UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Prácticas para la materia de Redes de Datos II

MATERIAL DIDÁCTICO

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Alejandro Garcia Garcia

ASESOR DE MATERIAL DIDÁCTICO

Dr. Víctor Rangel Licea

Ciudad Universitaria, Cd. Mx., 2016

Agradecimientos

A mi familia, mis padres y mis hermanos, que han sido el pilar de mi formación educativa. Que me han dado su apoyo incondicional de muchas maneras, enseñándome, dando palabras de aliento, trabajando para darme lo mejor e impulsándome a superarme cada día. Ellos han jugado un papel vital para mi formación profesional y mi formación como ser humano. Llevo con orgullo su legado y nunca encontrare palabras ni acciones que demuestren lo agradecido que estoy por tenerlos a mi lado.

A mis amigos, que han compartido tiempo y grandes alegrías conmigo, que me han ayudado a superar obstáculos académicos y personales. Se han convertido en mi segunda familia, les agradezco que hayan creído en mí y en mis proyectos cuando ni yo mismo creía en ellos. Sus consejos y amistad me han fortalecido a lo largo del tiempo y es algo que atesorare por el resto de mi vida.

A mi Universidad y a la Facultad de Ingeniería, los maestros con quienes he tenido el gusto de compartir un aula me han dado todo el conocimiento técnico y las habilidades para ejercer mi profesión. La institución y las personas que trabajan en ella me han dado el mejor trato y herramientas para lograr mis metas, estaré en deuda con ellos y con mi alma mater por haberme enseñado a amar lo que hago a pesar de todo.

Alejandro Garcia Garcia.

Contenido

Introducción y Aclaraciones previas

Posicionamiento e importancia de la interconexión de redes

Para comenzar con el pie derecho este trabajo, vamos a hablar sobre la importancia que tiene el hecho de tener conocimientos básicos de redes. Para ello vamos a enfocarnos en concreto sobre los conceptos que encontrara en este manual; los cuales forman parte de una colección básica de herramientas con las que cuenta para enfrentar diversos problemas.
Esto responde a la necesidad de que el lector, después de leer este material, pueda responder preguntas tan básicas como los son “¿Qué es?” y “¿Para qué sirve?”. Esto debido a que muchas veces nos enfocamos tanto en la estructura y funcionamiento de las cosas, que olvidamos la respuesta a preguntas tan sencillas como las anteriores. Así que desarrollaremos un contexto sencillo para responder dichas preguntas en los siguientes párrafos:

Direccionamiento y Subneteo IPv4

El direccionamiento y subneteo, tanto en IPv4 como IPv6 lo vamos a definir como; una forma ordenada de planear y asignar direcciones IP a los dispositivos. Lo anterior a simple vista no parece mucho, pero la relevancia de un buen diseño es vital, esto nos sirve para utilizar de manera eficiente todas las direcciones disponibles; también significa un gran impacto para el funcionamiento de todo internet, ya que es simple intuir que será “más sencillo buscar una dirección en una caja ordenada a buscarla en una desordenada”, además de asegurarnos que no exista alguna dirección repetida y no haya confusiones.

OSPFv2

OSPFv2 es un protocolo de ruteo dinámico, además de ser un protocolo link-state, lo anterior se traduce en 2 características importantes; primero que al ser dinámico no requiere que el administrador configure rutas de manera manual, lo cual llega a ser tedioso cuando se manejan redes enormes. Segundo, cuando hablamos de un protocolo link-state quiere decir que los dispositivos (routers) conocen toda la topología y el estado de esta. Para que se haga una idea, solo imaginé que de alguna manera usted conoce cada calle, vía de su ciudad, la distancia y el tiempo que cada una conlleva y además que sabe en tiempo real cuando cierran una de estas por alguna razón imprevista, seguramente esto le ahorraría mucho tiempo. Pues es lo que OSPF hace, sirve para que los routers aprendan información acerca de la topología por sí mismos, después utilizan esta información junto con el algoritmo Dijkstra para calcular la mejor ruta para enviar la información al destino.

Listas de control de acceso (ACL)

Las listas de control de acceso son una de las medidas de seguridad más importantes en las redes, es como un vigilante que registra cada paquete de información y después decide si deja entrar o salir cierta información de la red. Sirven principalmente como un filtro de paquetes, su implementación tiene tanto implicaciones positivas como negativas dependiendo de su buen uso, las implicaciones positivas son muchas desde restringir trafico basura hasta proteger información sensible como estados de cuenta, por otro lado si se aplica o diseña mal una ACL esto pude resultar en el bloqueo de servicios importantes tanto de red como de internet.

NAT

NAT es una herramienta que mitiga el problema de la escasez de direcciones IPv4, esto debido a que las direcciones no son infinitas y cada vez con más dispositivos conectándose a internet hace falta tener más direcciones. NAT sirve como una solución temporal, ya que lo recomendable es migrar a IPv6. NAT traduce direcciones privadas (repetibles y usadas por todo el mundo) en direcciones públicas (únicas en internet y el mundo). En la práctica nos encontramos que existen muchos direccionamientos privados usados en

empresas, escuelas y hogares; teniendo solo una dirección pública para conectarse a internet, esto es importante para los proveedores de internet ya que las direcciones públicas que poseen son limitadas.

Seguridad

Existen muchas medidas de seguridad que podemos tomar para proteger nuestros datos, es difícil conocer y manejar todas las medidas de seguridad. Pero siempre han existido medidas básicas que no necesitan muchos conocimientos, por ejemplo la construcción de contraseñas fuertes. Se recomienda usar un mínimo de 8 caracteres intercalando minúsculas mayúsculas y símbolos. Por ejemplo existe software que rompe la seguridad de las contraseñas probando cada combinación de caracteres posible, se han hecho pruebas y dichos programas pueden romper una contraseña de 6 caracteres con minúsculas en 10 minutos, en cambio con una contraseña de las características recomendadas el programa tardaría alrededor de 400 años en encontrar la combinación correcta. Estos datos son muy contrastantes y reflejan la importancia de algo simple “construir una contraseña fuerte”.

Principios de Routing en IPv6

El direccionamiento IPv6 es solo extrapolar lo que se sabe de ruteo en IPv4 a IPv6. El funcionamiento de los protocolos y conceptos de ruteo son los mismos para IPv6 que en IPv4. Tal vez la mayor diferencia que podemos visualizar es en la configuración de los dispositivos. Es muy relevante que se vaya introduciendo a IPv6 ya que este protocolo representa el futuro y la tendencia de la redes. Hay una campaña muy importante por parte de los proveedores de tecnología para hacer una transición y uso de IPv6 por lo que en los próximos años seguramente tendrá que lidiar con este nuevo protocolo.

Herramientas disponibles para practicar

Esta sección está dedicada a algunas aclaraciones previas que debe conocer antes de profundizar en este manual. Para comenzar hablaremos sobre las diferentes herramientas disponibles para la realización de las prácticas contenidas en este material.

