripción.

1.6 CARTA DE AUTORIZACION DEL BENEFICIARIO.

Continúa Siguiente Página...

San Salvador, 21 de Agosto de 2010

Universidad Tecnológica de El Salvador

UTEC

Cátedra de Redes

San Salvador

Reciban un cordial saludo, esperando gocen de perfecta salud y a la vez deseándoles que tengan éxitos en su ámbito familiar y profesional.

Al dirigirnos a ustedes, primeramente nos sentimos orgullosos que nos den la oportunidad de realizar el proyecto que se titula “Configuración de un Servidor DHCP con IPV6 en el Laboratorio de Redes”. A la vez en agradecimiento queremos asignar como beneficiarios a los alumnos que requieran el uso del Laboratorio, al igual al personal docente que se pueda valer del Proyecto para impartir sus clases teóricas y prácticas.

Atentamente

Dennys Chavarría

Alumno

Julio C. Chávez

Alumno

Samael Figueroa

Alumno

Ing. Salvador A. Franco

Asesor

Lic. Walter Navarrete

Asesor

CAPITULO II. DOCUMENTACION TECNICA.

2.1 MARCO TEORICO DE LA SOLUCIÓN

➤ INTRODUCCION IPv6

La versión actual del Protocolo Internet (denominada IP versión 4 o IPv4) no ha cambiado de forma significativa desde la publicación del documento RFC 791 en 1981. IPv4 ha demostrado ser un protocolo robusto, de fácil implementación e interoperable, y ha superado la prueba de ampliar un conjunto de redes interconectadas para un uso global del tamaño que Internet tiene en la actualidad. Éstas son las virtudes de su diseño inicial.

Sin embargo, el diseño inicial no previó las siguientes circunstancias:

El reciente crecimiento exponencial de Internet y el agotamiento inminente del espacio de direcciones IPv4. Las direcciones IPv4 han empezado a escasear relativamente, lo que ha obligado a algunas organizaciones a utilizar un traductor de direcciones de red (NAT, Network Address Translator) para asignar múltiples direcciones privadas a una única dirección IP pública. Si bien los NAT fomentan la reutilización del espacio de direcciones privadas, no admiten la seguridad de nivel de red basada en estándares o la asignación correcta de todos los protocolos de nivel superior y pueden crear problemas al conectar dos organizaciones que utilizan el espacio de direcciones privadas.

Además, la importancia cada vez mayor de los dispositivos y aparatos conectados a Internet garantiza que acabará por agotarse el espacio de

direcciones IPv4 públicas. El crecimiento de Internet y la capacidad de los enrutadores de la red troncal de Internet para mantener tablas de enrutamiento grandes.

Debido a la forma en que los Id. de red de IPv4 se han asignado y se siguen asignando, lo normal es que existan más de 70.000 rutas en las tablas de enrutamiento de los enrutadores de red troncal de Internet. La infraestructura actual de enrutamiento de la red Internet IPv4 es una combinación de enrutamiento plano y jerárquico. La necesidad de una configuración más sencilla. La mayoría de las implementaciones actuales de IPv4 se deben configurar manualmente o mediante un protocolo de configuración de direcciones con estado como el Protocolo de configuración dinámica de host (DHCP, *Dynamic Host Configuration Protocol*). Al existir más equipos y dispositivos que utilizan IP, surge la necesidad de una configuración de direcciones más sencilla y automática y otras opciones de configuración que no dependan de la administración de una infraestructura DHCP. El requisito de seguridad en el nivel de IP. La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que impidan que los datos enviados se puedan ver o modificar durante el tránsito. Aunque en la actualidad existe un estándar que proporciona seguridad para los paquetes IPv4 (denominado seguridad de Protocolo Internet o IPSec), este estándar es opcional y prevalecen las soluciones propietarias.

La necesidad de mayor compatibilidad con la entrega de datos en tiempo real (denominado también calidad de servicio). Aunque existen estándares de calidad de servicio (QoS, *Quality of Service*) para IPv4, la compatibilidad con el tráfico en tiempo real depende del campo Tipo de servicio (TOS, *Type of Service*) de IPv4 y la identificación de la carga, que suele utilizar un puerto UDP o TCP. Por desgracia, el campo TOS de IPv4 tiene una funcionalidad limitada y diferentes interpretaciones. Además, la identificación de la carga que utiliza un puerto TCP o UDP no es posible cuando la carga del paquete IPv4 está cifrada.

Para solucionar estos problemas, el Grupo de trabajo de ingeniería de Internet (IETF, *Internet Engineering Task Force*) ha desarrollado un conjunto de protocolos y estándares denominados IP versión 6 (IPv6). Esta nueva versión, anteriormente llamada IP-La siguiente generación (IPng, *IP-The Next Generation*), incorpora los conceptos de muchos métodos propuestos para la actualización del protocolo IPv4. IPv6 está diseñado con la intención de reducir al mínimo el impacto en los protocolos de nivel superior e inferior al evitar la adición arbitraria de nuevas características.

➤ **CARACTERÍSTICAS IPv6.**

El protocolo IPv6 tiene las características siguientes:

- Nuevo formato de encabezado

- Espacio de direcciones más grande
- Infraestructura de direcciones y enrutamiento eficaz y jerárquica
- Configuración de direcciones con y sin estado
- Seguridad integrada
- Mejora de la compatibilidad para la calidad de servicio (QoS)
- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

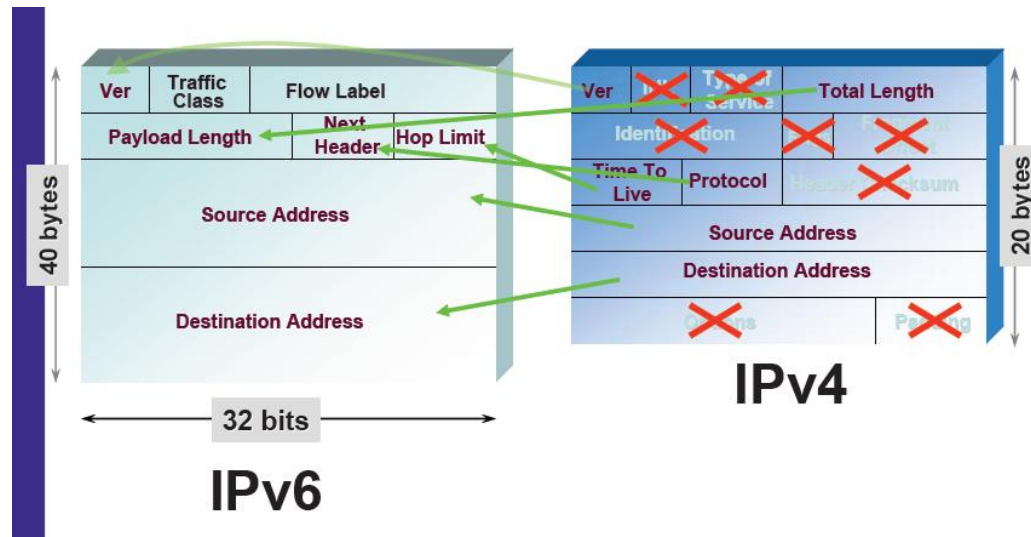


Figura 2.1 Comparativa de IPv6 e IPv4

En las secciones siguientes se trata en detalle cada una de estas nuevas características.

Nuevo formato de encabezado.

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

Los encabezados IPv4 y los encabezados IPv6 no son interoperables y el protocolo IPv6 no es compatible con el protocolo IPv4. Un host o un enrutador debe utilizar simultáneamente una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado IPv6 sólo tiene el doble de tamaño que el encabezado IPv4, a pesar de que las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4.

Espacio de direcciones más grande

IPv6 utiliza direcciones de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden proporcionar más de $3,4 \times 10^{38}$ combinaciones posibles, el amplio espacio de direcciones de IPv6 se ha diseñado para permitir múltiples niveles de división en subredes y asignación de direcciones de la red troncal Internet a las subredes individuales de una organización.

Aunque actualmente sólo un pequeño porcentaje de direcciones posibles se asignan para el uso de hosts, hay disponibles muchas direcciones para su uso en el futuro. Al tener un número mucho mayor de direcciones disponibles, ya no son necesarias las técnicas de conservación de direcciones, como la implementación de NAT.

Infraestructura de direcciones y enrutamiento eficaz y jerárquica

Las direcciones globales de IPv6 que se utilizan en la parte IPv6 de Internet están diseñadas para crear una infraestructura eficaz, jerárquica y que se puede resumir y que tiene en cuenta la existencia de múltiples niveles de proveedores de servicios Internet. En la red Internet IPv6, los enrutadores de red troncal tienen tablas de enrutamiento mucho más pequeñas.

Configuración de direcciones con y sin estado

Para simplificar la configuración de los hosts, IPv6 admite la configuración de direcciones con estado, como la configuración de direcciones con la presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones sin la presencia de un servidor DHCP). Con la configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (direcciones locales del vínculo) y con direcciones derivadas de prefijos anunciados por los enrutadores locales. Incluso sin la presencia de un enrutador, los hosts del mismo vínculo se

pueden configurar automáticamente con direcciones locales del vínculo y comunicarse sin necesidad de configuración manual.

Seguridad integrada

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las necesidades de seguridad de red y aumenta la interoperabilidad entre diferentes implementaciones de IPv6. Mejora de la compatibilidad para la calidad de servicio (QoS)

Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo Flow Label (etiqueta de flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec.

Nuevo protocolo para la interacción de nodos vecinos. El protocolo Descubrimiento de vecinos en IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, <i>Internet Control Message Protocol for IPv6</i>) que administran la interacción de nodos

vecinos (es decir, nodos que se encuentran en el mismo vínculo). El descubrimiento de vecinos reemplaza los mensajes de Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*), Descubrimiento de enrutadores ICMPv4 y Redirección ICMPv4 con mensajes eficaces de multidifusión y unidifusión, y proporciona funciones adicionales.

Capacidad de ampliación.

IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a continuación del encabezado IPv6. A diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

Formato de direcciones IPv6.

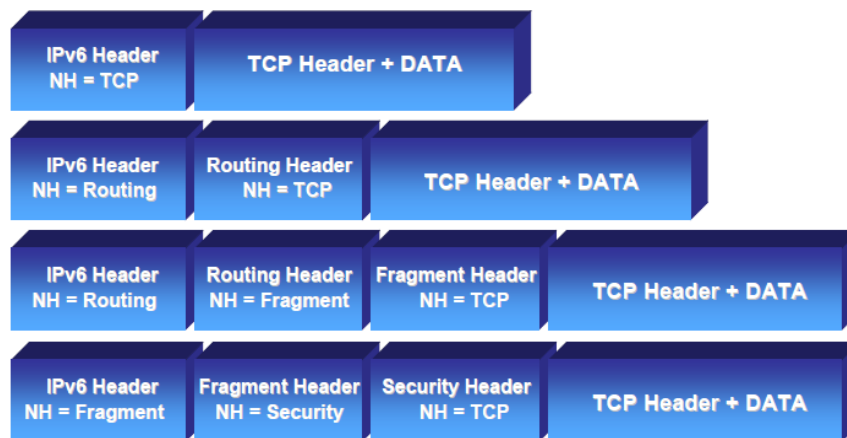


Figura 2.2 Formato IPv6

Las direcciones IPv4 se representan en formato decimal con punto. Estas direcciones de 32 bits se dividen en límites de 8 bits. Cada grupo de 8 bits se convierte a su equivalente decimal y se separa mediante puntos de los demás conjuntos. En IPv6, la dirección de 128 bits se divide en límites de 16 bits. Cada bloque de 16 bits se convierte a un número hexadecimal de 4 dígitos separado por dos puntos. La representación resultante se denomina hexadecimal con dos puntos.

A continuación se muestra una dirección IPv6 en formato binario:

```
0010000111011010000000000110100110000000000000000010111100111011
0000001010101010000000000111111111111110001010001001110001011010
```

La dirección de 128 bits se divide en límites de 16 bits:

```
0010000111011010      0000000011010011      0000000000000000
0010111100111011      0000001010101010      0000000011111111
1111111000101000 1001110001011010
```

Cada bloque de 16 bits se convierte a formato hexadecimal y se delimita con dos puntos. El resultado es el siguiente

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

La representación IPv6 se puede simplificar aún más si se quitan los ceros a la izquierda de cada bloque de 16 bits. No obstante, cada bloque debe tener al menos un dígito. Al suprimir los ceros a la izquierda, la representación de la dirección será la siguiente:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Compresión de ceros.

Algunos tipos de direcciones contienen largas secuencias de ceros. Para simplificar aún más la representación de las direcciones IPv6, una secuencia contigua de bloques de 16 bits establecidos como 0 en el formato hexadecimal con dos puntos puede comprimirse como "::" . Esto se denomina dos puntos dobles.

Por ejemplo, la dirección local del vínculo de FE80:0:0:0:2AA:FF:FE9A:4CA2 puede comprimirse como FE80::2AA:FF:FE9A:4CA2. La dirección de multidifusión de FF02:0:0:0:0:0:2 puede comprimirse como FF02::2.

La compresión de ceros sólo se puede usar para comprimir una serie contigua de bloques de 16 bits expresados en notación hexadecimal con dos puntos. No se puede usar para incluir parte de un bloque de 16 bits. Por ejemplo, no puede expresar FF02:30:0:0:0:0:0:5 como FF02:3::5.

Para determinar cuántos bits 0 representan los dos puntos dobles, cuente el número de bloques de la dirección comprimida, reste este número de 8 y, a continuación, multiplique el resultado por 16. Por ejemplo, la dirección FF02::2 tiene dos bloques (el bloque “FF02” y el bloque “2”). El número de bits 0 expresado por los dos puntos dobles es 96 ($96 = (8 - 2) \times 16$).

La compresión de ceros sólo se puede usar una vez en una dirección determinada. De lo contrario, no podrá determinar el número de bits 0 que representa cada instancia de dos puntos dobles.

Prefijos de IPv6.

El prefijo es la parte de la dirección que indica los bits que tienen valores fijos o reflejan el identificador de subred. Los prefijos de las rutas e identificadores de subred IPv6 se expresan de la misma forma que la notación CIDR (Enrutamiento de interdominios sin clases) de IPv4, es decir, con la notación dirección/longitud de prefijo. Por ejemplo, 21DA:D3::/48 es un prefijo de ruta y 21DA:D3:0:2F3B::/64 es un prefijo de subred. Las implementaciones de IPv4 suelen usar una representación decimal con punto del prefijo de red, que se

conoce con el nombre de máscara de subred. En IPv6 no se usan máscaras de subred. En IPv6 sólo se admite la notación con longitud del prefijo.

Tipos de direcciones IPv6

IPv6 admite tres tipos de direcciones:

Unidifusión.

Una dirección de unidifusión identifica una única interfaz en el ámbito del tipo de dirección de unidifusión. Con la topología de enrutamiento de unidifusión adecuada, los paquetes destinados a una dirección de unidifusión se entregan en una única interfaz. Para dar cabida a sistemas de equilibrio de carga, el documento RFC 3513 permite que varias interfaces usen la misma dirección siempre que aparezcan como una única interfaz en la implementación de IPv6 en el host.

Multidifusión.

Una dirección de multidifusión identifica varias interfaces. Con la topología de enrutamiento de multidifusión apropiada, los paquetes destinados a direcciones de multidifusión se entregan en todas las interfaces que la dirección identifica. Una dirección de multidifusión se usa para comunicaciones uno a varios, con entrega en varias interfaces.

Difusión por proximidad.

Una dirección por proximidad identifica varias interfaces. Con la topología de enrutamiento apropiada, los paquetes destinados a una dirección de difusión por proximidad se entregan en una única interfaz, la interfaz más próxima que la dirección identifica. La interfaz más próxima se define como la que está más cerca en cuanto a distancia de enrutamiento. La dirección de difusión por proximidad se usa para comunicaciones uno a uno de varios, con entrega en una única interfaz.

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.

El documento RFC 3513 no define direcciones de difusión. Todos los tipos de direcciones de difusión IPv4 se realizan en IPv6 con direcciones de multidifusión. Por ejemplo, las direcciones de difusión limitadas y subred de IPv4 se reemplazan por la dirección de multidifusión de FF02::1 de todos los nodos de ámbito local del vínculo.

Direcciones IPv6 de unidifusión.

Las direcciones IPv6 de unidifusión pueden ser las siguientes:

- Direcciones globales de unidifusión
- Direcciones locales del vínculo
- Direcciones locales del sitio
- Direcciones especiales
- Direcciones de compatibilidad
- 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 se muestra la estructura de una dirección global de unidifusión según la definición del documento RFC 3587.

Dirección global de unidifusión.

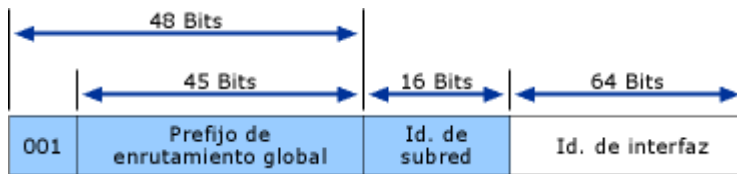


Figura 2.3

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 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 se muestra cómo los campos de una dirección global de unidifusión crean una estructura de tres niveles.

Estructura de tres niveles de la dirección global de unidifusión.

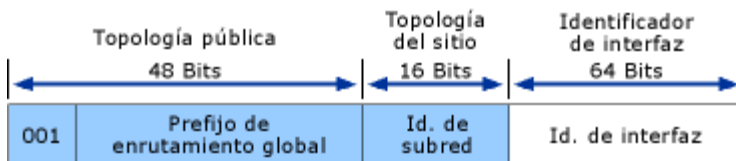


Figura 2.4

La topología pública es la colección de proveedores ISP 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. Para obtener más información acerca de las direcciones globales de unidifusión, consulte el documento RFC 3587 en la base de datos RFC de IETF en (puede estar en inglés).

Direcciones de unidifusión de uso local.

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.

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) 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 se muestra la estructura de la dirección local del vínculo.

Dirección local del vínculo.

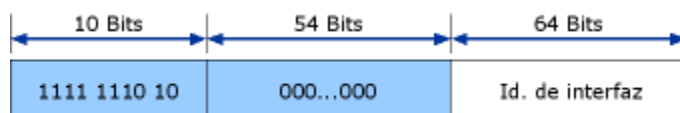


Figura 2.5

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.

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 se muestra la estructura de la dirección local del sitio.

Dirección local del sitio.

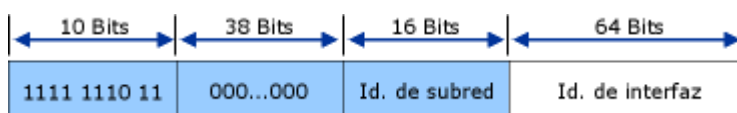


Figura 2.5

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.

El documento RFC 3879 ya no admite el uso de direcciones locales del sitio en futuras implementaciones de IPv6. Las implementaciones de IPv6 existentes pueden continuar usando las direcciones locales del sitio hasta que se haya estandarizado una alternativa. En la actualidad, una nueva versión del estándar de arquitectura de direccionamiento de protocolo de Internet versión 6 (IPv6) se ha publicado como borrador de Internet (draft-ietf-ipv6-addr-arch-v4-0x.txt) e incluye la especificación de obsoletas para las direcciones locales del sitio. El objetivo del nuevo borrador de Internet del estándar de direccionamiento IPv6 es sustituir el documento RFC 3513 obsoleto.

Direcciones IPv6 especiales: Las direcciones IPv6 especiales son las siguientes:

Dirección no especificada.

La dirección no especificada (0:0:0:0:0:0:0 o ::) 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 o ::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.

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:w.x.y.z o ::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:FFFF:w.x.y.z o ::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.

Dirección ISATAP.

El borrador de Internet titulado “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)” 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.

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:FFFF:62C3:FFFE`. Las direcciones Teredo se usan para representar un host que usa el mecanismo de túnel automático definido en el borrador de Internet titulado “Teredo: Tunneling IPv6 over UDP through NATs”.

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 se muestra la estructura de la dirección IPv6 de multidifusión.

Dirección IPv6 de multidifusión.



Figura 2.6

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, 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 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:

Dirección	Descripción
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.

Cuadro 2.1

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:

Dirección	Descripción
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.

Cuadro 2.2

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 se muestra la dirección IPv6 de multidifusión recomendada.

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



Figura 2.7

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 figura 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.

Asignación de direcciones IPv6 de unidifusión a direcciones IPv6 de nodo solicitado.

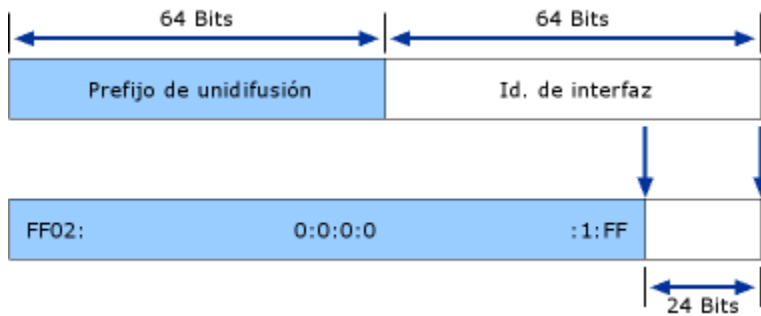


Figura 2.8

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 el 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.

