UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Prácticas para la materia Redes de Datos I

MATERIAL DIDÁCTICO

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Ulises Ortiz Vega

ASESOR DE MATERIAL DIDÁCTICO

Dr. Victor Rangel Licea

Ciudad Universitaria, Cd. Mx., 2016

Agradecimientos

A mis padres, Alfonso Ortiz Calderón y Angelina Vega Chávez; por ser ejemplos de responsabilidad, amor, honestidad y cariño que me han permitido desarrollarme como una persona íntegra, responsable, que siempre sigue hacia adelante con toda la esperanza que detrás de cada tormenta habrá un beneficio aún mayor.

A mis hermanos Aldebarán y Sally que siempre han sido, son y serán mis segundos padres apoyándome, escuchándome, comprendiéndome y siempre teniendo una palabra adecuada, un consejo o sugerencia adecuada para el momento que lo necesito, forjando en mi destrezas y seguridad para que sin importar lo que venga salir victorioso. Siempre recordándome que soy más grande que el miedo.

A mis amigos, aquella familia que escogemos, donde pase grandes momentos de risa y esfuerzo cada día, semestre tras semestre. Ellos que siempre sabían con qué cambiar una cara triste o de duda; con quienes estudié, hicimos grandes proyectos y siempre con quienes siempre encontrábamos una manera de apoyarnos. Sin ellos, sin duda, no sería quien soy ahora.

A mis maestros que me han permitido estar en sus aulas de clase y he podido aprender un poco de todo lo que han aprendido con la vida a través del tiempo, dedicándome tiempo para explicar, calificar y diciéndome en qué debería de mejorar para no ser uno más.

A mi querida Facultad de Ingeniería que durante poco más de 5 años ha sido mi razón para levantarme temprano, aprender al máximo, permitirme encontrar personas maravillosas y mostrarme que cada esfuerzo tiene una recompensa y mientras más grande el reto, más sabio me he hecho.

Y de manera general, a mi Alma Mater, la Universidad Nacional Autónoma de México, del cual me siento orgulloso de pertenecer desde el momento que pude estar en el CCH Naucalpan, mi amada universidad que con los brazos abiertos me recibió desde los 14 años y que a cambio de nuestro esfuerzo y dedicación nos otorgaba una de las herramientas más poderosas de este mundo: el conocimiento.

Gracias a todos los que depositaron conmigo uno de los recursos más importantes e invaluables de este mundo, su tiempo; espero haberlo convertido en grandes experiencias.

Abril 2016.

Contenido

Introducción

Interconectividad en redes

Actualmente vivimos en un mundo donde la tecnología y la vanguardia son palabras que definen ampliamente las necesidades de empresas y personas en general para la vida cotidiana; cada vez existe una mayor necesidad de estar sincronizados en todo momento donde nuestra computadora, celular, tablets y hasta el mismo automóvil se han convertido en herramientas que permiten que esta sincronización exista armoniosamente; he aquí donde entran en acción la interconectividad en redes.

Durante los comienzos de las redes de datos observamos redes limitados a intercambiar información en base a caracteres y letras mientras que ahora, gozamos con transmisión de voz, video, texto y gráficos en una vasta cantidad de dispositivos, lo que se traduce en una amplia variedad de métodos de comunicación alternativos y nuevos que permiten interactuar con otro ser humano de forma casi instantánea.

Y esto ha sido el reto que se han enfrentado las redes, permitir al mundo esta gran cantidad de trasmisión de información, pudiendo conectarse con muchas otras redes, intentado que cosas como el hardware y software de los diversos dispositivos pasen a segundo plano.

Un reto que implica no tener limitación por distancias, los tamaños de los paquetes de información, ancho de banda ni potencia de transmisión; que al mismo tiempo se busca tener la máxima seguridad, confiabilidad, desempeño y disponibilidad posible.

Y que finalmente lo vemos con nuestros propios ojos, la gran interacción que existe entre muchos de los aparatos que portamos que se han hecho parte de nuestra vida diaria, una comunicación constante y un gran medio de ayuda cuando se necesita. Sin embargo esto va mucho más allá y es que el gigantesco mundo lo

hacemos más pequeño y podemos tener una videollamada por internet, totalmente gratis con algún familiar o ser querido al otro lado del mundo.

Sin duda alguna, las redes han evolucionado en aspectos gigantescos y nos han permitido que sin importar el lugar, todos estemos un poco más cerca y que día con día confiemos más los dispositivos que portamos, porque utilizados adecuadamente se pueden convertir en importantísimas instrumentos de trabajo mejorando todo aspecto de nuestra vida actual, manteniéndonos comunicados donde quiera que estemos, haciendo la vida cada vez un poco más sencilla.

Para la primera práctica llamada fundamentos de switching, hacemos hincapié en la importancia que toma conocer la parte física de las redes, conocimiento y limitantes del material principal de transmisión como lo es el cable Ethernet; protocolos básicos como CSMA/CD y la identificación de dominios de broadcast y de colisión; llevándonos a conocer el modelo OSI y cómo opera el encapsulamiento de datos, culminando con la importancia y características de los switches y uno de sus protocolos auxiliares, el protocolo ARP.

Para esta segunda práctica, VLANs, vale la pena resaltar la gran ayuda que se obtiene, sobre todo a nivel económico, donde al necesitar una red segmentada (es decir, que no se comparta información con ninguna otra red), en vez de utilizar varios equipos y separar máquinas por área, con un solo dispositivo (switch) segmentamos la red virtualmente mediante la restricción de información según el puerto donde se esté conectando. Esto finalmente crea la segmentación de la red sin necesidad equipos auxiliares (una LAN tradicional segmentada físicamente) y que exista una concentración por áreas.

Sin duda alguna, es muy importante tener caminos redundantes en la red, puesto que si solo existiese un solo camino y este estuviera dañado, el flujo de información sería inexistente; sin embargo con caminos redundantes este problema se soluciona pues al existir más de un camino físico de llegar al destino, aseguramos que este llegará, aunque esta redundancia física trae problemas importantes como son “las tormentas de broadcast”. Por eso, Spanning Tree

Protocol (STP), es un protocolo pensado para garantizar la erradicación de bucles (“tormentas de broadcast”) en trayectos redundantes en la red.

Proseguimos a la cuarta práctica que se titula DHCP y donde rescatamos la importancia de este protocolo que configura de manera dinámica la configuración de red de un equipo; es decir, teniendo un equipo conectado a la red y mediante este protocolo, hace que el mismo equipo obtenga su configuración debida. La gran ventaja de este protocolo reside en que en redes de gran escala, pues sin necesidad de que un administrador de red se encargue de configurar cada equipo, este protocolo lo hace automáticamente, incluso disminuyendo la probabilidad de error.

Para la quinta práctica titulada principios de routing, se busca que quien realice esta práctica tenga un primer acercamiento a los protocolos de capa 3, por ejemplo, el protocolo RIP que se presenta en sus 2 versiones y da origen a nuevos protocolos como OSPF; además de comprender conceptos básicos como lo que es un vector distancia, tablas de enrutamiento, distancias administrativas y clases (así como ventajas y desventajas) de enrutamiento estático y dinámico.

Procedemos a dar los fundamentos de IPv6. Vale la pena recordar que en estos momentos empieza a surgir una emigración de IPv4 a IPv6, esta emigración existe puesto que el desperdicio de direcciones IPv4 a su principio, aunado al gran auge de equipos capaces de conectarse a la red en estos días ha hecho que dichas direcciones, poco a poco, ya no den abasto para los años siguientes; es por eso que IPv6 nació con una nueva forma de expresión y numeración (“hextetos” y un sistema hexadecimal); creando así innovadora solución para afrontar este problema.

Y finalmente, algo que no es menos importante es la forma del direccionamiento IP en esta mundo de IPv6, por lo que se dedica esta última práctica a comprender y ejercitar el subneteo de IPv6, principalmente; recordando la importancia de darle una mejor práctica a este IPv6 para evitar los problemas que surgieron por la irresponsabilidad de su predecesor.

Capítulo 1. Breve explicación sobre las prácticas.

Fundamentos de Switching

Para esta primera práctica se hablará de conocimientos básicos para el curso de Redes de Datos, iniciando por la descripción de conceptos fundamentales como lo que es un cuarto de telecomunicaciones, tipos de cableado (horizontal y vertical), consideraciones importantes para las instalaciones de cableado UTP, Ley A y B para la elaboración de cableado UTP en conectores RJ45, tipo de cables (directo, cruzado); se hablará del funcionamiento del protocolo CSMA/CD, descripción de los dominios de colisión y de broadcast, encapsulamiento de datos, funciones y proceso de aprendizaje MAC en switches, beneficios de los switches; métodos de procesamiento de tramas en switches (Store-and-forward, Cut-through y Fragment-free), el proceso de enrutamiento para un host y para un router, terminando con el funcionamiento del protocolo ARP. En esta práctica se incluirá un cuestionario de 15 preguntas de opción múltiple para asentar el conocimiento adquirido en el alumno.

Virtual LANS

En esta práctica se verá a detalle lo que son las Virtual LANs, denotaremos cuál es su uso cotidiano, la necesidad de su creación, configuración de VLANs en switches por diferentes métodos, enlaces troncales, etc.

Aquí veremos las ventajas que se obtienen tras la configuración de VLANS, se hará hincapié en los diferentes tipos de VLANs que existen; uso, importancia y configuración de enlaces troncales, creación y configuración paso a paso de una VLAN, el enrutamiento inter-VLAN; continuando con la una sencilla práctica a realizar, terminando con las conclusiones de la práctica y 10 preguntas de opción múltiple para aterrizar el conocimiento del alumno.

Spanning Tree Protocol (STP)

Para esta práctica abordaremos el protocolo STP (Spanning Tree Protocol por sus siglas en inglés o protocolo de árbol de expansión en español) que permite una jerarquización de la red de switches, evitando diversos eventos que provocarían una falla total en la red, además de algunos otros protocolos que son variantes de este STP original, denotando características y similitudes entre algunos de ellos.
De manera más precisa, primeramente, se hablará de las ventajas y desventajas de tener múltiples caminos en Capa 1, consecuencias de multitrayectorias en Capa 1 (por ejemplo, tramas duplicadas o tormentas de broadcast), características de SPT, conformación del Brigde ID (forma normal y extendida), comparación de diferentes variantes del STP, configuración de STP, características del protocolo PVST+, características del protocolo Rapid PVST+ y los conceptos previos terminan con la configuración del PortFast y BPDU de guardia. Continuamos con la práctica que ayudará al alumno a poner en práctica los conocimientos recién adquiridos, terminando con las conclusiones de la práctica y su cuestionario final.

Configuración de DHCP

Para esta práctica se verá la configuración de un servidor DHCP (Dynamic Host Configuration Protocol) que podría atender las solicitudes de varios clientes. Usualmente un servidor DHCP es usado para proveer automáticamente direcciones IP a los clientes, evitando la necesidad de que el adminitrador de red tenga que configurar manualmente las direcciones en cada computadora.
Siendo más específicos, en la práctica se verá: diferentes métodos de asignación de direcciones (tales como asignación manual, automática y dinámica), operación de DHCP (diferentes mensajes y sus contenidos), la forma de realizar este proceso (configuración de un cliente DHCP) y la comprobación de una configuración exitosa, comandos importantes que nos llevan a la realización de la práctica; terminando con sus debidas conclusiones y su cuestionario correspondiente.

Principios de Routing

Durante esta práctica se verá el protocolo de enrutamiento de información (por sus siglas en inglés, RIP) donde dicho protocolo está basado en el vector distancia cuya métrica son los “saltos” y que da origen a protocolos más avanzados como OSPF.

Más concisamente veremos definiciones que nos ayudarán a entender mejor este protocolo, tales como Vector Distancia, tablas de enrutamiento y distancia administrativa; una breve historia de cómo nació este protocolo, características y funcionamiento de RIP v1, características de RIP v2, similitudes y diferencias entre RIP v1 y v2, enrutamiento, ventajas y desventajas del ruteo estático y dinámico, algunos atros protocolos de enrutamiento en IPv4, agregando además una tabla de las distancias administrativas de diversos protocolos; pasando a la práctica describiendo la topología a usar, una tabla de direccionamiento y otra de comandos a utilizar, terminando con su respectivas conclusiones y un cuestionario de opción múltiple.

Fundamentos de IPv6

En esta práctica a abracarán varios fundamentos de IPv6, partiendo del conocimiento previo que se tiene de IPv4, en la práctica se hace una pequeña reseña histórica de IPv6, mostrando el porqué de su necesidad; pasamos a una descripción de las clases de direcciones que existen en IPv6 (Unicast, Multicast y Anycast) y las respectivas subdivisiones que tienes cada una de las 3 clases mencionadas anteriormente, se habla sobre la conformación de una dirección de IPv6 (prefijo, ID de subred, ID de interfaz), reglas para la abreviación de direcciones IPv6 (eliminación de ceros iniciales y uso de dobles puntos), prefijos en IPv6, compatibilidad de direcciones IPv6 con IPv4, el proceso de EUI-64 modificado), SLAAC (Stateless Address Autoconfiguration); para esta práctica se anexarán un ejemplo realizado de optimización de direcciones IPv6 y de EUI-64

modificado, dejando unos ejercicios extra para que los alumnos puedan practicar dichos conocimientos; terminando la práctica con sus respectivas conclusiones y su cuestionario de opción múltiple.

Direccionamiento IPv6

Para esta práctica utilizaremos todos los conceptos que ya se vieron en la práctica anterior (fundamentos de IPv6) y los llevaremos hacia el direccionamiento donde el alumno aprenderá a manejar las direcciones hexadecimales, a comprender mejor el uso de los hextetos, el sistema hexadecimal, la expresión y reglas de optimización de las direcciones en IPv6, un breve vistazo a las direcciones Global Unicast y Link Local y la estructura de cada una de ellas; desembocando en el subnetting. En esta última parte se hace un ejercicio muy didáctico donde se le da un prefijo /48 dado por el proveedor y se trata de ir obteniendo las direcciones para 20 ciudades con 10 oficinas por ciudad y 11 departamentos en cada oficina. En la actividad se incentiva al alumno a tratar de emular el ejercicio pero con diferentes números de ciudades, oficinas y departamentos, agregando en una última actividad el uso de direcciones sin desperdicio. El cuestionario final ayuda a los alumnos a plasmar lo aprendido y realizado durante la práctica.

Cabe mencionar que cada una de estas prácticas trae su solucionario, con tal de facilitar la labor a los docentes.

Capítulo 2: Fundamentos de Switching

Introducción

En esta práctica el alumno conocerá la base del trabajo en el área de Redes de datos; conocerá el cableado backbone, de distribución; cables directos y cruzados (según el estándar T568A o T568B); dominios de colisión y de broadcast, usos y beneficios de switches y sus funciones, procedimiento de ruteo y protocolos tales como CSMA/CD y ARP.

Conceptos previos

Tipos de conexiones físicas.

Al planificar la instalación del cableado LAN, existen cuatro áreas físicas que se deben considerar:

- **Área de trabajo**: trabajo son las ubicaciones destinadas para los dispositivos finales utilizados por los usuarios individuales. Se usa patch cable, máximo 10 m. Este tipo de cable se utiliza para conectar dispositivos finales, como computadoras, a una red.

- **Cuarto de telecomunicaciones, también denominado servicio de distribución**: es el lugar donde se realizan las conexiones a los dispositivos intermediarios. Los patch cords realizan conexiones entre los patch panels, donde terminan los cables horizontales, y los dispositivos intermediarios. Máximo 5 m.

- **Cableado backbone, también denominado cableado vertical:** se utilizan para el tráfico agregado, como el tráfico de entrada o de salida de Internet, y para el acceso a los recursos corporativos en una ubicación remota.

- **Cableado de distribución, también denominado cableado horizontal**: se refiere a los cables que conectan los cuartos de telecomunicaciones con las áreas de trabajo. La longitud máxima de cable desde el punto de terminación en el cuarto de telecomunicaciones hasta la terminación en la toma del área de trabajo no puede superar los 90 metros. Desde un patch panel en el cuarto de telecomunicaciones a un jack de pared en cada área de trabajo.

Para las instalaciones UTP, el estándar ANSI/TIA/EIA-568-B especifica que la longitud combinada total del cable que abarca las cuatro áreas enumeradas anteriormente se limita a una distancia máxima de 100 metros por canal. Este estándar establece que se pueden utilizar hasta 5 metros de patch cable para interconectar los patch panels. Pueden utilizarse hasta 5 metros de cable desde el punto de terminación del cableado en la pared hasta el teléfono o la computadora.

El conector RJ-45 es el componente macho engarzado al extremo del cable. Cuando se observan desde el frente, los pins se numeran del 8 al 1. Cuando se observan desde arriba con la entrada de apertura frente a usted, los pins se enumeran del 1 al 8, de izquierda a derecha.

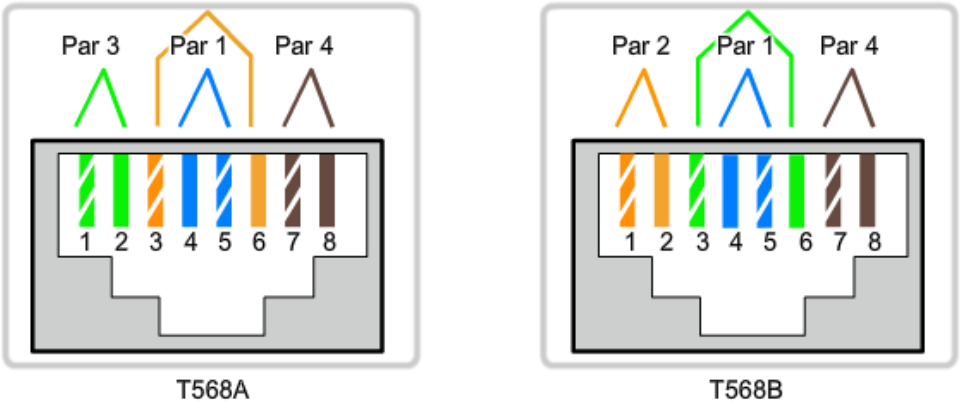


Figura 1. Ley A (izquierda) y Ley B (derecha) en el conector RJ-45

Cables UTP de conexión directa

Un cable de conexión directa tiene conectores en cada extremo y su terminación es idéntica conforme a los estándares T568A o T568B.

Se utilizan cables directos para las siguientes conexiones:

- Switch a puerto Ethernet del router
- Equipo (PC) a switch
- Equipo (PC) a hub

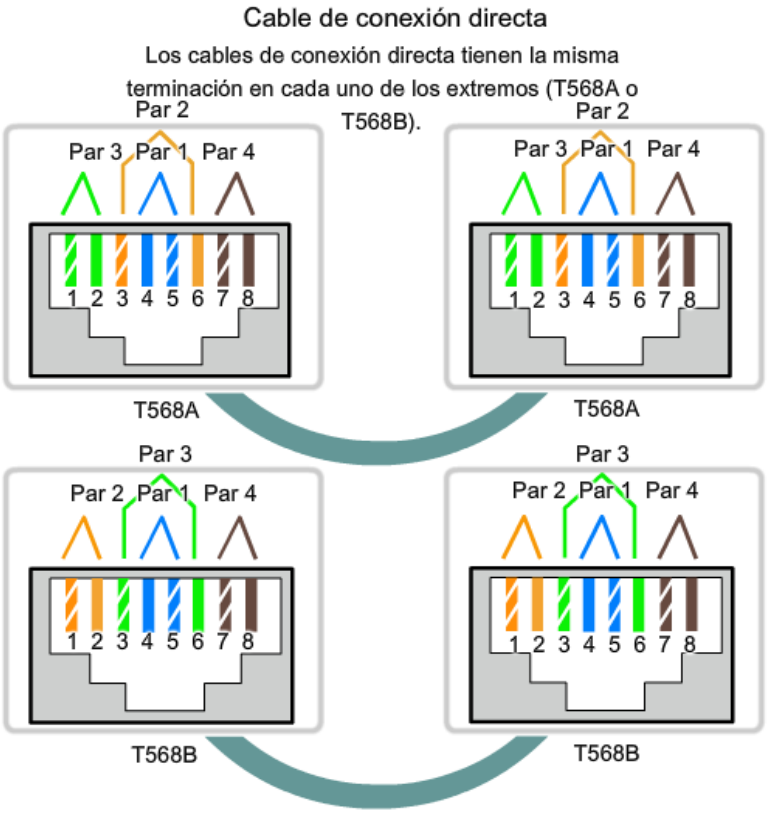


Figura 2. Cables de conexión directa según Ley A (arriba) y Ley B (abajo)

Cables UTP de conexión cruzada

Este tipo de conexión en un extremo debe tener una terminación como diagrama de pin EIA/TIA T568A y el otro, como T568B.

Los cables de conexión cruzada conectan directamente los siguientes dispositivos en una LAN:

- Switch a switch
- Switch a hub
- Hub a hub
- Router a router
- Equipo a equipo
- Equipo a puerto Ethernet del router

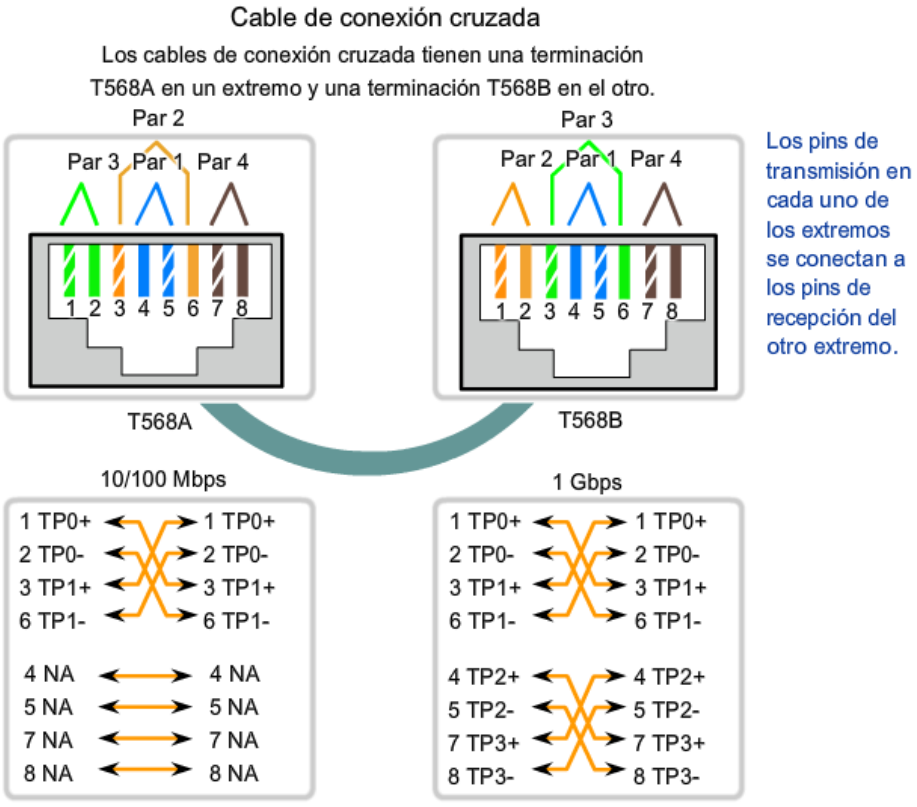
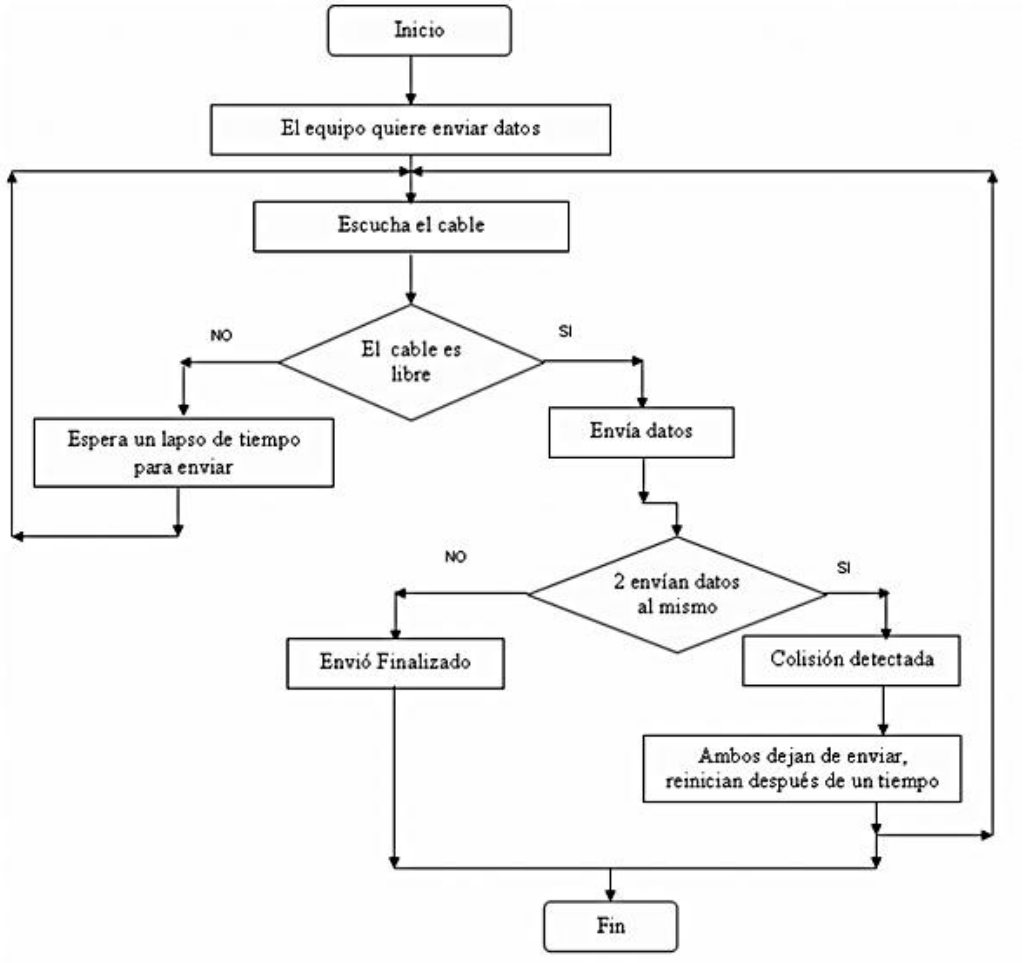


Figura 3. Diagrama para la realización de un cable cruzado y sus variantes en 10/100 Mbps y enlaces de 1 Gbps.