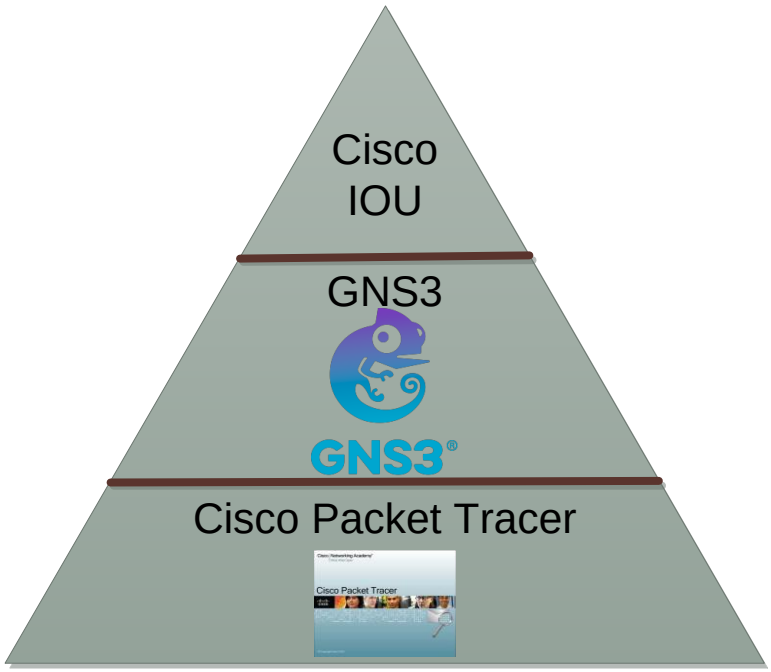


Figura 1: Herramientas recomendadas para practicar.

Como puede observar en la figura anterior se han dividido las herramientas en tres secciones de manera escalonada. Comenzare por decir que desde una perspectiva personal considero más accesible Packet Tracer que está en la base que los otros 2.
Tratare de explicar brevemente porque sugiero comenzar con Packet Tracer y luego ir escalando hacia las demás herramientas, no estoy diciendo que una sea mejor o no. Quiero dejar claro que las 3 tienen sus pros y contras, y que la colocación que tienen en la figura es totalmente un perspectiva personal, que puede ayudarlo a tener una idea más clara de que herramienta elegir.

Packet Tracer

Comenzare con el software de simulación propietario de Cisco, este es de los más completos y sencillos de manejar, Cisco ha hecho un gran trabajo y de hecho lo sigue haciendo al mejorar diferentes características de la simulación en Packet Tracer. Consume pocos recursos, además de que es fácil de instalar e intuitivo al armar las topologías, Cisco está incursionando en una aplicación para móviles que está expandiendo las posibilidades de los usuarios de este software.

Desafortunadamente nos encontraremos con limitaciones en cuanto a la semejanza de dispositivos reales, algunas funciones y protocolos, por ejemplo protocolos de redundancia en capa 3 no son admitidos en el simulador (al menos no una configuración detallada), los cuales son configurables en los mismos equipos reales que el software simula, así también tiene algunas limitaciones en cuanto al manejo de IPv6 en distintas versiones del IOS. Esto hace que prácticas con algunos conceptos avanzados sean difíciles de realizar.
Afortunadamente todas las prácticas contenidas en este material son realizables sin ningún problema en Packet Tracer, es por ello que se eligió esta plataforma para desarrollar todo el contenido.

GNS3

Graphical Network Simulator, esta plataforma es ya más compleja, debido a que es un set de herramientas y emuladores de varios sistemas operativos. Entre los emuladores con los que cuenta esta Dynamips, el cual es el encargado de emular routers Cisco además de proveer otros dispositivos e interfaces. También tenemos Quemu, Pemu y VirtualBox, los cuales proveen soporte para dispositivos como Cisco ASA, Cisco PIX Firewalls, routers Juniper, routers Vyatta y hosts con Linux y Windows.

Además de que tiene integrada la aplicación de Wireshark, la cual es una aplicación muy popular de software libre que funciona como capturadora de paquetes de red.

Esta plataforma es gratuita y se puede descargar en su sitio oficial. Uno de los principales elementos que juega un papel importante en GNS3 son los “Image Files”. Estos archivos son copias del IOS que emulara alguna plataforma de Cisco o Juniper, debido a los derechos de autor, GNS3 no puede proveer dichos archivos, por ello lo más recomendable es contactar instituciones u organismos que tengan acceso a estos archivos de forma legal, o que tengan algún contrato con estos proveedores. Esto hace más complicado acceder a GNS3 debido a que debes tener una copia de los IOS que deseas emular.

Aunado al problema de obtener los Image Files, tenemos que decir que la configuración de estos emuladores y de esta plataforma es un poco más compleja, por lo que necesita tiempo para aprender cómo funciona. Recuerde que esta plataforma trabaja con emuladores y máquinas virtuales, por lo que hay problemas inherentes al uso de estas tecnologías. Uno de los principales problemas que se tiene al usar esta plataforma es la sobrecarga de recursos de la PC, como el procesador y la memoria RAM.

Lo anterior tiene beneficios en cuanto a la inmersión en los sistemas operativos y las topologías de red. Esto es prácticamente lo que se encontrara en dispositivos reales, haciendo la experiencia más enriquecedora. Desafortunadamente no se pueden emular todos los IOS, pero definitivamente con los que tiene son más que suficientes para ahondar en temas más especializados.
Todo lo anterior nos hizo desistir de la idea de usar GNS3, si bien los beneficios son grandes, se tiene que invertir un buen tiempo de aprendizaje para entender y manejar la plataforma a la perfección lo cual no se hace en Packet Tracer.

Cisco IOU

Cisco IOU (IOS on Unix), Esto es un versión del IOS liberada o lanzada para uso interno de Cisco, permite ejecutar IOS de manera nativa en plataformas con arquitecturas x86, mientras GNS3 debe emular todo el hardware, la gran diferencia radica en que el IOU puede correr más sistemas operativos de diferentes dispositivos Cisco.

Es difícil conseguir acceso a esta tecnología si no se es parte de Cisco, pero hay varios proyectos en la web que claman tener permisos de diferentes proveedores para emular sus productos, uno de los más importantes que dice usar IOU es Unified Networking Lab.

De manera personal recomiendo el uso de esta tecnología si tiene conocimientos profundos de Unix, ya que la instalación de esta herramienta lo requerirá. Puedo asegurar que para prácticas que tengan que ver con seguridad, VoIP, y temas avanzados de Switching y Routing, será más que suficiente con GNS3.

Acerca de este manual

Este material está pensado para usarse de una manera en específico, la cual describiremos a continuación:

Primero que nada debe identificar que cada práctica está construida de la misma manera, por lo que puede estudiarlas todas en la misma manera.
Para comenzar tenemos una sección teórica de la práctica compuesta por la Introducción, Conceptos previos y Referencias. Esta sección teórica trata de manera superficial varios de los conceptos más importantes que se aplicaran en la práctica, los cuales puede profundizar leyendo el material sugerido en la sección de Referencias. Es importante que se lea esta sección debido a que es un reforzamiento de los conceptos que se ven en la teoría, así también se debe ver como autoevaluación para que el alumno identifique en que partes necesita profundizar su estudio.

Después viene la sección práctica compuesta por la Tabla de Comandos, Tabla de direccionamiento, Topología y Desarrollo. En esta parte se aplica en un ejercicio lo que se vio en teoría, tiene secciones bien identificadas que permiten ubicar información como el direccionamiento y la topología de la red. También se incluye un compendio de los comandos necesarios para completar toda la práctica. Lo que se sugiere hacer es primero leer y entender claramente lo que se pide, después ubicar el dispositivo donde se tiene que hacer y finalmente localizar el comando en la tabla para configurar dicho dispositivo.