Direcciones IPv6 para hosts.

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 siguientes direcciones de unidifusión:

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 de unidifusión).

La dirección de bucle invertido (::1) para la interfaz de bucle invertido.

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

enrutable. La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz y las direcciones de multidifusión de los grupos unidos a cada interfaz.

Direcciones IPv6 para enrutadores.

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

- 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 de unidifusión).
- Una dirección de difusión por proximidad de un enrutador de subred.
- Direcciones de difusión por proximidad adicionales (opcional).
- La dirección de bucle invertido (::1) para la interfaz de bucle invertido.
- Además, cada enrutador escucha el tráfico en las siguientes direcciones de multidifusión:

Dirección	Descripción
FF01::1	La dirección de multidifusión para todos los nodos de ámbito local de la interfaz

FF01::2	La dirección de multidifusión para todos los enrutadores de ámbito local de la interfaz
FF02::1	La dirección de multidifusión para todos los nodos de ámbito local del vínculo
FF02::2	La dirección de multidifusión para todos los enrutadores de ámbito local del vínculo
FF05::2	La dirección de multidifusión para todos los enrutadores de ámbito local del sitio

Cuadro 2.3

- La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz.
- Las direcciones de multidifusión de los grupos unidos a cada interfaz.

Autoconfiguración Configuración automática de direcciones y descubrimiento de vecinos.

El protocolo ND (Neighbor Discovery, descubrimiento de vecinos) de IPv6 facilita la configuración automática de direcciones IPv6. La configuración automática consiste en la capacidad de un host de IPv6 de generar automáticamente sus propias direcciones IPv6, cosa que facilita la administración de direcciones y supone un ahorro de tiempo.

El protocolo ND se corresponde con una combinación de los siguientes protocolos IPv4: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Router Discovery (RDISC), e ICMP Redirect. Los encaminadores de IPv6 utilizan el protocolo ND para anunciar el prefijo de sitio de IPv6. Los hosts de IPv6 utilizan el descubrimiento de vecinos con varias finalidades, entre las cuales está solicitar el prefijo de un encaminador de IPv6.

Simplificación del formato del encabezado.

El formato del encabezado de IPv6 prescinde o convierte en opcionales determinados campos de encabezado de IPv4. Pese al mayor tamaño de las direcciones, este cambio hace que el encabezado de IPv6 consuma el mínimo ancho de banda posible. Aunque las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4, el encabezado de IPv6 sólo tiene el doble de

tamaño que el encabezado de IPv4. Los cambios en la forma de codificar las opciones de encabezado de IP permiten un reenvío más eficaz. Asimismo, las opciones de IPv6 presentan unos límites de longitud menos estrictos. Los cambios aportan una mayor flexibilidad a la hora de incorporar opciones nuevas en el futuro. Descripción general de las redes IPv6. En esta sección se presentan términos básicos en la topología de redes IPv6. En la figura siguiente se muestran los componentes básicos de una red IPv6.

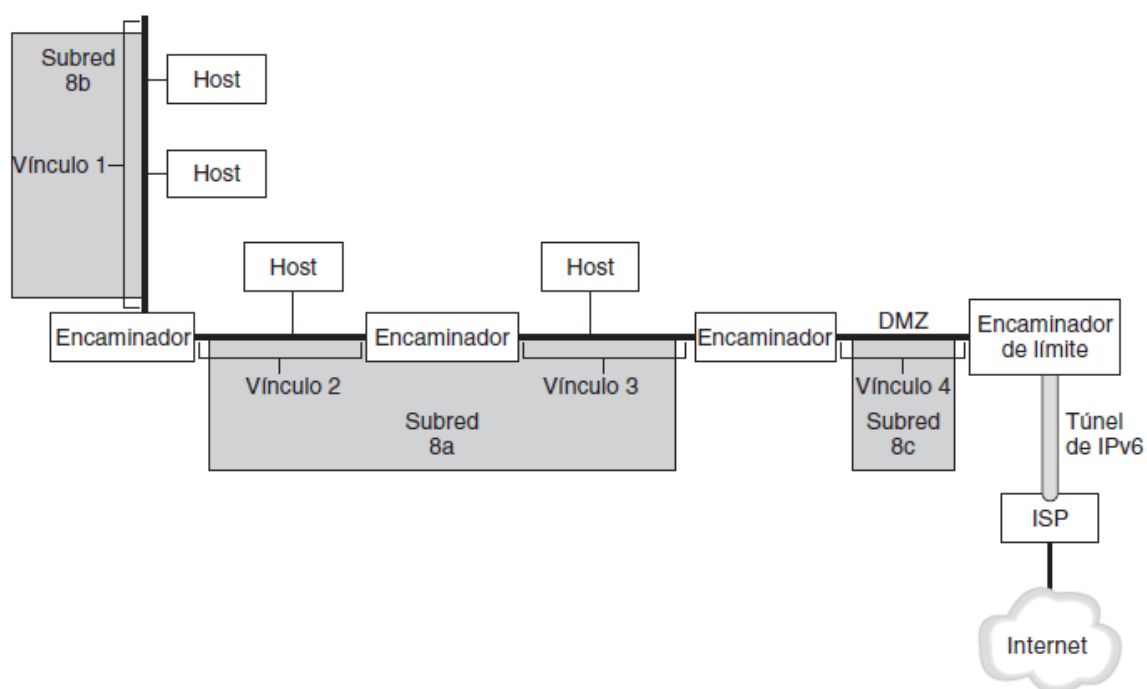


Figura 2.9 Componentes básicos de red IPv6

La figura ilustra 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

encaminador los termina. El vínculo 4, considerado laDMZ de la red, queda terminado en un extremo por el encaminador de límite. El encaminador 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 laDMZdel vínculo 4.

Como se muestra en la Figura 3–1, una red IPv6 tiene prácticamente los mismos componentes que una red IPv4.No obstante, la terminología de IPv6 presenta 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.

Terminología de IPv6

Nodo: Sistema con una dirección IPv6 y una interfaz configurada para admitir IPv6. Término genérico que se aplica a hosts y encaminadores.

Encaminador de IPv6: Nodo que reenvía paquetes de IPv6. Para admitir IPv6, debe configurarse como mínimo una de las interfaces del encaminador. Un encaminador 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 Encaminador 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.

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.

Encaminador de límite: Encaminador en el límite de una red que proporciona un extremo del túnel de IPv6 a un punto final fuera de la red local. Este encaminador debe tener como mínimo una interfaz de IPv6 a la red interna. En cuanto a la red externa, el encaminador puede tener una interfaz de IPv6 o IPv4.

DHCPv6

El Protocolo de configuración dinámica de host (DHCP) se diseñó para encargarse de la asignación de direcciones IP y otra información de red a los equipos, de forma que puedan comunicarse en la red automáticamente. DHCP para IPv6 (DHCPv6) puede proporcionar configuración de direcciones con estado o configuración sin estado a hosts de IPv6. Los hosts de IPv6 pueden utilizar varios métodos de configuración de direcciones.

La configuración automática de direcciones sin estado: se utiliza para configurar las direcciones locales de vínculos y las direcciones no locales de vínculos adicionales mediante el intercambio de mensajes de solicitud de enrutador y anuncio de enrutador con los enrutadores vecinos.

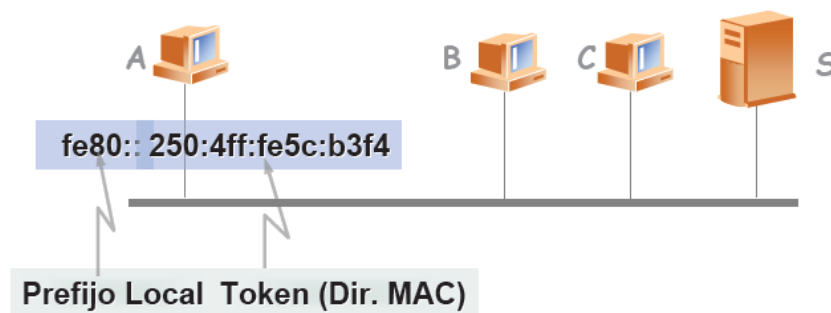


Figura 2.10 Configuración automática sin estado (I)

Arranque: Construcción de Dirección de ámbito local (Link Local).

Direcciones Locales: Comunicación dentro de subred (No se encaminan) y son muy útiles en redes sin router.

Direcciones Globales: Se encargan de envío periódico de paquetes (Router Advertisement o RA)

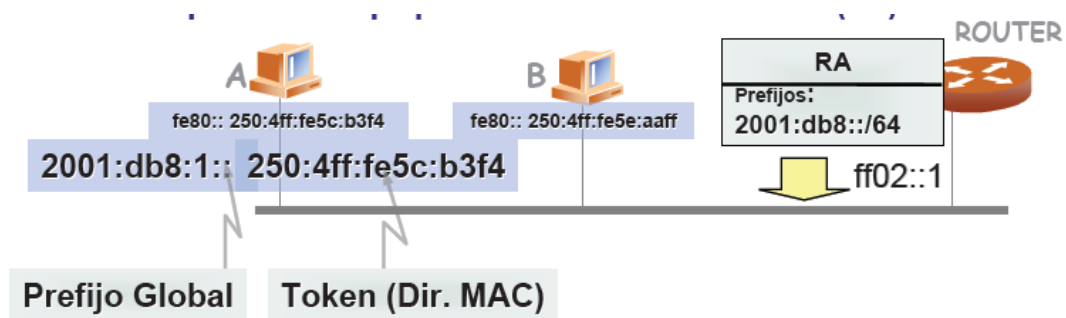


Figura 2.11 Configuración automática sin estado (II)

La configuración automática de direcciones con estado: se utiliza para configurar direcciones no locales de vínculos a través del uso de un protocolo de configuración como DHCP.

Un host de IPv6 realiza la configuración de direcciones sin estado automáticamente y utiliza un protocolo de configuración (como DHCPv6) en el mensaje de anuncio de enrutador basado en las siguientes marcas y enviado por un enrutador vecino.

Al igual que en DHCP para IPv4, los componentes de una infraestructura DHCPv6 están formados por clientes DHCPv6 que solicitan configuración,

servidores DHCPv6 que ofrecen configuración y agentes de retransmisión DHCPv6 que transmiten mensajes entre clientes y servidores cuando los clientes se encuentran en subredes que no tienen un servidor DHCPv6.

Mensajes DHCPv6.

Al igual que en DHCP para IPv4, DHCPv6 utiliza mensajes de Protocolo de datagramas de usuario (UDP). Los clientes DHCPv6 escuchan mensajes DHCP en el puerto 546 de UDP. Los agentes de retransmisión y los servidores DHCPv6 escuchan mensajes en el puerto 547 de UDP. La estructura de mensajes DHCPv6 es mucho más sencilla que la de DHCP para IPv4, que tuvo sus orígenes en el protocolo BOOTP para ofrecer compatibilidad con estaciones de trabajo sin disco. En la figura 2.12 se muestra la estructura de los mensajes DHCPv6 enviados entre cliente y servidor.

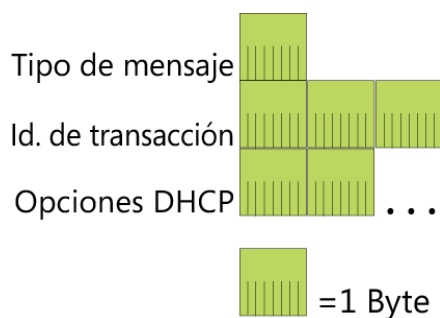


Figura 2.12 Mensajes DHCPv6 entre cliente y servidor

El campo de tipo de mensaje de 1 byte indica el tipo de mensaje DHCPv6. El campo de identificador de transacción de 3 bytes viene determinado por un cliente y se utiliza para agrupar los mensajes de un intercambio de mensajes DHCPv6. Después del campo de identificador de transacción, se utilizan las opciones DHCPv6 para indicar las direcciones y la identificación de servidor y cliente, además de otros valores de configuración. Para obtener una lista de opciones DHCPv6 definidas, consulte RFC 3315, como se indica en la barra lateral "Recursos RFC de DHCPv6".

Las opciones DHCPv6 tienen un formato de tipo-longitud-valor (TLV). En la figura 2 se muestra la estructura de las opciones DHCPv6.

El campo de código de opción de 2 bytes indica una opción específica. El campo de longitud de opción de 2 bytes indica la longitud del campo de datos de opción en bytes. El campo de datos de opción contiene los datos de la opción.

Existe una estructura independiente de mensajes correspondiente a los mensajes intercambiados entre agentes de retransmisión y servidores para registrar información adicional.

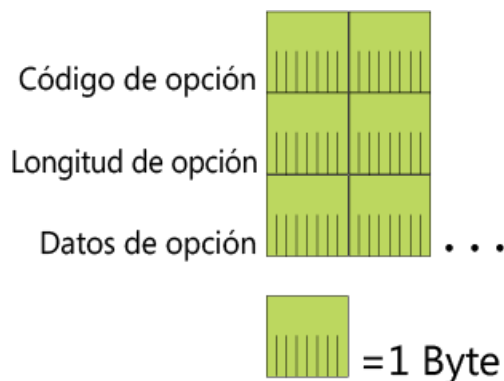


Figura 2.13 Estructura de opciones DHCPv6

El campo de número de saltos de 1 byte indica el número de agentes de retransmisión que han recibido el mensaje. Un agente de retransmisión receptor puede descartar el mensaje si excede el número de saltos máximo configurado. El campo de dirección del vínculo de 16 bytes contiene una dirección no local de vínculos que se asigna a una interfaz conectada a la subred en que está ubicado el cliente. Desde el campo de dirección del vínculo, el servidor puede determinar el ámbito de dirección correcto desde el que asignar una dirección. El campo de dirección del homólogo de 16 bytes contiene la dirección IPv6 del cliente que envió originalmente el mensaje o del agente anterior que retransmitió el mensaje. Después de este campo se encuentran opciones DHCPv6 que incluyen la opción de mensaje de retransmisión, que contiene el mensaje que se va a retransmitir, además de otras opciones. La opción de mensaje de retransmisión ofrece una encapsulación de los mensajes que se están intercambiando entre el cliente y el servidor.

No existen direcciones de difusión definidas para IPv6. Por lo tanto, el uso de la dirección de difusión limitada para algunos mensajes DHCPv4 se ha reemplazado por el uso de la dirección All_DHCP_Relay_Agents_and_Servers de FF02::1:2 para DHCPv6. Por ejemplo, un cliente DHCPv6 que intenta descubrir la ubicación del servidor DHCPv6 en la red envía un mensaje de petición desde su dirección local de vínculos a FF02::1:2. Si existe un servidor DHCPv6 en la subred del host, recibe el mensaje de petición y envía una respuesta apropiada. Más comúnmente, un agente de retransmisión DHCPv6 en la subred del host recibe el mensaje de petición y lo reenvía a un servidor DHCPv6.

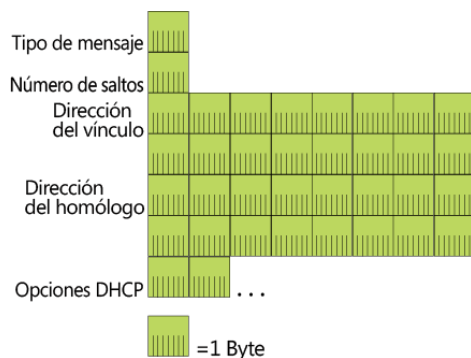


Figura 2.14 Estructura de mensajes entre el retransmisor y el servidor

Intercambio de mensajes con estado: Un intercambio de mensajes con estado de DHCPv6 para obtener configuración y direcciones IPv6 se compone generalmente de los siguientes mensajes:

Un mensaje de petición enviado por el cliente para ubicar los servidores.

Un mensaje de anuncio enviado por un servidor para indicar que puede ofrecer direcciones y configuración.

Un mensaje de solicitud enviado por el cliente para solicitar direcciones y configuración desde un servidor específico.

Un mensaje de respuesta enviado por el servidor solicitado que contiene direcciones y configuración.

Si existe un agente de retransmisión entre el cliente y el servidor, el agente envía mensajes de retransmisión-reenvío de servidor que contienen los mensajes de petición y solicitud encapsulados del cliente. El servidor envía los mensajes de retransmisión-respuesta del agente de retransmisión que contienen los mensajes de anuncio y respuesta encapsulados para el cliente. Para obtener una lista completa de mensajes DHCPv6.

Mensaje	Descripción	DHCP
---------	-------------	------

DHCPv6		equivalente para mensaje IPv4
Pedir	Enviado por un cliente para ubicar servidores.	DHCPDiscover
Anunciar	Enviado por un servidor en respuesta a un mensaje de petición para indicar disponibilidad.	DHCPOffer
Solicitar	Enviado por un cliente para solicitar configuración o direcciones de un servidor específico.	DHCPRequest
Confirmar	Enviado por un cliente a todos los servidores para determinar si la configuración de un cliente es válida para el vínculo conectado.	DHCPRequest
Renovar	Enviado por un cliente a un servidor específico para ampliar la duración de las direcciones asignadas y obtener una configuración actualizada.	DHCPRequest

Volver a enlazar	Enviado por un cliente a cualquier servidor si no se recibe una respuesta al mensaje de renovación.	DHCPRequest
Responder	Enviado por un servidor a un cliente específico en respuesta a un mensaje de petición, solicitud, renovación, nuevo enlace, solicitud de información, confirmación, liberación o rechazo.	DHCPAck
Liberar	Enviado por un cliente para indicar que el cliente ya no utiliza una dirección asignada.	DHCPRelease
Rechazar	Enviado por un cliente a un servidor específico para indicar que la dirección asignada se encuentra ya en uso.	DHCPDecline
Volver a configurar	Enviado por un servidor a un cliente para indicar que el servidor tiene una configuración nueva o actualizada. De este modo, el cliente envía un mensaje de renovación o solicitud de información.	N/A

Solicitar información	Enviado por un cliente para solicitar la configuración (pero no direcciones).	DHCPInform
Retransmitir-reenviar	Enviado por un agente de retransmisión para reenviar un mensaje a un servidor. Contiene un mensaje de cliente encapsulado como la opción de retransmisión-mensaje de DHCPv6.	N/A
Retransmitir-responder	Enviado por un servidor para enviar un mensaje a un cliente a través de un agente de retransmisión. Contiene un mensaje de servidor encapsulado como la opción de retransmisión-mensaje de DHCPv6.	N/A

Cuadro 2.4 Mensajes DHCPv6

Intercambio de mensaje sin Estado: Un intercambio de mensajes sin estado DHCPv6 para obtener sólo la configuración se compone generalmente de los siguientes mensajes: un mensaje de información-solicitud enviado por el cliente DHCPv6 para solicitar configuración de un servidor y un mensaje de respuesta enviado por un servidor que contiene la configuración solicitada.

En el caso de una red IPv6 con enrutadores configurados para asignar prefijos de direcciones sin estado a hosts de IPv6, el intercambio DHCPv6 de dos mensajes se puede utilizar para asignar servidores DNS, nombres de dominio DNS y otros valores de configuración que no se incluyen en el mensaje de anuncio de enrutador.

Compatibilidad de DHCPv6 en Windows: En Windows Server 2008 (WS08), Microsoft ha introducido DHCPv6 funcionalidad para el servidor DHCP.

En Windows Server 2008 (anteriormente conocido como "Longhorn" Server) Beta 2, se publican las DHCPv6 apátridas funcionalidad de servidor. En la versión Beta 3, se ha introducido la funcionalidad de servidor con estado DHCPv6. DHCPv6 behaviour en Windows Vista DHCPv6 se comporta como modo sin estado DHCPv6. Los clientes usan DHCPv6 para obtener sólo los parámetros de configuración de red diferente de la dirección IPv6. En este escenario, los clientes configurar una dirección IPv6 a través de un mecanismo basado en DHCPv6-no (posiblemente a través de IPv6 auto-configuración de la dirección basada en la prefijos IPv6 incluido en anuncios de enrutador, o por medio de una configuración estática.) En el modo con estado DHCPv6, los clientes adquieren tanto la dirección IPv6, así como otros parámetros de configuración de red a través de DHCPv6.