CSMA/CD

CSMA/CD es un protocolo de acceso al medio compartido, sus siglas provienen del inglés que significa ***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess with* ***C****ollision* ***D****etection* o, en español, *acceso múltiple con escucha de portadora y detección de colisiones*. En CSMA/CD, los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión.

Este protocolo funciona así:



Dominios de Colisión y de Broadcast (o difusión)

Un **dominio de colisión** es el grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales. Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda. Cuanto menor sea la cantidad de dispositivos afectados a un dominio de colisión mejor desempeño de la red. El uso de equipos como Hubs o Bridges (puentes) hace que una topología pueda ser más grande, pero aumentan la probabilidad de colisión.

Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.

Un **dominio de Broadcast** se trata de una porción de red en la que, a pesar de que pudo haber sido segmentada en capa 2 es aún una unidad a nivel de capa 3 por lo que un paquete de broadcast es transmitido a todos los puertos conectados.Si bien los switches filtran la mayoría de las tramas según las direcciones MAC de destino, no hacen lo mismo con las tramas de broadcast. Un conjunto de switches interconectados forma un dominio de broadcast simple.Para dividir dominios de broadcast es necesario implementar VLANs o dispositivos que operan en la capa 3 del modelo OSI, tales como switches multilayer o routers.

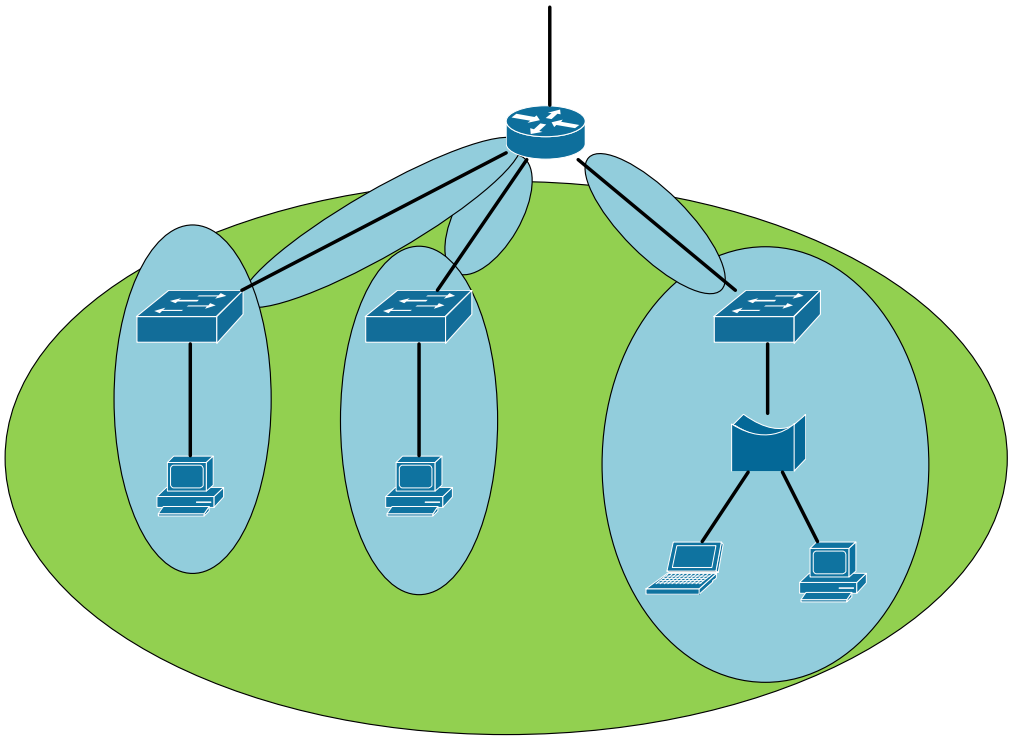


Figura 4. Muestra gráfica de dominios de colisión (azul) y de broadcast (verde)

Modelo OSI.

Recordemos las capas del Modelo OSI y su función.

- **Aplicación**: Proporciona los servicios utilizados por las aplicaciones para que los usuarios se comuniquen a través de la red.

- **Presentación**: Se encarga de presentar los datos a la capa de aplicación. En ciertos casos, la capa de presentación traduce los datos directamente de un formato a otro. Las grandes computadoras IBM utilizan una codificación de caracteres denominada EBCDIC, mientras que las computadoras restantes utilizan el conjunto de caracteres ASCII.

- **Sesión**: Se encarga del control de los diálogos entre distintos nodos. Un diálogo es una conversación formal en la que dos nodos acuerdan un intercambio de datos. Establece (negocia parámetros) y libera la conexión.

- **Transporte**: Divide los mensajes en fragmentos, en el lado receptor, la capa de transporte reensambla los fragmentos para recuperar el mensaje original. Multiplexaje, detección de errores. (Entrega fiable o no fiable)

- **Red**: Enrutamiento de paquetes, Direcciones de Red. Independiente del medio físico.

- **Enlace de datos**: Se encarga de proporcionar la comunicación nodo a nodo en una misma red de área local. Para ello, la capa de enlace de datos debe realizar dos funciones. Debe proporcionar un mecanismo de direcciones que permita entregar los mensajes en los nodos correctos y debe traducir los mensajes de las capas superiores en bits que puedan ser transmitidos por la capa física. Detección de errores (CRC).

- **Física**: Envía y recibe bits

Encapsulamiento de datos

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. Cada capa agrega su propio “encabezado” para que pueda ser recibido y leído correctamente al llegar a otro equipo.

Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

La capa de transporte divide los datos en unidades de un tamaño que se pueda administrar, denominadas segmentos. También asigna números de secuencia a los segmentos para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego la capa de red encapsula el segmento creando un paquete. Le agrega al paquete una dirección de red destino y origen, por lo general IP.

En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física.

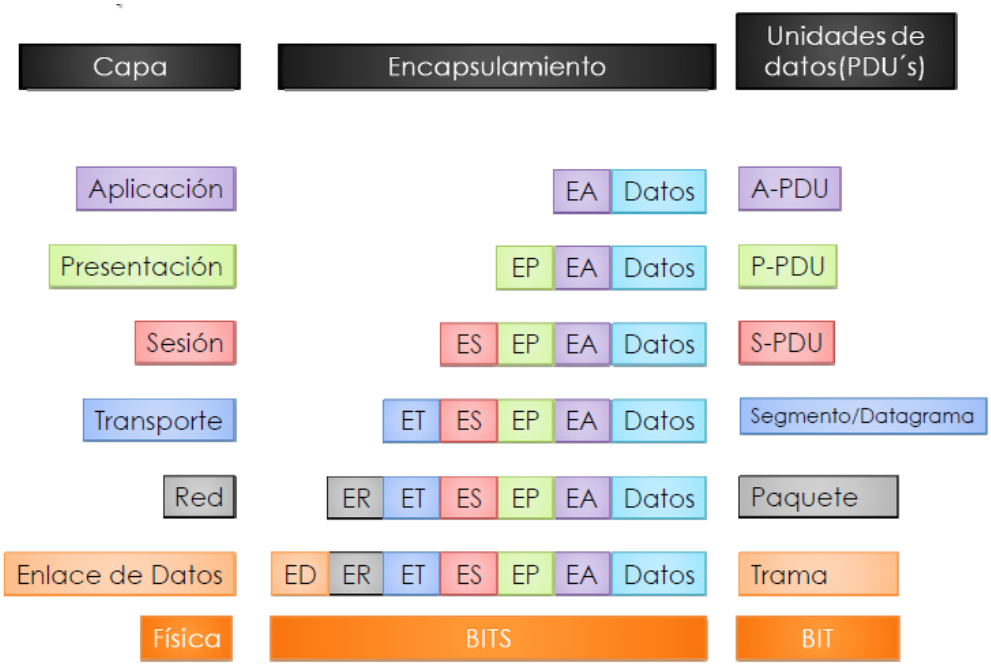


Figura 5. Modelo del encapsulamiento de datos

En la figura anterior, podemos notar como los datos puros llegan solo a la capa de aplicación (la parte que el usuario ve); vale la pena recalcar que cada vez que entra a una capa inferior se le suma un encabezado, por lo tanto, el encabezado y los datos de la capa anterior se convierten en un solo paquete de datos en la capa

inferior (es decir, el Encabezado de Aplicación + datos = Datos en capa de presentación).

Funciones y beneficios de un Switch

Un Switch es un dispositivo muy usado en redes, y entre sus funciones y principales ventajas tenemos:

- Es totalmente funcional a pesar de grandes distancias de cableado
- Crea múltiples dominios de colisión (como lo vimos en la figura 4, cada equipo conectado a un switch, es un dominio de colisión por sí mismo)
- Incrementa el ancho de banda (dado que cada conexión funciona en full-duplex[1])
- permiten múltiples y simultáneas conversaciones entre equipos en diferentes puertos
- Permite que aunque los equipos se comuniquen a diferentes tasas de trasmisión, exista comunicación entre ellos.

Proceso de aprendizaje de direcciones MAC (MAC tables) en un switch

Una MAC table es una lista donde el switch guarda 2 datos fundamentales: la dirección MAC del dispositivo y el puerto donde éste se encuentra. Al hacer una nueva red (o reiniciarse un switch y no haber guardado la configuración) esta tabla está vacía completamente.

La manera en que esta lista vuelve a llenarse es el siguiente:

1. Un equipo manda un paquete con la MAC origen y la MAC destino en ella, al llegar dicho paquete al switch, este equipo registra el puerto y la MAC de quien lo envio.

[1] Full-duplex significa que puede transmitir y recibir al mismo tiempo.

2. Como desconoce a donde debe enviarlo, lo envía a todos (a este proceso se le llama flooding[2]), esperando que algún otro equipo "le responda" que es para él.
3. Cuando obtiene respuesta y el segundo equipo manda la respuesta, el switch registra la MAC y el puerto del segundo equipo; si la MAC destino es conocida por el switch al compararla con la lista que ya tiene de direcciones MAC (supongamos que le responde) manda el mensaje directamente al primer equipo (no es necesario hacer flooding, pues ya se conoce el remitente).
4. Este ciclo continúa hasta que todas las direcciones MAC y los puertos son conocidos por el switch, una vez llegando a este punto, los mensajes ya se entregan directamente.

Procesamiento de Tramas en los switches.

Los switches tienes 3 maneras principales de procesar las tramas que le llegan.

- *Store-and-forward*: Aquí el switch recibe todos los bits de la trama (store) antes de enviarla (forward). Esto permite que el switch pueda verificarla a través de un FSC[3] antes de enviar la trama.
- *Cut-through*: El switch manda la trama lo más rápido que puede, esto reduce la latencia pero no permite que el switch descarte la trama si llegara a estar errónea (no puede aplicar FSC).
- *Fragment-Free:* el switch manda la trama después de haber recibido los primeros 64 bytes, evitando de este modo el reenvío de tramas con errores debido a una colisión.

[2] Flooding significa inundamiento, es decir, inunda la red con el mensaje.
[3] FSC. Frame Check Sequence. Verificación de la correcta secuencia de la trama recibida.

Procesos de ruteo.

El ruteo tiene la función de encontrar el mejor camino en una red, para encontrar la “mejor ruta” es básico definir que métrica se usa para poder medirla.

Existen 2 tipos de ruteo, el de un usuario y el de un router, a continuación de muestra la forma en que el ruteo es realizado.

Ruteo de un Usuario

- Si la dirección IP de destino está en la misma subred de donde sale el paquete, manda dicho paquete al destinatario.
- De otra manera, manda el paquete al *default gateway*.

Ruteo en un Router

- Se usa el FCS para asegurar que la trama no tiene errores; si los tuviera la trama es descartada.
- Asumiendo que la trama no es descartada, quita el viejo encabezado dejando solo el paquete IP.
- Compara la dirección destino IP con la tabla de routeo, y encuentra la mejor ruta hacia la dirección destino. Esta ruta identifica la interfaz de salida del router, y posiblemente el “salto-siguiente” (*next hop*) del router.
- Encapsula el paquete IP dentro de un nuevo encabezado tráiler de enlace de datos, apropiado para la interfaz de salida y envía la trama.

Protocolo ARP.

El protocolo ARP (Address Resolution Protocol) [RFC 826] se encarga de resolver direcciones IP. ARP proporciona los siguientes servicios.

- Las direcciones de control de acceso a medios se obtienen mediante una solicitud de difusión de red en forma de la pregunta "¿Cuál es la dirección de control de acceso a medios de un dispositivo configurado con la dirección IP adjunta?"

- Cuando se responde a una solicitud ARP, el remitente de la respuesta ARP y el solicitante de ARP original registran sus direcciones IP y de control de acceso a medios respectivas como una entrada en una tabla local, llamada la caché de ARP, para su uso posterior como referencia.

En resumen, cuando el equipo A conoce la dirección IP de un equipo B, pero desconoce su MAC, el protocolo ayuda a completar eso, con el ARP Request hace que encuentre al equipo (por medio de su dirección IP); al encontrar y desarrollar el ARP Request en el equipo B, este le responde al equipo A (conocido como ARP Reply), dándole su dirección MAC.

Referencias

www.cisco.com

A. Tanenbaum and D. Wetherall, Redes de computadoras*. México, Pearson Educación, 2012.*

Protocolo ARP: RFC 826

Conclusiones.

Tras concluir esta práctica, el alumno debe de dominar los siguientes temas:

- Definición de un cuarto de telecomunicaciones, el cableado backbone y horizontal, cable Ethernet y conector RJ45.
- Estándares T568A y T568B, como hacer y en qué casos usar un cable directo o cruzado.
- Funcionamiento del protocolo CSMA/CD.
- Dominios de colisión y broadcast.
- Modelo OSI y encapsulamiento de datos.
- Funciones y beneficios de un switch, así como el proceso de conformación de una MAC table y procesamiento de tramas.
- Procesos de ruteo.
- Protocolo ARP (Request y Reply)

Cuestionario

Recuerda que la respuesta correcta pueden ser una o varias, selecciónalas todas.

1. ¿Qué dispositivo es responsable de la regeneración de la señal de manera que la señal puede viajar una mayor distancia?

    a) Bridge
    b) Router
    c) Repetidor
    d) Switch
    e) Hub

2. ¿Qué dispositivo filtra el tráfico observando la dirección destino de la trama y luego envía la trama al puerto que el sistema de destino donde reside?

a) Hub
b) Router
c) Repetidor
d) Switch

3. ¿Cuál de los siguientes dispositivos trabaja en capa 3?

a) Bridge
b) Router
c) Repetidor
d) Switch
e) Hub

4. Un dispositivo que puede enviar y recibir información, pero no al mismo tiempo, se dice ser _____.

a) Simplex
b) Full Duplex
c) Multicast
d) Half Duplex

5. Un mensaje que se envía en la red y está destinado para todos los usuarios se conoce como un mensaje _____.

a) Unicast
b) Multicast
c) Full dúplex
d) Broadcast

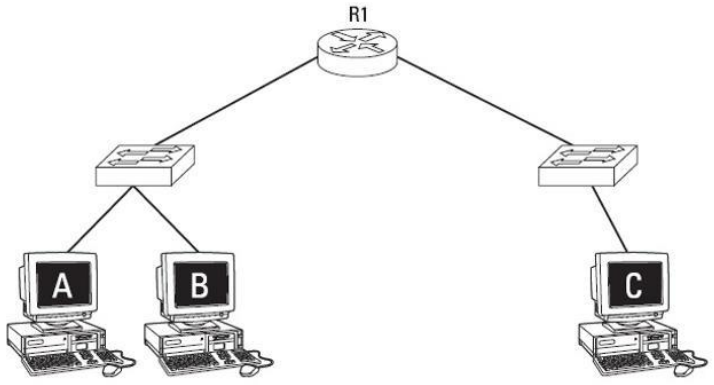
6. Un grupo de equipos que pueden recibir cualquier mensaje de broadcast es conocido como:

   a) Dominio de colisión
   b) Dominio de directorio activo
   c) Dominio totalmente calificado.
   d) Dominio de broadcast.

7. Un grupo de sistemas donde sus datos pueden chocan unos con otros se conoce como un:

   a) Dominio de broadcast
   b) VLAN
   c) Dominio de colisión
   d) Multicast.

8. ¿Cuántos dominios de colición y de broadcast hay en el siguiente diagrama?



   a) 1 dominio de broadcast y 5 dominios de colisión
   b) 2 dominio de broadcast y 3 dominios de colisión
   c) 1 dominio de broadcast y 3 dominios de colisión
   d) 2 dominio de broadcast y 5 dominios de colisión

9. Si alguien tuviera problemas entendiendo conceptos de redes y te pide ayuda respecto a tipos de direcciones, ¿Cuál de los siguientes es considerado una dirección de capa 2 (enlace de datos)?

    a) 192.168.2.200
    b) www.gleneclarcke.com
    c) COMPUTER1
    d) 00-AB-0F-2B-3C-4E

10. ¿Qué capa del modelo OSI es responsable de dividir los datos en segmentos más pequeños?

    a) Enlace de datos
    b) Física
    c) Red
    d) Transporte

11. ¿Qué capa del modelo OSI es responsable de enrutamiento y direccionamiento lógico?

    a) Red
    b) Física
    c) Enlace de datos
    d) Transporte

12. ¿Qué tipo de cable usarías si quería conectar un sistema a un puerto RJ45 en un switch?

    a) Fibra
    b) Cruzado
    c) Directo

d) Thinnet

13. Usted desea conectar dos sistemas mediante una conexión de una computadora a otra computadora. ¿Qué tipo de cable usarías?

a) Fibra
b) Cruzado
c) Directo
d) Thinnet.

14. Si necesitaras hacer un cable cruzado, ¿qué alambres cruzarias en uno de los extremos?

a) 1 y 2 con 3 y 4
b) 2 y 4 con 6 y 8
c) 2 y 4 con 5 y 6
d) 1 y 2 con 3 y 6

15. ¿Qué protocolo se encarga de convertir la dirección lógica a una dirección física?

a) TCP
b) IP
c) ICMP
d) ARP

Capítulo 3: VLANs (Virtual LANs)

Introducción

En la siguiente práctica se verá a detalle lo que son las VLANs, su uso cotidiano, necesidad de creación, diferentes usos para cada VLAN creada; llegando hasta a la configuración de VLANs en switches por métodos sencillos, con enlaces troncales a otros switches y routers.

Conceptos previos

VLAN viene del acrónimo (en inglés) de Virtual LAN; eso significa que se hace una segmentación virtual, un mecanismo que permite múltiples redes a través de un mismo medio físico.

Una solución realizada para abaratar costos, pues en vez de comprar varios switches para diferentes sectores, se usan los mismos equipos, con tan solo una configuración de puertos, muchos equipos terminales pueden conectarse a un mismo equipo manteniendo la privacidad de cada red.

De manera general obtenemos los siguientes beneficios:

- Seguridad
- Reducción de costos
- Mejor rendimiento
- Reduce el tamaño de los dominios de broadcast
- Mejora la eficiencia del personal de TI
- Hace más sencilla la protección y administración de aplicaciones.

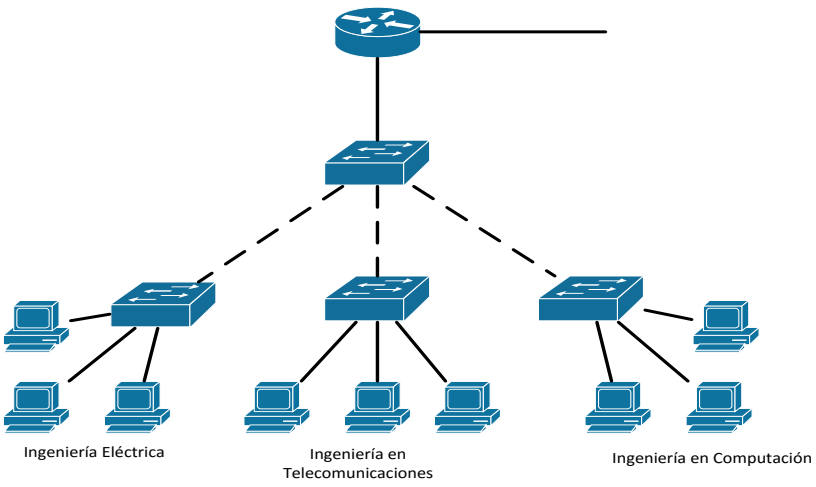


Figura 1. Red escolar segmentada por switches.

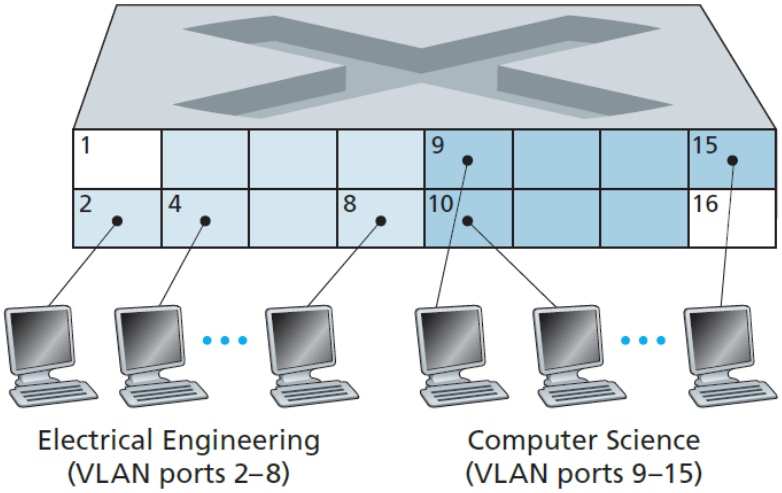


Figura 2. Segmentación de redes por medio de VLANS (un solo switch).[4]

A las diferentes VLAN se les puede nombrar de diferentes maneras, ya sea con números o incluso con colores (de esta última manera es más fácil hacer diagramas para ver cómo se segmenta la red).