Los comandos contenidos en la tabla identifican al principio el modo donde se debe ejecutar dicho comando, esto lo identificara por el prompt al inicio del comando, en la siguiente tabla se hace una ejemplificación de esto:

Inicio del comando	**Modo de configuración en donde se ejecuta el comando.**
(config)#	Configuración global.
(config-if)#	Configuración de interfaz.
#	Usuario privilegiado.

Figura 2: Modos de configuración.

Finalmente tenemos una sección de cierre compuesta por las Conclusiones y el Cuestionario. Donde damos una perspectiva general de lo que se tocó en la práctica así como de los conceptos que vale la pena recordar y volver a estudiar. El cuestionario es una herramienta de autoevaluación con la que cuenta el alumno para poder medir el aprendizaje que tiene sobre el tema, las repuestas a dicho cuestionario se encontraran al final de este material.

Es esencial que el alumno entienda que este material se hace con el propósito de incentivar el estudio autodidacta, debido a que las topologías desarrolladas aquí no son universales, así que una parte muy importante del proceso de aprendizaje es que el alumno repita los conceptos y comandos con topologías propias o desarrolladas por otras personas, entre más práctica se tenga con escenarios más diversos y que conjunten más conceptos, mejores resultados se tendrá con las habilidades adquiridas por el alumno tanto teóricas como prácticas.

Capítulo I: Direccionamiento IPv4

Introducción

El protocolo IPv4 es de gran relevancia en las redes de datos modernas. Debido que hasta el momento es el protocolo de direccionamiento más usado y difundido en la implementación de redes, en sus inicios no se pensó que fuera a ser tan difundido, pero con el crecimiento de internet, este protocolo comenzó a ser ampliamente usado en redes LAN, hasta el punto de agotar las direcciones IPv4 disponibles. En esta práctica veremos los principios del direccionamiento, que hace posible la comunicación a nivel de capa 3 en las redes de datos.

Conceptos previos

Estructura de una dirección IPv4

Una dirección IPv4 está conformada por 32 bits divididos en cuatro octetos. Estos octetos son normalmente separados por un punto decimal. La representación de las direcciones, se hace generalmente con números binarios o decimales. A veces también se pueden ver representados con el sistema hexadecimal u octal.

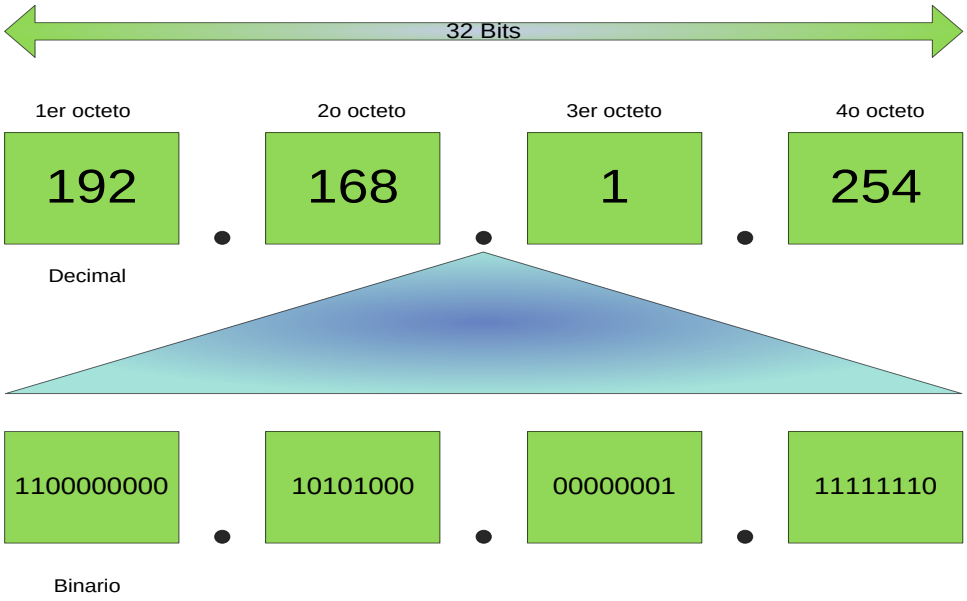
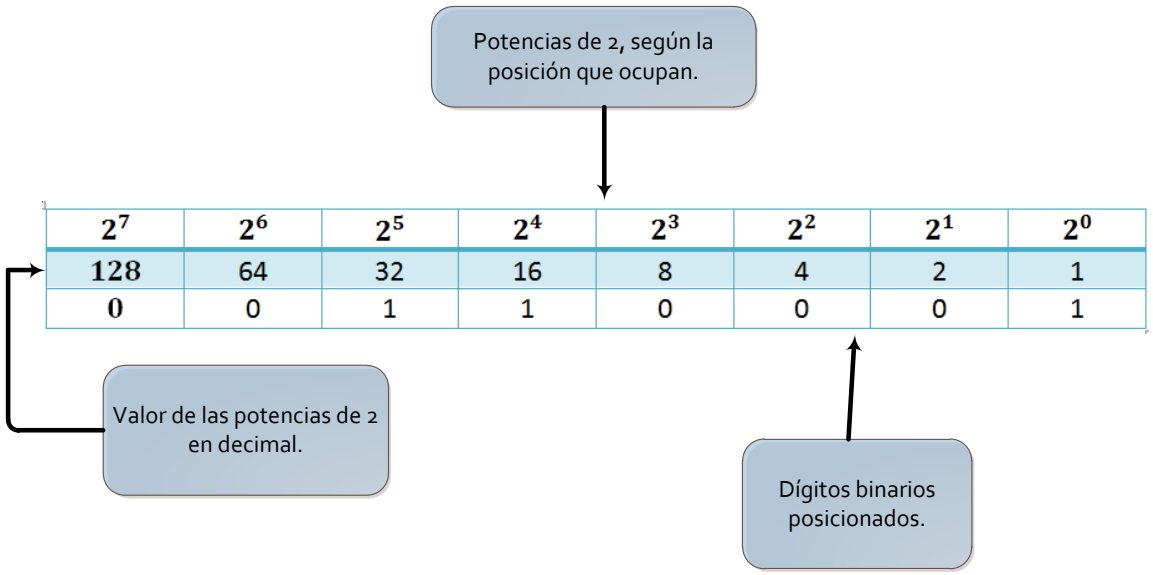


Figura 1.3: Estructura de una dirección IPv4.

Sistema binario

Para el tema de direccionamiento es importante que entendamos el uso del sistema binario y decimal. El sistema decimal es el que más comúnmente usamos, por lo que nos enfocaremos en el sistema binario y sus conversiones al sistema decimal. El sistema binario es importante en el mundo de la informática y por lo tanto en el mundo de las redes; debido a que los datos y las formas de comunicación son representados por este sistema. En pocas palabras es el lenguaje en el cual se codifican los datos y que las computadoras entienden.