En WS08 Beta 3, la Beta y clientes TAP tendrá acceso a las siguientes características DHCPv6:

- Asignación de direcciones IPv6
- Protocolo de configuración automática con estado para IPv6
- Mejor rendimiento debido al servidor DHCPv6 2.001 multibprocesado
- Remuneración con intercambio de mensajes iniciado por un servidor
- Varios prefijos para un enlace
- Identificadores totalmente únicos para el cliente y el servidor
- Configuraciones DNS, SIP, NIS y NIS+ mediante DHCPv6 2.001
- Autenticación para los mensajes RECONFIGURE
- Protocolo de configuración dinámica de sistemas host sin estado para IPv6
- Funcionalidad de agente de retransmisión
- Solicitud de parámetros de configuración desde servidores diferentes en el marco del mismo dominio
- Parámetros de configuración para un cliente individual

- Opciones específicas del proveedor basadas en la clase de proveedor o en la clase de usuario
- Mecanismo para actualizar los parámetros de configuración del sistema apropiados en el cliente

2.1.1 PROTOCOLO DE INTERNET IPv4

El Protocolo de configuración dinámica de host (DHCP) Es un protocolo de autoconfiguración utilizado en Redes IP. Los equipos que están conectados a redes IP deben ser configurados antes de que puedan comunicarse con otros ordenadores de la red. DHCP permite que una computadora se configure automáticamente, eliminando la necesidad de la intervención de un administrador de red. También proporciona una base de datos central para el seguimiento de los equipos que han sido conectados a la red. Esto evita que dos equipos de forma accidental se vayan a configurar con la misma Dirección IP.

A falta de DHCP, los hosts pueden ser configurados manualmente con una dirección IP en nuestros laboratorios de la Universidad Tecnológica.

Además de las direcciones IP, DHCP también proporciona otra información. Hay dos versiones de DHCP, uno para IPv4 y otro para IPv6. Mientras que

ambas versiones llevan el mismo nombre y llevar a cabo el mismo propósito, los detalles del protocolo para IPv4 e IPv6 son lo suficientemente diferentes que se pueden considerar protocolos separados.

DHCP se definió por primera vez como un protocolo de seguimiento de las normas en RFC 1531 en octubre de 1993, como una extensión a la Manos a la Obra Protocolo (BOOTP) . La motivación para la ampliación de BOOTP es que requiere intervención manual para agregar información de configuración de cada cliente, y no proporcionan un mecanismo para la recuperación de las direcciones IP en desuso.

Dynamic Host Configuration Protocol automatiza la asignación de parámetros de red a dispositivos de red de uno o más servidores DHCP. Incluso en pequeñas redes, DHCP es útil porque hace que sea fácil de añadir nuevas máquinas a la red.

Cuando un cliente DHCP configurado (un ordenador o cualquier otro dispositivo de red) se conecta a una red, el cliente DHCP envía una emisión consulta solicitando la información necesaria de un servidor DHCP. El servidor DHCP gestiona un conjunto de direcciones IP y la información acerca de los parámetros de configuración del cliente , tales como puerta de enlace predeterminada , máscara de red y los DNS.

Al recibir una solicitud válida, el servidor asigna al equipo una dirección IP, un contrato de arrendamiento (longitud de tiempo que el reparto), y otros parámetros de configuración IP , tales como la máscara de subred y el puerto de enlace predeterminada. La consulta suele iniciarse inmediatamente después de el arranque, y deben completar antes de que el cliente puede iniciar IP basado en la comunicación con otros hosts .

Dependiendo de la aplicación, el servidor DHCP puede tener tres métodos de asignación de direcciones IP :

- *asignación dinámica*: Un administrador de la red asigna un rango de direcciones IP para DHCP, y cada equipo cliente en la LAN está configurado para solicitar una dirección IP del DHCP servidor durante la inicialización de la red . El proceso de petición y concesión utiliza un concepto de arrendamiento con un periodo de tiempo controlable, permitiendo que el servidor DHCP para recuperar (y luego reasignar) las direcciones IP que no se renuevan.
- *la asignación automática*: El servidor DHCP asigna permanentemente una dirección IP libre a un cliente que solicita el rango definido por el administrador. Esto es como la asignación dinámica, pero el servidor DHCP mantiene una tabla de anteriores asignaciones de direcciones IP ,

por lo que preferentemente se puede asignar a un cliente la misma dirección IP que el cliente previamente tenía.

- *asignación estática*: El servidor DHCP asigna una dirección IP basado en una tabla con direcciones MAC/Dirección IP, que se llena manualmente en (tal vez por un administrador de la red)
- El cliente emite mensajes en la subred física para descubrir servidores DHCP disponibles. Los administradores de red pueden configurar un
- router local que transmita paquetes DHCP a un servidor DHCP en una subred diferente.

2.1.2 PROTOCOLO DE INTERNET IPv6

- Desde hace mucho tiempo, se hizo necesaria la creación de un método actualizado y sin las dificultades como las que aún, presenta el protocolo ipv4. Es por ello que hoy en día se analizan opciones mejoradas y ya probadas como ipv6. Las cuales resaltan por su solución. Nuestro trabajo se basa en la implementación de Ipv6 como protocolo, dentro de nuestros laboratorios de redes. De la universidad Tecnológica. De una forma fácil y sencilla. Como la usada en Protocolo de configuración Dinámico del Host o mejor conocido como DHCPv6. Es por ello que en adelante se analiza a profundidad su funcionamiento.

- El protocolo Internet versión 6 (IPv6) es una nueva versión de IP definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.
- Diseñado por Steve Deering Y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.
 - IPv4 posibilita (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etc. En cambio, IPv6 admite (2^{128}) cerca de 3.4×10^{20} (340 trillones de direcciones) por cada pulgada cuadrada de la superficie de La Tierra.
- Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o bien los nodos pueden ser configurados en forma estática.

- Internet Protocol Security (IPsec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6. El soporte IPsec es obligatorio en IPv6; a diferencia de IPv4, donde es opcional (pero usualmente implementado). Sin embargo, actualmente no se está usando normalmente IPsec excepto para asegurar el tráfico entre routers de BGP
- Direccionamiento IPv6
- El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. , son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.
- El número de direcciones IPv6 posibles es de 2^{128} . Este número puede también representarse como 16^{32} , con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores
- Notación para las direcciones IPv6
- Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales. Por ejemplo,
- 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
- es una dirección IPv6 válida.
- Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo,

- 2001:0db8:85a3:0000:1319:8a2e:0370:7344
- 2001:0db8:85a3::1319:8a2e:0370:7344
- Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:
- 2001:0DB8:0000:0000:0000:0000:1428:57ab
- 2001:0DB8:0000:0000:0000::1428:57ab
- 2001:0DB8:0:0:0:0:1428:57ab
- 2001:0DB8:0::0:1428:57ab
- 2001:0DB8::1428:57ab
- son todas válidas y significan lo mismo.
- Los ceros iniciales en un grupo también se pueden omitir:
- 2001:0DB8:02de::0e13
- 2001:DB8:2de::e13
- Si la dirección es una dirección IPv4 empotrada, los últimos 32 bits pueden escribirse en base decimal, así:
- ::ffff:192.168.89.9
- ::ffff:c0a8:5909
- No se debe confundir con:

- ::192.168.89.9
- ::c0a8:5909
- Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34).
- En IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo "Cabecera Siguierte" similar en funcionalidad en IPv4 al campo Protocolo.

2.1.3 DISEÑO DE LA SOLUCION

Como parte de nuestra propuesta de solución es la de dejar en operación un servidor con Windows 2008, el cual tendrá configurado un Dhcp Server basados en direcciones IPv6, utilizando también un cliente Windows 7 en una estación de trabajo que de igual forma estará configurado con el mismo protocolo.

Nuestro esquema será el de establecer todo un proceso de protocolo de tipo cliente/servidor basado en IPv6 con el que cada cliente tendrá asignada su dirección ip , el diagrama general de operación será como el mostrado a continuación:

f

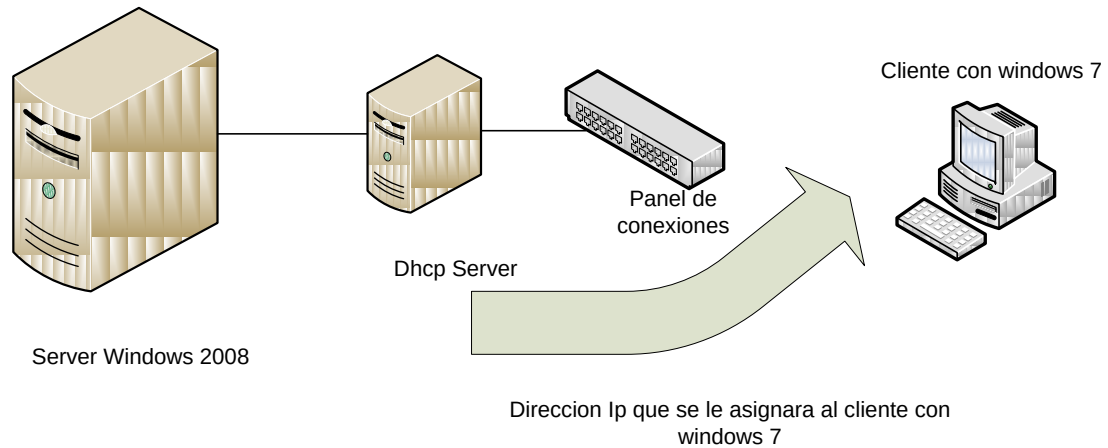
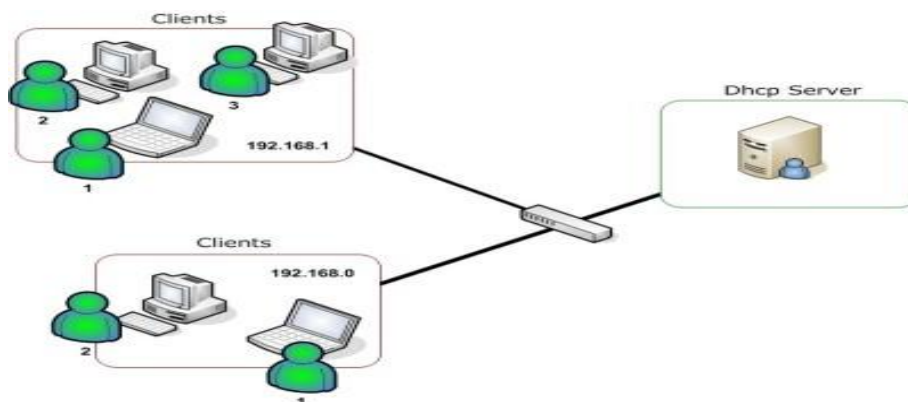


Figura 1.1 Funcionamiento de Dhcp Server

En el proceso el cliente con Windows 7, configurado con IPv6 de forma manual, tendrá configurado como servidor Dhcp el servidor de Windows 2008, en este primer proceso se realizará un protocolo de tipo [cliente/servidor](#) en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. basado en IPv6.

El implementar una red basada en IPv6 sería nuestra meta final, para lo cual estaremos realizando este escenario en equipos virtuales, pero se dejará montado en el laboratorio de redes de la Universidad Tecnológica de El Salvador, junto con las guías que detallen los pasos de configuración.

DHCP se utiliza extensamente para configurar los anfitriones con sus direcciones IPv4 e información adicional. Si usted tiene una red IPv6, usted no necesita DHCP configurar sus anfitriones con la información de la dirección. El mecanismo apátrida de la autoconfiguración configurará sus anfitriones para sus direcciones IPv6 sin la necesidad de instalar un servidor de DHCP. Todo lo que usted necesita hacer debe configurar sus rebajadoras de IPv6-enabled con la información del prefijo para los acoplamientos a los cuales se unen. Pero usted puede ser que inmóvil elija tener servidores de DHCP en algunos casos. Reciba la configuración que incluye la asignación de las direcciones IPv6 que usan DHCP se llama la autoconfiguración o Stateful DHCPv6 de Stateful. Usted tiene quizá un esquema de dirección específico IPv6; o usted necesita la asignación dinámica de los servidores del DNS; o usted elige no tener el MAC address como una parte de la dirección IPv6; o usted desea poner actualizaciones en ejecución dinámicas a DNS (RFC 2136). En estos casos, usted puede utilizar DHCP para la configuración de la dirección. Usted puede también combinar la autoconfiguración apátrida y de Stateful usando la autoconfiguración apátrida para la configuración de la dirección IPv6 y los servidores de DHCP para proporcionar la información adicional de la configuración que incluye pero no limitada a las direcciones del IP del servidor del DNS o a los dominios del DNS.



Conectividad de una red con dhcp IPv6

El RFC 3736 ofrece una opción adicional de la configuración. Define un servicio apátrida de DHCP para IPv6. Un servidor apátrida de DHCP puede configurar los anfitriones que tienen ya un IP address con la información adicional tal como servidores del DNS o del SIP. No puede hacer la asignación de dirección, aunque. DHCP apátrida se explica en el artículo, después de la sección en DHCPv6 stateful.

DHCPv6 y DHCPv4 son independientes. Si usted desea configurar los anfitriones con DHCP en dual-apilan la red, usted necesitarán actualmente dos servicios separados que funcionan, uno de DHCP para cada protocolo. En este caso, usted también tendrá que mirar hacia fuera para los conflictos de la configuración. En el mundo DHCPv4, configuran al cliente para saber si utilizar DHCP. En el mundo DHCPv6, el anuncio de la rebajadora tiene opciones para informar al cliente si utilizar DHCP. Puede haber información de la configuración

que diferencia que llega el cliente de diversas fuentes, o un nodo puede tener interfaces múltiples, e.g., uno que es IPv4-only y uno dual-siendo apilado. DHCPv6 utiliza un identificador único (DUID), que no existe para DHCPv4. En el reino de DHCPv4, el MAC address y la identificación del cliente se asemejan al DUID en DHCPv6 pero no son sinónimos. Hay trabajo que se enciende hacer el DUID disponible para DHCPv4 también.

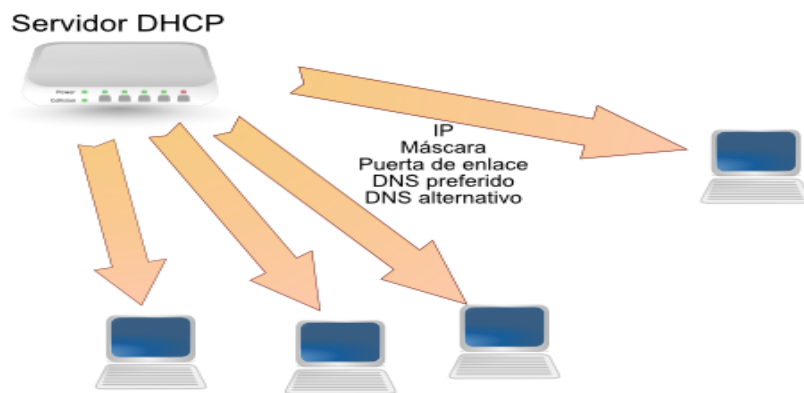
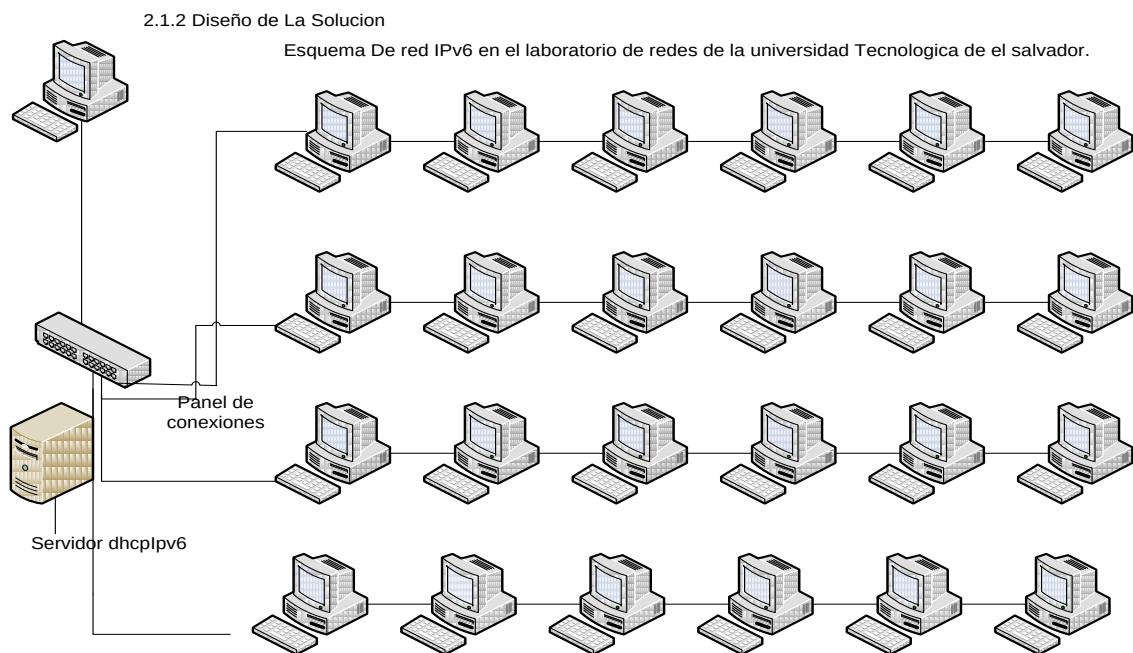


Figura 1.3 Direccionamiento lógico de Ip Con Dhcp IPv6

El grupo de funcionamiento de DHCP es más futuro determinando requisitos y las soluciones de evaluación, que permitirán dual-apilan los anfitriones que se configurarán para ambos protocolos por el servidor de unos o más DHCP. Draft-ietf-dhc-dual-stack-04.txt entra más detalle y describe las ediciones identificadas con interacciones duales de la versión DHCP del IP. El aspecto más importante es cómo manejar problemas potenciales en los clientes que procesan la

información de la configuración recibida los servidores de DHCPv4 y de DHCPv6.

En el diagrama general se puede observar la operación del laboratorio ya montado.



CAPITULO III. PROPUESTA DE LA SOLUCION.

3.1PROPUESTA DE SOLUCION

Nuestro proyecto está orientado en esclarecer las dudas y facilitar la comprensión sobre la implementación de servicio de Dhcp Server bajo el nuevo esquema de comunicación de TCP/IP versión 6, ya que parte de nuestros entregables es la de dejar un prototipo en operación junto con una guía de configuración que permita la fácil comprensión de los pasos requeridos para configurar este ambiente de trabajo.

La gran fundamentación de nuestro proyecto no está en los servicios de Dhcp Server ya que éstos funcionan como lo han venido haciendo, el reto realmente está en la comprensión de la nueva forma de comunicación y formato que ofrece este nuevo protocolo, que tiene un impacto indirecto en cómo los servicios mencionados anteriormente deben de ser configurados.

3.1.1 PLANTEAMIENTO DEL PROYECTO TEMÁTICO

El desarrollo de nuestro proyecto está dado en diferentes etapas en las cuales hemos tratado de contemplar todo lo necesario para poder documentar y detallar los aspectos importantes en el desarrollo del mismo:

Cuadro 1.1 Detalles del Proyecto Realizado

Etapa	Detalles realizados
Etapa I Situación Actual	Investigación sobre IPv6, sus nuevas características y diferencias con IPv4 y la necesidad que hay en implementar esta Y los problemas que resolveremos con esta tecnología.
Etapa II Documentación Técnica	Recopilación de información técnica sobre IPv6 y IPv6 su aplicación en sistemas operativos Windows Server 2008 y Windows 7 y diseños de red que se va a implementar.
Etapa III Propuesta De Solución	Propuesta de solución e información técnica sobre los servicios de Dhcp Server para sus aplicaciones con IPv6 e IPv4.

Etapa IV	Instalación de Windows Server 2008 en un ambiente
Instalación Del	de pruebas para iniciar a configurar IPv6 e instalar los
Proyecto	servicios de Dhcp bajo este protocolo.

3.1.2

CRONOGRAMA DE ACTIVIDADES

1	Nombres De Actividades	Duracion	Comienzo	Final
2	Proyecto Dhcp Server IPv6	10 días	06/09/2010	15/09/2010
3	Etapas I	6 días	20/09/2010	25/09/2010
4	Realización de documento de propuesta de la solución	2 días	27/09/2010	28/09/2010
5	Identificación de los recursos de hardware y software necesarios a utilizar	1 día	04/10/2010	04/10/2010
6	Preparación de equipo con VMWare Workstation para preparación del escenario de la solución	1 día	05/10/2010	05/10/2010
7	Instalación de servidor Windows 2008 Server	2 hrs	06/10/2010	06/10/2010
8	Inhabilitar protocolo IPv4 en servidor Windows 2008	1 hr	06/10/2010	06/10/2010
9	Asignar una IPv6 manual en servidor Windows 2008	1 hr	06/10/2010	06/10/2010
10	Instalar otro equipo virtual con Windows 7	2 hrs	06/10/2010	06/10/2010
11	Inhabilitar protocolo IPv4 en PC con Windows 7	1 hr	06/10/2010	06/10/2010
12	Asignar una IPv6 manual en PC con Windows 7	1 hr	06/10/2010	06/10/2010
13	Validar comunicación en red entre ambos equipos	2 hrs	06/10/2010	06/10/2010
14	Etapas II	5 días	07/10/2010	11/10/2010
15	Instalación de Servicio de Dhcp en Windows 2008 server	2 hrs	12/10/2010	12/10/2010
16	Configuración de Dhcp Server en windows 2008 server	3 hrs	12/10/2010	12/10/2010
17	Realización de pruebas con servidor de Dhcp desde la virtual con Windows 7	2 hrs	12/10/2010	12/10/2010
18	Etapas III	4 días	14/10/2010	17/10/2010
19	Documentar proceso de configuración	2 días	18/10/2010	19/10/2010
20	Realizar prueba final para configuración de todo el escenario configurado	2 días	20/10/2010	21/10/2010

3.1.3 TECNOLOGÍAS Y RECURSOS UTILIZADOS

A continuación detallamos todos los recursos tecnológicos que han tenido participación en el desarrollo de este proyecto:

Cuadro 1.2 Recursos de Hardware

Recursos de Hardware (Virtualizados)	
Servidor	Memoria: 1GB
	Disco Duro: 40GB
	Procesador: 1 de 2.5Ghz
	Tarjeta de red: 1 a 1 Gbps
Estación de trabajo	Memoria: 654 MB
	Disco Duro: 40GB
	Procesador: 1 de 2.5Ghz
	Tarjeta de red: 1 a 1 Gbps

Debido a que los recursos de hardware fueron virtualizados en un mismo equipo físico, no se requirió de un equipo de red adicional para poder comunicarlos.