[4] Imagen tomada de J. Kurose and K. Ross, Computer networking. Boston: Pearson/Addison Wesley, 2008, pág. 484.

Tipos de VLAN

- VLAN de datos: Son aquellas que crean dominios de broadcast entre grupos de usuarios y servicios.
- VLAN de voz: Una VLAN que crea dominios de broadcast entre grupos de teléfonos IP y servicios de voz.
- VLAN por defecto: es la VLAN que trae por defecto configurada en los switches y todos los puertos están asignados a esta.
- VLAN Nativa: es la VLAN que no se etiqueta en los enlaces troncales.
- VLAN de Administración: por creadas para asignarse a los servidores.

VLAN Trunks

Una VLAN troncal lleva 2 o más de una VLAN por un mismo medio físico. Usualmente esta troncal está establecida en un switch para que dispositivos de la misma VLAN se puedan comunicar, aunque estén conectados a diferentes switches.

Un VLAN troncal no se asocia a ninguna VLAN.

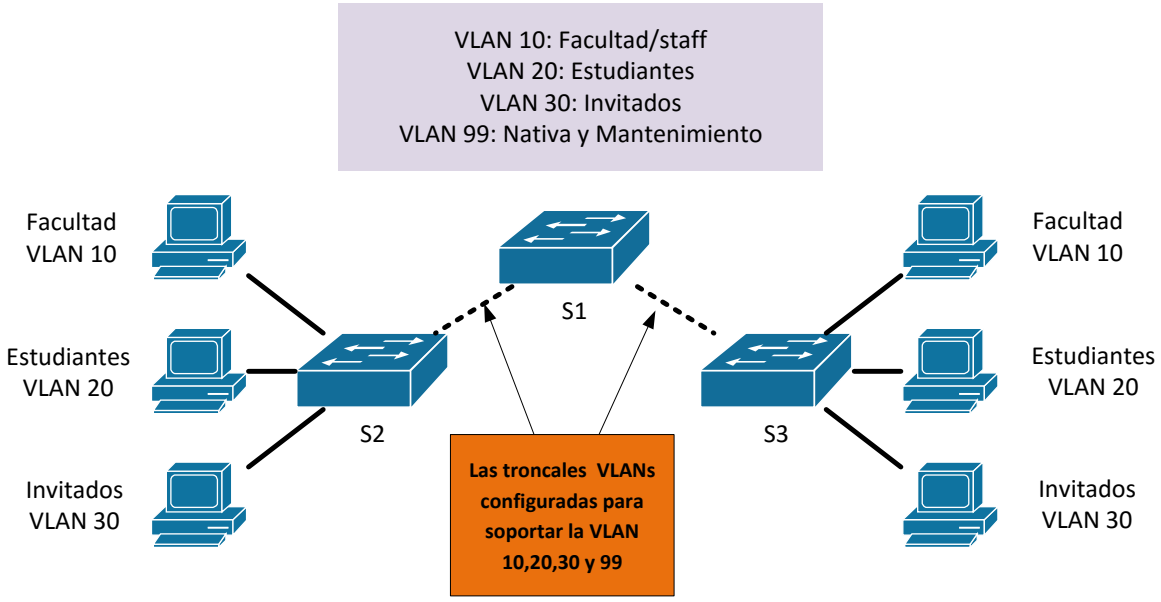


Figura 3. Red escolar segmentada por VLANs

Controlando los dominios de broadcast con VLANs

Las VLANs son usadas para limitar el alcance de las tramas de broadcast. Cada VLAN es un dominio de broadcast por sí misma. Por lo tanto, una trama broadcast enviada por un dispositivo en una VLAN específica es reenviada solamente dentro de esa VLAN, esto ayuda a controlar el alcance de las tramas de broadcast y su impacto en la red.

Tramas unicast y multicast son reenviadas también dentro de la VLAN originaria

Creando una VLAN

Función	Comando
Entrar al modo global de configuración	`s1# configure terminal`
Crear una VLAN con un número de identificación válido	`s1 (config)# vlan vlan_id`
Especificar un nombre único para identificar la VLAN	`s1 (config)# name vlan_name`
Regresar al modo EXEC privilegiado	`s1 (config)# end`

Tabla 1. Comandos para la creación y nombramiento de una VLAN

Configuración de los puertos de la VLAN

Función	Comando
Entrar al modo de configuración global	`s1# configure terminal`
Entrar al modo de configuración de la interface para los SVI*	`s1 (config)# interface interface_id`
Configurar la dirección IP para el manejo de la interfaz.	`s1 (config)# ip address 172.17.99.11`
Poner el puerto en modo de acceso	`s1 (config-if)# switchport mode access`
Asignar el puerto a una VLAN	`s1 (config-if)# switchport access vlan vlan_id`
Regresar al modo EXEC privilegiado.	`s1 (config-if)# end`

*(SVI) Switch Virtual Interface

Tabla 2. Comandos para la asignación de puertos a una VLAN

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

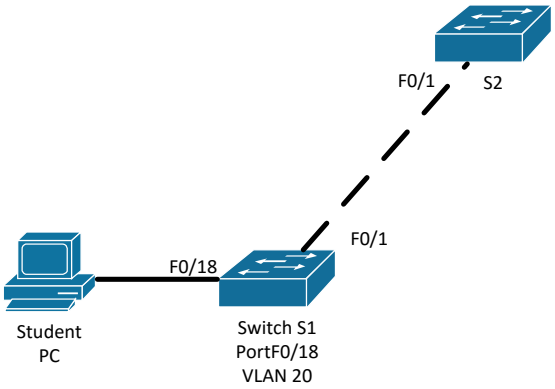


Figura 4. Ejemplo de asignación de puerto a una VLAN.

Configuración de enlaces troncales

Función	Comando
Entrar al modo de configuración global	`s1# configure terminal`
Entrar al modo de configuración de la interface para los SVI	`s1 (config)# interface` *interface_id*
Forzamos el enlace a ser un enlace truncal	`s1 (config)# switchport mode trunk`
Especificamos una VLAN nativa para las troncales 802.1Q sin etiquetar	`s1 (config-if)# switchport trunk native vlan` *vlan_id*
Especifica la lista de VLANs permitidas por la troncal	`s1 (config-if)# switchport trunk allowed vlan` *vlan_list*
Regresa el modo EXEC privilegiado.	`s1 (config-if)# end`

Tabla 3. Configuración de enlaces troncales.

```
s1(config)# interface FastEthernet0/1
s1(config-if)# switchport mode trunk
s1(config-if)# switchport trunk native vlan 99
s1(config-if)# switchport trunk allowed vlan 10,20,30
s1(config-if)# end
```

Figura 5. Ejemplo de configuración de enlaces troncales.

Borrando VLANs

```
s1# conf t
s1(config)# no vlan 20
s1(config)# end
```

Figura 6. Eliminación de VLANs.

Enrutamiento inter-VLAN.

En enrutamiento Inter-VLAN es el proceso para enviar tráfico de red desde una VLAN a otra usando un router.

Existen 2 modos principales de enrutamiento inter-VLAN

Router-On-A-Stick

Una de las interfaces físicas el router es configurada usando puertos troncales 802.1Q, ahora esa interface entiende etiquetas VLAN se deben crear subinterfaces lógicas, una por cada VLAN, cada subinterface es configurada con una dirección IP de la VLAN que representa y así los host de la VLAN son configurados para usar la dirección de la subinterface como puerta de enlace. El beneficio radica en que solo una de las interface físicas del router se usa.

Preparación

- Una alternativa al enrutamiento inter-VLAN heredado es usar troncales VLAN y subinterfaces

- Los troncales VLAN permiten a una sola interface física enrutar tráfico entre múltiples VLANs
- La inetrface física del router debe ser conctada a un enlace troncal hacia el switch cercano
- En el router, se crean las subinterfaces para cada VLAN en la red
- Cada subinterface tiene una dirección IP específica para cada VLAN e identifica los frames para dicha VLAN

```
s1 (config) # vlan 10
s1 (config-vlan) # vlan 30
s1 (config-vlan) # interface f0/5
s1 (config-if) # switchport mode trunk
s1 (config-if) # end
```

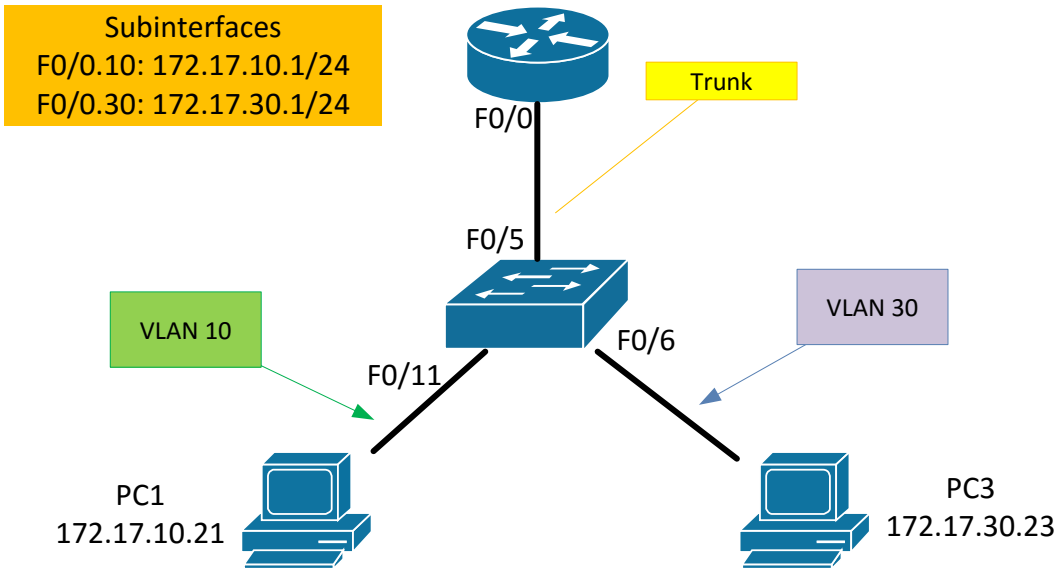


Figura 7. Modelo y ejemplo de enlace troncal.

```
R1 (config)# interface g0/0.10
R1 (config-subif)# encapsulation dot1q 10
R1 (config-subif)# ip address 172.17.10.1 255.255.255.0
R1 (config-subif)# encapsulation dot1q 30
R1 (config-subif)# ip address 172.17.30.1 255.255.255.0
R1 (config)# interface g0/0
R1 (config-if)# no shutdown
```

Figura 8. Configuración de la interfaces en el Router

Multicapa

Los switchs multicapa pueden desarrollar funciones de Capa 2 y 3. Ya no se necesitan routers, cada VLAN existente en el switch es una SVI, las SVI son vistas como interfaces de capa 3 así el switch entiende las PDU de capa de red, por lo tanto puede enrutar entre las SVI tal como lo hace un router entre sus interfaces, con un Switch multicapa, el tráfico es enrutado internamente en el dispositivo. Es una solución altamente escalable

Los Switches de Capa 3 procesan millones de paquetes por segundo (pps)

Las ventajas de las SVI son:

- Son mucho más rápidas que usar router-on-a-stick, porque toda la conmutación y enrutamiento se realiza por hardware.
- No se necesitan enlaces externos desde el switch a un router para enrutar.
- No se limita a un solo enlace. Técnicas de capa 2 como EtherChannels pueden ser usadas para obtener mayor ancho de banda.
- La latencia es más baja, debido a que no se necesita abandonar el switch.

Preparación de enrutamiento con SVIs

- Por defecto, se crea una SVI para la VLAN por defecto (VLAN 1). Esto permite la administración remota

- Cualquier SVI adicional debe ser creada por el administrador
- Las SVI son creadas la primera vez que se ingresa al modo de configuración para la SVI de una VLAN en particular
- La **interface vlan 10** crea una SVI llamada VLAN 10
- El número de VLAN usado corresponde a la etiqueta de VALN asociada con la encapsulación 802.1Q
- Cuando una SVI es creada, verificar que la VLAN es particular esta presente en la base de datos VLAN

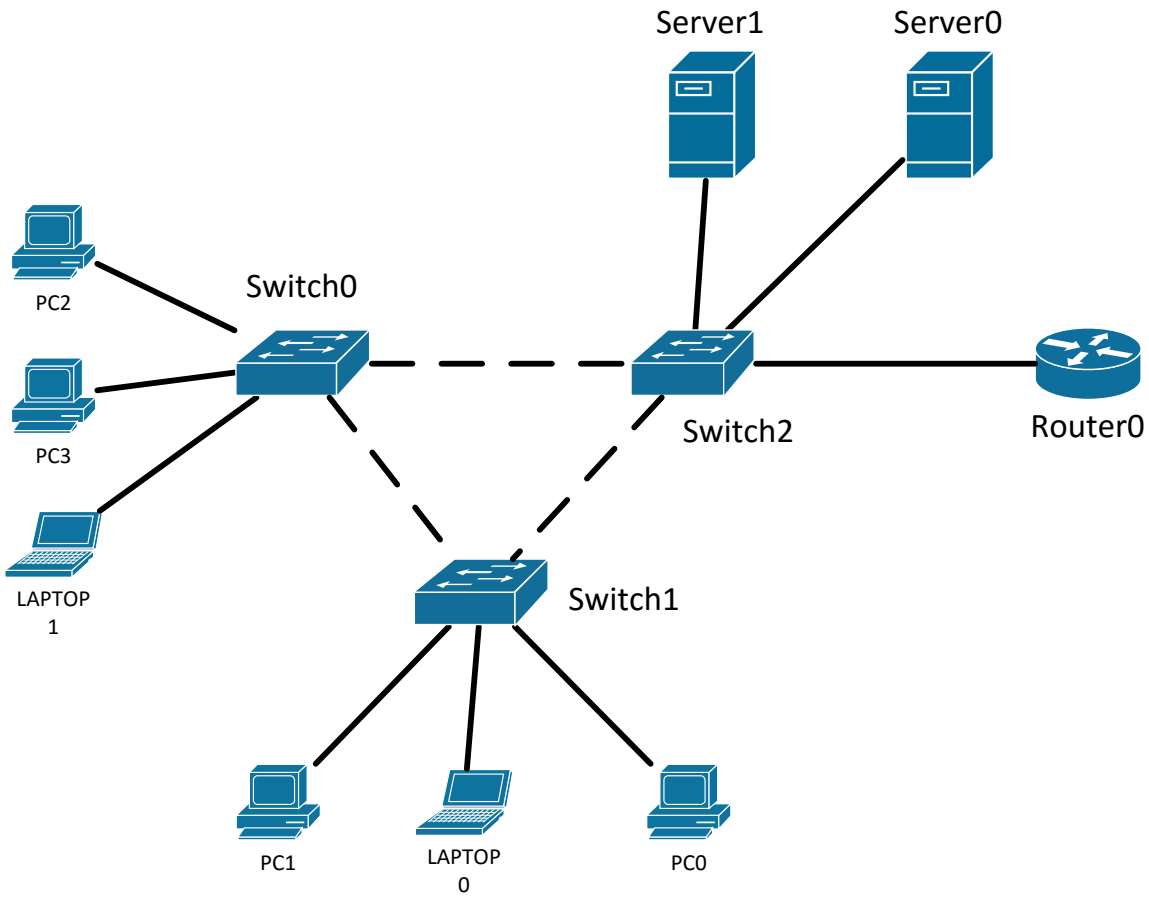
Referencias.

www.cisco.com

A. Tanenbaum and D. Wetherall, Redes de computadoras. México, Pearson Educación, 2012.

J. Kurose and K. Ross, Computer networking. Boston: Pearson/Addison Wesley, 2008.

VLAN: IEEE 802.1Q



Topología.

Desarrollo

Actividad 1.

En cada Switch cree 3 VLAN's, con los siguientes nombres:

- Admin.
- Services.
- Users.

Asigne los modos de los puertos correspondientes.

Asigne cada puerto en los switches a las VLAN's correspondientes usando la siguiente información.

Dispositivo	**VLAN a la que pertenece**
PC0	Admin
PC1	Users
PC2	Admin
PC3	Admin
Laptop0	Users
Laptop1	Admin
Server0	Services
Server1	Services

Actividad 2.

Implemente un esquema de direccionamiento privado en la topología. Usando redes con máscaras /24 en las VLANS.

Configure los links entre los switches como enlaces troncales que permitan el paso de información de las VLAN's que configuro anteriormente.

Haga pruebas de conectividad para verificar la configuración.

Configure el router para que direccione el tráfico entre las VLAN's.

Conclusiones

Durante la realización de esta práctica, el alumno aprendió técnicas y destrezas que lo ayudarán en su desarrollo en la materia, entre ellas destacamos:

- Referencia IEEE, significado y uso de lo que es una VLAN.
- Beneficios, importancia y necesidad de las VLAN.
- Tipos de VLANs
- Enlaces VLAN troncales.
- Creación y asignación de puertos de una VLAN en un switch.
- Configuración de enlaces troncales
- Tipos de enrutamiento inter-VLAN (Router-On-A-Stick y multicapa).
- Configuración de enrutamiento inter-VLAN: Router-On-A-Stick y multicapa.

Cuestionario

1. Sus compañeros han oído hablar de las funciones de las VLAN en switches y te preguntan cuál es el beneficio. ¿Cuál sería su respuesta?

    A. Para crear límites comunicación
    B. Filtros de tráfico basado en direcciones de capa 3
    C. Filtros de tráfico basado en direcciones de capa 4
    D. Se utiliza para evitar bucles en la red

2. ¿Cuál de los siguientes utilizarías para crear múltiples dominios de broadcast?

    A. STP
    B. VTP
    C. CDP
    D. VLANs

3. ¿Qué comando usarías en un puerto en específico para permitir llevar todo el tráfico de las VLANs a través del puerto?

   A. `switchport mode trunk`
   B. `switchport mode vlan`
   C. `switchport mode access`
   D. `switchport mode vlan access`

4. ¿Cuál de los siguientes comandos usarías para activar el puerto 6 para la VLAN 2?

   A. Usando los siguientes comandos:

   ```
   Switch(config)#interface f0/6
   Switch(config-if)#switchport access
   ```

   B. Usando los siguientes comandos:

   ```
   Switch(config)# switchport access vlan 2
   ```

   C. Usando los siguientes comandos:

   ```
   Switch(config)#interface f0/6
   Switch(config-if)#switchport access vlan 2
   ```

   D. Usando los siguientes comandos:

   ```
   Switch(config)#interface f0/8
   Switch(config-if)#switchport access vlan 2
   ```

5. ¿Cuál de las siguientes afirmaciones son ciertas sobre las VLANs y su uso? (Seleccione dos).

    A. La comunicación entre VLAN requiere un router.
    B. No se puede utilizar VLAN a través de los switches.
    C. Una VLAN que se extiende a través de los switches requiere un router.
    D. Cada VLAN requiere su propia subred IP.
    E. Múltiples VLANs pueden utilizar la misma subred IP si las subinterfaces son usadas en el router.

6. ¿Cuál de los siguientes es el protocolo de etiquetado de las VLAN? (seleccione dos)

    A. ISL
    B. 802.1d
    C. 802.1q
    D. 802.1l

7. Para asegurar que solo el tráfico de la VLAN 10 y la VLAN 20 pase por un enlace troncal, ¿qué comando usarías?

    A. `SW1(config-if)#trunk allowed vlan 10,20`
    B. `SW1(config)#switchport trunk allowed vlan 10,20`
    C. `SW1(config-if)#switchport trunk allowed vlan 10,20`
    D. `SW1(config)#trunk allowed vlan 10,20`

8. Tienes un router conectado a un switch que tiene tres VLAN. Quieres configurar el router para que pueda ser utilizado para enrutar el tráfico entre las tres VLAN. ¿Qué necesitas hacer?

    A. Agregar dos routers mas a la red (uno por cada VLAN)
    B. Activar RIP
    C. Configurar Router-On-A-Stick
    D. Configurar OSPF

9. Si desearas ver la configuración de VLANs en un switch, ¿qué comando usarías?

    A. `show port-security addresses`
    B. `show vlan`
    C. `show mac-address table`
    D. `show interfaces`

10. ¿Cuál de los siguientes protocolos son usados para llevar el tráfico de las VLAN entre switches? (escoge dos)

    A. VTP
    B. STP
    C. 802.1q
    D. ISL
    E. IGRP

Capítulo 4: Spanning Tree Protocol (STP)

Introducción

En esta práctica se verá el protocolo SPT (Spanning Tree Protocol) que permite una jerarquización de una red de switches, evitando que haya tormentas de broadcast u otras situaciones que harían que esta red se saturara y fallara. Además se hablará de algunas variantes de este mismo protocolo y características de algunos de ellos.

Conceptos previos

Redundancia en Capa 1

Cuando tenemos múltiples caminos cableados entre switches, generamos:

- Redundancia física en una red conmutada.
- Mejora la fiabilidad y disponibilidad de la red.
- Permite a los usuarios acceder a los recursos de red, incluso si hubiera una interrupción en el camino.

Cuando hablamos de redundancia en la capa física, debemos de tomar en cuenta la inestabilidad de la base de datos MAC, recordemos que las tramas Ethernet no tienen un tiempo de vida; eso genera que:

- Las tramas se siguen propagando entre los switches sin fin (por efecto de un Broadcast, por ejemplo) o hasta que un vínculo se pierde y rompe el bucle.
- Resulta en la inestabilidad de base de datos MAC.

Si hay más de un camino para la trama que se reenvíe, puede dar lugar a un bucle sin fin.

Cuando se produce un bucle, es posible que la tabla de direcciones MAC en un switch cambie constantemente con las actualizaciones de las tramas de broadcast, lo que resulta en la inestabilidad en la base de datos MAC.

Tormentas de Broadcast

Una tormenta de broadcast se produce cuando hay tantas tramas broadcast atrapados en un bucle de Capa 2 que se consume todo el ancho de banda disponible.

Una tormenta de Broadcast es inevitable en una red en bucle.

A medida que más dispositivos envían las transmisiones por la red, más tráfico está atrapado dentro de este bucle; consumiendo así más recursos.

Esto a la larga crea una tormenta de broadcast que hace que la red falle.

Tramas Duplicadas de Unicast

Las tramas Unicast enviados a una red en bucle pueden dar como resultado tramas duplicadas que llegan al dispositivo de destino; la mayoría de los protocolos de capa superior no están diseñados para reconocer, o hacer frente a transmisiones duplicadas.

Los protocolos de LAN en capa 2, tales como Ethernet, carecen de un mecanismo para reconocer y eliminar tramas en bucle sin fin.

El Algoritmo de Spanning Tree (STP)

- STP asegura que hay un solo camino lógico entre todos los destinos de la red, bloqueando intencionalmente los caminos que puedan causar un loop.
- Un puerto es considerado bloqueado cuando los datos del usuario no pasan por un determinado puerto. Esto no incluye BPDU’s que son usadas por el STP para prevenir loops.
- Los enlaces físicos seguirán existiendo para mantener la redundancia, pero estos caminos estarán deshabilitados para prevenir loops.

- Si el camino siempre es necesario para compensar un fallo en el cable o switch, el STP recalcula los caminos y desbloquea los puertos necesarios para permitir el camino redundante se convierta en activo.