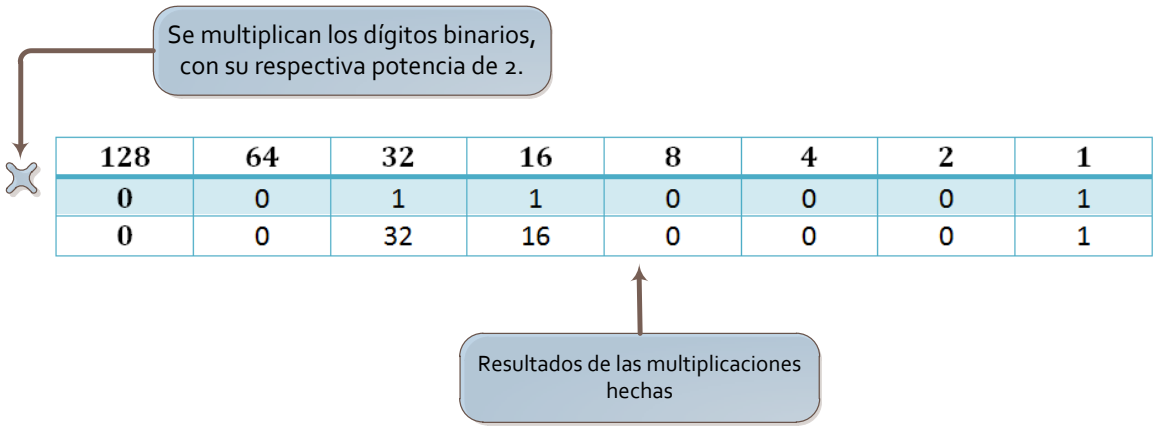
Para empezar debemos entender al sistema binario como otro sistema de numeración posicional así como lo es el decimal, en el sistema decimal se nos enseñó el uso de unidades, decenas, centenas, etc. Pues algo parecido ocurre en el sistema binario, al igual que en el sistema decimal la posición de los dígitos influirá en la representación de un número en específico, para ilustrar lo siguiente analicemos la Figura 1.2.



2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	1	1	0	0	0	1

Figura 1. 4: Potencias de 2 y dígitos binarios posicionados.

En ella vemos un número binario de 8 dígitos, tal número está representado en la última fila de la tabla; está conformado por los siguientes dígitos 00110001. Para poder hacer una conversión de este número binario a sistema decimal lo que haremos es: multiplicar el digito binario por el valor de la potencia de dos correspondiente y después sumar todos los resultados. Observe como se hizo en la figura 1.3.



128	64	32	16	8	4	2	1
0	0	1	1	0	0	0	1
0	0	32	16	0	0	0	1

Figura 1. 5: Conversión de binario a decimal.

$$numero_{Decimal} = 32 + 16 + 1 = 49$$

El número 00110001 en binario corresponde al 49 en sistema decimal.

Para hacer una conversión de decimal a binario solo debemos aplicar un método iterado de divisiones entre 2. Dicho método lo aplicaremos de la manera siguiente: primero dividiremos el número decimal entre 2, esto se hace tantas veces sea posible la división. En dicha división solo llegaremos a resultados enteros con residuos, finalmente tomaremos los cocientes para continuar dividiéndolos, esto se explica mejor con el siguiente ejemplo.

Supongamos que queremos convertir 66 en sistema decimal en su equivalente binario.

Numero dividido /2	Cociente	Residuo
66	33	0
33	16	1
16	8	0
8	4	0
4	2	0
2	1	0
1	0	1
0	X	X

Figura 1. 6: Conversión de decimal a binario.

Como se observa en la Figura 1.4 primero dividimos 66 entre 2, lo cual nos da un cociente de 33 y residuo 0, después dividimos el cociente 33 de nuevo entre 2, lo cual nos da un nuevo cociente de 16 y residuo de 1. Lo anterior se continúa haciendo hasta que ya no se pueda dividir más; es decir hasta llegar a cero. Finalmente tomamos los números de la columna de residuo y los escribimos empezando de abajo hacia arriba de la siguiente manera:

1000010

El resultado anterior es el numero 66 escrito en sistema binario.

Mascara de subred

Para poder entender el concepto de la máscara de subred primero tenemos que establecer otras ideas. Para empezar debemos saber que una dirección IPv4 se divide en 2 porciones bien definidas: una es llamada porción de red y otra la porción de host esto lo puede apreciar en la Figura 1.5.

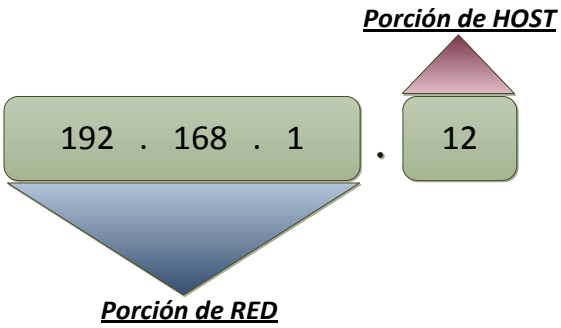


Figura 1. 7: Porciones en una dirección IPv4.

Estas porciones son una herramienta que nos ayuda a identificar varias cosas, la más importante que debe recordar es que; todos los dispositivos en una misma LAN o subred comparten la misma porción de RED, mientras que lo que los diferencia es la porción de HOST. En la figura vemos que los 3 primeros octetos conforman la porción de RED y el último la porción de HOST, pero esto no sucede así siempre, se debe tener en cuenta para futuras referencias.

Un dispositivo usa un patrón de 32 bits para poder identificar las porciones de RED y de HOST. A este patrón se le conoce como mascara de subred. Para lograr lo anterior se definen 2 reglas muy sencillas: todos los bits que conforman la porción de RED se establecerán en 1 en la máscara, mientras que todos los bits que conforman la porción de HOST se establecerán en 0, de esta manera la máscara de subred de la figura anterior se muestra en la Figura 1.6.

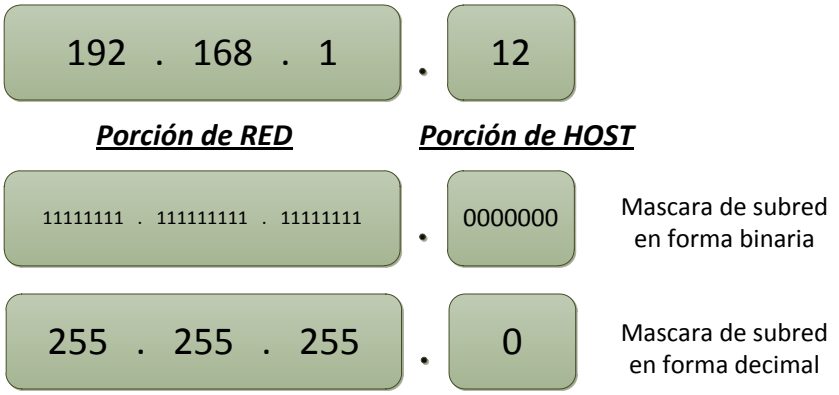


Figura 1. 8: Mascara de subred correspondiente a una dirección IPv4.

En la figura anterior podemos identificar claramente dos formas de escribir la máscara de subred: la primera de ellas es la binaria, la segunda de ellas es decimal. Existe una manera más de escribir las máscaras y es usando un prefijo decimal. Este prefijo es la cuenta de bits en 1 en la masca de subred, es decir en la máscara anterior existen un total de 24 bits en 1: por lo que se puede escribir la máscara usando una diagonal seguida del número 24. Como se muestra en la Figura 1.7.