Cuadro 1.3 Recursos de Software

Recursos de Software

Servidor Windows Server 2008 Enterprise

Servicios instalados:

✓ Dhcp Server

Estación de Windows 7 Professional
trabajo

Para ambos sistemas operativos se deshabilitó el protocolo IPv4 dejando únicamente el protocolo IPv6 para efecto de garantizar una comunicación bajo este único mecanismo de comunicación.

3.1.4 DISEÑO DE LA PROPUESTA

En el Laboratorio de Redes de la Universidad Tecnológica de El Salvador existe un buen numero de hosts, acá el servidor [DHCP](#) se convierte en pieza clave del despliegue de la red en dicho Laboratorio, puesto que hace más sencillo el proceso de asignación de direcciones IPs a los hosts que componen la red, así como permite realizar cambios en este direccionamiento IP sin apenas intervención humana.

El servidor se va a llamar **LabRedesV6** y va a ser controlador primario de dominio (**LRV6**). Debido a que todas las cuentas de usuario y todos los recursos pertenecerán al mismo dominio (**LabRedesV6**), no hay necesidad de configurar relaciones de confianza y todas las tareas administrativas pueden ser manejadas en un lugar. Los clientes que utilicen el servicio DHCPv6, trabajaran en la plataforma Windows 7. Este sistema operativo, viene adaptado de forma nativa para trabajar con IPv6.

Al ser una seguridad centralizada no es necesario especificar los permisos en cada una de las estaciones de trabajo de la red, dado que estas antes de llevar a cabo cualquier petición, esperan la autorización del **LRV6**.

Se utilizará el protocolo TCP/IP para la configuración de la conexión a la red entre el servidor y las estaciones de trabajo. Utilizamos este protocolo porque es un estándar que se utiliza en la red de redes (Internet); es un protocolo que

puede ser encaminado, lo que hace disminuir el tráfico total de la red; es un protocolo un protocolo robusto que incorpora prestaciones de fiabilidad de transmisión y capacita a las aplicaciones con una interfaz para los sockets de formas de comunicación especializadas (como FTP o comunicaciones de bases de datos cliente/servidor).

En una red normal cada equipo debe tener asignada una dirección IP para acceder a Internet, pero en una red con un servidor DHCP (Dynamic Hosts Configuration Protocol) que es un sistema desarrollado para asignar direcciones IP dinámicamente, esta dirección la proporciona el servidor cuando sea necesario. Es decir los ordenadores solicitarán una dirección IP al servidor y este se la proporcionará durante un período de tiempo determinado.

El proceso a seguir por un equipo que quiera acceder a Internet es el siguiente:

1. Manda un mensaje al servidor DHCP solicitando una dirección IP.
2. El servidor DHCP responde ofreciendo varias direcciones IP que tiene disponibles de las indicadas en la instalación (se han eliminado las que se han considerado oportuno).
3. El cliente selecciona una y envía una solicitud de uso de la dirección al servidor DHCP.

4. El servidor DHCP admite la solicitud y garantiza al cliente la concesión del uso de la dirección.
5. El cliente utiliza la dirección para conectarse a la red.

Uno de los aspectos más importantes de la planificación de una implementación de DHCP es la topología de Red. Al entender la topología de red, se podrá identificar rápidamente los intervalos de direcciones IP para DHCP, la información de configuración que cada cliente necesita, los dispositivos que deben ser configurados para reenviar mensajes DHCP, DHCP y si puede trabajar con su DNS o servidores PPP. Se va a incluir todos los host y los dispositivos que se conectan a la LAN, y las direcciones IP de los dispositivos y clientes (por ejemplo, una impresora) que necesitan una dirección IP definida.

La topología a utilizar para la configuración de Servicio DHCP, es de Estrella. Se considera esta por estar conectada directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de éste. Los dispositivos no están directamente conectados entre si y además de que no se permite tanto tráfico de información. Dado su transmisión, una red en estrella activa tiene un nodo central *activo* que normalmente tiene los medios para prevenir problemas relacionados con el eco.

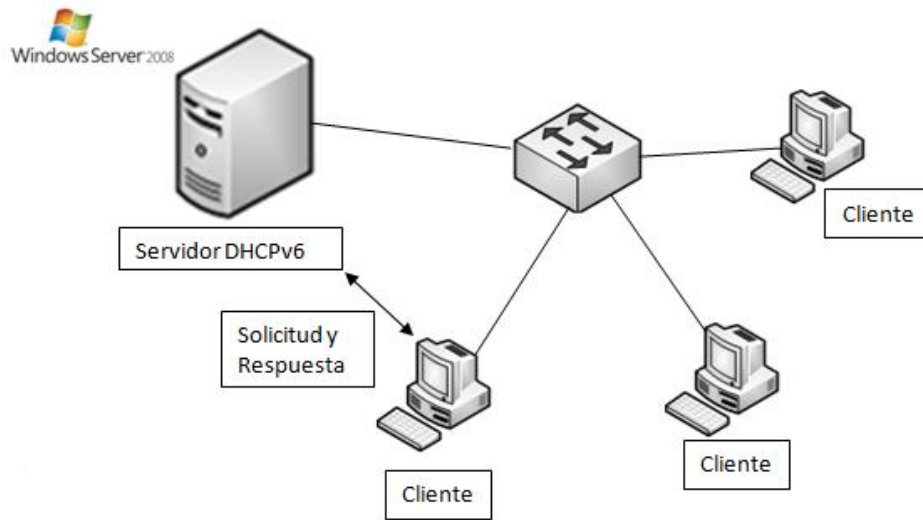


Diagrama de Funcionalidad

Como se puede observar en la figura 3.1.4.1, los clientes están conectados a un dispositivo central (Switch). Solicitan una dirección IP, el servidor se encarga de asignar automáticamente una dirección IP versión 6. Se puede observar además que se utiliza la topología en Estrella.

Microsoft Windows Server 2008's built-in DHCP server allows Windows machines (and any other TCP/IP-based machines and devices) to obtain their IP addresses and network settings automatically, which can vastly simplify network configuration. Microsoft Windows Server 2008 está integrado en el servidor DHCP permite a las máquinas de Windows (y cualquier otro TCP / IP basada en

máquinas y dispositivos) para obtener sus direcciones IP y configuración de red automáticamente, que pueden simplificar enormemente la configuración de red.

3.1.5 IMPLEMENTACION DE LA PROPUESTA

El protocolo de Internet versión 4 (IPv4) ha sido el principal protagonista del desarrollo y expansión de Internet en las últimas décadas. El crecimiento explosivo de Internet y la diversificación de los servicios que entrega, han expuesto los problemas existentes actualmente en IPv4. Es por este motivo que se ha desarrollado el protocolo de Internet versión 6 (IPv6), que corrige dichos problemas y permite crear la base para el desarrollo de Internet durante las próximas décadas. En la actualidad, el soporte IPv6 que ofrecen los fabricantes de equipos y programas computacionales ha alcanzado un desarrollo que permite la implementación de redes IPv6 nativas. Ya no es necesario depender de herramientas de traducción y/o túneles para poder desarrollar redes IPv6 que implementen el mismo tipo de servicios otorgados en redes IPv4. Este trabajo presenta el desarrollo e implementación de una red IPv6 en la UNIVERSIDAD TECNOLOGICA DE EL SALVADOR conectada directamente a Internet. Se entregan los criterios utilizados para la actualización de los equipos de la red junto al plan de integración de IPv6. Se realiza una revisión del soporte IPv6 en sistemas operativos y servicios de red junto a un análisis sobre posibles ataques que afecten la seguridad de la red implementada.

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 en cómo nos comunicamos y relacionamos con personas a lo largo del mundo. Poco a poco observamos 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 usuarios 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 fue desarrollado en la década de los 70 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 en 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 adopción de IPv6 ha sido un proceso lento. A la fecha, el tráfico IPv6 en Internet representa menos de un 1% 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 características del protocolo. Sin embargo, este tipo de implementaciones entrega un panorama 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. El principal objetivo de este trabajo es diseñar e implementar una red IPv6 nativa al interior de la UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR, con salida directa hacia Internet. En este trabajo se cubren diversos aspectos, desde la creación de un plan de actualización del

equipamiento de la red, hasta la evaluación de alternativas de monitoreo y políticas de seguridad en la red. El trabajo y los resultados aquí expuestos constituyen el primer paso para una futura migración a IPv6 de todos los servicios ofrecidos por la red institucional de la UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR., y como estos justifican la necesidad de adoptar IPv6., con el fin de establecer el marco teórico necesario para permitir al lector comprender los pasos realizados en la implementación de la red IPv6 en la UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR. Se establece el plan de actualización de equipos, y se evalúan las diversas alternativas tecnológicas y de fabricantes para la implementación de la red.

Describiendo los protocolos de enrutamiento utilizados, el plan de direccionamiento creado y la configuración utilizada en los equipos. Se entrega un breve acercamiento al soporte IPv6 existente en sistemas operativos y aplicaciones. Se hace un énfasis especial en los programas de monitoreo de redes y su comportamiento en redes IPv6. Se analizan los aspectos del protocolo IPv6 que afectan su desempeño en comparación a IPv4. Se presentan dos escenarios de prueba que comparan el desempeño de IPv6 en aplicaciones de uso masivo. se describen las principales debilidades en la seguridad de la red IPv6 implementada, junto a la evaluación de alternativas para mitigar posibles ataques. Finalmente, se entregan las conclusiones finales

del trabajo, definiendo cuales son los siguientes pasos y aspectos a evaluar en un futuro plan de migración total a IPv6.

El protocolo de Internet (IP) es un protocolo no orientado a la conexión usado para transmitir información a través de una red de paquetes conmutados. Se ubica en la capa 3 del modelo ISO/OSI y su función es entregar paquetes desde un nodo de origen a uno de destino, basado en la dirección escrita en cada paquete. El protocolo de Internet versión 4 (IPv4) es la cuarta iteración del protocolo IP y la primera versión en ser utilizada en ambientes de producción. Es el protocolo dominante en Internet, utilizado para conectar redes de forma interna y hacia el exterior. Dentro de sus principales características se encuentran:

- Enrutamiento y direccionamiento: Provee una dirección única a cada dispositivo de una red de paquetes. IPv4 fue especialmente diseñado para facilitar el enrutamiento de información (paquetes) a través de redes de diversa complejidad.
- Encapsulación: El protocolo IPv4 nace como una división del antiguo protocolo TCP ("Transmission Control Protocol"). Se ubica en la capa 3 del modelo ISO/OSI y puede funcionar sobre diversos protocolos de nivel inferior.

□ Mejor esfuerzo: El protocolo IP provee un servicio de transmisión de paquetes no fiable (o de mejor esfuerzo). No se asegura que los paquetes enviados lleguen correctamente al destino.

La versión de IPv4 usada actualmente en Internet no ha cambiado sustancialmente desde su publicación inicial en 1981. IPv4 ha demostrado ser un protocolo robusto, fácil de implementar y con la capacidad de operar sobre diversos protocolos 5 de capa 2. Si bien fue diseñado inicialmente para interconectar unos pocos computadores en redes simples, ha sido capaz de soportar el explosivo crecimiento de Internet. Sin embargo en el último tiempo, se han hecho notar diversos problemas existentes en IPv4, asociados al crecimiento de Internet y a la aparición de nuevas tecnologías y servicios que requieren conectividad IP.

Agotamiento direcciones IP

Una dirección IPv4 tiene un tamaño de 32 [bit], lo que permite un máximo teórico de 2^{32} (4.294.967.296) direcciones a asignar. En los inicios de Internet, se utilizaron métodos de distribución poco eficientes, como la asignación por clases, mediante los cuales se asignaron grandes bloques de direcciones a organizaciones que solo requerían unas pocas. Esto ha generado que

actualmente muchas organizaciones posean un gran número de direcciones que no se encuentran utilizadas.

Los primeros reportes de alerta sobre el inminente agotamiento de direcciones IP se dieron a conocer alrededor de 1990 . Diversas soluciones y protocolos han permitido extender la vida útil de IPv4, tales como la traducción de direcciones de red (NAT), el enrutamiento sin clases entre dominios (CIDR) y el uso de asignaciones temporales de direcciones con servicios tales como DHCP y RADIUS/PPP. Actualmente, se ha establecido una política jerarquizada para la asignación de direcciones IPv4, en donde el IANA (“Internet Assigned Numbers Authority”) tiene a su cargo el manejo de los bloques de direcciones IPv4 que se encuentran libres. Junto al IANA, se encuentran los registros regionales de Internet (AFRINIC, APNIC, ARIN, LACNIC y RIPENCC) quienes reciben bloques de direcciones delegados por el IANA y los distribuyen entre los proveedores de servicios (ISP) de la región del mundo que administran.

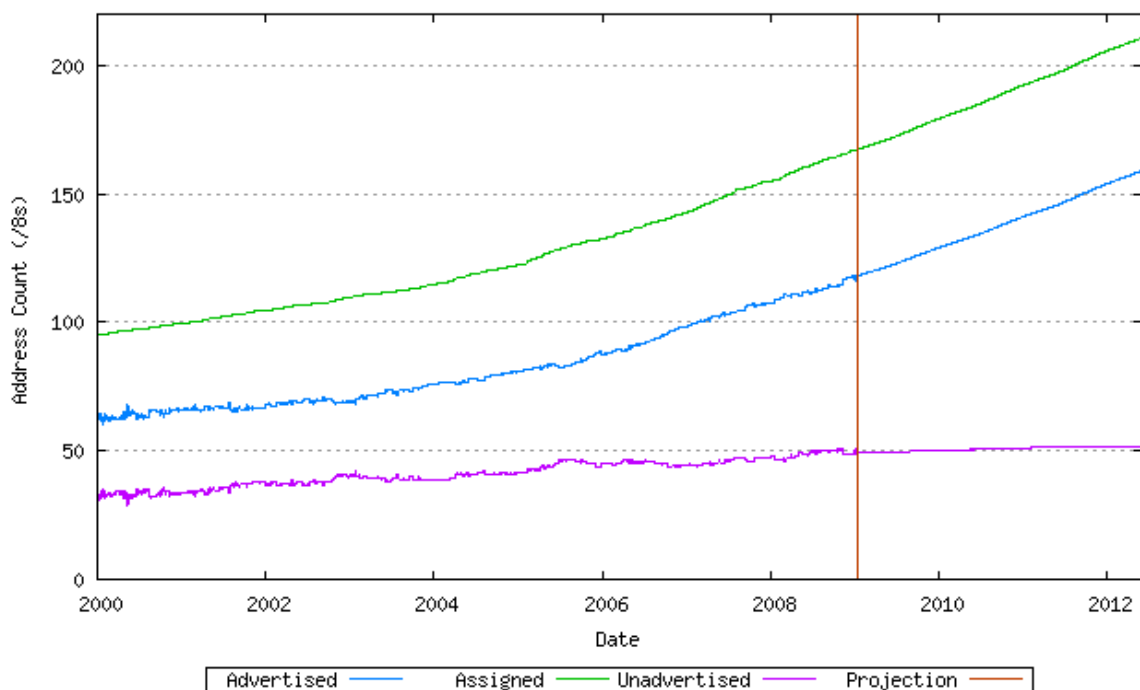
El IANA asigna bloques de prefijo /8, (equivalentes a 1/256 del total de direcciones) a los registros regionales. Dado que el rango de direcciones comprendido entre 224.X.X.X y 239.X.X.X se encuentra reservado para tráfico “multicast”, y el rango 6

entre 240.X.X.X y 254.X.X.X se encuentra reservado para trabajos experimentales, el espacio real de direcciones disponibles para ser asignadas

es de 223 bloques /8, los cuales representan 16.777.214 direcciones cada uno. En la Figura 2.1 se observa la distribución actual¹ de bloques /8.

Es complicado estimar la fecha exacta en que se agotarán todas las direcciones IPv4 disponibles, ya que diversos factores pueden adelantar o retrasar dicha fecha. Dentro de esos factores se encuentran posibles cambios en la política de asignación, 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” [1], que a partir de la información publicada por el IANA y los registros regionales, entrega una fecha estimada de agotamiento de direcciones IPv4.

En la Figura 2.2 se presenta una proyección del agotamiento de bloques /8. Este análisis modela el comportamiento de cada registro regional, considerando su demanda histórica de bloques de direcciones IP. En la figura se observan tres curvas, una asociada a los bloques asignados a registros regionales (“Assigned”), otra que representa aquellos bloques asignados que son anunciados efectivamente hacia internet (“Advertised”) y una que señala aquellos bloques asignados que no son anunciados (“Unadvertised”).



En base a estas proyecciones, se estima que en Marzo del 2011 se agotará el total de los bloques /8 libres manejados por el IANA. A partir de dicho momento, los registros regionales no tendrán la posibilidad de solicitar bloques de direcciones adicionales, sólo podrán administrar las direcciones que ya tienen asignadas. La segunda fecha a considerar es cuando los registros agoten su reserva de direcciones y ya no puedan solicitar un bloque adicional al IANA. Se ha estimado que ello ocurra en Mayo del 2012, un año después del agotamiento de los bloques disponibles. Todos estos cálculos y estimaciones están realizados en base al crecimiento histórico que ha tenido la demanda de direcciones IP a nivel mundial. Sin embargo, se espera que en los próximos

años, la demanda por direcciones IP sea aún mayor debido a diversos factores tales como:

- Grandes poblaciones en China, India, Indonesia y África aun no están conectadas.
- El número de individuos conectados a Internet crece en 77 millones por año [4].
- Dispositivos electrónicos de todo tipo están paulatinamente conectándose a Internet.

De todas formas, es posible advertir que en estos días ya estamos en presencia de problemas relacionados con la baja disponibilidad de direcciones IP:

- Las organizaciones normalmente obtienen pocas direcciones IP para toda su red, limitando las posibilidades de implementar servidores y aplicaciones.
- Algunos proveedores de servicios (ISP) están asignando direcciones IP privadas a sus subscriptores, lo que significa que el suscriptor no puede ser contactado directamente desde internet.
- Gran parte de las compañías de telefonía celular no proveen de direcciones públicas a los usuarios de servicios 3G.

- Muchas aplicaciones disminuyen su rendimiento al no disponer de conectividad punto a punto auténtica.

Problemas de arquitectura

Dado el fuerte crecimiento que ha experimentado Internet en los últimos años, ha sido necesario introducir modificaciones y protocolos complementarios a IPv4, con el fin de poder satisfacer la creciente demanda. Estos cambios han causado que las redes IP estén perdiendo paulatinamente el principio de conectividad punto a punto bajo el cual se diseñó IPv4. Dicho principio establece lo siguiente:

- Ciertas funciones solo pueden ser realizadas por los nodos finales. El estado de una comunicación punto a punto debe ser mantenida únicamente por los nodos finales y no por la red. La función de la red es enrutar paquetes de forma eficaz y transparente.
- Los protocolos de transporte están designados para proveer las funciones deseadas sobre una red que no ofrece garantías (mejor esfuerzo).
- Paquetes deben viajar sin modificación a través de la red.

□ Las direcciones IP son usadas como identificadores únicos para nodos finales.

Una de las medidas introducidas para frenar el agotamiento de direcciones IPv4 es el protocolo de traducción de direcciones de red (NAT). NAT es un protocolo que permite convertir en tiempo real las direcciones utilizadas en los paquetes transportados en una red. El uso de NAT permite que un grupo de dispositivos configurados con direcciones IPv4 privadas compartan un reducido grupo de direcciones IPv4 públicas, permitiendo el acceso hacia Internet. Si bien el uso de NAT ha permitido la expansión actual de Internet, su uso introduce una serie de problemas y desventajas, asociados a la pérdida del principio de conectividad punto a punto. Dentro de las desventajas del uso de NAT podemos encontrar: 10

Complejidad: NAT representa un nivel de complejidad adicional al momento de configurar y manejar una red. Se deben crear grupos de dispositivos y/o redes que comparten un número limitado de direcciones IPv4 públicas.

□ Compatibilidad con ciertas aplicaciones: Muchas aplicaciones no funcionan correctamente cuando se ejecutan desde dispositivos que están en una red donde se realiza NAT. Los desarrolladores han tenido que inventar nuevos mecanismos para poder funcionar correctamente en dichas redes.