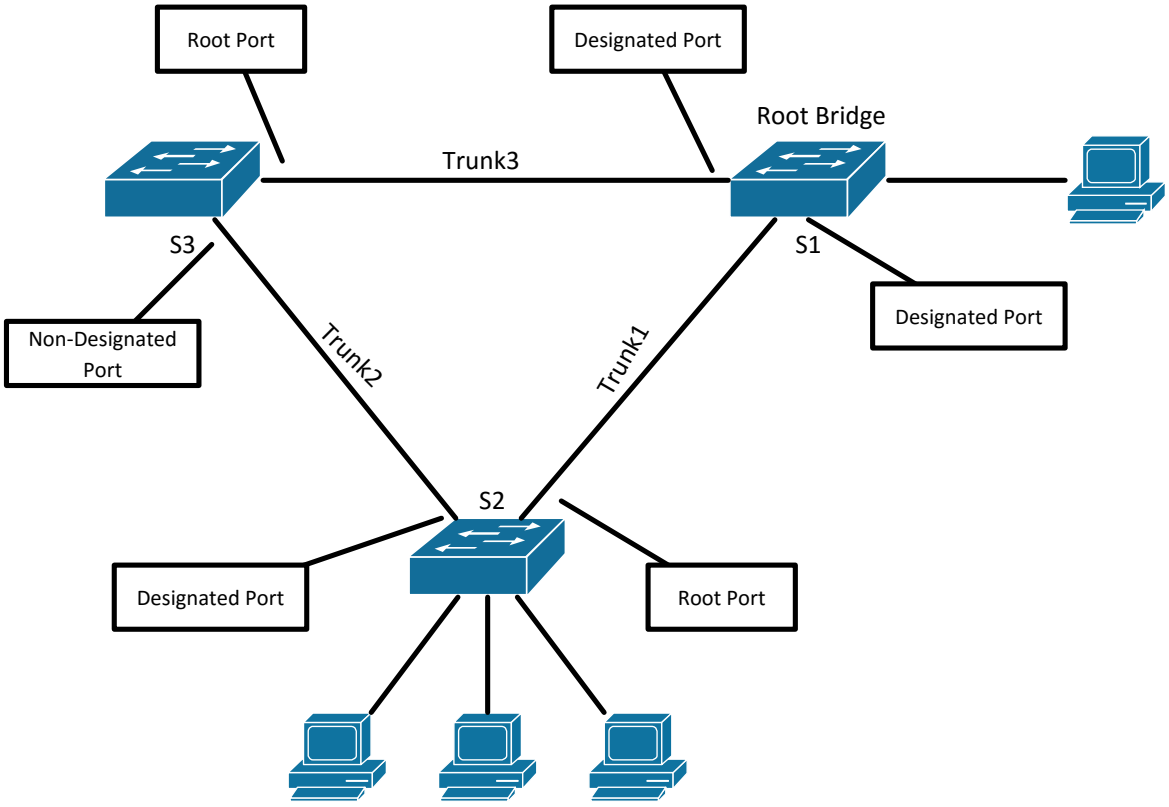


Figura1. Red de switches con STP y el estado de sus puertos.

Para escoger el que será el switch raíz, el primer criterio es la Prioridad de cada switch (el que tenga la menor será el Switch Raiz (Root)), si 2 o más switches tuvieran la misma prioridad, el segundo criterio es la MAC más pequeña.

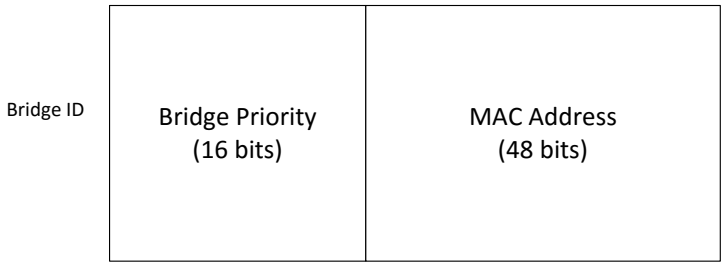


Figura 2. Conformación del Bridge ID

Pasos para escoger el Switch Raiz

1) Los switches conectados (como en la figura 1, 3 switches conectados) asumen que son el Switch Raiz y se mandan un mensaje con su Bridge ID.
2) Al compararse todos los Brigde ID, el menor queda como el Switch Raiz, todos los demás switches cambian su Root ID por el del Switch Raiz.
3) A continuación, cada switch determina el mejor trayecto para llegar al switch raíz. Los switches determinan este trayecto mediante una comparación de la información en todas las BPDU que los switches reciben de todos los puertos. El switch utiliza el puerto con la menor cantidad de información en la BPDU es el puerto raíz. Además, cada vez que un BPDU es intercambiado, se manda la informacion del Root ID y el costo del enlace.
4) Una vez determinados los puertos raíz los puertos designados y los no designados (o bloqueados), el algoritmo queda listo, ahora aunque exista redundancia física entre los equipos, se crea una arquitectura libre de loops.

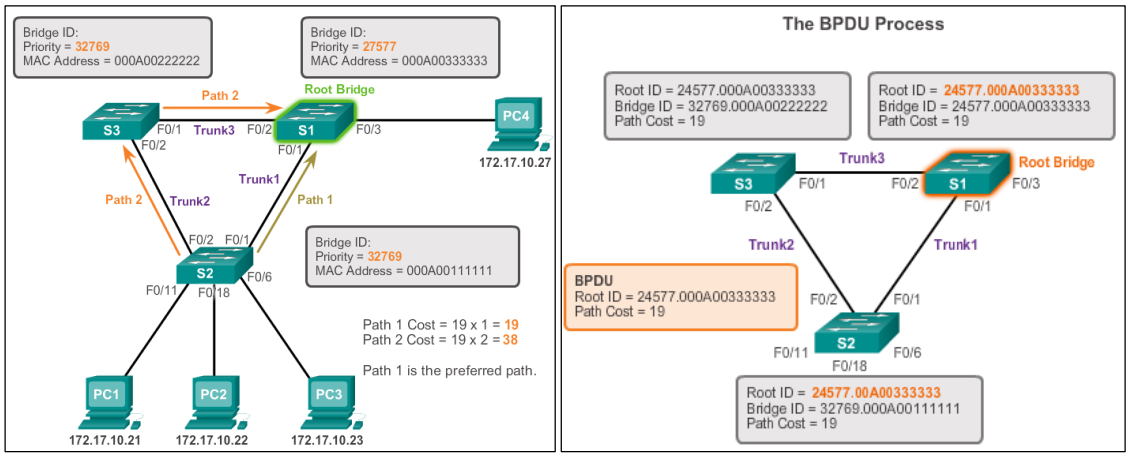


Figura 3. A la izquierda se ilustra el paso 2, a la derecha el paso 3.[5]

[5] Imagen tomada de www.cisco.com

Velocidad del Enlace	Costo (Especificación IEEE)
10 Gb/s	2
1Gb/s	4
100 Mb/s	19
10 Mb/s	100

Tabla 1. Tabla de costos de los enlaces.

Sistema Extendido ID

Por otra parte, STP se ha sido mejorado para incluir soporte para VLANs, lo que requiere la VLAN ID para ser incluidos en el marco de BPDU mediante el uso de la ID de sistema extendido

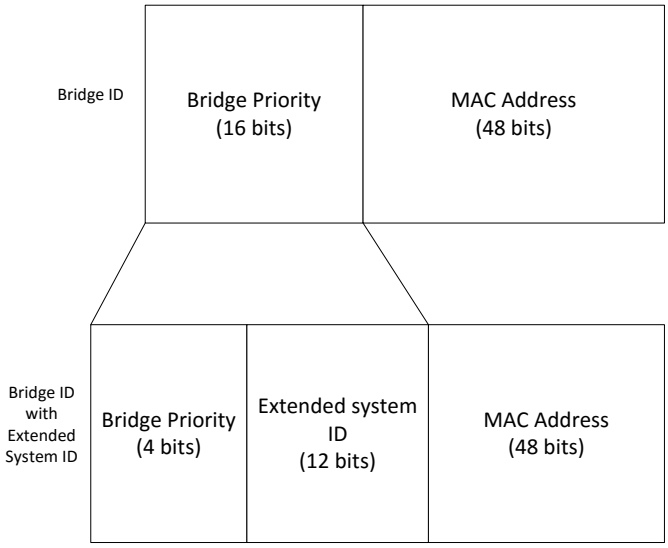


Figura 4. Modificación del Bridge ID con el sistema extendido ID

Por ejemplo, imagínese la misma red de switches de la figura 3, pero configurados con diferentes VLANs; la prioridad de todos los switches es 32769. El valor está basado en el valor por default de prioridad (32768) y la VLAN 1 hace que se le sume 1 al valor de prioridad, cambiando el valor a cada switch (32678 + 1).

Lista de Spanning Tree Protocols (STP)

- STP o IEEE 802.1D (1998)
- PVST+
- IEEE 802.1D (2004)
- Rapid Spanning Tree Protocol (RSTP) ó IEEE 802.1w
- Rapid PVST+
- Multiple Spanning Tree Protocol (MSTP) ó IEEE 802.1s

Protocolo	Standart	Uso de Recursos	Convergencia	Calculación del árbol
STP	802.1D	Bajo	Lenta	Todas las VLAN's
PVST+	Cisco	Alto	Lenta	Por VLAN
RSTP	802.1w	Medio	Rápida	Todas las VLAN's
Rapid PVST+	Cisco	Muy Alto	Rápida	Por VLAN
MSTP	802.1s Cisco	Medio - Alto	Rápida	Según situación.

Tabla 2. Resumen de los diferentes STP's

Analizando la Topología de STP.

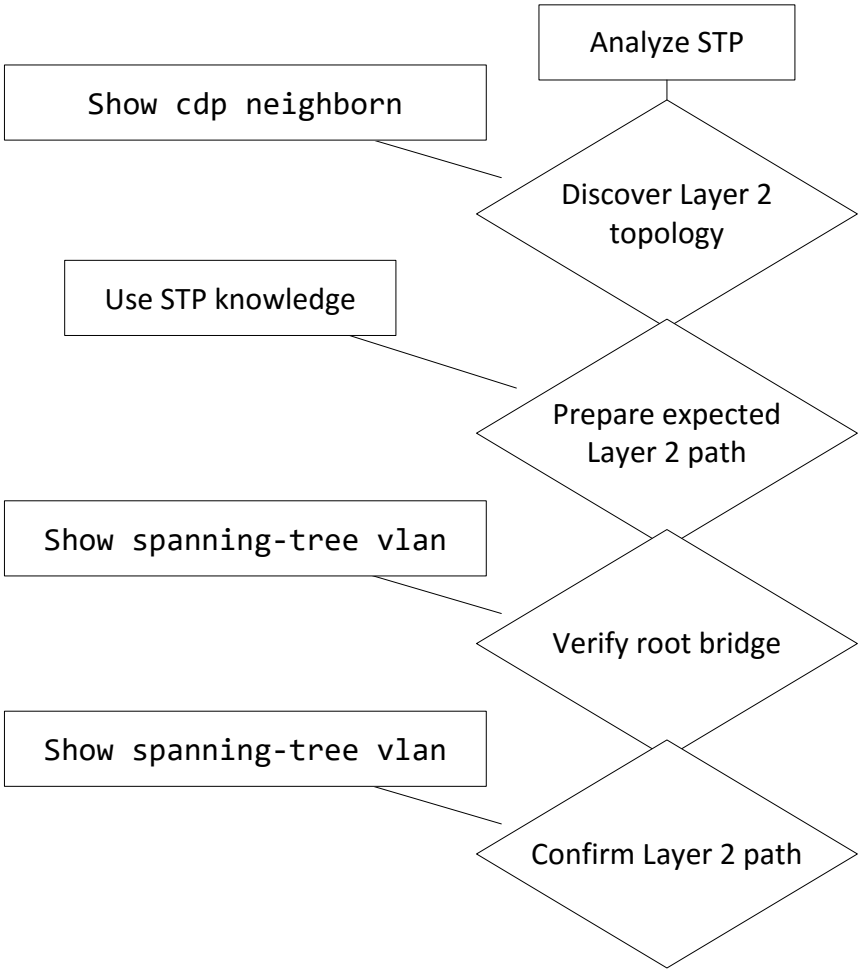


Figura 5. Esquema base del funcionamiento de STP.

Configurando STP

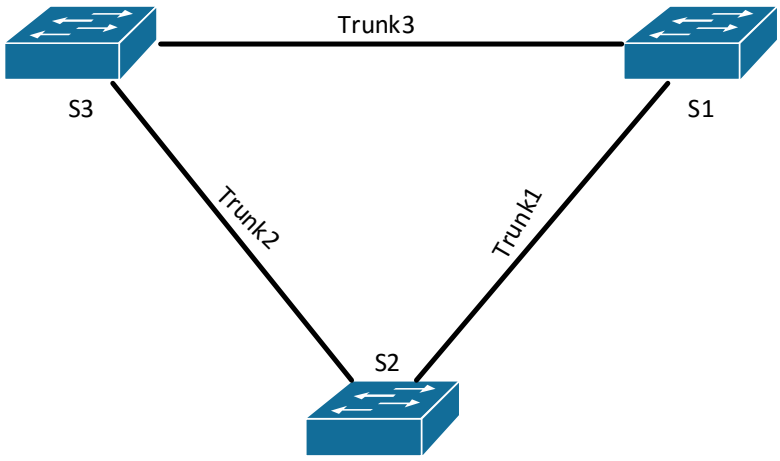


Figura 6. Arreglo de ejemplo para la configuración de STP.

Podemos configurar STP de maneras sencillas, a continuación 2 métodos para hacerlo:

Método 1

- Comandos para S1

```
s1(config)# spanning-tree VLAN 1 root primary
s1(config)# end
```

- Para S2

```
s2(config)# spanning-tree VLAN 1 root secundary
s2(config)# end
```

De esta manera, queda ya configurado STP

Método 2

- Comandos para S3

```
s3(config)# spanning-tree VLAN 1 priority 24576
s3(config)# end
```

De esta manera, queda ya configurado STP

Una vez que ya configuramos el STP, es bueno que verifiquemos que los puertos estén correctamente configurados, de lo contrario, una trama puede entrar en loop, inundando nuestra red hasta colapsar.

PVST+

Redes con el protocolo PSVT+ tienen las siguientes características:

- Una red puede correr independientemente STP (IEEE 802.1D) en cada VLAN de la red.
- El balanceo de la carga óptima puede funcionar.
- Un segmento con STP para cada VLAN puede significar una pérdida considerable de ciclos de CPU en todos los switches en la red. Además del ancho de banda que se utiliza para cada instancia para enviar su propios BPDU.

Recordemos también los estados que pueden tomar los puertos en este protocolo:

Proceso	Bloqueado (Blocking)	Escuchando (Listening)	Aprendiendo (Learning)	Permitiendo (Forwarding)	Deshabilitado (Disabled)
Procesa BPDUs recibidos	Si	SI	SI	SI	NO
Manda tramas de datos recibidos	NO	NO	NO	SI	NO
Manda tramas de datos recibidos de otra interfaz	NO	NO	NO	SI	NO
Aprende direcciones MAC	NO	NO	SI	SI	NO

Tabla 3. Acciones permitidas de los puertos en diferentes estados.

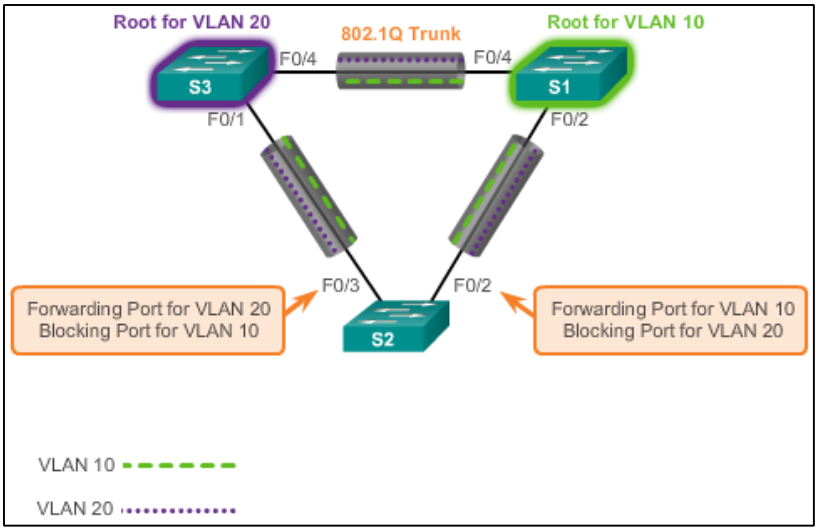


Figura 7. Red de switches con 2 VLANs bajo PVST+ [6]

En un ambiente de PVST+, la extended ID asegura cada switch tiene un Bridge ID única para cada VLAN.

Por ejemplo, para la VLAN 2 el Brigde ID predeterminada sería 32.770; el switch tiene una prioridad 32.768, más el sistema ID extended de 2. (Véase sistema de extended ID de la figura 4)

Rapid PVST+

- RSTP es el protocolo preferido para la prevención de bucles de Capa 2 en un entorno de redes conmutadas.
- Con Rapid PVST+, una instancia independiente de RSTP funciona para cada VLAN.
- RSTP admite un nuevo tipo de puerto: un puerto alternativo en estado “descartado”.
- No hay puertos bloqueados. RSTP define estados de los puertos como: discarding, learning o forwarding
- RSTP (802.1w) reemplaza a STP (802.1D) y al tiempo, conserva la compatibilidad anterior.

[6] Imagen tomada de www.cisco.com

- RSTP mantiene el mismo formato de BPDU's como IEEE 802.1D, excepto que el campo de versión se establece en 2 para indicar RSTP, y el campo de banderas (flag) utiliza los 8 bits.

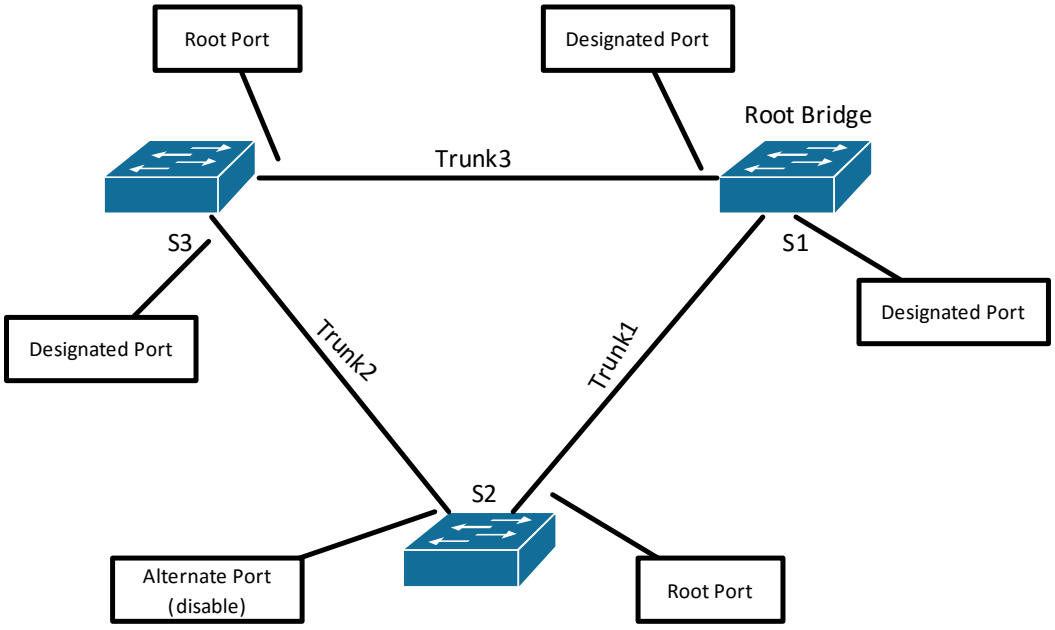


Figura 8. Estado de los puertos en RSTP

PortFast y BPDU de guardia.

Cuando un puerto es configurado con PortFast, un puerto en "blocking" pasa a "forwarding" inmediatamente. Los BPDU's de guardia pone el puerto en un estado de "error-disabled" en la recepción de un BPDU.

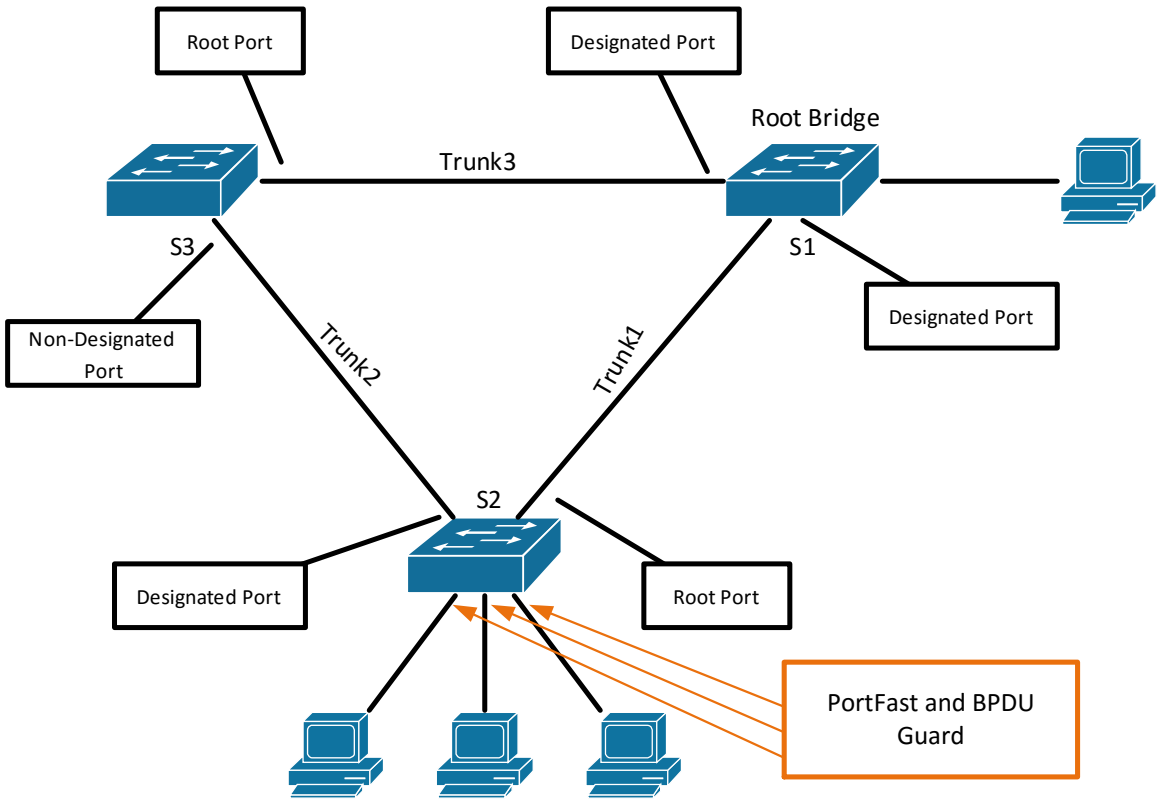


Figura 9. Puertos configurados con PortFast

Para la configuración del PorfFast y BPDU Guard en S2

```
s2(config)# interface Fast Ethernet ###
s2(config-if)# spanning-tree portfast
s2(config-if)# spanning-tree bpduguard enable
s2(config-if)# end
```

De esta manera configuramos el BPDU Guard y el PorfFast; cabe mencionar que en la línea de comandos anterior vemos al final de la primera línea “###”, esto significa que el puerto cambia según donde se encuentre un equipo conectado.

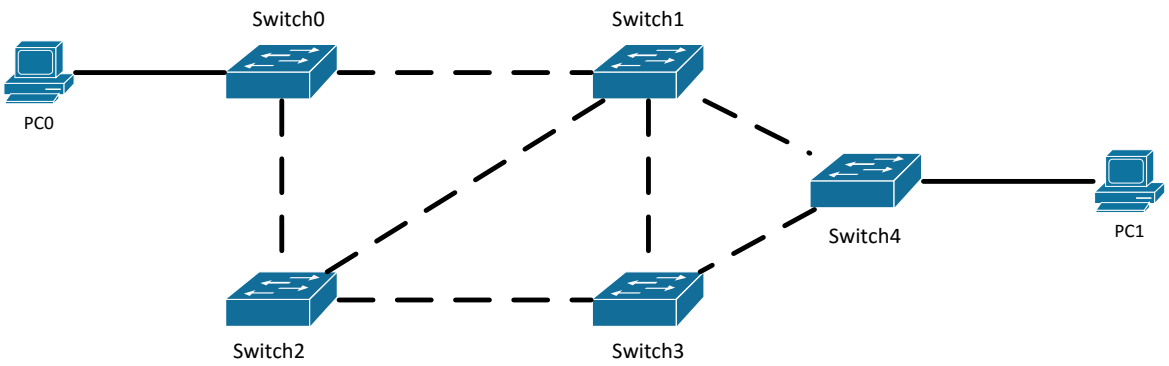
Referencias

www.cisco.com

W. Stallings, Data And Computer Communications, 8th ed. New Jersey, 2007.

STP: IEEE 802.1D

RSTP: IEEE 802.1w



Topología

Desarrollo

1. Dibuje el diagrama de red anotando las direcciones MAC y la prioridad de cada switch en la topología.
2. Haga el cálculo y llene el diagrama con la siguiente información:
    - Rol de cada switch (raíz, no raíz).
    - Rol de cada puerto (raíz, designado, bloqueado, etc).