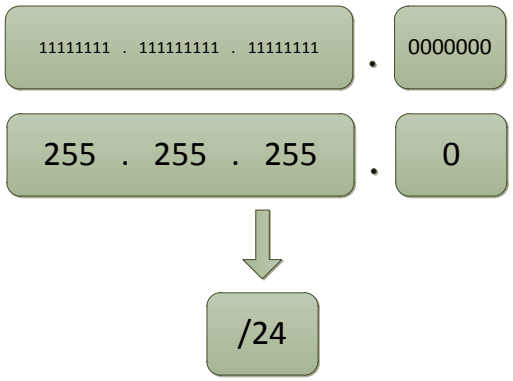


Figura 1. 9: Formas de escribir una mascara de subred.

Lo anterior nos sirve para identificar fácilmente la máscara de subred, las tres formas de escribirla son muy útiles así que se sugiere se acostumbre a usar las tres.

Dirección de RED, BROADCAST Y HOST

En el direccionamiento IPv4 vamos a tener 3 tipos de direcciones. Para poder identificar cada una de ellas haremos uso de la máscara de subred y de las porciones de RED y HOST que previamente hemos aprendido. Cada tipo de dirección tiene una función en específico la cual describiremos a continuación:

Dirección de RED (Figura 1.8): Esta dirección nos sirve para identificar un grupo de computadoras o una subred, la dirección de RED la podemos identificar cuando todos los bits en la porción de HOST en una dirección IPv4 están establecidos en 0.

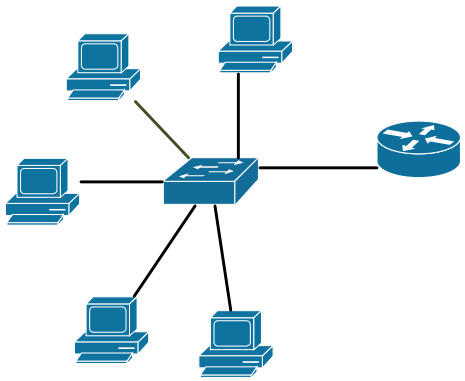


Figura 1. 10: Grupo de hosts que se identifican a través de una dirección de subred.

Dirección de BROADCAST (Figura 1.9): La dirección de BROADCAST sirve para mandar un mensaje de broadcast en la red: un mensaje de broadcast es aquel que está destinado llegar a todos los dispositivos que pertenezcan a la misma red o subred. La dirección de BROADCAST la identificaremos cuando todos los bits en la porción de HOST estén establecidos en 1.

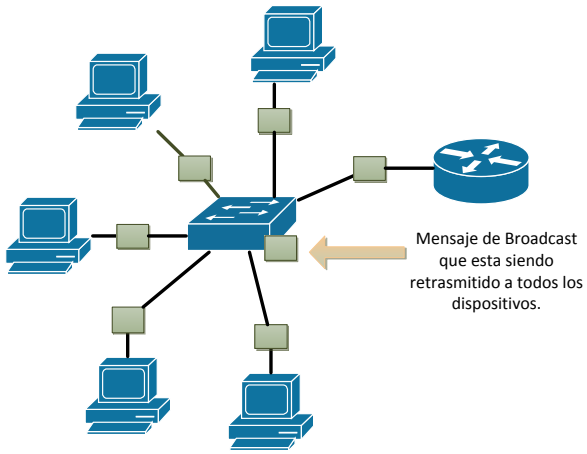


Figura 1. 11: Grupo de hosts que reciben un mensaje a través de su dirección de broadcast.

Dirección de HOST (Figura 1.10): Esta dirección identifica a un solo dispositivo en específico o a una interfaz especifica si el dispositivo cuenta con varias interfaces de red. Esta dirección la podemos identificar porque hay 0’s y 1’s en la porción de Host de la dirección.

Figura 1. 12: Host que representa una dirección IPv4.

Operación bit a bit (AND)

Antes de continuar vamos a explicar cómo se hace una operación AND bit a bit ya que la utilizaremos más adelante. La operación AND es una operación lógica que generalmente se asocia con el sistema binario, de manera homologa podemos mencionar que esta es una operación como la multiplicación en el sistema decimal. Al igual que en el sistema decimal se tiene una tabla (Figura 1.11) que nos ayuda a ver el resultado de dicha operación.

			RESULTADO
1	AND	0	0
1	AND	1	1
0	AND	1	0
0	AND	0	0

Figura 1. 13: Tabla de operación AND.

Vamos a operar 2 números binarios de 8 bits, esta operación la haremos bit a bit: estos números son 00011110 y 00011011.

0	**0**	**0**	**1**	**1**	**1**	**1**	**0**	
0	0	0	1	1	0	1	1	
0	0	0	1	1	0	1	0	Resultado

Figura 1. 14: Ejemplo de operación AND bit a bit.

La operación bit a bit la podemos ver en la tabla anterior (Figura 1.12) y el resultado da el numero binario de 8 dígitos 00011010.

Obtención de la dirección de RED y de BROADCAST a partir de una dirección IP y la máscara de subred

Muchas veces en el estudio de las redes nos vamos a encontrar con que solo nos darán la máscara de subred y una dirección IP cualquiera. Con estos 2 elementos nosotros nos tenemos que hacer una idea de cuáles son las direcciones de RED y BROADCAST asociadas a la IP, así también cuáles son las direcciones de HOST (direcciones de los dispositivos) a las que hace referencia la máscara y la dirección IP dada. Para ello es recomendable que se exploren ejercicios donde podamos identificar tres elementos esenciales: Direcciones de RED, y BROADCAST y rango asignable de direcciones de HOST.
Vamos a plantear un método sencillo para poder obtener dichos elementos, esto lo haremos conforme se resuelve un ejemplo para hacer más ilustrativo el método.
Ejemplo: Obtener las direcciones de RED, BROADCAST y rango asignable de direcciones de HOST, si tenemos la siguiente información:
192.168.1.5/27.

Primero vamos a obtener la dirección de RED, esto lo podemos hacer aplicando lo que hemos aprendido anteriormente. La dirección de RED es aquella que tiene los bits de la parte de HOST en 0, la parte de HOST esta explicita en la máscara de subred, por lo que solo basta con multiplicar bit a bit la máscara de subred con la dirección IP, como se muestra en la Figura 1.13.

11111111	**11111111**	**11111111**	**11100000**	**Mascara**
11000000	10101000	00000001	00000101	Dirección IP
11000000	10101000	00000001	00000000	Resultado

Figura 1. 15: Operación AND entre una mascara de subred y una dirección IPv4.

El resultado si lo escribimos de manera decimal es 192.168.1.0.
Ahora debemos continuar con la dirección de BROADCAST, ahora que ya tenemos identificados los bits de la porción de HOST en la máscara (los últimos 5 bits), para obtener la dirección de BROADCAST solo tenemos que cambiar dichos bits en la dirección IP a 1's (Vea la Figura 1.14).

11111111	**11111111**	**11111111**	**11100000**	**Mascara**
11000000	10101000	00000001	00000101	Dirección IP

11000000	10101000	00000001	00011111	Resultado

Figura 1. 16: Proceso de obtención de la dirección de broadcast.