□ Problemas con protocolos de Seguridad: Protocolos de seguridad tales como IPSec están designados para detectar modificaciones en las cabeceras de los paquetes, que es precisamente lo que hace NAT al traducir direcciones. El uso de NAT dificulta la implementación de este tipo de protocolos.

□ Reducción de rendimiento: Por cada paquete que atraviesa una red donde opera NAT, se deben realizar una serie de operaciones adicionales. Dichas operaciones introducen mas carga a la CPU del dispositivo que realiza la traducción, disminuyendo su rendimiento.

□ Manejo de estados TCP: El dispositivo que realiza NAT debe manejar y mantener correctamente los estados de cada conexión TCP entre equipos de la red interna y externa.

A pesar de todas sus desventajas, NAT permitió posponer en varios años el agotamiento de direcciones IPv4. Sin embargo, en la actualidad se ha llegado a un punto en donde el uso de NAT no es suficiente para la creciente demanda de direcciones IPv4. Esto ha motivado la evaluación de otras alternativas, tales como IPv6.

Motivadores del cambio a IPv6

El cambio desde IPv4 a IPv6 se suele comparar con la crisis que se vivió a fines de los 90 ante la llegada de año 2000 y sus consecuencias en los sistemas informáticos. Sin embargo, en el caso de IPv6 no existe una fecha límite o “flag day” en que se 11 puedan deshabilitar todas las redes IPv4 y actualizarlas a IPv6. El proceso de migración debe realizarse en forma progresiva, se prevé que IPv4 siga en funcionamiento durante la próxima década.

El mayor problema que enfrenta IPv6 es que desde el punto de vista de las empresas y organizaciones, su implementación se ve como un gasto poco justificado. En la actualidad, el tráfico IPv6 representa menos de un 1% del tráfico total de Internet [5], y la mayoría corresponde a Universidades e instituciones que trabajan en el tema. Sin embargo, existen una serie de motivadores para la implementación a IPv6, los que se pueden agrupar en las siguientes categorías.

El protocolo IPv6 comenzó a desarrollarse en el año 1990, tras la primera voz de alerta sobre el posible agotamiento de direcciones IP [3]. Se creó un grupo de trabajo al interior de la IETF, quienes presentaron sus primeras recomendaciones [7] sobre el nuevo protocolo que debería reemplazar a IPv4. En el mismo año se publicó oficialmente la primera versión del protocolo IPv6 [8].

En líneas generales, el protocolo IPv6 es considerado una evolución más que una revolución respecto al protocolo IPv4. Se han mantenido los conceptos principales del protocolo, removiendo aquellas características de IPv4 que son poco utilizadas en la práctica. Se han añadido nuevas características que buscan solucionar los problemas existentes en el protocolo IPv4, discutidos en el capítulo 2.

Características del protocolo IPv6

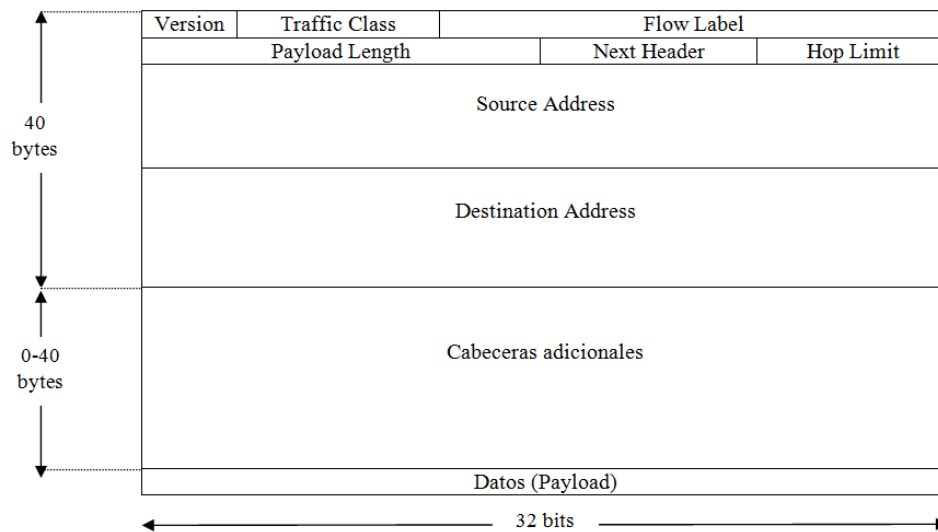
Dentro de las principales características de IPv6 se encuentran:

- Mayor número de direcciones: El tamaño de una dirección aumenta desde 32 a 128[bit] lo que se traduce en alrededor de $3,4 \cdot 10^{38}$ direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.
- Direccionamiento jerárquico: Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables. Nuevo formato de cabecera: Aún cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado

campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.

□ Autoconfiguración: IPv6 incorpora un mecanismo de auto configuración de direcciones, “stateless address configuration”, mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

□ Nuevo protocolo para interactuar con vecinos: El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y “Router Discovery” de IPV4. Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo “broadcast”.



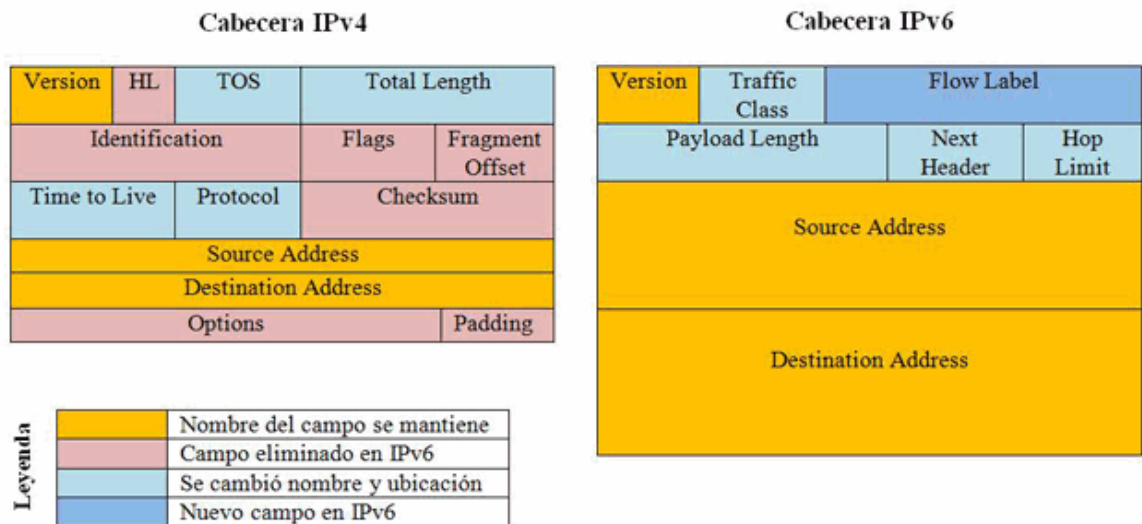
Un paquete IPv6 tiene una cabecera de tamaño fijo e igual a 40 [byte], el doble de la cabecera IPv4. Este aumento se debe a que el tamaño de los campos

“Source Address” y “Destination Address” aumentaron su tamaño de 32 a 128 [bit] cada uno. La cabecera posee los siguientes 8 campos:

- Versión (“Version”): Indica la versión del protocolo IP, en este caso su valor es igual a 6.
- Clase de tráfico (“Traffic Class”): Incluye información que permite a los “routers” clasificar el tipo de tráfico al que el paquete pertenece, aplicando distintas políticas de enrutamiento según sea el caso. Realiza la misma función que el campo “Type of Service” de IPv4.
- Etiqueta de flujo (“Flow Label”): Identifica a un flujo determinado de paquetes, permitiendo a los “routers” identificar rápidamente paquetes que deben ser tratados de la misma manera.
- Tamaño de la carga útil (“Payload Length”): Indica el tamaño de la carga útil del paquete. Las cabeceras adicionales son consideradas parte de la carga para este cálculo.
- Próximo encabezado (“Next Header”): Indica cual es el siguiente encabezado es la siguiente cabecera adicional presente en el paquete. Si no se utilizan, apunta hacia la cabecera del protocolo capa 4 utilizado.

- Límite de saltos (“Hop Limit”): Indica el máximo número de saltos que puede realizar el paquete. Este valor es disminuido en uno por cada “router” que reenvía el paquete. Si el valor llega a cero, el paquete es descartado.
- Dirección de origen (“Source Destination Address”): Indica la dirección IPv6 del nodo que generó el paquete.
- Dirección de origen (“Source Destination Address”): Indica la dirección de destino final del paquete.

En la Figura 3.2 se pueden apreciar los cambios de la cabecera IPv6 respecto a la cabecera IPv4.



3.1.6 PRESENTACIÓN DE LA PROPUESTA

3.1.5.1 OFERTA TÉCNICA

San Salvador, 16 de Octubre 2010.

Sres. Universidad Tecnológica de El Salvador

Presente:

Es un gusto saludarles y desearles éxitos en sus labores. Por medio de la presente agradecemos la oportunidad de presentarles la propuesta de implementación de El Servidor DHCP sobre la plataforma de Microsoft Windows Server 2008, basado en el nuevo protocolo IPv6 que será una solución rápida y efectiva de asignación automática de direcciones IP para el Laboratorio de Redes.

El protocolo DHCP permite configurar automáticamente los host de una red TCP/IP durante el arranque de los sistemas. DHCP utiliza un mecanismo de cliente-servidor, a la vez los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan. Esta información incluye la dirección IP del cliente y los servicios de red de los que el cliente puede disponer. Windows Server 2008 es parte de la nueva generación de sistemas operativos de Windows Server que permite el control más efectivo de la infraestructura de red, ofrece disponibilidad y capacidades de

administración sin precedentes, logrando un entorno de servidor significativamente más seguro, confiable y robusto. Windows Server 2008 asegurar que todos los usuarios, sin importar su ubicación, accedan a todos los servicios de la red, también brinda un panorama de lo que ocurre con el sistema operativo y con las capacidades de diagnóstico.

Las ventajas que ofrece la nueva tecnología IPv6 son las siguientes:

- Capacidad Extendida de direccionamiento
- Autoconfiguración y Reconfiguración
- Mecanismos de movilidad más eficiente y robusta
- Encriptación y Autenticación
- Formato de cabecera simple

La Fusión de estas Tecnologías darán como resultado una Poderosa y Efectiva herramienta que mejorara en su totalidad la comunicación entre Cliente – Servidor.

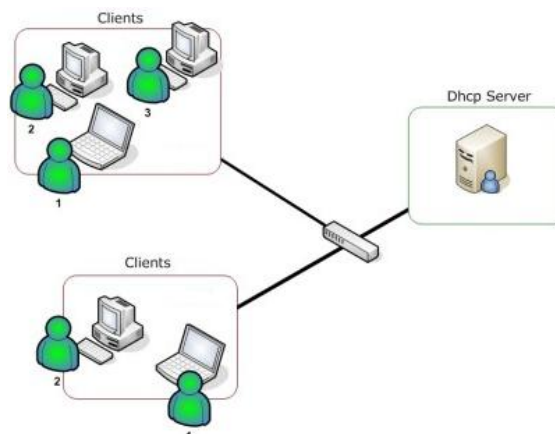


Figura 3.1.6.1 Servidor DHCPv6 Instalado y Configurado

3.1.5.2

OFERTA ECONÓMICA

<i>Cantidad</i>	<i>Descripción</i>	<i>Precio Unitario</i>	<i>Precio Total</i>
1	Configuración del Servicio DHCP	\$ 850.00	\$ 850.00
1	Capacitación de Configuración, Soporte y Funcionalidad	\$ 450.00	\$ 450.00
<i>Total de la Oferta</i> <i>\$ 1,300.00</i>			

Tiempo de Entrega: 5 días

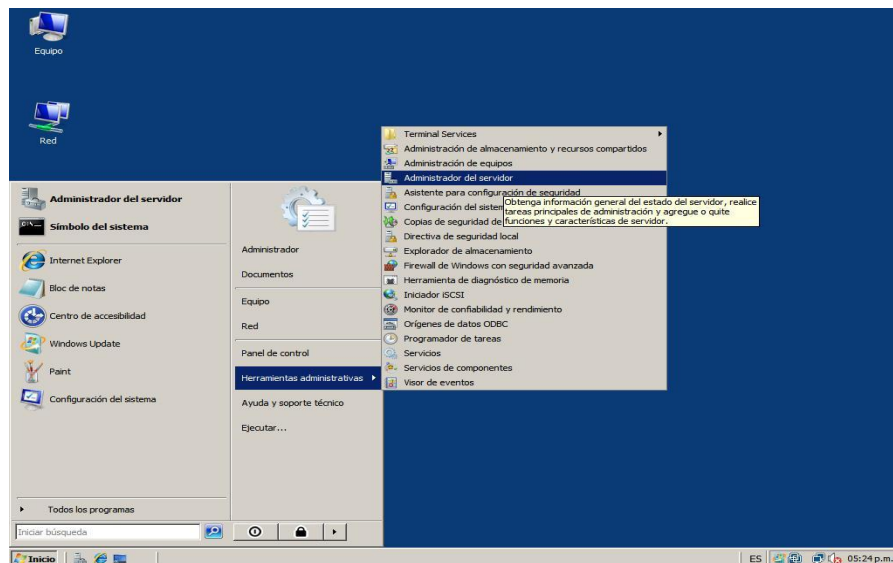
Entregables:

- Guía de la instalación y configuración del Servidor DHCP

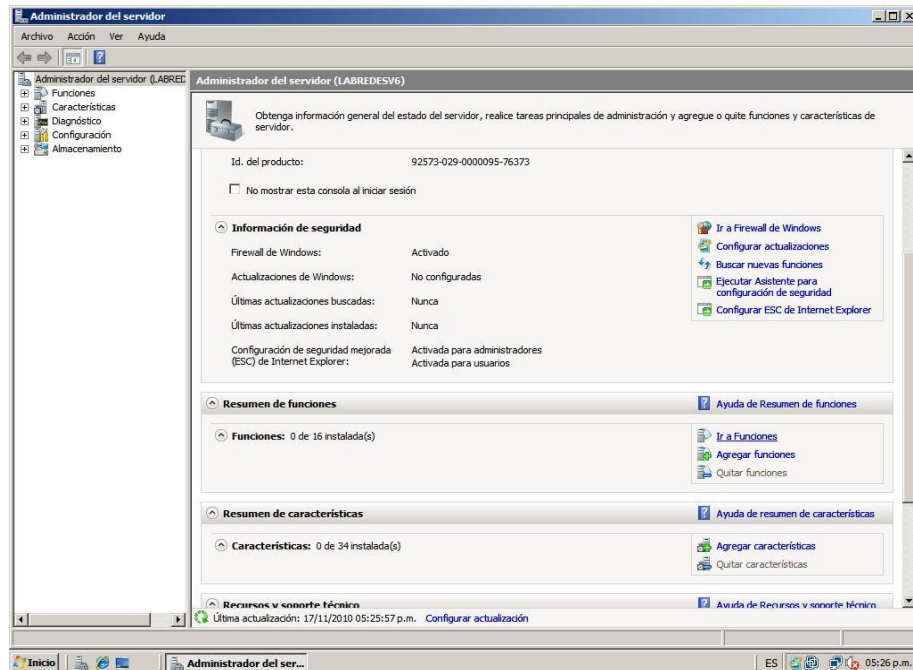
Prerrequisitos para la Instalación del Servidor:

- Sistema operativo Windows Vista o 7 en cada uno de las computadoras conectadas al servidor
- Se requiere que este diseñan, configurada y en funcionamiento la red sobre la cual se va a instalar el servidor (Esta debe de incluir los dispositivos de interconexión de red)

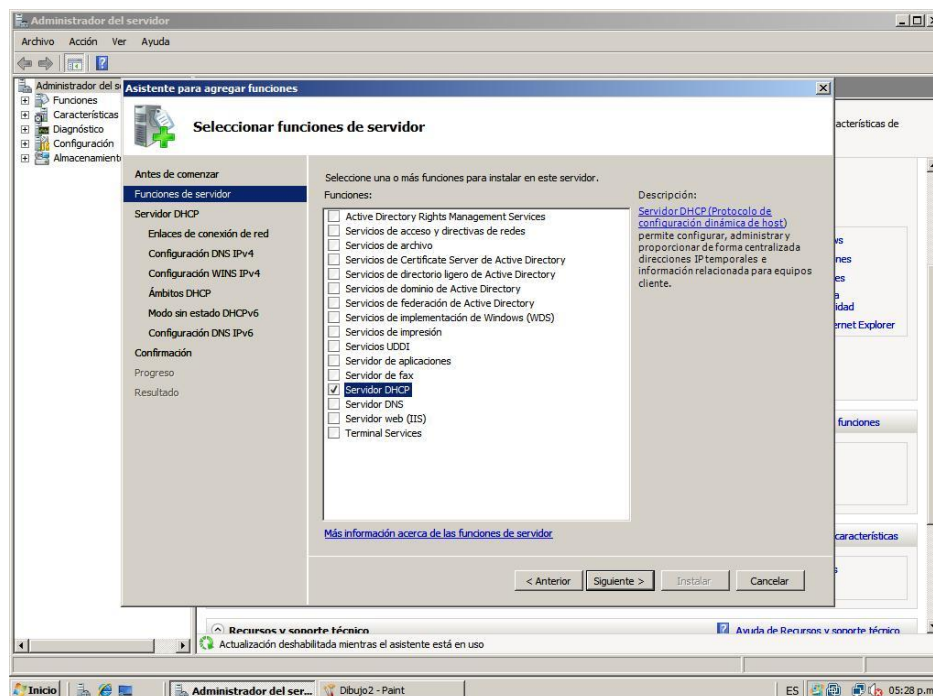
3.2 EVIDENCIAS DEL PROYECTO



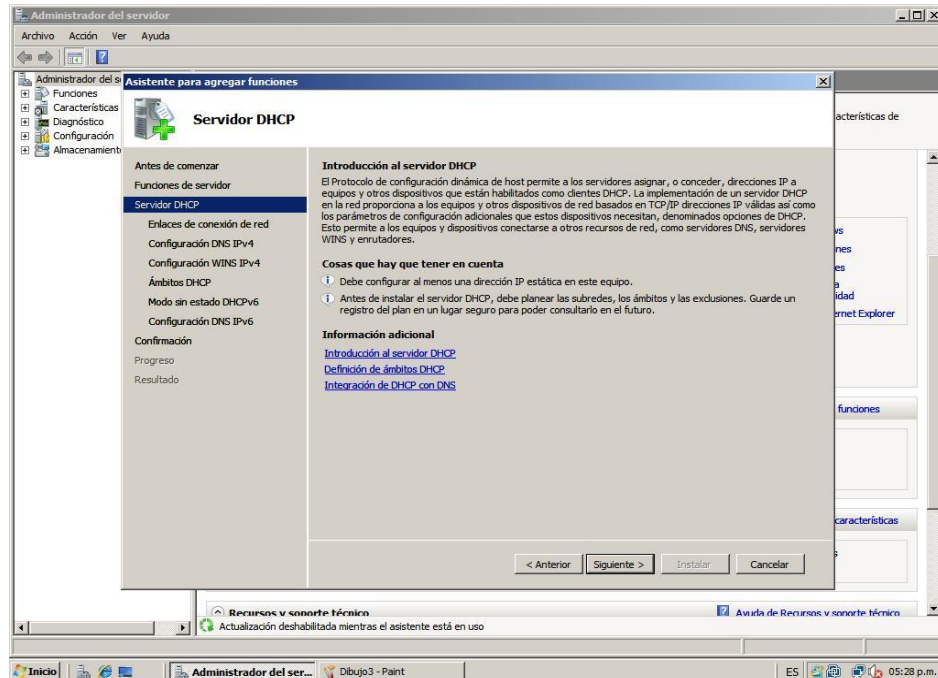
Búsqueda de servicio DHCP. Inicio, Herramientas Administrativas,
Administrador del Servicio y enter