3. Modifique la prioridad de Switch2 para que este se convierta en el switch raíz.
4. Observe los cambios que hace STP.
5. Modifique la velocidad de trasmisión entre el link que conecta a Switch1 y Switch2 a 10 Mbps.
6. Vuelva a dibujar la topología de red con los datos actualizado pedidos en el paso 2.
7. Configure PortFast donde crea necesario.
8. Configure BPDU Guard donde sea necesario.

Conclusiones

Durante el desarrollo de esta práctica, el alumno ha adquirido los conocimientos teóricos y prácticos del protocolo STP, entre los cuales podemos resaltar los siguientes:

- Ventajas y desventajas de tener redes de switches con caminos redundantes.
- Qué son y cómo se crean fenómenos como tormentas de broadcast y tramas duplicadas
- Algoritmo y funcionamiento de Spanning Tree Protocol
- Pasos a seguir para escoger el switch raíz
- Cómo formar el Bridge ID, el Extended Bridge ID y su uso.
- Protocolos similares y mejorados de STP.
- Configuración de STP en Packet Tracer.
- Sistema PVST+, acciones y estados de sus puertos.
- PortFast y BPDU Guard.

Cuestionario.

1. Se recibe el siguiente mensaje en un switch:

```
S2#sh spanning-tree
VLAN0001
       Spanning tree enabled protocol rstp
       Root ID    Priority    32769
                  Address     0001.42A7.A603
                  Cost        4
                  Port        26(GigabitEthernet1/2)
                  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
     [output cut]
```

   ¿Cuál de los siguientes enunciados son verdaderos? (Escoge dos.)

   A. El switch es un switch raíz.
   B. El switch es un no puente raiz.
   C. El puente raíz está a cuatro switches de distancia.
   D. El interruptor está ejecutando 802.1w.
   E. El switch está ejecutando STP PVST+.

2. ¿Cuál de los siguientes protocolos de capa 2 es usado para mantener una red libre de loops?
   A. VTP
   B. STP
   C. RIP
   D. CDP

3. ¿Qué enunciado describe una red spanning-tree que ha convergido?
   A. Todos los switches y puertos puente (bridge ports) están en el estado de reenvío.
   B. Todos los switches y puertos puente se asigna como puertos raíz o puertos designados.

C. Todos los switches y puertos puente están, ya sea en estado de reenvío o bloqueo.
D. Todos los switches y puertos puentes están ya sea bloqueados o en bucle.

4. ¿Qué trabajo realiza los BPDU de guardia (BPDU Guard)?
   A. Asegura que el puerto está recibiendo BPDUs de un switch de subida (upstream) correctamente.
   B. Asegura que el puerto no está recibiendo BPDUs de un switch de subida (upstream), sólo el Switch Raíz.
   C. Si un BPDU se recibe en un puerto BPDU de guardia, PortFast se utiliza para cerrar el puerto.
   D. Apaga un puerto si un BPDU en ese puerto.

5. ¿Qué comandos garantizaría el switch sea el puente raíz (root bridge) para la VLAN 30? (Escoge dos.)
   A. spanning-tree vlan 30 priority 0
   B. spanning-tree vlan 30 priority 16384
   C. spanning-tree vlan 30 root guarantee
   D. spanning-tree vlan 30 root primary

6. ¿Cuál de los siguientes estados pertenecen a STP? (escoge todos los que pertenezcan)
   A. Blocking (Bloqueado)
   B. Discarding (Descartado)
   C. Root (Raíz)
   D. Non-designated (No asignado)
   E. Forwarding (reenvío)
   F. Designated (Designado)

7. En STP, ¿cuál es la prioridad por defecto en un switch?
    A. 32,768
    B. 16,384
    C. 8,192
    D. 4,096

8. ¿Cuál de los siguientes enunciados muestra cómo STP escoge el puente raíz (root bridge)?
    A. El switch con la más alta prioridad.
    B. El switch con la mayor Brigde ID.
    C. El switch con la dirección IP más baja configurada.
    D. El switch con el Bridge ID más bajo.

9. Se te da la siguiente información, ¿qué hay que hacer para hacer el switch C el switch raíz?

    Name: SwitchA
    Priority: 32768
    MAC: 00-00-0c-00-b0-01

    Name: SwitchB
    Priority: 32768
    MAC: 00-50-0d-10-00-00

    Name: SwitchC
    Priority: 32768
    MAC: 0b-3f-27-00-93-3a

A. Incrementar prioridad
B. Bajar la prioridad
C. Cambiar la dirección MAC
D. Cambiar el nombre.

10. Se te da la siguiente información. ¿Cuál de los siguientes switches quedaría configurado como el switch raíz?

Name: SwitchA
Priority: 32768
MAC: 00-00-0c-00-b0-01

Name: SwitchB
Priority: 32768
MAC: 00-50-0d-10-00-00

Name: SwitchC
Priority: 32768
MAC: 0b-3f-27-00-93-3a

A. Switch A
B. Switch B
C. Switch C
D. Todos

Capítulo 5: Configuración de DHCP

Introducción

Este laboratorio corresponde al tema de Servicios Básicos de Red, se configurara un servidor DHCP (Dynamic Host Configuration Protocol) para que atienda las solicitudes de varios clientes. Un servidor DHCP es usado para proveer automáticamente direcciones IP a los clientes, evitando la necesidad de que el administrador de red tenga que configurar manualmente las direcciones en cada computadora.

Conceptos previos

DHCP: Protocolo de configuración dinámica de host, es un protocolo de red que proporciona un direccionamiento automático a los clientes además de otra información importante, como máscara de subred, dirección de Default Gateway y dirección de servidor DNS.

Métodos de asignación.

DHCP utiliza tres diferentes métodos de asignación de direcciones, los cuales se describen a continuación:

1. Asignación manual: El administrador de red asigna una dirección IPv4 pre-asignada al cliente, y DHCP comunica solo esta dirección IPv4 al dispositivo.
2. Asignación automática: DHCP asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo, seleccionándolo de un conjunto de direcciones disponibles. No hay arrendamiento.
3. Asignación dinámica: DHCP asigna dinámicamente, o renta una dirección IPv4 de un conjunto de direcciones por un periodo limitado de tiempo

elegido por el servidor, o hasta que el cliente ya no necesita la dirección, este es el más comúnmente utilizado.

Operación de DHCP.

DHCP utiliza distintos mensajes para poder establecer el servicio entre el cliente y el servidor, entre los más importantes están DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.

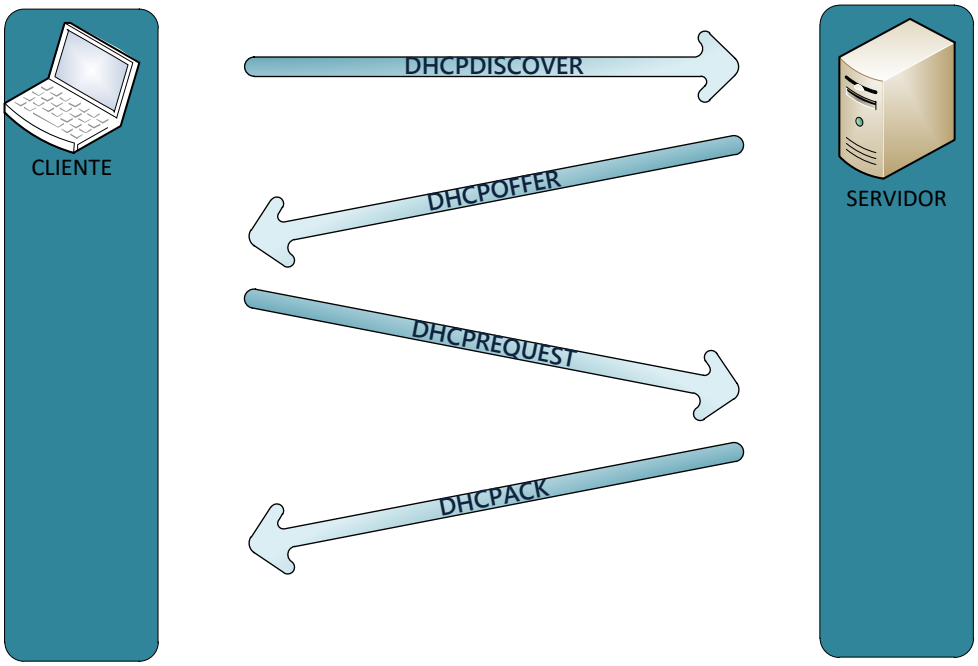


Figura 1. Mensajes entre cliente y servidor

En una primera fase el cliente que ha llegado a una nueva red y hace uso de este protocolo, envía un mensaje DHCPDISCOVER , con este mensaje está tratando de descubrir algún servidor que le pueda ofrecer el servicio en la LAN, este mensaje contiene los siguientes parámetros importantes:

- Dirección MAC Destino: FF: FF: FF: FF: FF: FF (Dirección de Broadcast).
- Dirección IP Destino: 255.255.255.255 (Dirección de Broadcast)
- Dirección MAC Fuente: Dirección del cliente.
- Dirección IP Fuente: 0.0.0.0 (Dirección reservada).
- Puerto UDP: 67.

En la segunda fase el servidor recibe el mensaje anterior y este responde con un mensaje DHCPOFFER, en donde el servidor oferta una dirección IP al cliente, para esto el servidor usa como direcciones destino las direcciones de Broadcast de la LAN donde está el cliente, debido a que en este punto el cliente a ´un no tiene una dirección IP, además utiliza el puerto UDP 68.

En la tercera fase el cliente debe responder con un mensaje DHCPREQUEST, donde hace la solicitud de una dirección IP en específico que el servidor le haya ofertado, esto lo hace usando los mismos parámetros de la primera fase.

En la cuarta fase el servidor responde con un mensaje DHCPACK el cual es una acuse de recibo donde el servidor notifica al cliente que la dirección IP es suya de esta manera a partir de este paso el cliente ya puede comenzar a usar la dirección IP y los parámetros que consiguió del servidor.

Configuración de un cliente DHCP en Windows.

Para poder configurar un cliente DHCP en un sistema operativo Windows los pasos a seguir son los siguientes.

1. Diríjase al panel de control y de clic sobre el apartado de Redes e Internet.

Figura 2. Visualización primera ventana para configuración de DHCP

2. Ahora de clic sobre el apartado de Centro de redes y recursos compartidos.

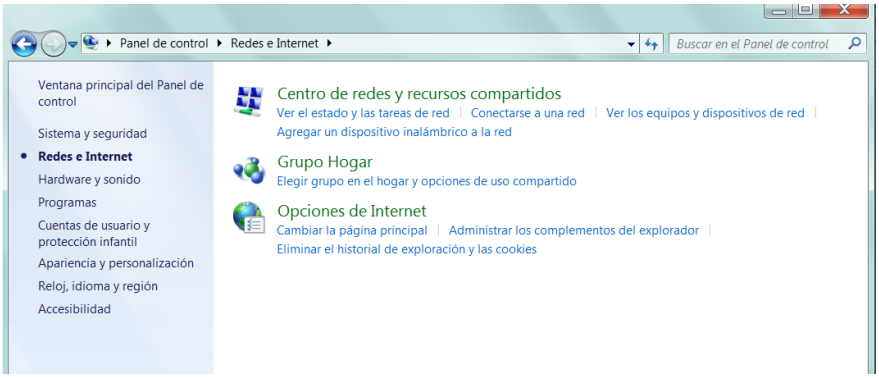


Figura 3. 2da ventana para configuración de DHCP

3. En la pestaña izquierda de clic sobre la opción “cambiar configuración del adaptador”.

Figura 4. Inicia la configuración

4. Elija el adaptador de red el cual desea configurar. En este caso configuraremos el inalámbrico. De clic izquierdo sobre él y elija el apartado propiedades.

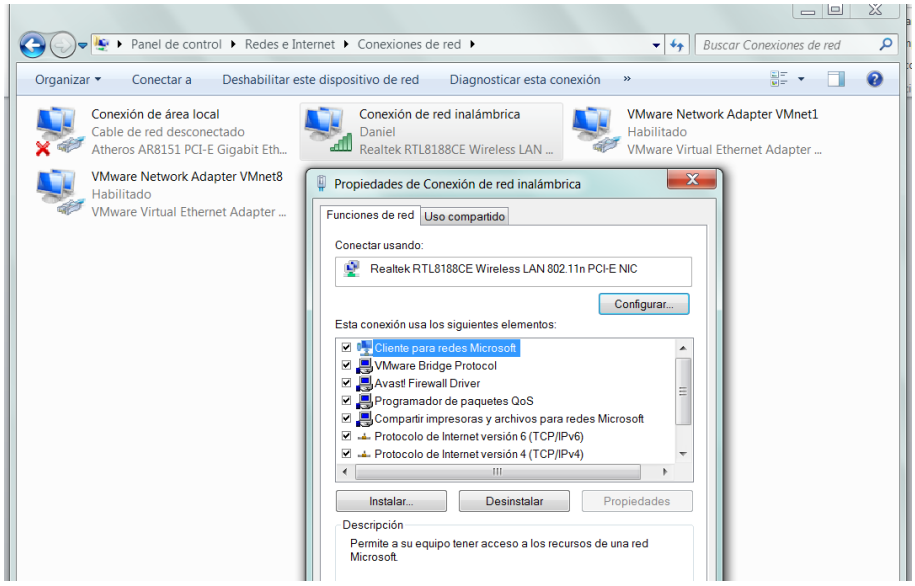


Figura 5. Configuración (inalámbrica) del DHCP

5. De clic sobre la parte que dice Protocolo de Internet versión 4 (TCP/IPv4) para marcar el protocolo, y después de clic sobre propiedades.

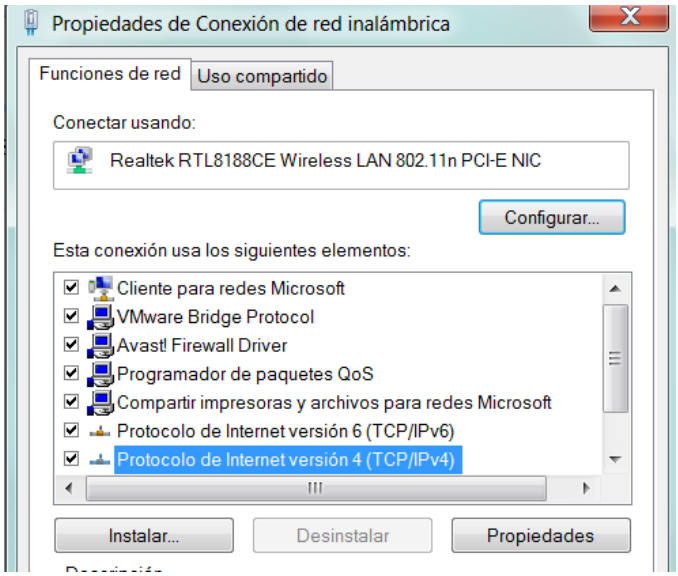


Figura 6. Configuración bajo IPv4

6. Finalmente aparecerá una nueva ventana donde debe marcar la opción “obtener una dirección IP automáticamente”.

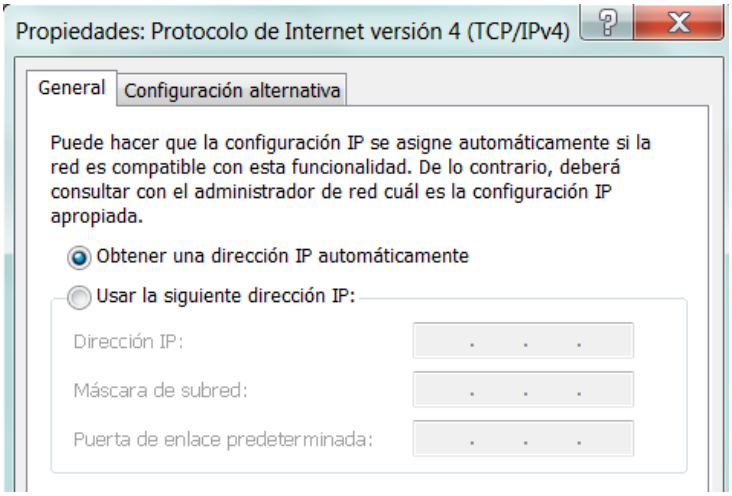


Figura 7. Paso final de la configuración de DHCP.

7. Puede verificar los resultados en línea de comando (cmd) usando el comando ipconfig/all.

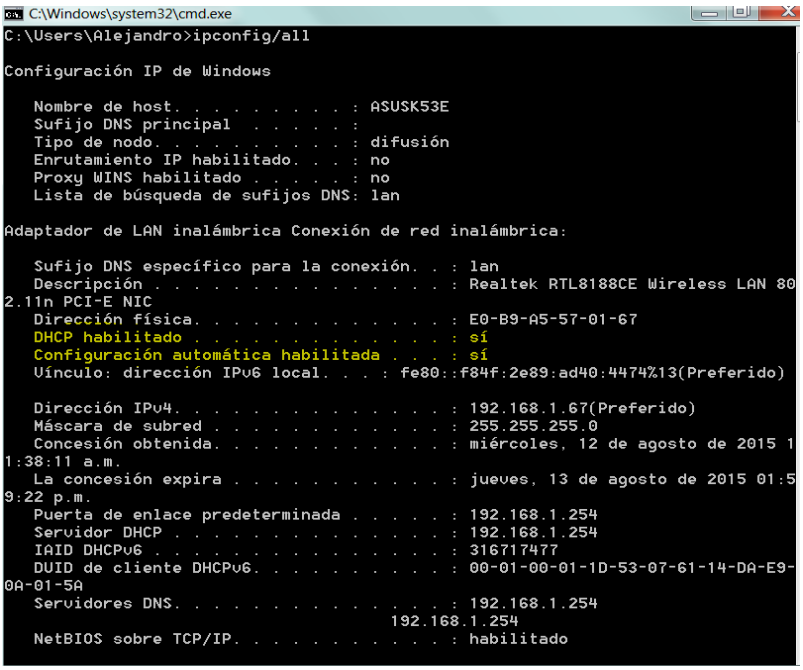


Figura 8. Comprobación de la correcta configuración de DHCP

Referencias

D. Comer, Internetworking with TCP IP. Englewood Cliffs, NJ: Prentice-Hall, 2000.

B. Forouzan, TCP/IP protocol suite. Boston: McGraw-Hill Higher Education, 2010.

W. Odom, Official cert guide Cisco CCENT, CCNA ICND1 100-101. Indianapolis, In.: Cisco Press, 2013.

T. Lammle, CCNA routing and switching study guide. Indianapolis, Ind.: Sybex Wiley, 2013.

RFC 3396.

RFC 2131.

RFC 4388.

COMANDO	DESCRIPCIÓN.
configure terminal	Habilita el modo EXEC privilegiado
default-router *[address]*	Especifica el Default Gateway para los clientes DHCP
domain-name *[domain]*	Especifica el dominio para los clientes DHCP
ip address dhcp	Configura un router como un cliente DHCP
ip dhcp excluded-address *[start-ip] [last-ip]*	Configura el rango de direcciones excluidas
ip dhcp pool *pool-name*	Crea un pool de direcciones IP
network *[ip address] [subnet mask]*	Define el rango de direcciones que serán arrendadas.
dns-server *[dns ip address]*	Define la dirección del servidor DNS.
lease *[days] [hours] [minutes]*	Define el tiempo de arrendamiento de las direcciones IP otorgadas, el tiempo por default es de 1 día.

ip helper-address *[ip address]*	Define la dirección del servidor DHCP al cual serán re direccionadas las peticiones DHCP.
show ip dhcp biding	Muestra una lista de la direcciones IP que han sido arrendadas.

Tabla 1. Tabla de comandos.

Comandos importantes

En esta sección vamos a mostrar algunas capturas de pantalla, de los comandos antes descritos, sugerimos que se ponga especial atención en el modo en que se ejecutan estos comandos (privilegiado, configuración global, etc.) así como en la aplicación de la sintaxis.

Comando: ip dhcp excluded-address 172.16.1.1 172.16.1.10

Excluye el rango de direcciones desde 172.16.1.1 hasta 172.16.1.10.

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#
```

Comando: ip dhcp pool Mypool

Crea un pool de direcciones llamado "Mypool". Note el cambio en el prompt del modo de configuración global al modo de configuración dhcp.

```
Router(config)#
Router(config)#ip dhcp pool Mypool
Router(dhcp-config)#
```

Comando: network 172.16.1.0 255.255.255.0

Define el rango de direcciones que se van a arrendar, en este caso todas las direcciones excepto las excluidas en la subred 172.16.1.0/24 serán arrendadas.

```
Router(dhcp-config)#
Router(dhcp-config)#network 172.16.1.0 255.255.255.0
Router(dhcp-config)#
```

Comando: default-router 172.16.254.254

Establece la dirección del Default Gateway que configurara a los clientes.