Como se observa anteriormente los bits resaltados en la dirección IP que nos son 1's fueron cambiados en el resultado, quedando como dirección de BROADCAST en forma decimal lo siguiente:

192.168.1.31

El rango de direcciones asignables a HOST se puede obtener fácilmente, ya que es el rango de direcciones IP entre las direcciones de RED y BROADCAST sin incluir estas dos. Es por ello que el rango asignable de direcciones lo podemos ver en la Figura 1.15.

192.168.1.0	**Dirección de RED.**
192.168.1.1	Dirección de HOST asignable.
192.168.1.2	Dirección de HOST asignable.
192.168.1.3	Dirección de HOST asignable.
192.168.1.4	Dirección de HOST asignable.
192.168.1.5	Dirección de HOST asignable.
192.168.1.6	Dirección de HOST asignable.
192.168.1.7	Dirección de HOST asignable.
192.168.1.8	Dirección de HOST asignable.
192.168.1.9	Dirección de HOST asignable.
192.168.1.10	Dirección de HOST asignable.
192.168.1.11	Dirección de HOST

	asignable.
192.168.1.12	Dirección de HOST asignable.
192.168.1.13	Dirección de HOST asignable.
192.168.1.14	Dirección de HOST asignable.
192.168.1.15	Dirección de HOST asignable.
192.168.1.16	Dirección de HOST asignable.
192.168.1.17	Dirección de HOST asignable.
192.168.1.18	Dirección de HOST asignable.
192.168.1.19	Dirección de HOST asignable.
192.168.1.20	Dirección de HOST asignable.
192.168.1.21	Dirección de HOST asignable.
192.168.1.22	Dirección de HOST asignable.
192.168.1.23	Dirección de HOST asignable.
192.168.1.24	Dirección de HOST asignable.
192.168.1.25	Dirección de HOST asignable.
192.168.1.26	Dirección de HOST asignable.
192.168.1.27	Dirección de HOST asignable.
192.168.1.28	Dirección de HOST asignable.
192.168.1.29	Dirección de HOST

	asignable.
192.168.1.30	Dirección de HOST asignable.
192.168.1.31	Dirección de BROADCAST.

Figura 1. 17: Rango asignable de direcciones del ejemplo planteado.

Tipos de asignación de direcciones IP

Manual: Una dirección IPv4 puede ser asignada a un dispositivo de manera manual, cuando al administrador de red o del dispositivo, configura en el la dirección IP, insertando todos los campos requeridos por el dispositivo, como la máscara de subred la dirección de Default Gateway y la dirección del servidor DNS.

Dinámica: La asignación dinámica como su nombre lo indica, es aquel donde el administrador de red configura un servidor a través del cual este asignando dinámicamente las direcciones IPv4, conforme los dispositivos las vayan solicitando. Para este método se usa un servicio de Red llamado DHCP del cual hablamos con más profundidad en otra práctica.

Tipos de trasmisión de mensajes

Existen tres formas bien definidas en los mensajes que se trasmiten en IPv4, debe saber identificar cada una de ellas muy bien, estos tipos de trasmisión los explicamos a continuación:

Unicast: Esto se refiere al proceso de enviar un paquete de un dispositivo a otro.

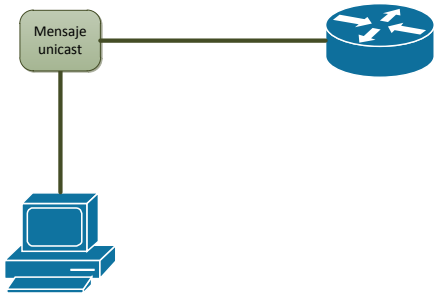


Figura 1. 18: Trasmisión de una mensaje Unicast.

Broadcast: Es el proceso de enviar un paquete de un host a todos los demás hosts en la red.

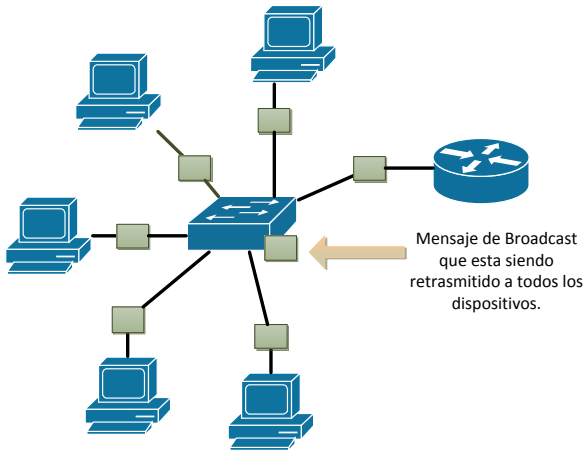


Figura 1. 19: Trasmisión de un mensaje Broadcast.

Multicast: El proceso de enviar un paquete de un host a un grupo seleccionado de hosts.

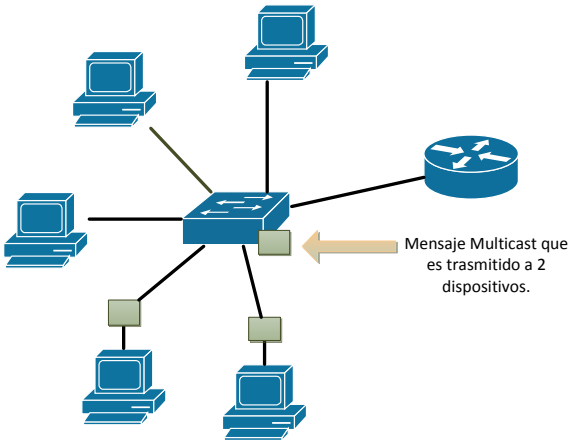


Figura 1. 20: Trasmisión de un mensaje de Multicast.

Direccionamiento Classful y Classless.

El direccionamiento Classful se refiere al direccionamiento que se usó en los principios de implementación de IPv4; donde las direcciones eran divididas en bloques llamados clases, dichos bloques eran asignados dependiendo de la necesidades de la organización que los solicitara. Las clases de direccione IPv4 se muestran en la Figura 1.19.

Clase	Rango del primer octeto en decimal	Mascara de subred	Rango de direcciones.
A	1 - 126	255.0.0.0	1.0.0.0 hasta 126.255.255.255
B	128 - 191	255.255.0.0	128.0.0.0 hasta 191.255.255.255
C	192 - 223	255.255.0.0	192.0.0.0 hasta 223.255.255.255
D	224 - 239	NA (Multicast)	224.0.0.0 hasta 239.255.255.255
E	240 - 255	NA (Experimental)	240.0.0.0 hasta 255.255.255.255

Figura 1. 21: Tabla de clases de direcciones.

Los bloques de direcciones que se asignaban eran de clase A, B y C, debido a que los demás bloques eran especiales para otros usos.

El direccionamiento Classless mas formalmente llamado Classless Inter-domain Routing (CIDR), es un nuevo esquema de direccionamiento que permite la asignación de direcciones o bloques de direcciones que no estén catalogados como una clase. Este direccionamiento lo veremos más a profundidad en subneteo IP.