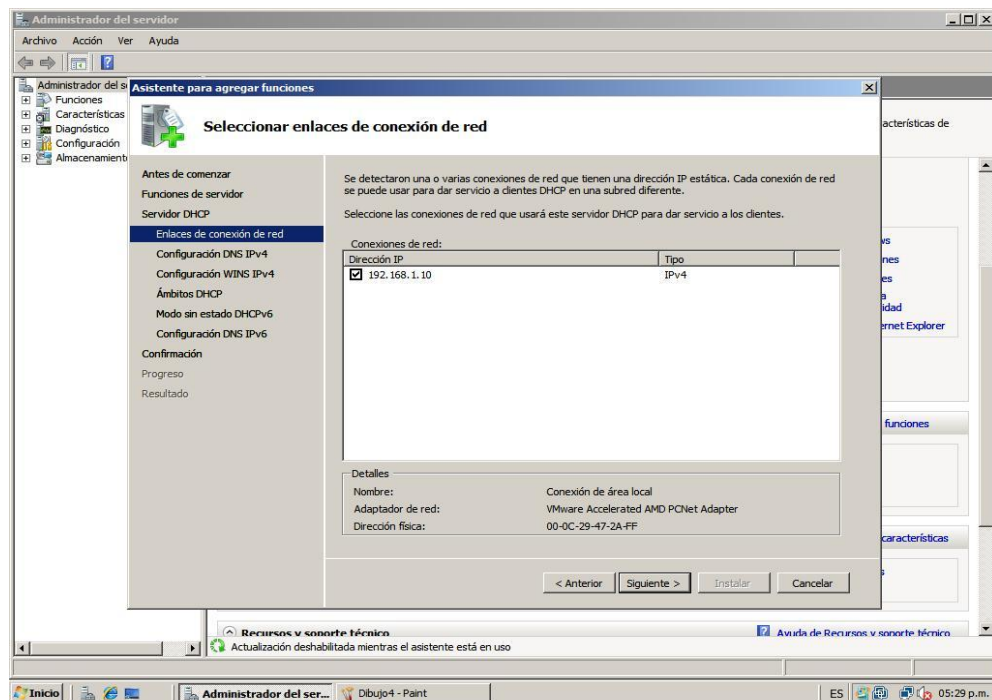
Clic en ir a funciones y Presionamos Enter



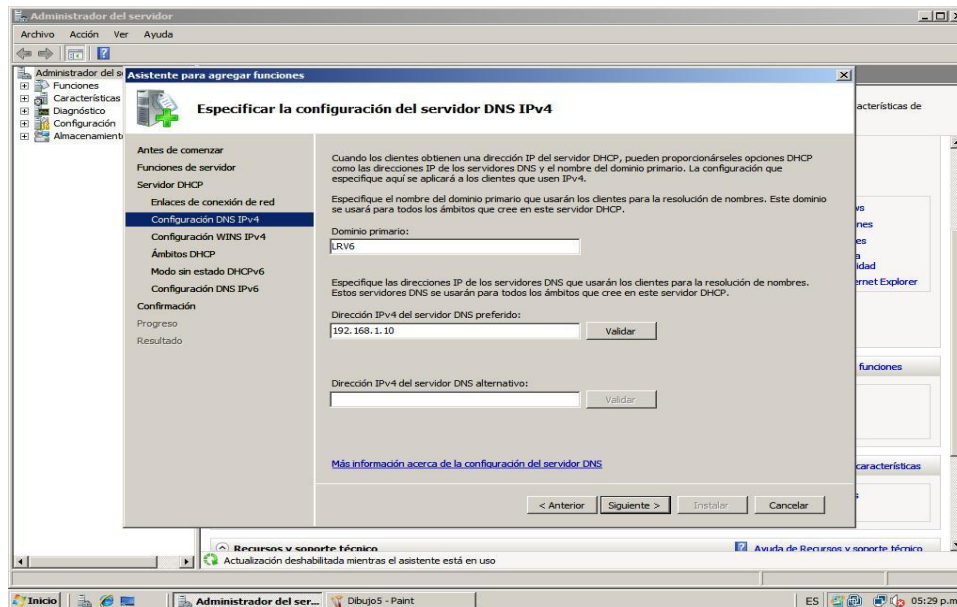
Seleccionar Servidor DHCP y dar clic en siguiente



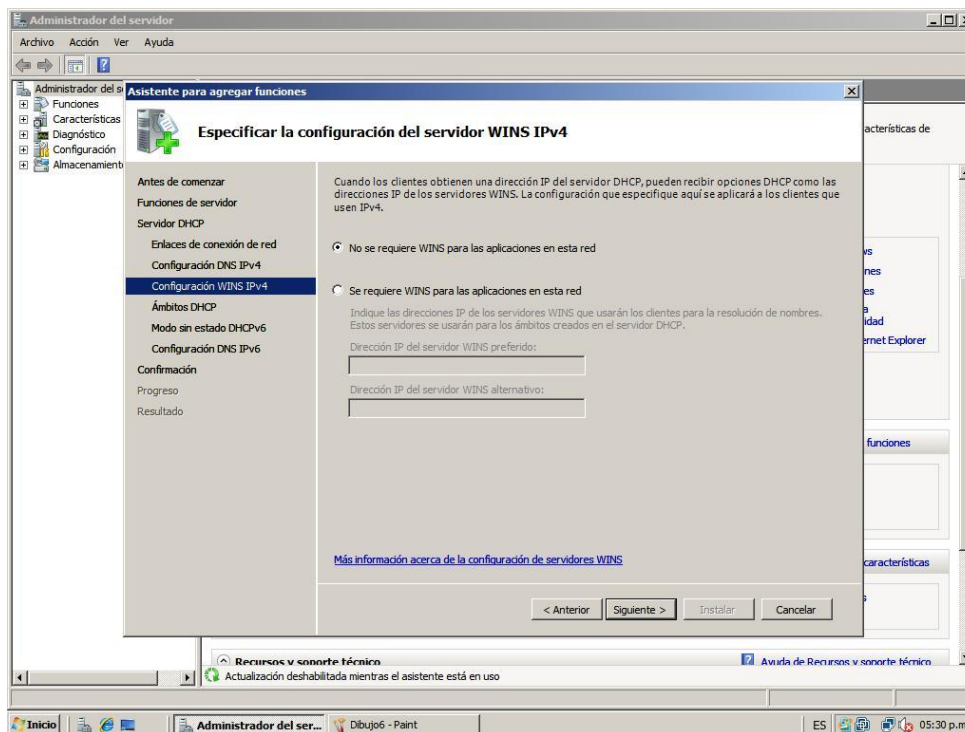
Nos aparecerá la introducción del servidor DHCP y damos clic en siguiente



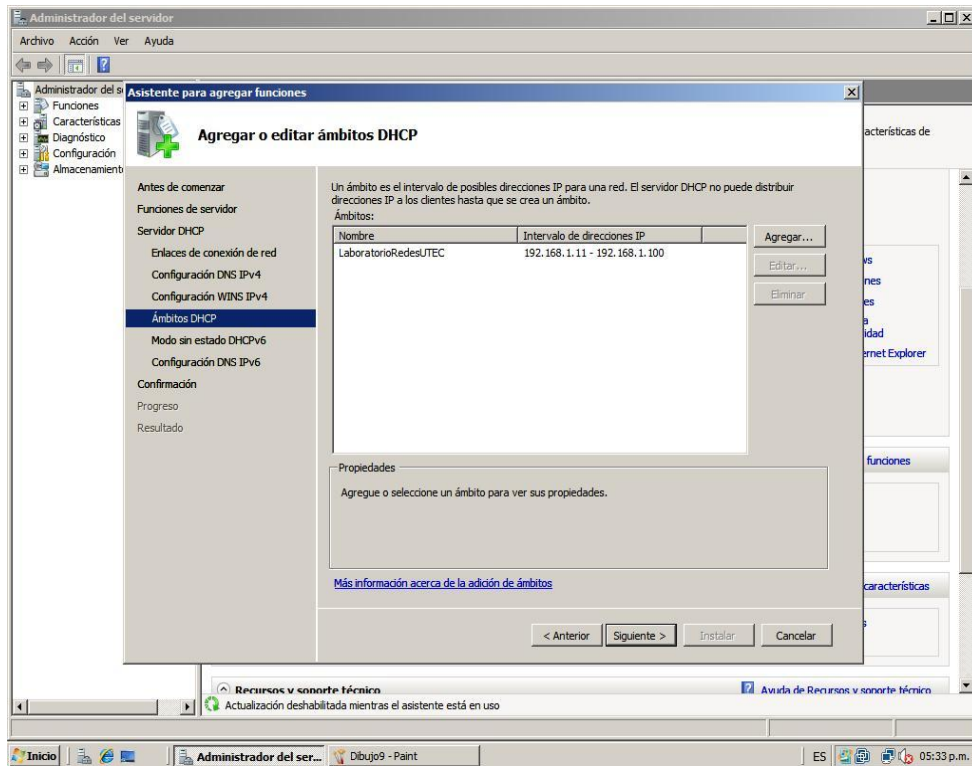
Selecciona el enlace de red se comenzara con Ipv4



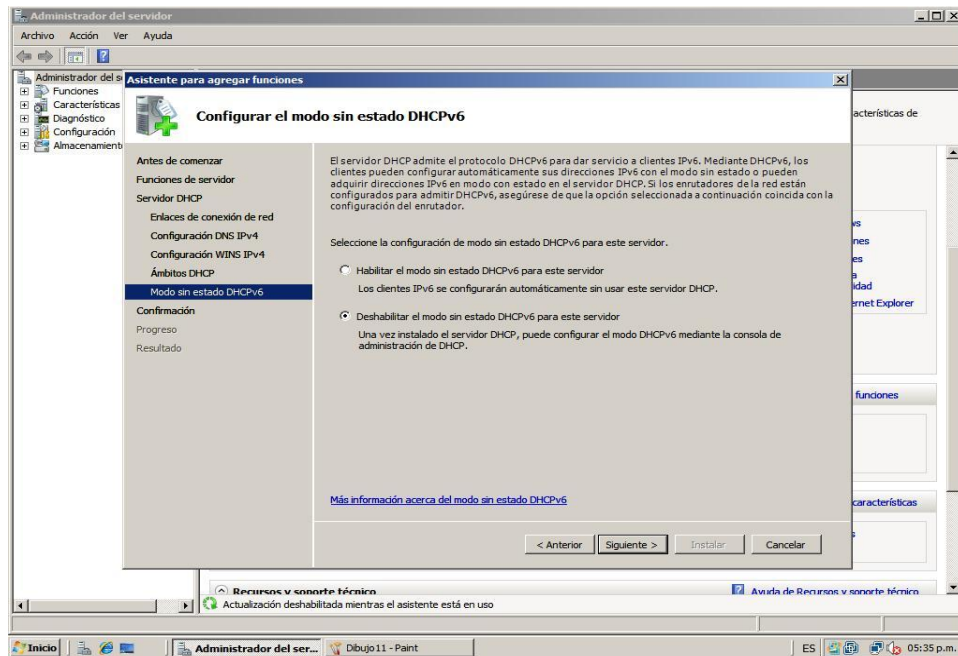
Especificar y configurar dominio primario y dirección ipv4



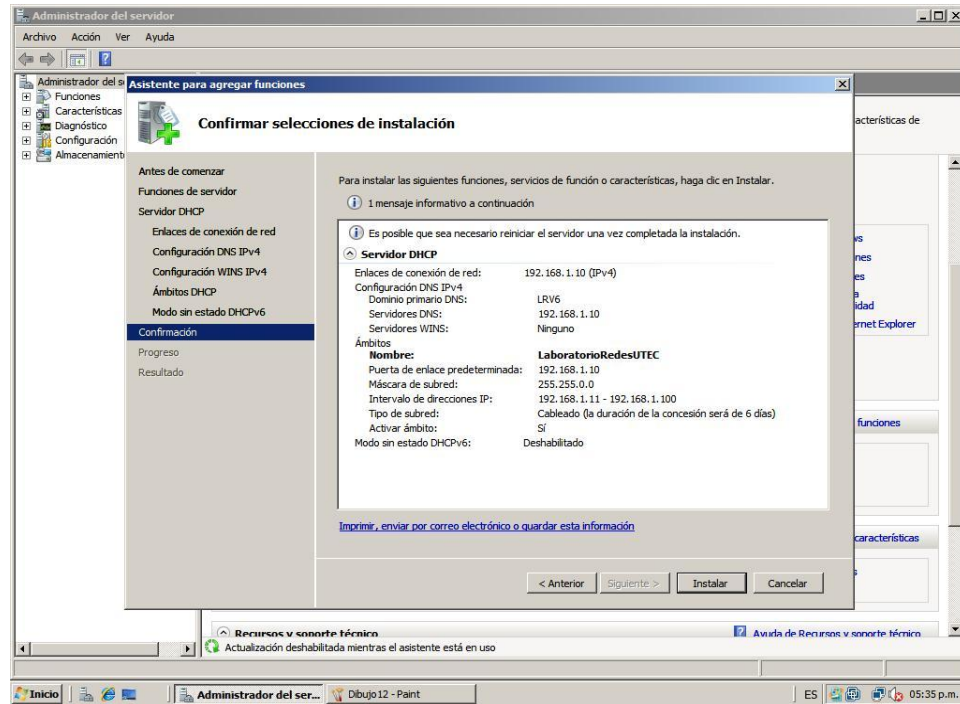
No se requiere especificar el servidor wins IPv4



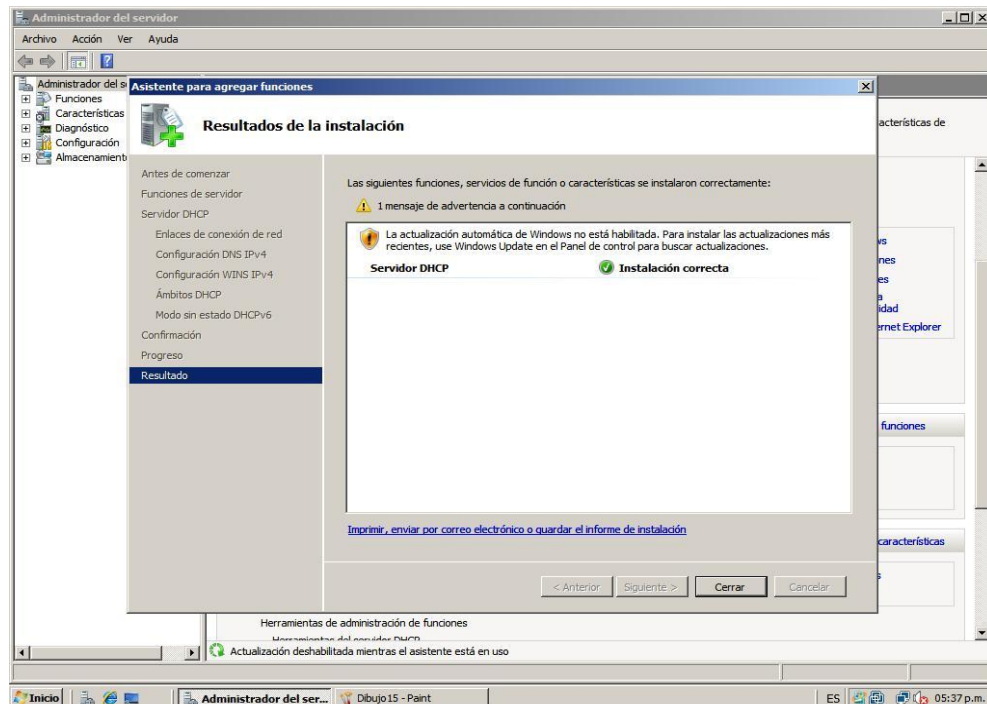
Se agrega un ámbito de direcciones IP que no puede distribuir



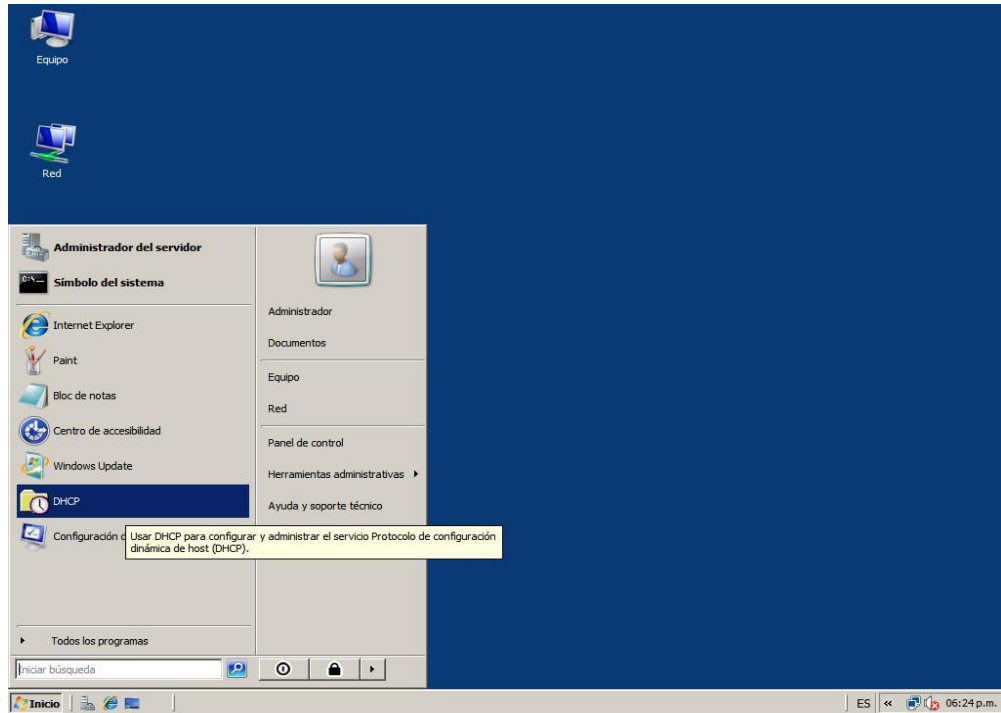
Deshabilitamos el modo sin estado Dhcpv6 para el servidor