```
Router(dhcp-config)#default-router 172.16.254.254
Router(dhcp-config)#
```

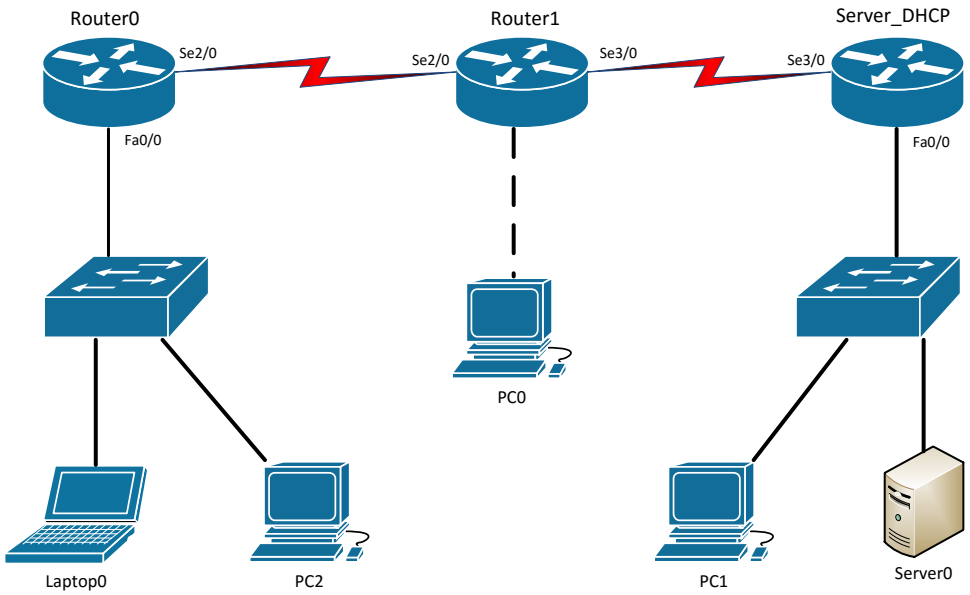
Comando: dns-server 172.16.2.254

Define la dirección del servidor DNS como la 172.16.2.254

```
Router(dhcp-config)#dns-server 172.16.2.254
Router(dhcp-config)#
Router(dhcp-config)#
```

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Router0	Fa0/0	172.16.1.254	255.255.255.0
	Se2/0	172.16.2.1	255.255.255.252
Router1	Fa0/0	172.16.3.254	255.255.255.0
	Se2/0	172.16.2.2	255.255.255.252
	Se3/0	172.16.4.1	255.255.255.252
Server_DHCP	Fa0/0	172.16.5.254	255.255.255.0
	Se3/0	172.16.4.2	255.255.255.252

Tabla 2. Tabla de direccionamiento.



Topología.

Desarrollo

Actividad 1

En esta actividad se configurara el router ***Server_DHCP*** para que responda a las peticiones DHCP de los clientes que están en una de las LAN directamente conectadas al router.

1. Configura el router para que no asigne las direcciones IP de la interfaz Fa0/0 y la Se3/0.
2. Configura un pool llamado **RED5** para la red asignada al puerto Fa0/0. Dicho pool debe de dar servicio DHCP a la red 172.16.5.0/24.
3. Configura el servidor para que establezca al puerto Fa0/0 como Default Gateway para la red 172.16.5.0/24.
4. Configura el servidor para que establezca un servidor DNS externo con dirección 10.10.10.10.

Actividad 2

En esta actividad se configuraran 2 nuevos pool en el router ***Server_DHCP***.

1. Excluye las direcciones de todos los puertos en ***Router0 y Router1***.
2. Configura un pool llamado **RED1** para que dé servicio a la red asignada al puerto Fa0/0 del router *Router0*.
3. Configura el servidor para que establezca al puerto Fa0/0 del *Router0* como Default Gateway para la red 172.16.1.0/24.
4. Configura el servidor para que establezca un servidor DNS externo con dirección 10.10.10.10.
5. Configura un pool llamado RED3 para que dé servicio a la red asignada al puerto Fa0/0 del router Router1.
6. Configura el servidor para que establezca al puerto Fa0/0 del Router1 como Default Gateway para la red 172.16.3.0/24.
7. Configura el servidor para que establezca un servidor DNS externo con dirección 10.10.10.10.

Actividad 3

En esta actividad se configuraran ***Router0*** y ***Router1***, para que redirijan las peticiones de los clientes en sus respectivas LAN hacia Server_DHCP.

1. ¿Qué comando o comandos son necesarios para que Router0 y Router1 redirijan las peticiones DHCP?
2. ¿En cuales interfaces en ambos routers es necesario aplicar el comando o comandos de la pregunta anterior?
3. Configura los routers ***Router0 y Router1*** para que redirijan las peticiones DHCP hacia Server_DHCP.

Actividad 4.

En esta actividad se configuraran todos los clientes en la topología para hacer peticiones DHCP al servidor, finalmente verificaremos los resultados de nuestra configuración.

1. Configure todos las PC para que obtengan una configuración IP a través de DHCP.
2. ¿Qué comando en un dispositivo cisco se tiene que ejecutar para que haga una petición DHCP?
3. ¿Qué comando de consola utilizaría para verificar la configuración IP en una PC? Verifique la configuración en todas las PC.

Conclusiones

En esta práctica se logró entender más claramente cuál es la importancia del protocolo DHCP, tener una visión general del funcionamiento y los mensajes que este protocolo utiliza es vital para poder ver su papel en una red, entre los conceptos más importantes que le sugerimos recordar se encuentran los siguientes.

- Cada computadora o dispositivo conectado a una red TCP/IP debe conocer su dirección IP, la dirección de su Default Gateway, la dirección de sus servidor DNS y la máscara de subred asignada para poder comunicarse con la red. DHCP es una aplicación cliente-servidor que envía esta información vital hacia los dispositivos.
- Existen diferentes tipos de mensajes DHCP que ayudan a su operación, entre los más importantes debemos destacar; DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK.
- Cuando un cliente DHCP y un servidor están en redes diferentes (diferentes LAN's), existen "agentes de retrasmisión" que son configurados para re direccionar las peticiones de los clientes hacia los servidores.
- Existen tres diferentes métodos de asignación de direcciones usados por DHCP, los cueles son; asignación manual, asignación automática y asignación dinámica.
- El método más usado es el de asignación dinámica, en el cual se renta una dirección IPv4 por un periodo de tiempo establecido o hasta que el cliente deje de usar esa dirección, este periodo de tiempo por default es de 1 día.

Cuestionario

1. En la figura que se muestra a continuación, ¿A que hace referencia la dirección 10.10.10.10?

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip helper-address 10.10.10.10
Router(config-if)#
```

   a. La dirección IP de la interfaz donde ingresa una petición DHCP.
   b. La dirección IP de la interfaz donde sale una petición DHCP.
   c. La dirección IP del siguiente dispositivo en la ruta hacia el servidor DHCP.
   d. La dirección IP del servidor DHCP.

2. ¿Cuál de los siguientes comandos utilizarías para establecer el Default Gateway al configurar el servicio de DHCP?

   a. Router(dhcp-config)#default-router 172.16.1.254
   b. Router(dhcp-config)#default-gateway 172.16.1.254
   c. Router(config)#default-router 172.16.1.254
   d. Router#default-router 172.16.1.254

3. Si tú deseas configurar el servicio de DHCP en tu router, para que otorgue direcciones de la subred 192.168.1.0/27 por un periodo de 5 días ¿Qué comandos usarías?

   a.
```
Router(config)#ip dhcp pool Mypool
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#lease 7 0 0
```

   b.
```
Router(config)#ip dhcp pool Mypool
Router(dhcp-config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#lease 7 0 0
```

c.
```
Router(config)#dhcp pool Mypool
Router(dhcp-config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#lease 7 0 0
```

d.
```
Router#ip dhcp pool Mypool
Router(config)#network 192.168.1.0 255.255.255.224
Router(dhcp-config)#lease 7 0 0
```

4. Escribe el nombre de los 4 mensajes principales de los cuales hace uso DHCP.

5. Para poder ver la lista de direcciones IP otorgadas a través de DHCP por un router Cisco ¿Qué comando usarías?

   a. show biding
   b. show dhcp biding
   c. show dhcp pool
   d. show dhcp address

6. ¿Qué direcciones IP (destino y fuente) usa un cliente DHCP, cuando se comunica por primera vez con el servidor DHCP?

   a. 127.0.0.1 y 254.254.254.0
   b. 172.16.1.254 y 255.255.255.255
   c. 0.0.0.0 y 254.254.253.254
   d. 0.0.0.0 y 255.255.255.255

7. ¿Cuál es el comando en cmd (línea de comandos en Windows) con el cual puede verificar la configuración ip de su dispositivo?

8. Al excluir direcciones IP para que DHCP no las otorgue. ¿Qué direcciones IP se recomienda excluir antes que nada?

   a. Broadcast y Red.
   b. 255.255.255.255 y 0.0.0.0
   c. Las direcciones usadas por las interfaces del router.
   d. Ninguna.

9. Si usted desea solo excluir la primera y última ***dirección asignable*** de la subred 172.16.1.0/24 ¿Qué comando usaría?

   a. `Router(config)#ip dhcp excluded-address 172.16.1.0 172.16.1.255`

   b. `Router(config)#ip dhcp excluded-address 172.16.1.0`
      `Router(config)#ip dhcp excluded-address 172.16.1.255`

   c. `Router(config)#ip dhcp excluded-address 172.16.1.1`
      `Router(config)#ip dhcp excluded-address 172.16.1.254`

   d. `Router#ip dhcp excluded-address 172.16.1.0`
      `Router#ip dhcp excluded-address 172.16.1.255`

10. Relaciona con una línea el propósito de cada mensaje DHCP con su respectivo mensaje.

DHCPOFFER	Lo usa el cliente para solicitar una dirección IP específica al servidor.
DHCPREQUEST	Lo usa el servidor para ofertar una dirección IP al cliente.
DHCPDISCOVER	Se utiliza como acuse de recibo.
DHCPACK	Lo usa el cliente para descubrir servidores DHCP que le puedan ofrecer el servicio.

Capítulo 6: Principios de Routing

Introducción

A continuación se verá el protocolo de enrutamiento de información (RIP por sus siglas en inglés); un protocolo basado en el vector distancia cuya métrica son los "saltos" y que dio origen a otros protocolos tales como OSPF. En la práctica se verán características de RIP v1 y RIP v2, ventajas, desventajas y similitudes entre estos protocolos.

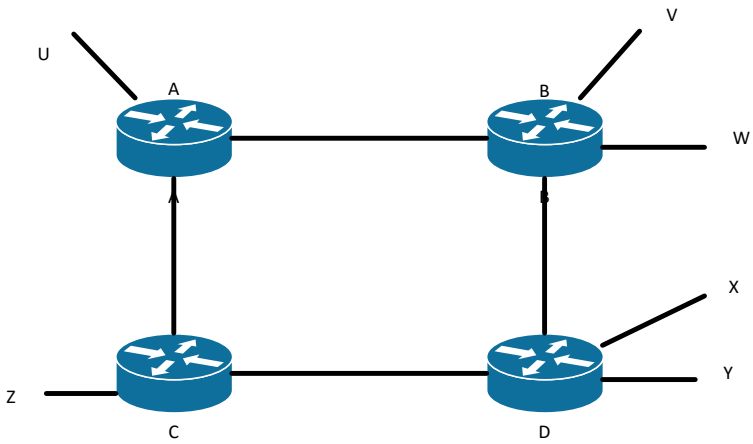
Conceptos previos

- **Vector Distancia**: éste algoritmo es *iterativo, asíncrono y distribuido*. Es *distribuido* en el sentido de que cada nodo recibe información de uno o más de sus vecinos directamente conectados, realiza un cálculo y luego distribuye los resultados de su cálculo de vuelta a sus vecinos. Es *iterativo* porque este proceso continúa hasta que no hay disponible más información para ser intercambiada entre los vecinos. (Además, el algoritmo también finaliza por sí mismo, es decir, no existe ninguna señal que indique que los cálculos deberían detenerse; simplemente se detienen.) Y es asíncrono, en el sentido de que no requiere que todos los nodos operen sincronizados entre sí.
- **Tablas de enrutamiento**: matrices donde cada fila es un vector de distancias y que también contiene el vector de cada uno de sus vecinos.
- **Distancia administrativa:** La distancia administrativa es la función que utilizan los routers para seleccionar el mejor trayecto cuando hay dos o más rutas hacia el mismo destino desde dos protocolos de enrutamiento diferentes. La distancia administrativa define la fiabilidad del protocolo de enrutamiento. Se establecen prioridades para cada protocolo de enrutamiento en orden de mayor a menor fiabilidad (credibilidad) con la

ayuda de un valor de distancia administrativa. La distancia administrativa por defecto de RIP es 120

RIP fue uno de los primeros protocolos de enrutamiento de Internet internos para los AS y todavía hoy es ampliamente utilizado. Sus orígenes están en la arquitectura XNS (Xerox Network Systems) a la que debe su nombre. La extensa implantación de RIP se ha debido en gran parte a su inclusión en 1982 en la versión BSD (Berkeley Software Distribution) de UNIX que soportaba TCP/IP. *La versión 1 de RIP está definida en [RFC 1058], y la versión 2 compatible hacia abajo está definida en [RFC 2453]*.

RIP es un protocolo de vector de distancias que opera de una forma muy parecida al protocolo DV (Vector Distancia) ideal. La versión de RIP especificada en el documento RFC 1058 utiliza como métrica de coste el recuento de saltos; es decir, cada enlace tiene un coste de 1. RIP utiliza el término salto (hop), que es el número de subredes que se atraviesan al seguir la ruta más corta desde el router de origen hasta la subred de destino, incluyendo esta última. La Figura 1 ilustra un sistema autónomo con seis subredes terminales. La tabla incluida en la figura indica el número de saltos desde el origen A a cada una de las subredes terminales.



Destino	Saltos
U	1
V	2
W	2
X	3
Y	3
z	2

Figura 1. Número de saltos desde el router de origen A a varias subredes.

RIP v1

Características de RIPv1

- Un protocolo de enrutamiento de vector de distancia (DV) classful (No envía las máscaras de subred durante las actualizaciones de enrutamiento).
- Métrica = conteo de saltos.
- Las rutas con un conteo de saltos superior a 15 no se pueden alcanzar.
- Se envía un broadcast de las actualizaciones cada 30 segundos.
- No soporta VLSM ni las subredes no contiguas
- Los mensajes RIP se encapsulan en un segmento UDP con los puertos de origen y de destino establecidos en 520.

Funcionamiento de RIP

RIP usa 2 tipos de mensajes:

- Mensaje de solicitud (Request)
  - Cada interfaz habilitada con RIP lo envía en el inicio.
  - Solicita a todos los vecinos con RIP habilitado que envíen la tabla de enrutamiento.

- Mensaje de respuesta (Response)
  - Mensaje enviado al router solicitante con la tabla de enrutamiento.

RIP v2

El formato de mensajes de RIP v2 es similar al de RIP v1, pero tiene 2 extensiones:

- La primera extensión es el campo de la máscara de subred (classfull, recordemos que en RIP v1 no existía y por eso es classless)
- La segunda es la adición de la dirección del siguiente salto.

Similitudes entre RIPv1 y RIPv2

- Uso de temporizadores para evitar bucles de enrutamiento
- Uso de horizonte dividido u horizonte dividido con actualización inversa
- Uso de updates disparados
- Número máximo de saltos: 15

Diferencia entre RIP v1 y RIP v2

- RIP v1
  - Protocolo de enrutamiento de vector de distancia classful
  - No proporciona soporte para subredes no contiguas
  - No proporciona soporte para VLSM
  - No envía las máscaras de subred durante las actualizaciones de enrutamiento
  - Se envían las actualizaciones de enrutamiento por medio de broadcasts

- RIP v2
  - Protocolo de enrutamiento de vector de distancia classless que es una mejora de las funciones de RIP v1
  - Se incluye la próxima dirección de salto en las actualizaciones
  - Las actualizaciones de enrutamiento se envían por medio de multicast
  - El uso de autenticación es opcional

A continuación, veremos una tabla resumen con las comparación de diversas características entre RIP v1 y v2.

Protocolo de enrutamiento	**RIP v1**	**RIP v2**
Vector de distancia	Si	Si
Protocolo de enrutamiento classless	No	Si
Uso de Hold-Down Timers	Si	Si

Uso de horizonte dividido u horizonte dividido con envenenamiento en reversa	Si	Si
Número máximode saltos = 15	Si	Si
Sumarización automática	Si	Si
Soporte para CIDR	No	Si
Soporte para VLSM	No	Si
Utiliza autenticación	No	Si

Tabla 1. Resumen de Protocolo RIP

Enrutamiento

El enrutamiento (o ruteo) es la forma en que los Routers conocen rutas y poder escoger la mejor de ellas para poder enviar paquetes entre distintas subredes.

Recordemos que los Routers son computadores especializados que usan los siguientes componentes para operar:

- Unidad de procesamiento central (CPU)
- Sistema Operativo (OS)
- Dispositivos de almacenamiento (RAM, ROM, NVRAM, Flash, hard drive)

Continuando, nos encontramos con que existen 2 tipos de ruteo:

- Ruteo Estático
  - Ventajas
    - Configurada manualmente.
    - Defina una ruta explícita entre dos dispositivos de red.
    - Debe actualizarse manualmente si cambia la topología.
    - Los beneficios incluyen la mejora de la seguridad y el control de los recursos.

- Dentro del control de recursos encontramos que las rutas estáticas usan menos ancho de banda que los protocolos de enrutamiento dinámico, no se usan ciclos de CPU para calcular y comunicar rutas.

- Desventajas
  - La configuración inicial y su mantención consumen tiempo.
  - Su configuración es propensa a errores, especialmente en redes grandes.
  - La intervención del administrador es necesaria para mantener la información actualizada ante cambios de rutas.
  - No tiene buen escalamiento ante redes en crecimiento, haciendo que su mantención sea dificil.
  - Necesita conocimiento de la red completa para una correcta implementación.

- Ruteo Dinámico
  - Ventajas
    - Automáticamente comparte información acerca de las redes remotas
    - Determina la mejor ruta a cada red y agrega esta información a sus tablas de enrutamiento
    - En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos gastos administrativos
    - Ayuda al administrador de red a gestionar procesos de configuración y mantenimiento de rutas estáticas, el que requiere mucho tiempo
  - Desventajas

- ❖ Dedicar parte de los recursos del router para el funcionamiento del protocolo, incluyendo el tiempo de CPU y el ancho de banda del enlace de red

Entre los diversos protocolos existentes, podemos denotar los siguientes que son protocolos de enrutamiento en IPv4:

- **EIGRP –** Enhanced Interior Gateway Routing Protocol
- **OSPF –** Open Shortest Path First
- **IS-IS –** Intermediate System-to-Intermediate System
- **RIP –** Routing Information Protocol

Referencias

RIP v1: [RFC 1058]

RIP v2: [RFC 2453]

J. Kurose and K. Ross, Computer networking. *Boston: Addison-Wesley, 2010.*

www.cisco.com

Anexos

Tabla de Distancias Administrativas de distintos protocolos.

Origen de la ruta	Valores de distancia predeterminados
Interfaz conectada	0
Ruta estática	1
Ruta de resumen del Protocolo de enrutamiento de	5

gateway interior mejorado (EIGRP)	
Protocolo de gateway de frontera externa (BGP)	20
EIGRP interno	90
IGRP	100
OSPF (Abrir trayecto más corto primero)	110
Sistema intermedio a sistema intermedio (IS-IS)	115
Protocolo de información de enrutamiento (RIP)	120
Protocolo de gateway exterior (EGP)	140
Enrutamiento a pedido (ODR)	160
EIGRP (zona desmilitarizada) externa	170
BGP interno	200
Desconocido*	255

* Si la distancia administrativa es 255, el router no reconoce esa ruta como fiable y no la instala en la tabla de enrutamiento.

Tabla 2. Distancias administrativas de diversos protocolos.

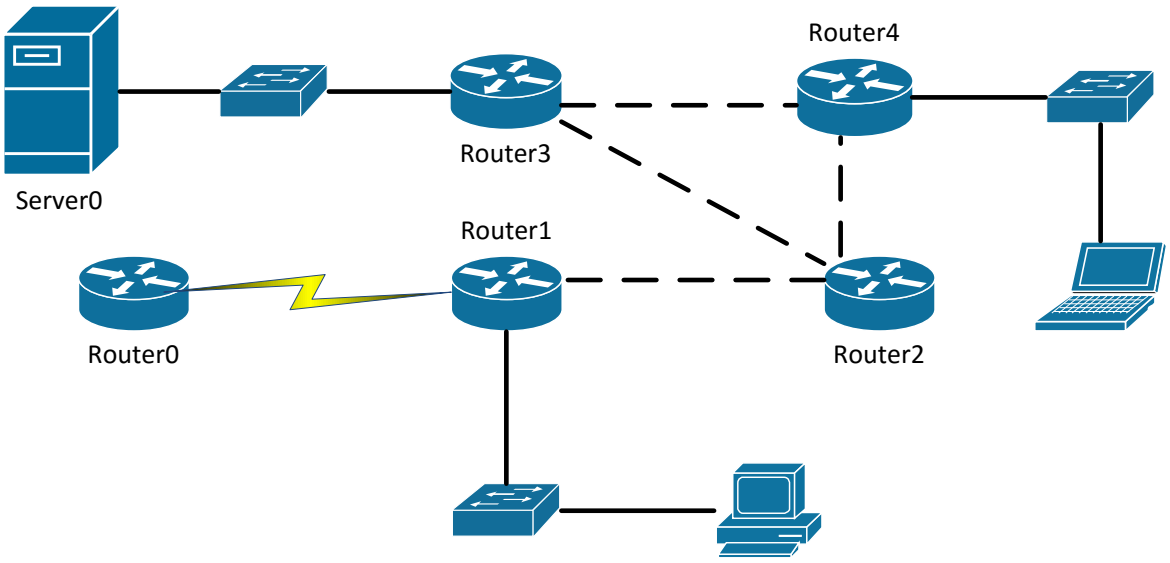
COMANDO	DESCRIPCIÓN.
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2	Podemos leerlo como: "Para llegar a la red 172.16.20.0, con la máscara 255.255.255.0, manda los todos paquetes a 172.16.10.2."
Router(config)#ip route 172.16.20.0 255.255.255.0 serial 0/0/0	Podemos leerlo como, "Para llegar a la red 172.16.20.0, con la máscara 255.255.255.0, manda todos los paquetes por el interfaz serial 0/0/0."
Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2 permanent	Configuración de una ruta estática permanente

Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2 [XXX]	Configuración de una ruta estática con distancia administrativa (sustitúyase [XXX] por algún valor de la tabla de distancias administrativas)
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.2	Manda todos los paquetes destinados a redes no existentes en la tabla de enrutamiento a 172.16.10.2.
Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0	Manda todos los paquetes destinados a redes no existentes en la tabla de enrutamiento al puerto serial 0/0/0.
Router#show ip route	Muestra la tabla de enrutamiento.

Tabla de comandos.

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Router0	*Serial 2/0*	*172.16.1.1*	*255.255.255.252 /30*
Router1	*FastEthernet 0/0*	*172.16.2.1*	*255.255.255.252 /30*
	Serial 2/0	*172.16.1.2*	*255.255.255.252 /30*
	FastEthernet 7/0	*172.16.6.254*	*255.255.255.0 /24*
Router2	*FastEthernet 0/0*	*172.16.2.2*	*255.255.255.252 /30*
	FastEthernet 1/0	*172.16.3.2*	*255.255.255.252 /30*
	FastEthernet 6/0	*172.16.4.2*	*255.255.255.252 /30*
Router3	*FastEthernet 0/0*	*172.16.5.1*	*255.255.255.252 /30*
	FastEthernet 6/0	*172.16.4.1*	*255.255.255.252 /30*
	FastEthernet 7/0	*172.16.8.254*	*255.255.255.0 /24*
Router4	*FastEthernet 0/0*	*172.16.5.2*	*255.255.255.252 /30*
	FastEthernet 1/0	*172.16.3.1*	*255.255.255.252 /30*
	FastEthernet 7/0	*172.16.7.254*	*255.255.255.0 /24*

Tabla de direccionamiento.



Topología.

Desarrollo

Actividad 1.

1. Configure una ruta estática adecuada en Router4 para que los mensajes de Laptop0 puedan llegar hacia Server0. Haga lo anterior indicando el siguiente salto en la ruta estática.
2. Observe la tabla de enrutamiento de Router4 ¿Cuál es la distancia administrativa de la ruta que acaba de configurar?
3. Haga un ping entre Laptop0 y Server0. ¿Describa que es lo que sucede al hacer el ping?
4. Configure una ruta estática en Router3 para comunicar las subredes 172.16.7.0/24 y 172.16.8.0/24. Haga lo anterior indicando la interfaz de salida en Router3.
5. Haga un ping entre Laptop0 y Server0. Observe en Router3 la ruta estática que acaba de configurar.

6. Modifique las distancias administrativas de las rutas estáticas, que configuro anteriormente, a un valor de 200.

Actividad 2.

1. Configure todos los routers en el diagrama con RIP v1 para que intercambien información de las rutas que disponen.
2. Observe la tabla de enrutamiento en cada router, y ponga especial atención a las rutas que aprendió a través de RIP. ¿Qué distancia administrativa observa?
3. Haga un ping entre PC0 y Server0 ¿Qué es lo que sucede y por qué?
4. Deshabilite RIP v1 de todos los routers donde lo configuro.

Actividad 3.

1. Pase al modo de simulación en Packet Tracer. Configure los filtros de tal manera que solo pueda ver mensajes RIP v2.
2. Configure todos los routers para que envíen y reciban información de ruteo a través de RIP v2.
3. Observe la estructura de los mensajes RIP v2 y anótela.
4. Haga pruebas de conectividad enviando un ping. Verifique que todos los dispositivos se pueden comunicar.
5. Configure a Router0 como router de último recurso, y propague esta ruta por defecto hacia los demás routers usando RIP v2.
6. Haga ping a la red 10.0.0.0 desde Server0 y observe hacia donde se dirige el tráfico.

Conclusiones

Podemos observar que entre las diversas habilidades adquiridas por el alumno en el desarrollo y culminación de esta práctica podemos destacar:

- Conocimiento de conceptos básicos como vector distancia, tablas de enrutamiento y distancia administrativa.
- Origen del protocolo RIP.
- Características y funcionamiento de RIP v1.
- Características y funcionamiento de RIP v2.
- Similitudes y diferencias entre ambos protocolos.
- Características, ventajas y desventajas del enrutamiento estático.
- Características, ventajas y desventajas del enrutamiento dinámico.
- Configuración de enrutamiento y protocolo RIP en el simulador Cisco Packet Tracer.