Direcciones IP públicas y privadas

Las direcciones IP privadas las definiremos como aquellas direcciones que no necesitan salir a Internet: es decir solo son usadas para el enrutamiento dentro de las organizaciones o empresas. Debido a esta característica muchas organizaciones y personas pueden implementar un direccionamiento privado en sus LAN, para poder comunicar los equipos dentro de su administración. A diferencia de las direcciones privadas las públicas son aquellas que salen y son usadas en internet: debido a que cada dispositivo en internet debe tener una dirección IP única, estas direcciones son administradas de tal forma que no se dupliquen en todo internet.
En la siguiente Figura mostramos los bloques de direcciones privadas que existen.

Clase	Bloque	Rango
A	10.0.0.0/8	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0/12	172.16.0.0 hasta 172.31.255.255
C	192.168.0.0/16	192.168.0.0 hasta 192.168.255.255

Figura 1. 22: Bloques de direcciones privadas.

Asignamiento de direcciones

Como lo mencionamos antes existen organizaciones encargadas de gestionar las direcciones IPv4 públicas, la primera que se encargó de esto fue la IANA (Internet Assigned Numbers Authority**).** Con el tiempo esto fue cambiando y ahora el organismo internacional que se encarga de esto es la ICANN (Internet Corporation for Assigned Names and Numbers); es la responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

La ICANN delega las direcciones IP y la responsabilidad de asignarlas a los RIR (Regional Internet Registry), que son organizaciones regionales que supervisan estos recursos. A continuación un diagrama con estas organizaciones.

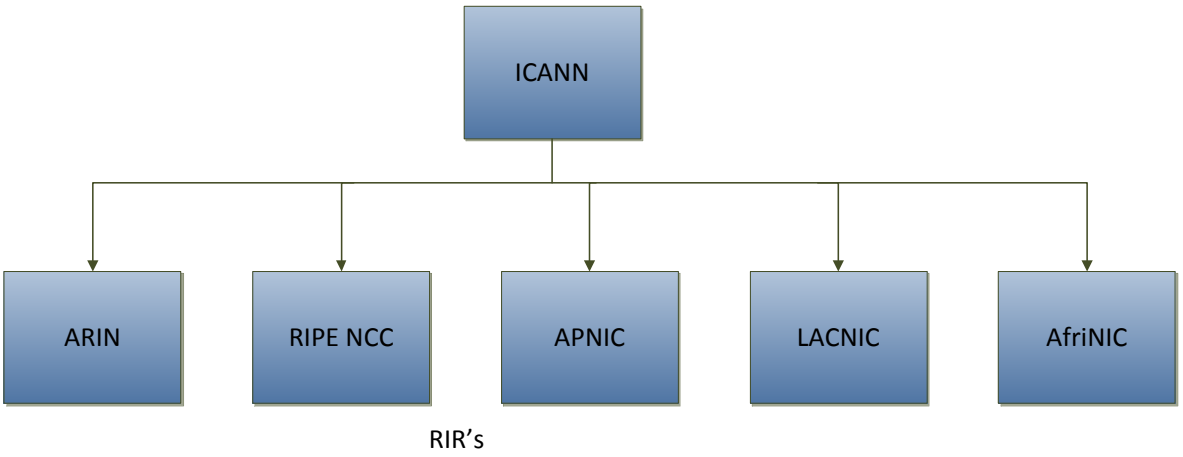


Figura 1. 23: Entidades encargadas del direccionamiento IP.

- American Registry for Internet Numbers (ARIN) para América Anglosajona.
- RIPE Network Coordination Centre (RIPE NCC) para Europa, el Oriente Medio y Asia Central.
- Asia-Pacific Network Information Centre (APNIC) para Asia y la Región Pacífica.
- Latin American and Caribbean Internet Address Registry (LACNIC) para América Latina y el Caribe.
- African Network Information Centre (AfriNIC) para África.

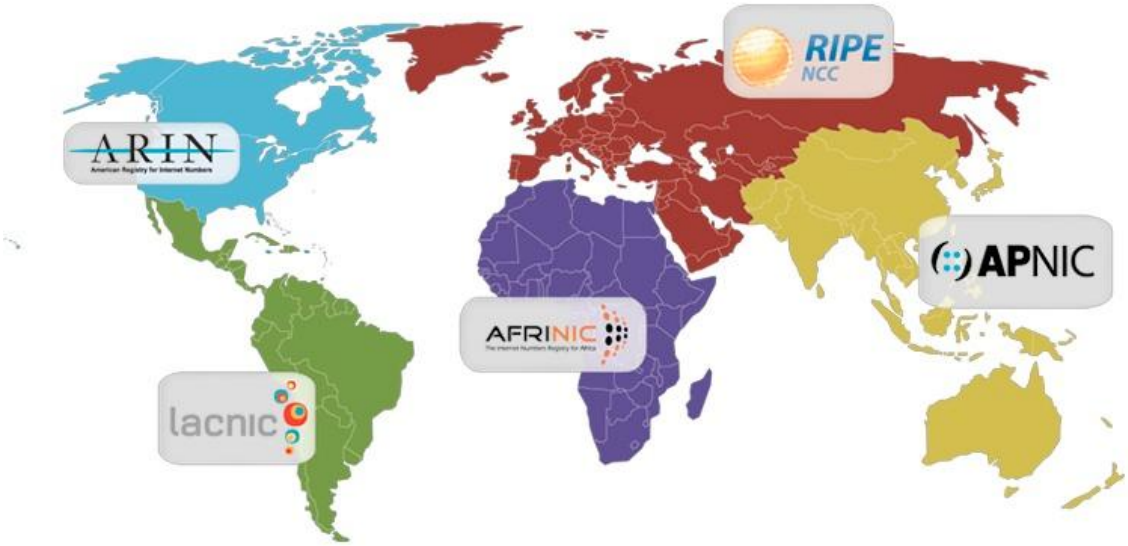


Figura 1. 24: Dominio geográfico de la entidades encargadas del direccionamiento IP.

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.
A. Tanenbaum and D. Morales Peake, Redes de computadoras. México: Prentice-Hall Hispanoamericana, 1997.
RFC 5735.
RFC 791.

Desarrollo

Actividad 1

1. Convierta los siguientes números de decimal a binario.
    a. 368.
    b. 224
    c. 192
    d. 1356

2. Convierta los siguientes números de binario a decimal.
    a. 0001111110111.
    b. 0011110.
    c. 11100011.
    d. 10101010100.