Confirmación selecciones de instalación

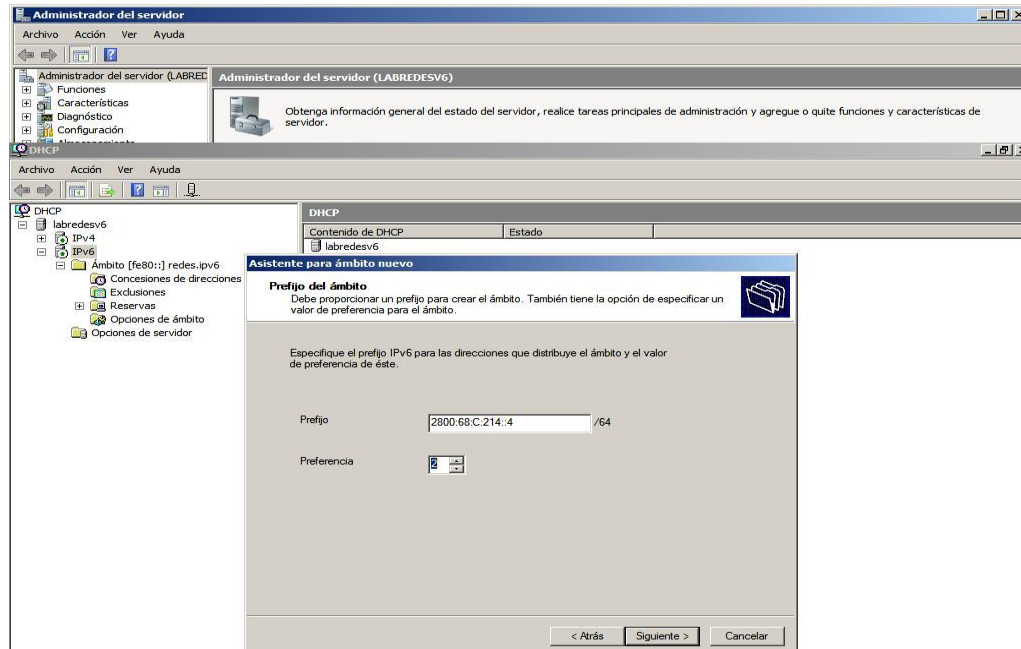


Servidor DHCP instalación correcta

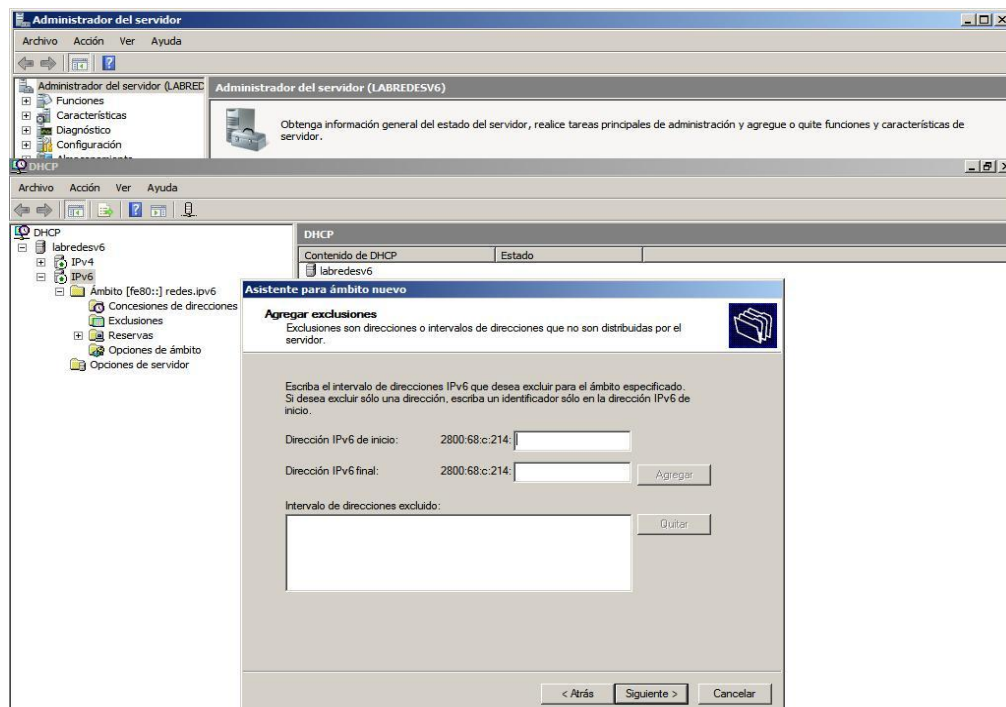


Buscamos el servidor DHCP en inicio, y dar clic en DHCP

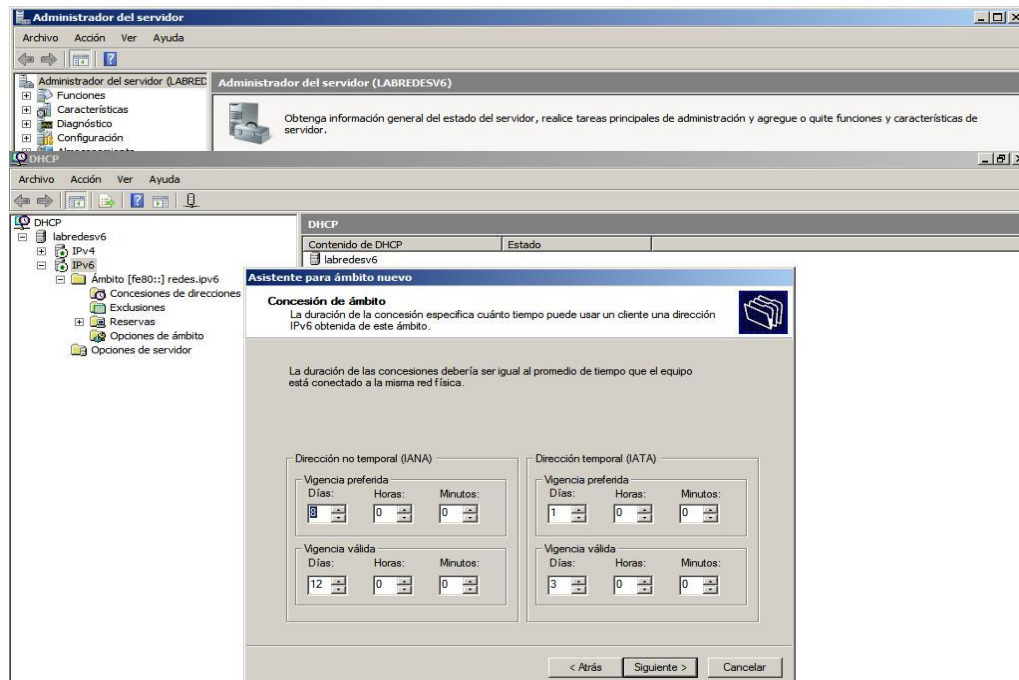
Poner nombre de ámbito y su descripción



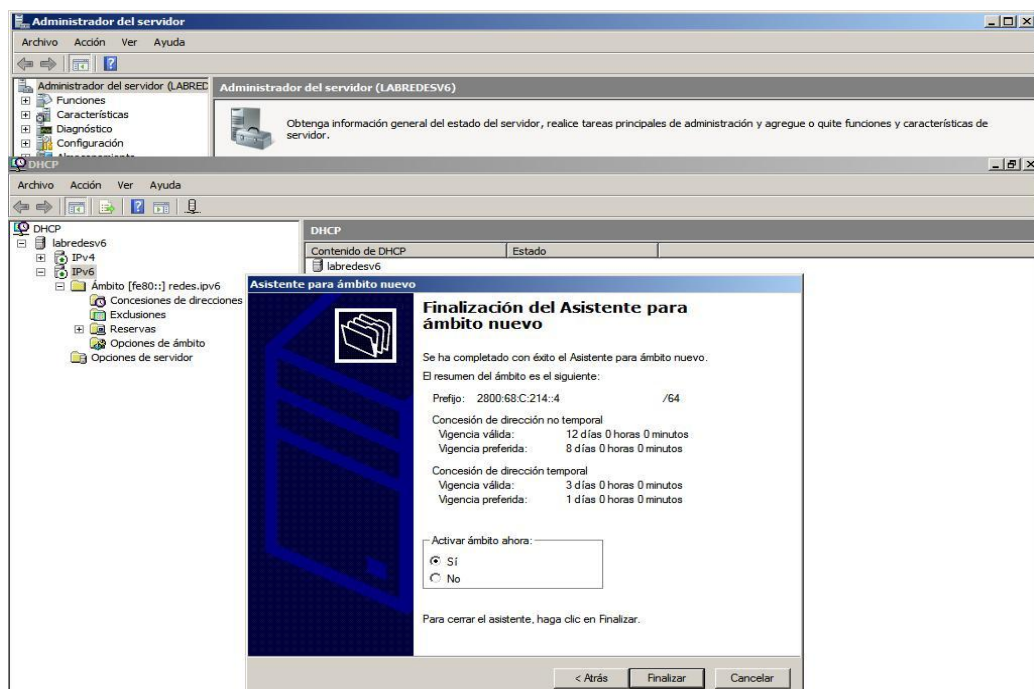
Perfil del ámbito poner dirección IPv6 en prefijo y su preferencia de acuerdo a la Ip que se esté utilizando



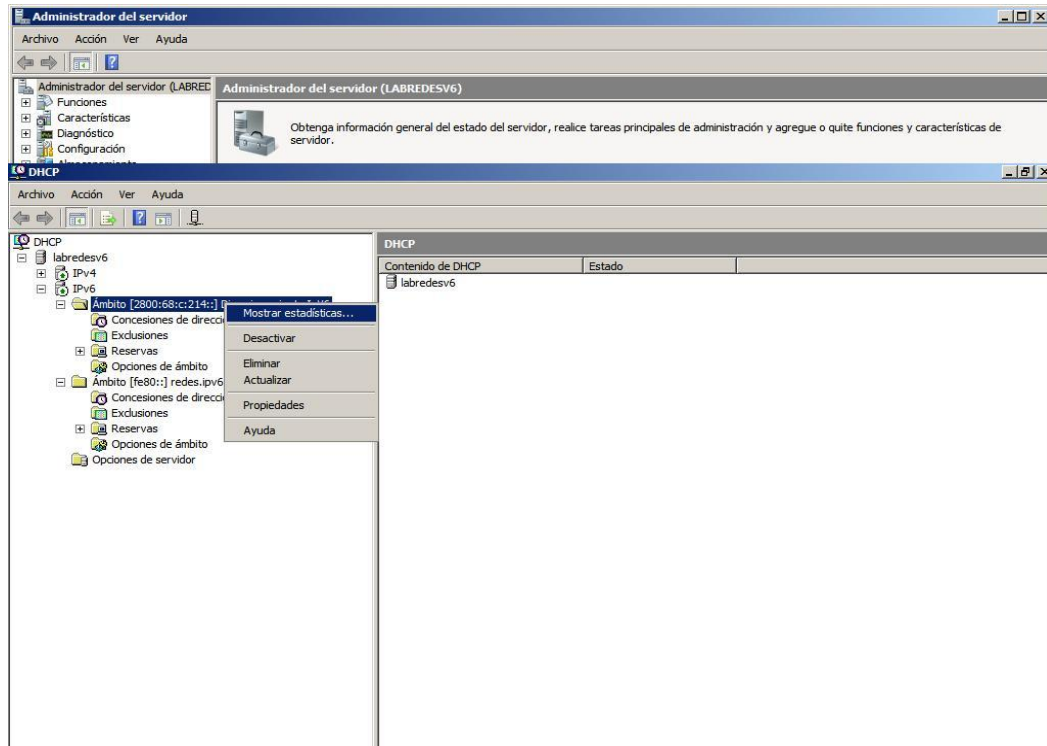
Exclusiones direcciones que no son distribuidas por el servidor



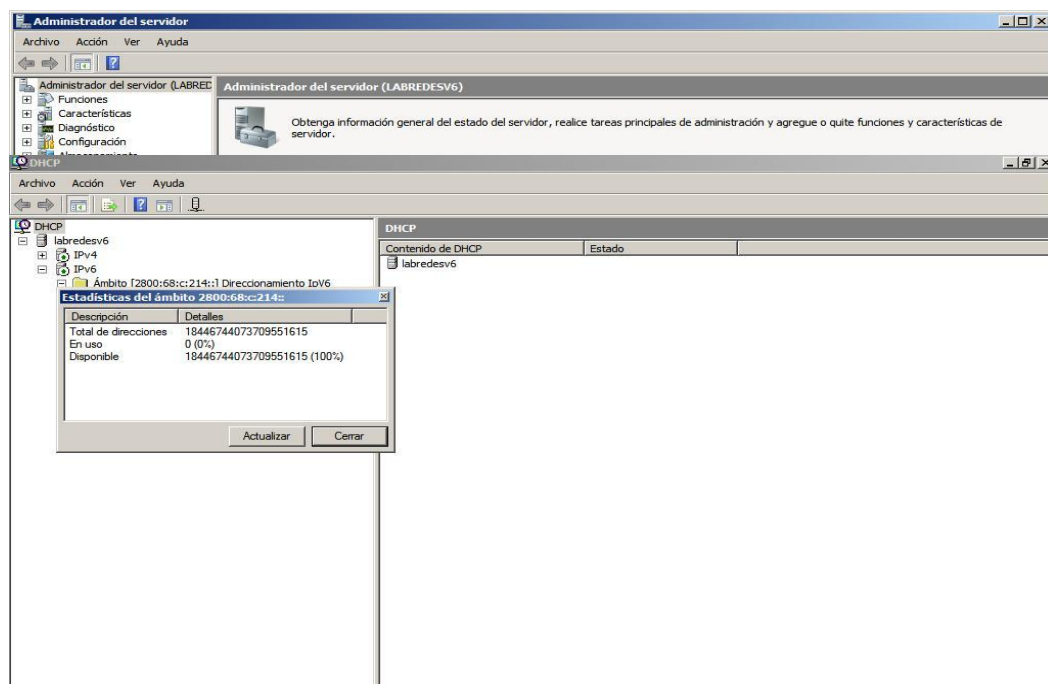
Concesión cuánto tiempo puede usar un cliente una dirección IPv6 obtenida por este ámbito



Finalización para crear este ámbito



Clic derecho y seleccionamos mostrar estadísticas



El total de direcciones Ipv6

CONCLUSIONES

En base a lo anteriormente expuesto se concluye lo siguiente:

DHCP-server provee de facilidad de configuración y archivos de configuración en los cuales podemos definir ciertos parámetros para nuestro servicio DHCP. El cual nos provee de un servicio fundamental en una red con gran numero de computadores, el cual nos ahorra tiempo para la configuración de cada una de las terminales.

El servidor DHCP permite la administración centralizada de IP's y asignaciones a la red

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande.

El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red.

Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

RECOMENDACIONES

- ✓ Asegúrese de que las personas no autorizadas no puedan obtener acceso físico o inalámbrico a la red.

Restringir los usuarios que pueden administrar el servicio DHCP.

Deberá ser miembro del grupo Administradores o del grupo Administradores DHCP para administrar servidores DHCP mediante la consola de DHCP o los Comandos Netsh para DHCP. Asimismo, solamente los miembros del grupo Administradores de dominio pueden autorizar o desautorizar un servidor DHCP en Active Directory. Debería restringir la pertenencia a estos grupos al número mínimo de usuarios necesarios para administrar el servidor. Si hay usuarios que necesitan acceso de sólo lectura a la consola de DHCP, agréguelos al grupo Usuarios DHCP en lugar de al grupo Administradores DHCP

BIBLIOGRAFÍA

- ✓ MICROSOFT (2011) *Instalar el Protocolo de configuración dinámica de host (DHCP)* Extraído el 12 de Junio del 2010.

Desde: [http://technet.microsoft.com/es-es/library/dd894454\(W.S.10\).aspx](http://technet.microsoft.com/es-es/library/dd894454(W.S.10).aspx)

- ✓ WIKIPEDIA (2010) *Dynamic Host Configuration Protocol*. Extraído el 08 de Julio del 2010.

Desde: http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

- ✓ MICROSOFT (2011), *Sitio oficial Microsoft*, Extraído el 25 de Agosto del 2010

Desde: [http://technet.microsoft.com/es-es/library/cc776482\(W.S.10\).aspx](http://technet.microsoft.com/es-es/library/cc776482(W.S.10).aspx)

- ✓ MICROSOFT (2011), *Compatibilidad Ipv6 de los productos Windows*, Extraído el 04 de Septiembre del 2010.

Desde:

[http://technet.microsoft.com/es-es/library/bb629624\(EXCHG.80\).aspx](http://technet.microsoft.com/es-es/library/bb629624(EXCHG.80).aspx)

- ✓ WIKIPEDIA (2010), *Ipv6 wikipedia*, Extraído el 16 de Noviembre del 2010

Desde: <http://es.wikipedia.org/wiki/IPv6>

- ✓ MICROSOFT. (2011), *Compatibilidad Ipv6 de los productos Windows*, Extraído el 27 de Diciembre del 2010.

Desde:

[http://technet.microsoft.com/es-es/library/bb629624\(EXCHG.80\).aspx](http://technet.microsoft.com/es-es/library/bb629624(EXCHG.80).aspx)

ANEXOS



Microsoft Windows Server 2008 está diseñado para ofrecer a las organizaciones la plataforma más productiva para vitalización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, Windows Server 2008 incluye nuevas funciones de gran valor y eficacia y mejoras impactantes en el sistema operativo base.

Windows Server 2008 proporciona a los profesionales de TI más control sobre sus servidores e infraestructura de red y les permite centrarse en las necesidades críticas del negocio. Capacidades mejoradas en secuencias de comandos y automatización de tareas, como las que ofrece Windows PowerShell, ayudan a los profesionales de TI a automatizar tareas comunes de TI. La instalación y administración basadas en funciones con Administrador del Servidor facilita la tarea de administrar y proteger las múltiples funciones de servidor en una empresa. La nueva consola del Administrador del servidor proporciona un único origen para administrar la configuración del servidor y la información del sistema. El personal de TI puede instalar sólo las funciones y

características que sean necesarias, y hay asistentes que automatizan muchas de las tareas de implementación de sistemas que tardan más tiempo. Herramientas mejoradas de administración del sistema, como el Monitor de rendimiento y confiabilidad, ofrecen información sobre sistemas y alertan al personal de TI sobre problemas potenciales antes de que sucedan.

Windows Server 2008 proporciona una serie de tecnologías de seguridad nuevas y mejoradas, que aumentan la protección del sistema operativo al ofrecer una base sólida para la dirigir y construir un negocio. Incluye innovaciones de seguridad, como PatchGuard, que reducen la exposición a ataques del núcleo, lo que produce un entorno de servidor más seguro y estable. El sistema de protección de servicios de Windows ayuda a mantener más seguros los sistemas al evitar que los servicios críticos de servidor estén en riesgo por actividades anormales en el sistema de archivos, registro, o red. La seguridad también se mejora en el sistema operativo Windows Server 2008 por medio de protección de acceso a redes (NAP), controlador de dominio de sólo lectura (RODC), mejoras en la infraestructura de clave pública (PKI), un nuevo firewall de Windows bidireccional y compatibilidad con criptografía de última generación.

Windows Server 2008 está diseñado para permitir que los administradores modifiquen su infraestructura para adaptarla a las necesidades cambiantes del negocio y continuar siendo ágiles. Se mejora la flexibilidad para trabajadores

móviles mediante tecnologías que permiten que los usuarios ejecuten programas desde cualquier ubicación remota, como RemoteApp y Terminal Services Gateway. Windows Server 2008 acelera la implementación y el mantenimiento de sistemas de TI con Servicios de Implementación de Windows (WDS) y ayuda en la consolidación de servidores con Windows Server virtualization (WSv). Para organizaciones que necesitan controladores de dominio en sucursales, Windows Server 2008 ofrece una nueva opción de configuración: el Controlador de Dominio de sólo lectura (RODC), que evita exponer las cuentas si el Controlador de Dominio estuviera en riesgo.

GLOSARIO

6OVER4

Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

6TO4

Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

AMBITO (SCOPE)

Para las direcciones IPv6, el ámbito es la porción de la red a la que se supone que se va a propagar el tráfico.

ANUNCIO DE ROUTER

Mensaje de descubrimiento de vecinos enviado por un router bien de forma pseudo-periódica o como respuesta a un mensaje de solicitud de router. El anuncio incluye al menos información acerca de un prefijo que será el que luego utilice el host para calcular su dirección IPv6 unicast según el mecanismo “stateless”.

ARQUITECTURA DE PILA DUAL

Una arquitectura para nodos IPv6/IPv4 en la que existen dos implementaciones completas de la pila de protocolos, una para IPv4 y otra para IPv6, cada una de ellas con su propia implementación de la capa de transporte (TCP y UDP).

AUTOCONFIGURACIÓN DE DIRECCIONES

Proceso de configuración automática de direcciones IPv6 en un interfaz.

BUCLE DE ENCAMINADO

Situación indeseable en una red, que provoca que el tráfico se retransmita siguiendo un bucle cerrado, con lo cual nunca llega a su destino.

CABECERA DE FRAGMENTACIÓN

Una cabecera de extensión IPv6 que contiene información para reensamblado para ser utilizada en el nodo receptor.

CABECERA DE OPCIÓN DE SALTO-A-SALTO

Una cabecera de extensión de IPv6 que contiene opciones que deben ser procesadas por todos los routers intermedios y el final.

CABECERAS DE EXTENSIÓN

Cabeceras que se sitúan entre la cabecera IPv6 y las cabeceras de los protocolos de nivel superior que son empleadas para dotar de funcionalidades adicionales a IPv6.

CACHE DE ROUTERS

Ver caché de destinos.

CACHÉ DE DESTINOS

Tabla mantenida por cada nodo IPv6 que mapea cada dirección (o rango de direcciones) destino con la dirección del siguiente router al que hay que enviar el datagrama. Además almacena la MTU de la ruta asociada.

CACHÉ DE VECINOS

Es una caché mantenida por cada nodo IPv6 que almacena la dirección IP de sus vecinos en el enlace, sus correspondientes direcciones de nivel de

enlace, y una indicación de su estado de accesibilidad. La caché de vecinos es equivalente a la caché ARP en IPv4.

CHECKSUM DE LA CAPA SUPERIOR

Cálculo del checksum realizado en ICMPv6, TCP y UDP que utiliza la pseudo-cabecera IPv6.

CONTROL DE ACCESO AL MEDIO

Es un subnivel del nivel de enlace de datos ISO definido por el IEEE. Sus funciones son la creación de tramas y la gestión del acceso al medio.

DESCUBRIMIENTO DE MTU DE LA RUTA

Consiste en el empleo del mensaje Too Big mediante ICMPv6 para descubrir el valor máximo de MTU IPv6 en todos los enlaces entre dos equipos.

DESCUBRIMIENTO DE PARÁMETROS

Proceso de descubrimiento de vecinos que permite a los equipos conocer los parámetros de configuración, incluyendo la MTU del enlace y el límite de saltos por defecto para los paquetes salientes.

DESCUBRIMIENTO DE ROUTERS

Procedimiento de descubrimiento de vecinos que permite descubrir los routers conectados en un determinado enlace.

DESCUBRIMIENTO DE VECINOS

Es un conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nodos vecinos. El descubrimiento de vecinos reemplaza a ARP, el descubrimiento de rutas ICMP y el mensaje de redirección ICMP empleados en IPv4. También proporciona detección de vecino inaccesible.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

DIRECCIONES DE COMPATIBILIDAD

Direcciones IPv6 que son empleadas al enviar tráfico IPv6 sobre una infraestructura IPv4. Ejemplos de direcciones de compatibilidad son: las direcciones compatibles-IPv4, las direcciones 6to4 y las direcciones ISATAP.

DIRECCIÓN

Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en datagramas IPv6.

DIRECCIÓN 6OVER4

Una dirección del tipo [prefijo 64-bit]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4.

DIRECCIÓN 6TO4

Una dirección del tipo [prefijo 64-bit]:0:0:WWXX:YYZZ, en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica o privada IPv4), empleada para representar una máquina en la tecnología 6over4. Una dirección del tipo 2002:WWXX:YYZZ:[SLA ID]:[Interfaz ID], en la que WWXX:YYZZ es la representación hexadecimal de w.x.y.z (una dirección publica IPv4), empleada para representar un nodo en la tecnología 6to4.

DIRECCIÓN ANYCAST

Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un rutado apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, el más cercano.

DIRECCIÓN ANYCAST DE ROUTER DE SUBRED

Dirección anycast (prefijo de 64 bits::) que se asigna a las interfaces de los routers.

DIRECCIÓN ANÓNIMA

Ver dirección temporal.

DIRECCIÓN COMPATIBLE CON IPv4

Es una dirección de la forma 0:0:0:0:0:w.x.y.z o ::w.x.y.z, donde w.x.y.z es la representación decimal de una dirección pública IPv4. Por ejemplo, ::131.107.89.42 es una dirección compatible con IPv4. Estas direcciones se emplean en túneles IPv6 Automáticos.