Cuestionario

1. ¿Cuál de los siguientes enunciados son verdaderos dado el siguiente comando? (Escoge dos.)

```
ip route  172.16.4.0 255.255.255.0 192.168.4.2
```

   A. El comando es usado para establecer una ruta estática.
   B. Se utiliza la distancia administrativa por defecto.
   C. El comando se utiliza para configurar la ruta por defecto.
   D. La máscara de la dirección de origen es 255.255.255.0.
   E. El comando se utiliza para establecer una red de conexión única.

2. ¿Qué afirmación es verdadera con respecto a los protocolos de enrutamiento sin clase (classless)? (Escoge dos.)

A. No se permite el uso de las redes no contiguas.
B. Se permite el uso de máscaras de subred de longitud variable.
C. RIPv1 es un protocolo de enrutamiento sin clase.
D. IGRP soporta enrutamiento sin clase dentro del mismo sistema autónomo.
E. RIPv2 soporta enrutamiento sin clase.

3. ¿Cuál de las siguientes NO es una ventaja de enrutamiento estático?

A. Menos sobrecarga al CPU del router
B. No uso de ancho de banda entre los routers
C. Añade seguridad
D. Recupera automáticamente de rutas perdidas

4. ¿Qué métrica utiliza RIPv2 para encontrar el mejor camino hacia una red remota?

A. Conteo de Saltos
B. MTU
C. Retraso interfaz acumulativa
D. Carga
E. Valor de ancho de banda

5. Si una tabla de enrutamiento estática tiene, un RIP, y una ruta EIGRP a la misma red, ¿qué ruta se utilizará para enrutar paquetes por defecto?

A. Cualquier ruta disponible.
B. La ruta por RIP.
C. La ruta estática.
D. La ruta EIGRP.

6. ¿Cuál de las siguientes es una ventaja de enrutamiento estático?

    A. Menos sobrecarga al CPU del router
    B. No uso de ancho de banda entre los routers
    C. Añade seguridad
    D. Recupera automáticamente rutas perdidas

7. En el siguiente comando, ¿qué significa el 150 al final del comando?

```
Router(config)#ip route 172.16.3.0 255.255.255.0 192.168.2.4 150
```

    A. Métrica.
    B. La distancia administrativa.
    C. Contador de saltos.
    D. Costo.

8. Si varios routers están ejecutando el protocolo de enrutamiento RIP, ¿cuál es el resultado de escribir este comando?

```
ip route 0.0.0.0 0.0.0.0 55.12.4.38
```

    A. Si no hay una red de destino coincidente en la tabla de enrutamiento, el router envía el paquete a 55.12.4.38.
    B. Se han configurado RIP para difundir el conocimiento de la red 55.12.4.38.
    C. Que ha configurado una ruta conectada para reenviar el tráfico a 55.12.4.38.
    D. Ha configurado Gateway de último recurso para que, si hay un paquete destinado a la red 55.0.0.0, a continuación, el router se transmita en 0.0.0.0.

9. ¿Qué protocolo de enrutamiento tiene una distancia administrativa de 120?

    A. Estático
    B. Conectado
    C. RIP
    D. OSPF

10. ¿Cuál de los siguientes enunciados son verdaderos hablando de los protocolos de enrutamiento por vector distancia? (Seleccione dos).

    A. Los routers de la tabla de enrutamiento comparten con todos los demás routers en la red.
    B. Los routers comparten tabla de enrutamiento con enrutadores vecinos.
    C. Las actualizaciones sólo se envían cada 60 segundos.
    D. Mantiene varias tablas en la memoria - una para los routers vecinos, uno para almacenar toda la topología, y la tabla final es la tabla de enrutamiento.
    E. Envía toda la tabla de enrutamiento como una actualización

Capítulo 7: Fundamentos de IPv6

Introducción

En la siguiente práctica se abarcarán fundamentos para el manejo de IPv6. Como sabemos, IPv6 nació por el mal uso de IPv4; este mal uso hizo que las direcciones IPv4 se agotaran (además de la creciente demanda de aparatos con conexión a internet y que cada uno necesita una IP propia); de esta manera, se busca que al meter más campos para el direccionamiento, en conjunto de un formato hexadecimal y un uso adecuado, los problemas vividos con IPv4 no se repitan.

Conceptos previos

Un poco de Historia

A principios de la década de 1990, el *Internet Engineering Task Force* comenzó a desarrollar un sucesor para el protocolo IPv4. La principal motivación de esta iniciativa fue que se dieron cuenta de que el espacio de direcciones IP de 32 bits estaba comenzando a agotarse, a causa de las nuevas subredes y nodos IP que estaban conectándose a Internet (a los que se les estaban asignando direcciones IP únicas) a una velocidad sobrecogedora. Para responder a esta necesidad de un espacio de direcciones IP más grande, se desarrolló un nuevo protocolo IP, el protocolo IPv6. Los diseñadores de IPv6 también vieron aquí la oportunidad de ajustar y aumentar otros aspectos de IPv4, basándose en la experiencia acumulada sobre el funcionamiento de IPv4.

Aunque estas estimaciones (de alrededor de 1996) y datos sugerían que quedaba bastante tiempo para que el espacio de direcciones de IPv4 se agotara, se dieron cuenta de que se necesitaría un tiempo considerable para implantar una nueva tecnología a tan gran escala, y por eso se comenzó a trabajar en IPng (Next

Generation IP, IP de siguiente generación). El resultado de este esfuerzo fue la especificación de la versión 6 de IP (IPv6); una pregunta que se plantea a menudo es qué ocurrió con IPv5. Inicialmente se pensó que el protocolo ST-2 se convertiría en IPv5, pero ST-2 fue descartado más tarde en favor del protocolo RSVP.

Descripción general de las direcciones IPv6

Las direcciones IPv6 se asignan a interfaces en lugar de a nodos, teniendo en cuenta que en un nodo puede haber más de una interfaz. Asimismo, se puede asignar más de una dirección IPv6 a una interfaz. Además, a diferencia de IPv4 donde representábamos la dirección con números solo con números decimales; en IPv6 podemos representarlas de 2 maneras, en formato decimal y/o formato decimal.

IPv6 abarca tres clases de direcciones:

- ***Unicast.*** Se utiliza únicamente para identificar una interface de un nodo IPv6. Un paquete enviado a una dirección unicast es entregado a la interface identificada por esa dirección.

- ***Multicast.*** Se utiliza para identificar a un grupo de interfaces IPv6. Un paquete enviado a una dirección multicast es procesado por todos los miembros del grupo multicast.

- ***Anycast.*** Se asigna a múltiples interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección anycast es entregado a una de estas interfaces, usualmente la más cercana.

Cada uno de los tres tipos se subdivide en direcciones diseñadas para resolver casos específicos de direccionamiento IP, los cuales a continuación se presentan y describen.

Unicast agrupa los siguientes tipos:

- ***Enlace Local (Link-Local)***: Direcciones desde FE80::/10 hasta FEBF::/10
- ***Unique Local***: Direcciones desde FC00::/7 hasta FDFF::/7
- ***Global Unicast***: Direcciones desde 2000::/3 hasta 3FFF::/3
- ***Loopback***: Direcciones ::1/128
- ***Sin-Especificar (Unspecified)***: Direcciones de la forma ::/128
- ***Compatible con IPv4 (Embedded IPv4)***: Direcciones con la forma ::/80

Multicast agrupa:

- ***Asignada (Assigned):*** Abarca direcciones de la forma FF00::/8
- ***Nodo Solicitado (Solicited Node):*** Con direcciones de la forma FF02::1:FF00:0000/104

Anycast agrupa:

- ***Agregable Global (Aggregatable Global).***
- ***Sitio Local (Site Local).***
- ***Enlace Local (Link Local).***

Importante: En IPv6 no existe el Broadcast.

Partes de una dirección IPv6

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

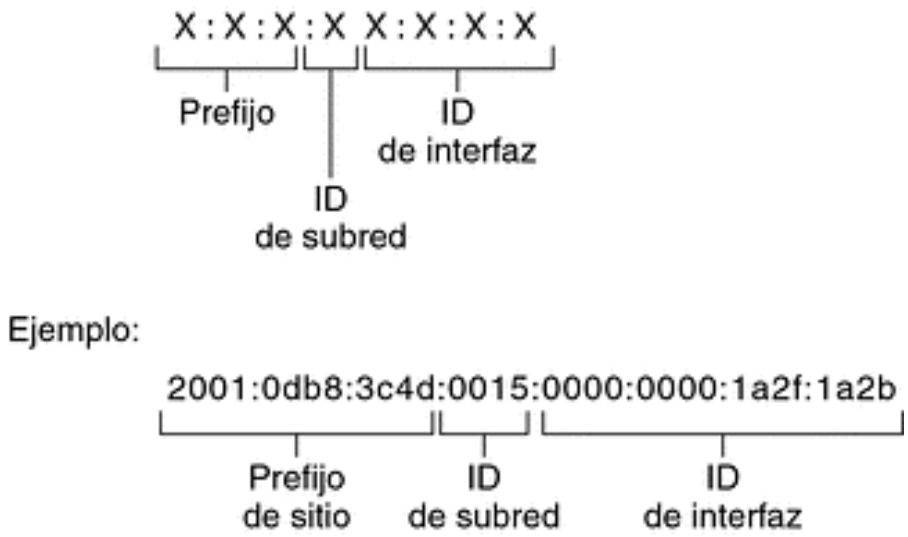


Figura 1: Formato básico de las direcciones IPv6

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

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

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

Examine de nuevo la dirección de la figura Figura 1:

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

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, `2001:0db8:3c4d`, contienen el prefijo de sitio y representan la

topología pública. Los siguientes 16 bits, `0015`, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, `0000:0000:1a2f:1a2b`, contienen el ID de interfaz.

Abreviación de direcciones IPv6

- Regla 1: Ceros Iniciales

Los ceros iniciales en cualquier segmento de 16 bits se pueden omitir.

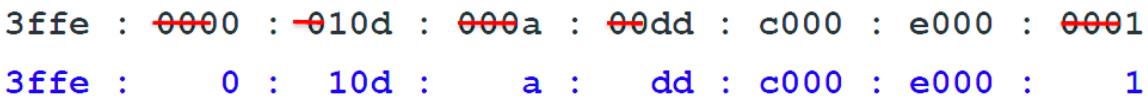


Figura 2: Ejemplo de aplicación Regla 1 IPv6

- Regla 2: Dobles puntos (::)

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenados con ceros o que sólo contienen ceros.

La arquitectura de direcciones IPv6 permite utilizar la notación de dos puntos consecutivos (: :) para representar campos contiguos de 16 bits de ceros. Por ejemplo, la dirección IPv6 de la Figura 1 se puede abreviar reemplazando los dos campos contiguos de ceros del ID de interfaz por dos puntos. La dirección resultante es:

`2001:0db8:3c4d:0015::1a2f:1a2b.`

Otros campos de ceros pueden representarse como un único 0. Asimismo, puede omitir los ceros que aparezcan al inicio de un campo, como por ejemplo cambiar 0db8 por db8 (Regla 1).

Así pues, la dirección:

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

se puede abreviar en:

2001:db8:3c4d:15::1a2f:1a2b.

La notación de los dos puntos consecutivos se puede emplear para reemplazar cualquier campo contiguo de ceros de la dirección IPv6.

Por ejemplo, la dirección IPv6:

2001:0db8:3c4d:0015:0000:d234::3eee:0000

se puede contraer en

2001:db8:3c4d:15:0:d234:3eee::

Importante: Es posible sustituir, una única vez, una secuencia de 0's contiguos, en uno o más segmentos de 16-bits, por doble dos puntos "::". Sólo se puede aplicar esta regla una única vez, para evitar ambigüedades

2001 : 0d02 : 0000 : 0000 : 0014 : 0000 : 0000 : 0095

2001 : d02 :: 14 : 0 : 0 : 95

o

2001 : d02 : 0 : 0 : 14 :: 95

Figura 3: Ejemplos de aplicación Regla 2 IPv6

En la figura anterior podemos denotar la dirección `2001:0d02:0000:0000:0014:0000:0000:0095` y podemos apreciar que cualquiera de las opciones que se nos muestra con válidas; en la figura 4, apreciamos las ambigüedades que se pueden dar por un mal uso de esta regla.

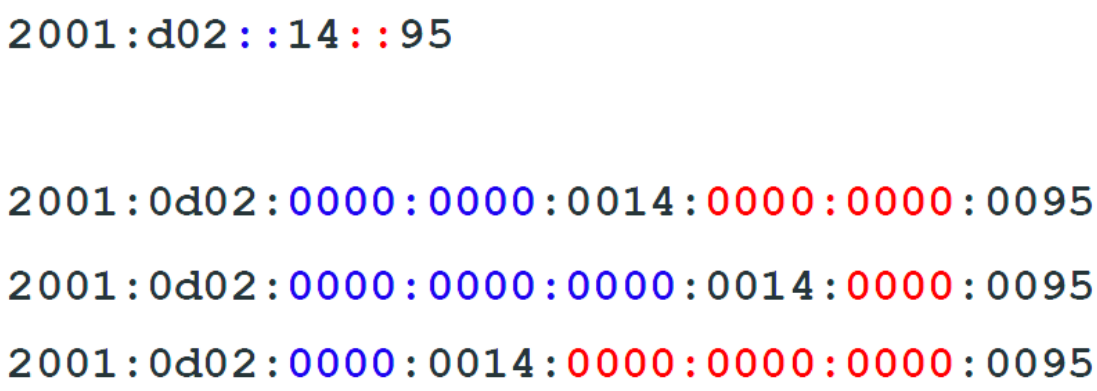


Figura 4: Ejemplo de ambigüedades por mal uso de la Regla 2 IPv6

Prefijos de IPv6

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6. Los prefijos de IPv6 tienen el formato siguiente: *prefijo/tamaño en bits*

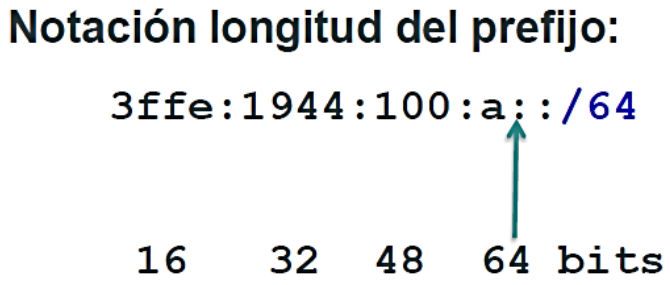


Figura 5: Ejemplo de prefijo en IPv6

El tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits.

El **prefijo de sitio** de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 `2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48` se ubica en los 48 bits que hay más a la izquierda, `2001:db8:3c4d`.

Direcciones IPv6 compatibles con IPv4

Estas son direcciones especiales asignadas a dispositivos son soporte para IPv6, llamados dispositivos de "doble pila" que hablan tanto IPv4 como IPv6. Ellas tienen los 16 bits del centro con un valor de cero, por lo que comienzan con una cadena de 96 ceros, seguida de la dirección IPv4. Un ejemplo de dicha dirección, mostrada en la siguiente figura, sería `0:0:0:0:0:0:101:45:75:219` en notación mixta, o más brevemente, `::101:45:75:219`.

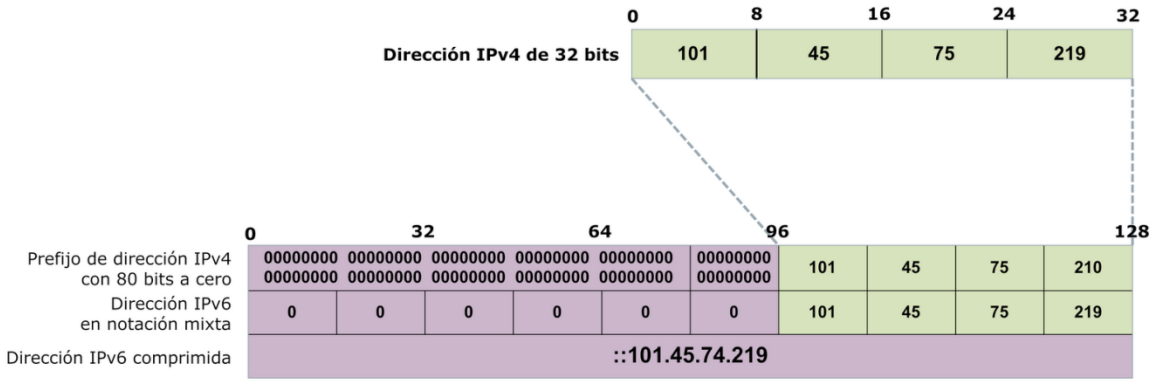


Figura 6. Dirección IPv6 compatible con IPv4

Proceso de la EUI 64 Modificado

Recordemos que la EUI-64 toma la MAC del dispositivo; los 48 bits de la MAC del host (los primeros 24 bits del OUI y los segundos 24 bits del identificador del dispositivo)

1. Esos 48 bits los divide en dos partes de 24 bits cada una.
2. La Interface id se construye de la siguiente manera: Los primeros 24 bits de la MAC seguidos de 16 bits propios de EUI-64, estos 16 bits siempre serán FF - FE, y los segundos 24 bits de la MAC.
3. Se le invierte el séptimo bit (si es cero, a 1 y viceversa), este séptimo bit es correspondiente al OUI.
4. Finalmente, la dirección resultante es nuestro Interface ID con el formato EUI-64 Modificado.

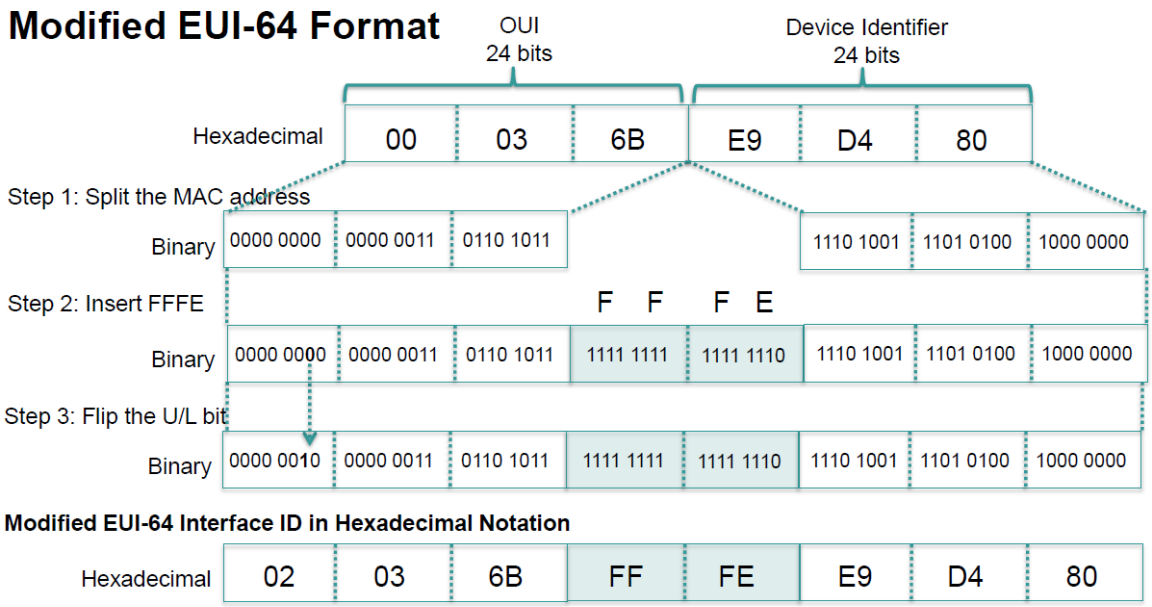


Figura 7. Explicación gráfica del formato EUI 64 Modificado (para IPv6).

Stateless Address Autoconfiguration (SLAAC)

El Stateless Address Autoconfiguration (SLAAC) es un método automático de obtener la dirección global de unicast

Entre las características del SLAAC tenemos:

- No es necesario disponer de servidor DHCP
- El router sólo informa el prefijo de red y el default gateway
- La computadora asigna el interface id utilizando su MAC address

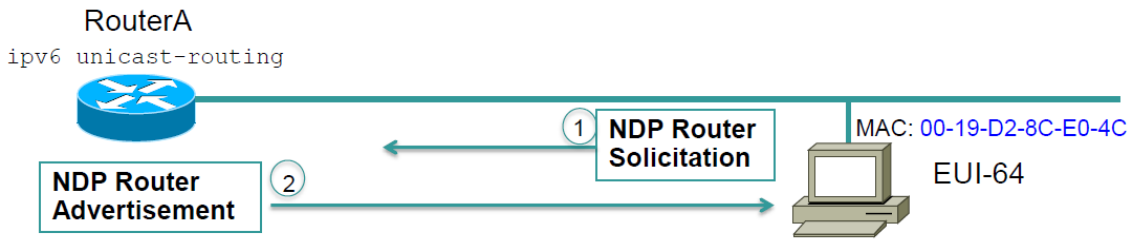


Figura 8. Proceso SLAAC.

Referencias.

https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/

www.cisco.com

IPng [RFC 1752]

IPv6 [RFC 2460]

J. Kurose and K. Ross, *Computer networking*. Boston: Pearson/Addison Wesley, 2008.

Desarrollo

Ejercicios a realizar.

Optimización direcciones IPv6

- 2001:1111:0000:0000:1111:2222:1111:A1A1
- 3001:0000:0000:0000:0000:0000:0000:1111
- 3001:0000:0000:0000:1111:0000:0000:1111
- FF02:0000:0000:0000:0000:0001:FF00:0001

Ejercicios EUI-64

- MAC: 39-A7-94-CB-D0
- MAC: FC-99-47-75-CE-E0
- MAC: 48-1E-C9-21-85-0C

Conclusiones

Durante la lectura y realización de ejercicios en esta práctica, el alumno comprendió:

- El concepto de IPv6.
- La necesidad de creación de IPv6.
- Tipos de direcciones en IPv6.
- Conformación de una dirección en IPv6.
- Reglas de Optimización de direcciones de IPv6.
- Errores al aplicar la Regla 2 de Optimización.
- Uso adecuado de prefijos en IPv6 (análogo a la máscara en IPv4).
- Realización del Interface ID por medio del EUI-64 Modificado
- Proceso de Autoconfiguración SLAAC

Cuestionario

1. ¿Cuál de las siguientes afirmaciones sobre las direcciones IPv6 son verdaderas? (Escoge dos.)

    A. Se requieren ceros a la izquierda.
    B. Los dobles dos puntos (::) se utilizan para representar los campos hexadecimales sucesivas de ceros.
    C. Los dobles dos puntos (::) se utilizan para separar los campos.
    D. Una interfaz única tendrá varias direcciones IPv6 de diferentes tipos.

2. ¿Qué dos afirmaciones acerca de las direcciones IPv4 e IPv6 son verdaderas? (Escoge dos.)

    A. Una dirección IPv6 es de 32 bits de largo, representado en hexadecimal.
    B. Una dirección IPv6 es de 128 bits de longitud, representado en decimal.
    C. Una dirección IPv4 es de 32 bits de largo, representado en decimal.
    D. Una dirección de IPv6 es de 128 bits de longitud, representado en hexadecimal.

3. ¿Cuál de las siguientes descripciones acerca de IPv6 es la correcta?

    A. Las direcciones no son jerárquicas y se asignan al azar.
    B. Los Broadcast han sido eliminados y reemplazados con multicast.
    C. Hay 2,7 billones de direcciones.
    D. Una interfaz sólo se puede configurar con una dirección IPv6.

4. ¿Cuántos bits hay en una dirección IPv6?

    A. 24

B. 4
C. 3
D. 16
E. 32
F. 128

5. ¿Cuál de las siguientes afirmaciones son verdaderas en la representación de direcciones IPv6? (Escoge dos.)

   A. Los primeros 64 bits representan el ID de interfaz creado dinámicamente.
   B. Una única interfaz se puede asignar múltiples direcciones IPv6 de cualquier tipo.
   C. Cada interfaz IPv6 contiene al menos una dirección de bucle de retorno.
   D. Los ceros a la izquierda en un campo hexadecimal IPv6 de 16 bits son obligatorios.

6. ¿Cuál de los siguientes direcciones IPv6 es el equivalente de a 127.0.0.1?
   A. 127 ::
   B. 127 :: 1
   C. :: 1
   D. FE80 ::

7. ¿Cuál de las siguientes afirmaciones son ciertas acerca de las direcciones unicast IPv6? (Seleccione dos).

   A. Una dirección de enlace local comienza con FE00.
   B. Una dirección global comienza con 2000.
   C. La dirección de bucle de retorno (loopback) es de 127 :: 1.

D. Cuando se asigna una interfaz una dirección global, que sólo se permite una dirección de IPv6.
E. La dirección de bucle de retorno (loopback) es :: 1.

8. ¿Cuáles son algunos de los beneficios de la transición de IPv4 a IPv6? (Seleccione dos).

A. IPSec es opcional.
B. No hay mensajes de broadcast.
C. El esquema de dirección de 64 bits.
D. Las contraseñas de Telnet son encriptadas.
E. Configuración automática.

9. Utilizando las 2 reglas de optimización de direcciones IPv6, optimice las siguientes direcciones.
   a) 0000:0000:0000:0000:0000:0000:0000:0000
   b) 0000:0000:1000:0000:0000:0000:0000:0001
   c) 2001:0410:0000:1234:FE00:1000:0050:45FF
   d) 3FFA:0B00:00C1:0001:0000:128C:AB34:0002

Capítulo 8: Direccionamiento IPv6

Introducción

En la siguiente práctica partiremos de los conocimientos ya adquiridos del direccionamiento en IPv4 pero extendiéndolo para IPv6; como sabemos el protocolo IPv4 es el protocolo de direccionamiento más utilizado en la implementación, sin embargo, un mal uso de él provocó la necesidad del nacimiento del protocolo IPv6, aquí recordaremos los fundamentos de las direcciones en IPv6 para establecer las bases de la creación de redes (subneteo) en IPv6.

Conceptos previos

Conceptos Generales de IPv6

IPv6 ofrece un espacio de direccionamiento mucho mayor al de IPv4, estamos hablando de 2^128 que eso nos daría alrededor de 340 sextillones de direcciones utilizables. IPv6 satisface las demandas actuales y futuras de direccionamiento IP. Ejemplo de una dirección IPv6:

2001:BBBB:0000:1118:0000:0000:0000:0A00

Las direcciones IPv6 se expresan en formato Hexadecimal separadas por dos puntos. Estas direcciones están compuestas por 8 hextetos, un hexteto es un bloque de 16 bits. Para expresar una dirección IPv6 se puede hacer usando letras mayúsculas o minúsculas. La dirección anterior se puede dividir como sigue:

2001 ----> Primer Hexteto

BBBB ----> Segundo Hexteto

0000 ----> Tercer Hexteto

....

0A00 ----> Octavo Hexteto

En total 8X16= 128 bits

Recordando un poco el sistema Hexadecimal.

El sistema Hexadecimal está compuesto por 16 elementos, desde el 0 hasta F. Para formar un número en hexadecimal sólo requerimos de 4 bits, diferente al sistema binario donde se necesita mínimo 8 bits. Observe la siguiente tabla:

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Tabla 1. Números en decimal del 0 al 15 y su equivalente en binario y hexadecimal

Los números decimales del 0 al 9 se expresan de esa misma forma en Hexadecimal, pero del número 10 al 15 se expresan con letras.

Cómo expresar direcciones IPv6

- Regla 1: Al momento de expresar cualquier dirección IPv6 tenga en cuenta que los 0s a la izquierda pueden omitirse. Ejemplo:

2001:00CB:0001:1108:00BA:0000:0000:0A00

Puede expresarse como sigue:

2001:CB:1:1108:BA:0000:0000:A00.

- Regla 2: Los puntos dobles (::) pueden sustituir un conjunto de hextetos compuestos por ceros consecutivos. Ejemplo:

2001:CB:1:1108:BA:0000:0000:A00

Se expresa como sigue:

2001:CB:1:1108:BA::A00.

Recuerde que solo se puede usar esta última regla solo una vez, para evitar ambigüedades.

Direcciones Unicast

Hay dos tipos de direcciones Unicast: **Global Unicast y Link Local.**

- **Direcciones Global Unicast:** estas direcciones son parecidas a las direcciones públicas IPv4. Se pueden enrutar hacia el internet y son asignadas por un ISP.

- **Direcciones Link Local:** estas direcciones son usadas por los dispositivos para comunicarse con otros que se encuentran en el mismo segmento (subred). No se pueden enrutar fuera de un determino segmento. Estas direcciones se encuentran en el rango FE80::/10.

Los protocolos de enrutamiento utilizan la dirección Link local (enlace local) para establecer adyacencias con sus respectivos vecinos.

Es una buena práctica modificar la dirección Link Local del Router, y configurar una dirección más fácil de documentar, Ya que los últimos 64 bits de una dirección Link Local son tomados de la MAC address de la interface Ethernet, entonces tendríamos una Link Local diferente para cada interfaces del Router; pero si la modificamos podemos tener un sola link local por Router.

Estructura de una Dirección Unicast

Una dirección Unicast Global tiene 3 elementos:

- **Prefijo de enrutamiento Global:** es la porción de red asignada por el proveedor de servicio al cliente. Esta parte está compuesta por los primeros 48 bits.

- **Identificador de Subred:** Son los Bits usados por el cliente para subnetting. Compuesto por 16 bits.

- **Identificador del Hosts:** Identifica a un dispositivo. Compuesto por los últimos 64 bits.

Ejemplo:

2001:CB00:1000:BA23:0000:0000:A00:AAAA

-La parte en Rojo representa el prefijo /48 asignado por el ISP a un cliente.
-Parte Azul: 16 bits usados por el cliente para subnetear.
-Parte negra: identificador del host.

Esto quiero decir que el prefijo /64 (48+16) corresponde a los bits de red y los últimos 64 bits corresponden al host.

Subnetting IPv6

Para realizar el subnetting IPv6 usamos los 16 bits del campo de subred. Tome en cuenta que el RFC 4291[7] recomienda que las subredes cuenten con una máscara /64. Ejemplo:

Una compañía nacional cuenta con Oficinas en 20 ciudades importantes de ese país. En cada Ciudad hay 10 oficinas. Cada oficina no tiene más de 11 departamentos.
Dirección asignada por el proveedor de servicios: 2001:ABCD:CAFE::/48

Resumen:

- 20 ciudades
- 10 oficinas por ciudad
- 11 departamentos por oficina

[7] RFC 4291 hace referencia al documento que habla sobre la arquitectura de las direcciones en IPv6.

1. Prefijo para cada Ciudad (20 ciudades)

Para 20 ciudades necesitamos 5 bits, 2^5=32 ciudades. Sólo nos interesa prefijos para 20 ciudades, las demás quedan para futuro crecimiento.

Recuerden que se realiza el subntetting con los bits del **cuarto hexteto** (parte azul en el ejemplo anterior).

Cuarto Hexteto				
	Primer dígito (4 bits)	**Segundo dígito (4 bits)**	Tercer dígito (4 bits)	Cuarto dígito (4 bits)
Bits del dígito	**0 0 0 0**	**0 0 0 0**	0 0 0 0	0 0 0 0
Bits que serán usados (*)	*** * * ***	*** 0 0 0**	0 0 0 0	0 0 0 0

Lo que nos resulta en 2^5 = 32 diferentes segmentos para las ciudades.
Se recomienda que cuando se realice un subnetting en IPv6 se tomen los bits individuales pues aunque podría volverse un poco complicado, ahorraremos muchas direcciones en IPv6, evitando así las malas prácticas que se vivieron en IPv4.

Sin embargo, para fines didácticos, en este ejemplo usaremos todo el segundo dígito, (con un total de 8 bits) dándonos 256 diferentes prefijos para 256 diferentes ciudades (recordemos que 2^8=256).

El prefijo sería: 48 bits (por la dirección proporcionada por el proveedor) + 8 bits (dado que usaremos 2 dígitos del cuarto hexteto) = 56 bits (es decir una máscara **/56**).

De esta manera, tenemos:

Ciudad 1	2001:ABCD:CAFE:0000::/56
Ciudad 2	2001:ABCD:CAFE:1000::/56
Ciudad 3	2001:ABCD:CAFE:2000::/56
Ciudad 4	2001:ABCD:CAFE:3000::/56
Ciudad 5	2001:ABCD:CAFE:4000::/56
Ciudad 6	2001:ABCD:CAFE:5000::/56
Ciudad 7	2001:ABCD:CAFE:6000::/56
Ciudad 8	2001:ABCD:CAFE:7000::/56
Ciudad 9	2001:ABCD:CAFE:8000::/56
Ciudad 10	2001:ABCD:CAFE:9000::/56
Ciudad 11	2001:ABCD:CAFE:A000::/56
Ciudad 12	2001:ABCD:CAFE:B000::/56
Ciudad 13	2001:ABCD:CAFE:C000::/56
Ciudad 14	2001:ABCD:CAFE:D000::/56
Ciudad 15	2001:ABCD:CAFE:E000::/56
Ciudad 16	2001:ABCD:CAFE:F000::/56
Ciudad 17	2001:ABCD:CAFE:0100::/56
Ciudad 18	2001:ABCD:CAFE:0200::/56
Ciudad 19	2001:ABCD:CAFE:0300::/56
Ciudad 20	2001:ABCD:CAFE:0400::/56

Nótese que los cambios en la numeración solo ocurren en el primer y segundo dígito del cuarto hexteto.

*Se dejaron expresados los Ceros a la izquierda con fines de aprendizaje.

2. Prefijo para cada Oficina (10 oficinas por ciudad)

Debemos usar para esta tarea el **tercer dígito**, ya que los dos primeros están siendo usados para las ciudades.

Para 10 oficinas necesitamos 4 bits, 2^4=16 oficinas.

Cuarto Hexteto				
	Primer dígito (4 bits)	Segundo dígito (4 bits)	**Tercer dígito (4 bits)**	Cuarto dígito (4 bits)
Bits del dígito	0 0 0 0	0 0 0 0	**0 0 0 0**	0 0 0 0
Bits que serán usados (*)	~~~~~~~~	~~~~~~~~	* * * *	0 0 0 0

El prefijo para las oficinas será: /60 (56+4=60).

Ciudad 1 2001:ABCD:CAFE:0000::/56

Oficina 1 2001:ABCD:CAFE:0000::/60
Oficina 2 2001:ABCD:CAFE:0010::/60
Oficina 3 2001:ABCD:CAFE:0020::/60
Oficina 4 2001:ABCD:CAFE:0030::/60
Oficina 5 2001:ABCD:CAFE:0040::/60
Oficina 6 2001:ABCD:CAFE:0050::/60
Oficina 7 2001:ABCD:CAFE:0060::/60
Oficina 8 2001:ABCD:CAFE:0070::/60
Oficina 9 2001:ABCD:CAFE:0080::/60
Oficina 10 2001:ABCD:CAFE:0090::/60

Ciudad 2 2001:ABCD:CAFE:1000::/56

Oficina 1 2001:ABCD:CAFE:1000::/60
Oficina 2 2001:ABCD:CAFE:1010::/60
Oficina 3 2001:ABCD:CAFE:1020::/60
Oficina 4 2001:ABCD:CAFE:1030::/60
Oficina 5 2001:ABCD:CAFE:1040::/60
Oficina 6 2001:ABCD:CAFE:1050::/60
Oficina 7 2001:ABCD:CAFE:1060::/60
Oficina 8 2001:ABCD:CAFE:1070::/60
Oficina 9 2001:ABCD:CAFE:1080::/60
Oficina 10 2001:ABCD:CAFE:1090::/60

Llegando hasta la oficina 20…

Ciudad 20 2001:ABCD:CAFE:0400::/56

Oficina 1 2001:ABCD:CAFE:0400::/60
Oficina 2 2001:ABCD:CAFE:0410::/60
Oficina 3 2001:ABCD:CAFE:0420::/60
Oficina 4 2001:ABCD:CAFE:0430::/60
Oficina 5 2001:ABCD:CAFE:0440::/60
Oficina 6 2001:ABCD:CAFE:0450::/60
Oficina 7 2001:ABCD:CAFE:0460::/60
Oficina 8 2001:ABCD:CAFE:0470::/60
Oficina 9 2001:ABCD:CAFE:0480::/60
Oficina 10 2001:ABCD:CAFE:0490::/60

*Nótese que una vez que teníamos el prefijo **/56** referente de cada ciudad, se mantuvo intacto, solo cambiando el tercer dígito de este cuarto hexteto.*

3. Prefijo para cada Departamento de las diferentes oficinas

Debemos mencionar que existe la recomendación es que cada subred debe tener un /64. Sin embargo, para una optimización en las direcciones de IPv6, se recomiendas que tras un estudio de crecimiento en una red, se haga lo más justo posible; en este caso vemos que tener un direccionamiento /64 para solo 11 equipos, es un inmenso desperdicio de direcciones.

11 departamentos, 2^4=16 departamentos. Tomando el hexteto completo tenemos:

Cada departamento tendrá un prefijo /64 (60 (ciudad y oficina) + 4 (departamento))

Ciudad 1 2001:ABCD:CAFE:0000::/56

Oficina 1 2001:ABCD:CAFE:0000::/60

Departamento 1	2001:ABCD:CAFE:0000::/64
Departamento 2	2001:ABCD:CAFE:0001::/64
Departamento 3	2001:ABCD:CAFE:0002::/64
Departamento 4	2001:ABCD:CAFE:0003::/64
Departamento 5	2001:ABCD:CAFE:0004::/64
Departamento 6	2001:ABCD:CAFE:0005::/64
Departamento 7	2001:ABCD:CAFE:0006::/64
Departamento 8	2001:ABCD:CAFE:0007::/64
Departamento 9	2001:ABCD:CAFE:0008::/64
Departamento 10	2001:ABCD:CAFE:0009::/64
Departamento 11	2001:ABCD:CAFE:000A::/64

Oficina 2 2001:ABCD:CAFE:0010::/60 (de la ciudad 1)

Departamento 1	2001:ABCD:CAFE:0010::/64
Departamento 2	2001:ABCD:CAFE:0011::/64
Departamento 3	2001:ABCD:CAFE:0012::/64
Departamento 4	2001:ABCD:CAFE:0013::/64
Departamento 5	2001:ABCD:CAFE:0014::/64
Departamento 6	2001:ABCD:CAFE:0015::/64
Departamento 7	2001:ABCD:CAFE:0016::/64
Departamento 8	2001:ABCD:CAFE:0017::/64
Departamento 9	2001:ABCD:CAFE:0018::/64
Departamento 10	2001:ABCD:CAFE:0019::/64
Departamento 11	2001:ABCD:CAFE:001A::/64

Nótese como el cambio se realiza ahora en el último dígito del cuarto hexteto. La máscara de la ciudad (**/56**) se manteniene intacta al igual el el prefijo de la oficina (**/60**).

Continuamos ejemplificando el ejercicio.

Ciudad 2 2001:ABCD:CAFE:1000::/56

Oficina 1	2001:ABCD:CAFE:1000::/60
Oficina 2	2001:ABCD:CAFE:1010::/60
Oficina 3	2001:ABCD:CAFE:1020::/60
Oficina 4	2001:ABCD:CAFE:1030::/60
Oficina 5	2001:ABCD:CAFE:1040::/60
Oficina 6	2001:ABCD:CAFE:1050::/60
Oficina 7	2001:ABCD:CAFE:1060::/60
Oficina 8	2001:ABCD:CAFE:1070::/60
Oficina 9	2001:ABCD:CAFE:1080::/60

Oficina 10 2001:ABCD:CAFE:1090::/60

Oficina 1 2001:ABCD:CAFE:1000::/60 (de la ciudad 2)

Departamento 1	2001:ABCD:CAFE:1000::/64
Departamento 2	2001:ABCD:CAFE:1001::/64
Departamento 3	2001:ABCD:CAFE:1002::/64
Departamento 4	2001:ABCD:CAFE:1003::/64
Departamento 5	2001:ABCD:CAFE:1004::/64
Departamento 6	2001:ABCD:CAFE:1005::/64
Departamento 7	2001:ABCD:CAFE:1006::/64
Departamento 8	2001:ABCD:CAFE:1007::/64
Departamento 9	2001:ABCD:CAFE:1008::/64
Departamento 10	2001:ABCD:CAFE:1009::/64
Departamento 11	2001:ABCD:CAFE:100A::/64

Oficina 2 2001:ABCD:CAFE:1010::/60 (de la ciudad 2)

Departamento 1	2001:ABCD:CAFE:1010::/64
Departamento 2	2001:ABCD:CAFE:1011::/64
Departamento 3	2001:ABCD:CAFE:1012::/64
Departamento 4	2001:ABCD:CAFE:1013::/64
Departamento 5	2001:ABCD:CAFE:1014::/64
Departamento 6	2001:ABCD:CAFE:1015::/64
Departamento 7	2001:ABCD:CAFE:1016::/64
Departamento 8	2001:ABCD:CAFE:1017::/64
Departamento 9	2001:ABCD:CAFE:1018::/64
Departamento 10	2001:ABCD:CAFE:1019::/64
Departamento 11	2001:ABCD:CAFE:101A::/64

Ahora ejemplificamos la ciudad 11

Ciudad 11 2001:ABCD:CAFE:A000::/56

Oficina 1 2001:ABCD:CAFE:A000::/60
Oficina 2 2001:ABCD:CAFE:A010::/60
Oficina 3 2001:ABCD:CAFE:A020::/60
Oficina 4 2001:ABCD:CAFE:A030::/60
Oficina 5 2001:ABCD:CAFE:A040::/60
Oficina 6 2001:ABCD:CAFE:A050::/60
Oficina 7 2001:ABCD:CAFE:A060::/60
Oficina 8 2001:ABCD:CAFE:A070::/60
Oficina 9 2001:ABCD:CAFE:A080::/60
Oficina 10 2001:ABCD:CAFE:A090::/60

Oficina 1 2001:ABCD:CAFE:A000::/60 (de la ciudad 11)

Departamento 1 2001:ABCD:CAFE:A000::/64
Departamento 2 2001:ABCD:CAFE:A001::/64
Departamento 3 2001:ABCD:CAFE:A002::/64
Departamento 4 2001:ABCD:CAFE:A003::/64
Departamento 5 2001:ABCD:CAFE:A004::/64
Departamento 6 2001:ABCD:CAFE:A005::/64
Departamento 7 2001:ABCD:CAFE:A006::/64
Departamento 8 2001:ABCD:CAFE:A007::/64
Departamento 9 2001:ABCD:CAFE:A008::/64
Departamento 10 2001:ABCD:CAFE:A009::/64
Departamento 11 2001:ABCD:CAFE:A00A::/64

Oficina 6 2001:ABCD:CAFE:A010::/60 (de la ciudad 11)

Departamento 1 2001:ABCD:CAFE:1050::/64

Departamento 2	2001:ABCD:CAFE:1051::/64
Departamento 3	2001:ABCD:CAFE:1052::/64
Departamento 4	2001:ABCD:CAFE:1053::/64
Departamento 5	2001:ABCD:CAFE:1054::/64
Departamento 6	2001:ABCD:CAFE:1055::/64
Departamento 7	2001:ABCD:CAFE:1056::/64
Departamento 8	2001:ABCD:CAFE:1057::/64
Departamento 9	2001:ABCD:CAFE:1058::/64
Departamento 10	2001:ABCD:CAFE:1059::/64
Departamento 11	2001:ABCD:CAFE:105A::/64

Vale la pena recalcar que cuando hablamos de ciudades, solo se modificaron los primeros 2 dígitos del hexteto (correspondientes a 8 bits; de ahí que pasa de /48 a /56), cuando hablamos de oficinas solo movimos el tercer dígito del hexteto (pasamos de la /56 a la /60) y finalmente en los departamentos modificamos el 4to dígito del hexteto (haciéndonos pasar de la /60 a la /64).

Referencias

www.cisco.com
RFC 4291: Referencia a arquitecturas de las direcciones en IPv6

Desarrollo

A continuación se les planteará 2 casos donde una empresa desea hacer una red para todos sus empleados, aplicando los conceptos anteriores, muestre en una tabla las diferentes direcciones que así se les pida.

Caso 1

Dirección otorgada por el proveedor de servicios es 2001:0DB8:3C4D::/48.

La empresa está presente 30 ciudades con 15 oficinas en cada ciudad y 10 equipos en cada oficina.

- Muestre en una tabla como quedarían las direcciones IPv6 de las 30 ciudades. (muestre claramente las máscaras de red)
- En otra tabla muestre las direcciones correspondientes a cada oficina de la ciudad 5, la ciudad 20 y la ciudad 28. (muestre claramente las máscaras de red)
- En otra tabla muestre las direcciones para cada equipo de la ciudad 30 en la oficina 8. (muestre claramente las máscaras de red)

Nota importante: para el caso 1 use los bits completos (tal y como se hizo en el ejemplo realizado anteriormente).

Caso 2

El proveedor de servicios le otorga la siguiente dirección 2001:AAFF:5D6A::/48

La empresa está presente 30 ciudades con 20 oficinas en cada ciudad y 20 equipos en cada oficina.

- Muestre en una tabla como quedarían las direcciones IPv6 de las 30 ciudades. (muestre claramente las máscaras de red)
- En otra tabla muestre las direcciones correspondientes a cada oficina de la ciudad 1, la ciudad 10 y la ciudad 20. (muestre claramente las máscaras de red)
- En otra tabla muestre las direcciones para cada equipo de la ciudad 30 en la oficina 15. (muestre claramente las máscaras de red)

Nota importante: para el caso 2 use solo los bits que sean necesarios, caso contrario en el caso 1, si usted solo necesita 6 bits para cumplir la demanda, deberá continuar la partición hacia las oficinas en el 7mo bit, recordemos:

Cuarto Hexteto				
	Primer dígito (4 bits)	**Segundo dígito (4 bits)**	Tercer dígito (4 bits)	Cuarto dígito (4 bits)
Bits del dígito	**0 0 0 0**	**0 0 0 0**	0 0 0 0	0 0 0 0
Bits que serán usados (*)	*** * * ***	*** 0 0 0**	0 0 0 0	0 0 0 0

Para este ejemplo (tomado del ejemplo realizado anteriormente), originalmente cumplíamos la demanda con solo 5 bits (tomábamos uno del segundo hexteto) pero simplificábamos todo tomando los 3 bits restantes. Para este caso 2, haciendo una analogía con el cuadro anterior, solo debemos tomar los primeros 5 bits, obteniendo nuestras direcciones con máscara /53 y no /56 como el ejercicio previamente realizado.

Conclusiones

Tras culminar esta práctica, el alumno debió obtener los siguientes conocimientos:

- Conformación de una dirección en IPv6 (hextetos expresados en forma hexadecimal).
- Reglas 1 (eliminación de ceros a la izquierda) y 2 (uso de dobles puntos) para la optimización de escritura en IPv6.
- Conversión de decimal a binario y hexadecimal.
- Direcciones Global Unicast y Link Local
- Estructura de una dirección global unicast (prefijo de enrutamiento, identificador de subred e identificador de host).

- Subneteo en IPv6 y el uso de VLSM (Variable Length Subnet Mask) en IPv6.

Cuestionario

1. Supóngase que las siguientes direcciones que se te proporcionan tienen problemas, que usted deberá resolver; ¿a qué ciudad, oficina y departamento deberá ir?

a) 2001:ABCD:CAFE:6006::/64
b) 2001:ABCD:CAFE:405A::/64
c) 2001:ABCD:CAFE:C094::/64
d) 2001:ABCD:CAFE:0146::/64
e) 2001:ABCD:CAFE:0330::/64

2. Pase las direcciones del ejercicio anterior (del inciso a al e) de forma hexadecimal a decimal.

3. Usando los mismos bits que se usaron la creación de direcciones del ejercicio realizado anteriormente (solo el cuarto hexteto), ¿cuál sería la última dirección que se podría formar? (no tome en cuenta las limitantes del ejercicio realizado).

4. De la dirección obtenida en el ejercicio anterior, hipotéticamente, ¿a qué ciudad, oficina y departamento correspondería dicha dirección?