DIRECCIÓN DE LAZO LOCAL

Es la dirección IPv6 ::1, que se asigna a la interfaz local.

DIRECCIÓN DE NODO SOLICITADA (SOLICITED-NODE ADDRESS)

Dirección multicast utilizada por los nodos durante el proceso de resolución de direcciones. La dirección de nodo solicitada se construye con el prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 unicast. Esa dirección se emplea a modo de pseudo dirección unicast para llevar a cabo una resolución de direcciones más eficiente en los enlaces IPv6.

DIRECCIÓN DE USO LOCAL

Dirección unicast IPv6 que no es alcanzable en la Internet IPv6. Las direcciones de uso local incluyen direcciones locales del enlace y direcciones locales del sitio.

DIRECCIÓN EUI-64

Una dirección del nivel de enlace de 64 bits que se usa como base para la generación de identificadores de interfaz en IPv6.

DIRECCIÓN GLOBAL

Ver dirección global agregable unicast.

DIRECCIÓN GLOBAL AGREGABLE UNICAST

También conocidas como direcciones globales, las “direcciones globales agregables unicast” se identifican por el formato del prefijo 001 (2000::/3). Las direcciones globales IPv6 son equivalentes a las direcciones públicas IPv4 y son globalmente rutables y alcanzables en el fragmento IPv6 de Internet.

DIRECCIÓN IPv4 MAPEADA

Es una dirección de la forma 0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, donde w.x.y.z es una dirección IPv4. Las direcciones IPv4 mapeadas se emplean para representar un nodo con soporte sólo IPv4 ante un nodo IPv6.

DIRECCIÓN ISATAP

Es una dirección del tipo [prefijo de 64-bit]:0:5EFE:w.x.y.z, siendo w.x.y.z una dirección IPv4, pública o privada, que se asigna a un equipo ISATAP.

DIRECCIÓN LOCAL DE SITIO

Dirección de uso local identificada por el prefijo 1111 1110 11 1111 1110 11 (FEC0::/10). El ámbito de utilización de ese tipo de direcciones es el “sitio” local (de una organización), sin la necesidad de un prefijo global. Las direcciones locales de sitio no son accesibles desde otros sitios y los routers no deberían encaminar tráfico correspondiente al sitio local fuera del propio sitio. En la actualidad, se debate la necesidad de las mismas, y muy probablemente desaparezcan de la especificación de IPv6.

DIRECCIÓN MAC

Dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se la conoce como dirección física, dirección del hardware o dirección del adaptador de red.

DIRECCIÓN MULTICAST

Es una dirección que identifica múltiples interfaces y que se emplea en entregas de datos uno-a-muchos. Mediante la topología de rutado multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

DIRECCIÓN NO ESPECIFICADA

La dirección 0:0:0:0:0:0:0 (::) se emplea para reflejar la ausencia de una dirección, de forma equivalente a la dirección 0.0.0.0 de IPv4.

DIRECCIÓN TENTATIVA

Dirección unicast cuya unicidad no se ha comprobado todavía.

DIRECCIÓN UNICAST

Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquél en el que esa dirección es única.

DNS

(Domain Name System.) Ver sistema de nombres de dominio.

DOS PUNTOS DOBLES (DOUBLE COLON)

Práctica de comprimir series continuas de bloques de 0, en direcciones IPv6 como "::". Por ejemplo, la dirección de multicast FF02:0:0:0:0:0:0:2 se expresa como FF02::2. Si hay dos series de bloques de 0, de longitud máxima, sólo se codifica de esta manera el bloque que figura más a la izquierda de la dirección.

ENCAMINADO ESTÁTICO

Utilización de rutas introducidas manualmente en las tablas de rutado de los routers.

ENCAPSULADO DE SEGURIDAD ESP (ENCAPSULATING SECURITY PAYLOAD) (arriba)

Una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga del datagrama encapsulado por la cabecera y cola.

ENLACE

Uno o más segmentos de una red de área local limitados por routers.

ENLACE DE ACCESO MÚLTIPLE NO-BROADCAST

Es una tecnología de nivel de enlace que soporta enlaces con más de dos nodos, pero sin permitir el envío de un paquete a múltiples destinos (broadcast). Por ejemplo, X.25, Frame Relay y ATM.

ENLACE PROPIO

Home link. En IP móvil, el enlace en el que el nodo móvil reside en su red. El nodo móvil, emplea el prefijo del enlace propio para crear su dirección propia.

ESTADO DEL ENLACE

Tecnología de protocolo de rutado, que intercambia información de rutas, que consta de los prefijos de las redes conectadas a un router y su coste asociado. La información del estado del enlace se anuncia en el arranque, así como cuando se detectan cambios en la topología de la red.

EUI (EXTENDED UNIQUE IDENTIFIER)

Dirección del nivel de enlace definida por el IEEE (Institute of Electrical and Electronic Engineers).

FICHERO HOSTS

Un fichero de texto empleado para contener correspondencias nombre-dirección IP. En windows XP o .NET server está en el directorio \SystemRoot\System32\Drivers\Etc. En máquinas Unix está en el directorio /etc.

FICHERO HOSTS

Un fichero de texto empleado para contener correspondencias nombre-dirección IP. En windows XP o .NET server está en el directorio \SystemRoot\System32\Drivers\Etc. En máquinas Unix está en el directorio.

FICHERO HOSTS

Un fichero de texto empleado para contener correspondencias nombre-dirección IP. En windows XP o .NET server está en el directorio \SystemRoot\System32\Drivers\Etc. En máquinas Unix está en el directorio /etc.

FLUJO

Una serie de datagramas intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto de 0.

FRAGMENTACIÓN

Proceso por el que se divide la carga de un datagrama IPv6 en fragmentos por la máquina emisora de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

FRAGMENTO

Una porción de una carga enviada en un datagrama IPv6 enviada por un host. Los fragmentos contienen una cabecera de fragmentación.

GRUPO MULTICAST

Conjunto de equipos escuchando una dirección multicast específica.

HOST

Ver máquina (host).

ICMPV6 (INTERNET CONTROL MESSAGE PROTOCOL FOR IPv6)

Protocolo para los mensajes de control de Internet para IPv6. Un protocolo que proporciona mensajes de error para el rutado y entrega de datagramas IPv6 y mensajes de información para diagnóstico, descubrimiento de vecinos, descubrimiento de receptores multicast y movilidad IPv6.

IDENTIFICADOR DE AGREGACIÓN DE MÁXIMO NIVEL

TLA ID (Top-Level Aggregation Identifier). Campo de 13 bits dentro de la dirección unicast global reservada para grandes organizaciones o ISP por el IANA, y que por tanto identifica el rango de direcciones que tienen delegado.

IDENTIFICADOR DE AGREGACIÓN DE SIGUIENTE NIVEL

NLA ID (Next-Level Aggregation Identifier). Es un campo de 24 bits en la dirección unicast global agregable que permite a los ISPs crear varios niveles jerárquicos de direccionamiento en sus redes para organizar las direcciones y el rutado hacia otros ISPs, así como para identificar los sitios de la organización.

IDENTIFICADOR DE AGREGACIÓN DE SITIO

SLA ID (Site-Level Aggregation Identifier). Campo de 16 bits dentro de la dirección global unicast que utiliza una organización para identificar subredes dentro de su red.

IDENTIFICADOR DE GRUPO

Los últimos 112 bits o los últimos 32 bits (de acuerdo a la recomendación de la RFC 2373) de una dirección IPv6 multicast, que identifica un grupo de multicast.

IDENTIFICADOR DE INTERFAZ

Los 64 últimos bits de una dirección IPv6 unicast o anycast.

INTERFAZ

Una representación de un nexo físico o lógico de un nodo a un enlace. Un ejemplo de un interfaz físico es un interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de túnel.

INTERFAZ LOCAL

Interfaz interna que permite que un nodo se envíe paquetes a sí mismo.

IP6.INT

El dominio DNS creado para la resolución inversa en IPv6. La resolución inversa tiene por objeto determinar el nombre de una máquina a partir de su dirección.

IPSEC (INTERNET PROTOCOL SECURITY)

Seguridad del protocolo de Internet. Un marco de estándares abiertos que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPSEC soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección ante repeticiones.

IPv6 EN IPv4

Ver túneles IPv6 sobre IPv4.

ISATAP (INTRA-SITE AUTOMATIC TUNNELING ADDRESSING PROTOCOL)

Ver protocolo de Direccionamiento de Túneles Internos Automáticos.

JUMBOGRAMA

Paquete IPv6 que tiene una carga útil mayor de 65.535 bytes. Los jumbogramas se indican con un valor 0 en el campo de longitud de carga útil de la cabecera IPv6, e incluyendo una opción de carga útil del Jumbo en la cabecera de opciones Salto-a-Salto.

LISTA DE PREFIJOS

Lista de prefijos de enlace mantenida por cada host. Cada entrada define directamente el rango de direcciones IP que son alcanzables directamente, esto es, vecinos.

LISTA DE ROUTERS DE DEFECTO

Una lista mantenida por cada máquina, en la que aparecen todos los routers de los que se ha recibido un anuncio de router con un valor de "Tiempo de vida de

MAC

Ver control de acceso al medio, dirección MAC.

MTU

Ver unidad máxima de transmisión.

MTU DE LA RUTA

Tamaño máximo de un paquete IPv6 que puede enviarse sin emplear fragmentación entre una fuente y un destino sobre una ruta en una red IPv6. La MTU de la ruta coincide con la menor MTU de enlace para todos los enlaces de dicha ruta.

MTU DEL ENLACE

La unidad de transmisión máxima (MTU) -número de bytes en el paquete IPv6 más grande- que puede enviarse sobre el enlace. Dado que el tamaño máximo de trama incluye las cabeceras y colas de nivel de enlace, la MTU del enlace no coincide con el tamaño máximo de trama del enlace. La MTU del enlace coincide con el máximo tamaño de carga útil de la tecnología de nivel de enlace.

MTU IPv6

El tamaño máximo de un paquete IP que se puede enviar sobre un enlace.

MÁQUINA (HOST)

Un nodo que no puede reenviar datagramas no originados por sí mismo. Una máquina es típicamente el origen y destino del tráfico IPv6 y va a descartar discretamente tráfico que no esté dirigido específicamente a él mismo.

MÁQUINA 6TO4

Una máquina IPv6 que está configurada con al menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Las máquinas 6to4 no requieren configuración manual y crean las direcciones 6to4 empleando

mecanismos clásicos de autoconfiguración.

MÁQUINA ISATAP

Es un equipo al que se le asigna una dirección ISATAP.

NAT

Ver traductor de direcciones de red.

ND

Ver descubrimiento de vecinos.

NODO CORRESPONSAL

Un nodo que se comunica con un nodo móvil que se encuentra fuera de su red propia.

NODO IPv4

Un nodo que implementa IPv4; puede enviar y recibir paquetes IPv4. Puede ser un nodo con soporte sólo IPv4 o un nodo dual IPv4/IPv6.

NODO IPv6

Nodo que implementa IPv6; puede enviar y recibir paquetes IPv6. Un nodo IPv6 puede ser bien un nodo con soporte IPv6 o un nodo dual IPv6/IPv4.

NODO IPv6/IPv4

Es un nodo que dispone de implementaciones de IPv4 e IPv6.

NOMBRE ISATAP

El nombre resuelto por ordenadores con sistema operativo Windows XP Service Pack 1 o bien de la familia de Windows .NET Server 2003 para

descubrir automáticamente la dirección del router ISATAP. Los equipos con Windows XP tratan de resolver el nombre "_ISATAP."

NOTACIÓN HEXADECIMAL SEPARADA CON DOS PUNTOS (COLON HEXADECIMAL NOTATION)

La notación empleada para expresar direcciones IPv6. La dirección de 128 bits es dividida en 8 bloques de 16 bits. Cada bloque se expresa como un número hexadecimal y éstos se separan del siguiente por medio del signo ortográfico dos puntos (:). Dentro de cada bloque, los ceros situados a la izquierda son eliminados. Un ejemplo de una dirección IPv6 unicast representada en notación hexadecimal separada por dos puntos es 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

NOTACIÓN PREFIJO-LONGITUD

Notación mediante la cual se expresan los prefijos de red. Tiene la forma dirección/longitud del prefijo, siendo dicha longitud el número de bits iniciales de la dirección que se fijan para definir el prefijo.

OBTENCIÓN DEL SALTO SIGUIENTE

Es el proceso de obtención de la dirección o interfaz del siguiente salto para enviar o reenviar un paquete basándose en el contenido de la tabla de rutado.

OPCIONES DE DESCUBRIMIENTO DE VECINOS

Son las opciones de los mensajes de descubrimiento de vecinos que indican las direcciones de nivel de enlace, información sobre los prefijos, MTU, redirecciones, rutas e información de configuración para movilidad IPv6.

OPCIÓN DE CARGA ÚTIL DEL JUMBO

Una opción en la cabecera de opciones Salto-a-Salto que indica el tamaño del jumbograma.

PAQUETE

La unidad de datos del protocolo (PDU) existente a nivel Internet. En el caso

de IPv6, un paquete consta de una cabecera y la carga útil IPv6.

PDU

Ver unidad de datos del protocolo (PDU).

PREFIJO DE FORMATO

Los bits de orden alto con un valor fijo que definen un tipo de dirección IPv6.

PREFIJO DE RED

Es la parte fija de la dirección que se utiliza para determinar el identificador de la subred, la ruta o el rango de direcciones.

PREFIJO DE SITIO

Típicamente un prefijo de 48 bits que se utiliza para referirse a todas las direcciones del sitio. Los prefijos de sitio se almacenan en una tabla de prefijos que se emplea para confinar todo el tráfico asociado a esos prefijos dentro del sitio.

PROTOCOLO DE DIRECCIONAMIENTO DE TÚNELES INTERNOS AUTOMÁTICOS

Una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

PROTOCOLO DEL NIVEL SUPERIOR

Protocolo que utiliza IPv6 como transporte y se sitúa en la capa inmediatamente superior a IPv6, como ICMPv6, TCP y UDP.

PROTOCOLO PUNTO-A-PUNTO

Método de encapsulación de red punto-a-punto que proporciona delimitadores de tramas, identificación del protocolo y servicios de integridad a nivel de bit.

PSEUDO-CABECERA

Cabecera temporal que se construye para calcular el checksum necesario para asociar la cabecera IPv6 con la carga. En IPv6 se utiliza un nuevo

formato de pseudo-cabecera al calcular el checksum de UDP, TCP y ICMPv6.

PSEUDO-PERIÓDICO

Suceso que se repite en intervalos no constantes. Por ejemplo, el anuncio de rutas enviado por un router IPv6 se produce en intervalos que se calculan aleatoriamente entre un mínimo y un máximo.

RED

Dos o más subredes conectadas por routers. Otro término empleado es interred.

REDIRECCIONAR

Procedimiento englobado dentro de los mecanismos de descubrimiento de vecinos por el cual se informa a un host de la dirección IPv6 de otro que resulta más adecuado como siguiente salto hacia un determinado destino.

REENSAMBLADO

Proceso mediante el cual se reconstruye la carga original de un datagrama a partir de varios fragmentos.

REENSAMBLADO

Proceso mediante el cual se reconstruye la carga original de un datagrama a partir de varios fragmentos.

RELAY ROUTER 6TO4

Un router IPv6/IPv4 que redirige tráfico dirigido a direcciones 6to4 entre routers 6to4 en Internet y máquinas de la Internet IPv6.

RESOLUCIÓN DE DIRECCIONES

Proceso de resolución de direcciones del nivel de enlace para la dirección de next-hop (siguiente salto, gateway) en un enlace.

RESOLUCIÓN DE NOMBRES

Es el proceso de obtención de una dirección a partir de un nombre. En IPv6, la resolución de nombres permite obtener direcciones a partir de nombres de

equipos o nombres de dominio totalmente cualificado (FQDN).

RESOLUCIÓN DE NOMBRES

Es el proceso de obtención de una dirección a partir de un nombre. En IPv6, la resolución de nombres permite obtener direcciones a partir de nombres de equipos o nombres de dominio totalmente cualificado (FQDN).

RETARDO DE UNIÓN

Tiempo transcurrido entre el envío de un mensaje de Informe de Escucha de Multicast (Multicast Listener Report) por parte de un nuevo miembro de un grupo multicast en una subred que no dispone de miembros de grupo, y el envío de los paquetes multicast de ese grupo sobre la subred.

ROUTER

Nodo que puede retransmitir datagramas que no van específicamente destinados a él. En una red IPv6 un router suele enviar además anuncios relativos a su presencia y su información de configuración. A veces denominado encaminador.

ROUTER 6TO4

Router para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

ROUTER ADVERTISEMENT

Ver anuncio de routers.

ROUTER ISATAP

Un router IPv6/IPv4 que responde a las solicitudes de equipos ISATAP a través de túneles y encamina el tráfico entre equipos y nodos ISATAP de otra red o subred ISATAP.

RUTA ASOCIADA A UNA SUBRED

Ruta cuyo prefijo de 64 bits corresponde al de una subred en concreto.

RUTA POR DEFECTO

La ruta con prefijo `::/0`. La ruta de defecto, recoge todos los destinos y es la ruta empleada para obtener la siguiente dirección de destino cuando no hay otras rutas coincidentes.

SEGMENTO DE RED

Ver subred.

SEGMENTO DE UNA RED DE ÁREA LOCAL

Porción de un enlace que consta de un único medio limitado por puentes o conmutadores de nivel 2.

SELECCIÓN DE RUTA ADECUADA

Es el algoritmo empleado por el proceso de selección de rutas para escoger las rutas de la tabla de rutado que más se acercan a la dirección de destino a la que se debe enviar o encaminar el paquete.

SISTEMA DE DETERMINACIÓN DE RUTA

Proceso por el cuál se selecciona cuál es la ruta concreta de la tabla de rutado por la que se va a encaminar el datagrama. Esto es, se selecciona el siguiente router al que se va a mandar el datagrama.

SISTEMA DE NOMBRES DE DOMINIO

Un sistema jerárquico de almacenamiento y su protocolo asociado para almacenar y recuperar información sobre nombres y direcciones IP.

SUBRED

En IPv6 uno o más enlaces que utilizan el mismo prefijo de 64 bits.

TABLA DE ENCAMINADO IPv6

Conjunto de rutas empleadas para determinar la dirección e interfaz del siguiente nodo en el tráfico IPv6 enviado por un equipo o reencaminado por un router.

TIEMPO DE VIDA EN ESTADO “PREFERRED” PREFERIDA

Tiempo durante el que una dirección unicast obtenida mediante el mecanismo de autoconfiguración stateless permanece en estado “preferred” o de preferida. Este tiempo viene indicado por el campo “Preferred Lifetime” de la opción “Prefix Information” (información de prefijo) de los mensajes de anuncio de routers.

TIEMPO MÁXIMO DE VALIDEZ DE UNA DIRECCIÓN

Tiempo en el que una dirección unicast conseguida mediante el proceso de autoconfiguración stateless permanece en estado válido (tanto preferido como desaprobado o deprecated).

TRADUCTOR DE DIRECCIONES DE RED

Es un router IPv4 que traduce direcciones y puertos al reenviar paquetes entre una red con direcciones privadas e Internet.

TRANSICIÓN

Hablando de IPv6, consiste en la conversión de nodos sólo IPv4 a nodos con doble pila, o sólo IPv6.

TÚNEL

Un túnel IPv6 sobre IPv4, en los que los puntos finales son determinados por configuración manual.

TÚNEL AUTOMÁTICO

Un túnel IPv6 sobre IPv4 en el que los puntos finales son determinados por el empleo de interfaces lógicas de túneles, rutas y direcciones orígenes y destino IPv6.

TÚNEL IPv4 MULTICAST

Ver 6over4.

TÚNEL MÁQUINA-A-MÁQUINA

Un tunelado IPv6 sobre IPv4 en el que los dos extremos son máquinas.

TÚNEL MÁQUINA-A-ROUTER

Un tunelado IPv6 sobre IPv4 en el que el túnel empieza en un host y acaba en un router IPv6/IPv4.

TÚNELES IPv6 AUTOMÁTICOS

Creación automática de túneles que se emplea con direcciones compatibles con IPv4.

TÚNELES IPv6 SOBRE IPv4

Consiste en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

UNIDAD DE DATOS DEL PROTOCOLO (PDU)

Conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

UNIDAD MÁXIMA DE TRANSMISIÓN

Es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

VECINO

Nodo conectado al mismo enlace.

VECTOR DE DISTANCIA

Una tecnología para protocolos de rutado que propaga información de rutado en la forma de un identificador de red y su distancia en número de

saltos.

VECTOR DE RUTA

Se trata de una tecnología de protocolo de rutado que intercambia secuencias de información de saltos indicando el camino a seguir en una ruta. Por ejemplo, BGP-4 intercambia secuencias de números de sistemas autónomos. Un sistema autónomo es una porción de la red perteneciente a la misma autoridad administrativa.