Actividad 2

1. Exprese las siguientes máscaras de subred en su forma decimal y binaria.
    a. /27.
    b. /24.
    c. /19.
    d. /7.
2. Exprese la siguientes mascara en su forma corta (con diagonal) y binaria.
    a. 255.255.255.255
    b. 255.0.0.0
    c. 255.255.224.0
    d. 255.192.0.0

3. Obtenga las máscaras de subred en cualquiera de sus formas con la información de la tabla.

Dirección de RED.	**Dirección de BROADCAST.**
172.16.32.0	172.16.63.255

192.168.1.0	192.168.1.7
10.0.0.0	10.3.255.255
10.0.128.0	10.0.255.255

4. Obtenga las direcciones de BROADCAST, RED y el rango de direcciones asignables a HOST de los siguientes incisos.
    a. 192.168.1.34/27
    b. 172.16.2.2/15
    c. 10.0.1.1/8
    d. 192.168.15.15/19

Conclusiones

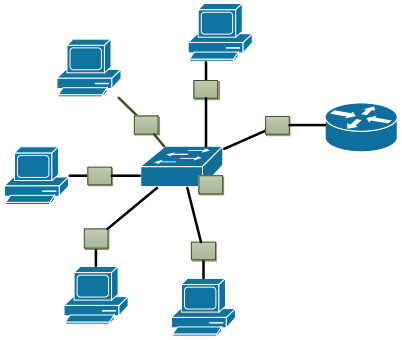
En esta práctica logramos analizar el direccionamiento usado en IPv4, los diferentes tipos de direcciones y su uso, así como procedimientos para la obtención de tres datos importantes: las direcciones de RED, BROADCAST y el rango asignable de direcciones de HOST. Se le sugiere mantener en mente y practicar los siguientes conceptos:

- Recuerde que una dirección IPv4 tiene 32 bits divididos en 4 octetos, no las confunda con las direcciones MAC de 48 bits y las direcciones IPv6 de 128 bits.
- Practique las conversiones de binario a decimal y de decimal a binario, de tal manera que llegue el punto de que pueda hacerlas de manera mental.
- La máscara de subred es una herramienta de 32 bits que nos ayuda a identificar de manera clara cuál es la porción de RED y la porción de HOST.
- Existen 3 tipos de direcciones usadas en IPv4, estas son: la de RED, BROADCAST y la de HOST, recuerde cual es la función de cada una.
- Recuerde y practique las tres diferentes formas de escribir una máscara de subred. Así como el proceso en que obtiene la dirección de RED, BROADCAST y el rango asignable de direcciones de HOST.
- Existen 3 tipos de mensajes IPv4 no los confunda con los tipos de direcciones, estos mensajes son: Unicast, Multicast y Broadcast.

- El direccionamiento classful se refiere al direccionamiento usado en los inicios de IPv4, las clases asignables eran A, B y C, así también se designaron otras clases para su propósito, Memorice el rango de direcciones de cada clase, es muy importante.
- Las direcciones privadas son aquellas que no salen a internet, es decir que solo son ruteables en la intranet de la organización, están bien definidas y al igual que las clases de direcciones es mejor que las memorice.

Cuestionario

1. ¿Cómo definiría el siguiente tipo de mensaje?



   A. Mensaje que está destinado a solo un grupo específico de la red (Multicast).
   B. Mensaje que está destinado a un solo dispositivo en la red (Unicast).
   C. Mensaje que está destinado a todos los dispositivos en la red (BROADCAST).

2. ¿Cuáles de las siguientes direcciones son direcciones públicas?

   A. 192.169.2.2
   B. 192.168.1.5
   C. 172.16.5.3
   D. 172.31.255.255
   E. 172.15.5.5

3. Mencione los 5 Registros Regionales de Internet.

4. ¿Qué tipo de dirección es la dirección 172.16.255.255/24? Seleccione todas las opciones que apliquen.

    A. Dirección privada.
    B. Dirección pública.
    C. Dirección que pertenece al bloque A.
    D. Dirección que pertenece al bloque B.
    E. Dirección que pertenece al bloque C.
    F. Dirección de RED.
    G. Dirección de BROADCAST.

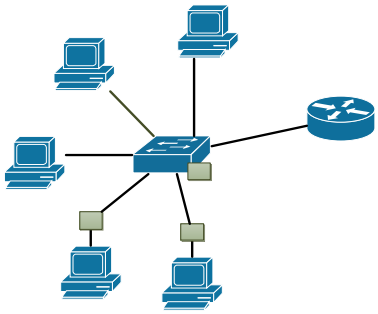
5. ¿Cuál es el rango de direcciones del bloque de direcciones clase C?

    A. 192.168.0.0 hasta 192.168.255.255
    B. 128.0.0.0 hasta 191.255.255.255
    C. 192.0.0.0 hasta 223.255.255.255
    D. 10.0.0.0 hasta 10.255.255.255

6. A usted le dan los siguientes datos: 172.16.64.0/18 ¿Cuáles son las direcciones de BROADCAST Y DE RED?

    A. 172.16.64.0
    B. 172.16.0.0
    C. 172.16.127.255
    D. 172.16.128.0.0
    E. 172.16.255.255

7. ¿Cómo definiría el siguiente tipo de mensaje?



   A. Mensaje que está destinado a solo un grupo específico de la red (Multicast).
   B. Mensaje que está destinado a un solo dispositivo en la red (Unicast).
   C. Mensaje que está destinado a todos los dispositivos en la red (BROADCAST).

8. ¿Cuáles de las siguientes direcciones son direcciones privadas?

   A. 192.168.1.1
   B. 191.168.1.1
   C. 172.15.255.255
   D. 10.0.0.0
   E. 1.0.0.0
   F. 172.16.255.255

9. ¿Para qué se usa una dirección de BROADCAST?

   A. Para enviar mensajes a todos los host en la red.
   B. Para enviar mensajes a un solo host.
   C. Para enviar mensaje a cierto grupo de hosts.

10. Obtenga las direcciones de BROADCAST, RED y el rango de direcciones asignables a HOST de la siguiente subred 172.16.4.1/22.

Capítulo II: Subneteo de Redes IPv4

Introducción

En esta práctica vamos a aprender los conceptos de VLSM (Variable Length Subnet Mask), para poder aplicarlos al subneteo de redes, la importancia de esto es el "no desperdicio de direcciones IP", así como crear un direccionamiento que se acople a las necesidades de la red con la que estemos trabajando.

Conceptos previos

Direccionamiento Classless y Classful

Como recordara el direccionamiento Classful fue aquel que se utilizó en los inicios de las redes, donde se le asignaba un bloque de direcciones A, B o C al solicitante, obviamente no todas las necesidades de las organizaciones se ajustaban a estas clases, por ejemplo un bloque clase C podía albergar hasta 254 hosts, un bloque clase B podía albergar hasta 65,534 hosts, si por alguna razón usted solo necesitaba 534 direcciones, se le asignaba todo un bloque B dejando las otras 65,000 direcciones sin asignar. Esto era un gran desperdicio de direcciones, a pesar de esto esté direccionamiento se utilizó hasta el final de la década de los 90.

El direccionamiento Classless vino a solucionar el problema anterior, donde se asignaran bloques de direcciones adecuadas a las necesidades de cada quien,

este direccionamiento es el que se utiliza en la actualidad, y es muy importante entenderlo para poder hacer buen uso de esta herramienta.

Razones para la segmentación de redes

El proceso de segmentación de grandes redes en redes más pequeñas (subredes) se le conoce como subneteo (subnetting), es muy común que para ajustar los bloques de direcciones a las necesidades de cada red se haga un subneteo de una red más grande. El subneteo trae grandes beneficios a las redes, entre los que podemos destacar:

- Mejoramiento del rendimiento de la red.
- Evita el desperdicio de direcciones.
- Evita sobrecargar la red de tráfico.
- Ayuda a aislar y controlar ciertos problemas en la red.

Para comunicar estas subredes que vamos a crear, vamos a necesitar de un router que podrá dirigir el tráfico entre las diferentes subredes, para esto él debe tener conectada una de sus interfaces a la subred, y también debe tener asignada una dirección IP a la interfaz.

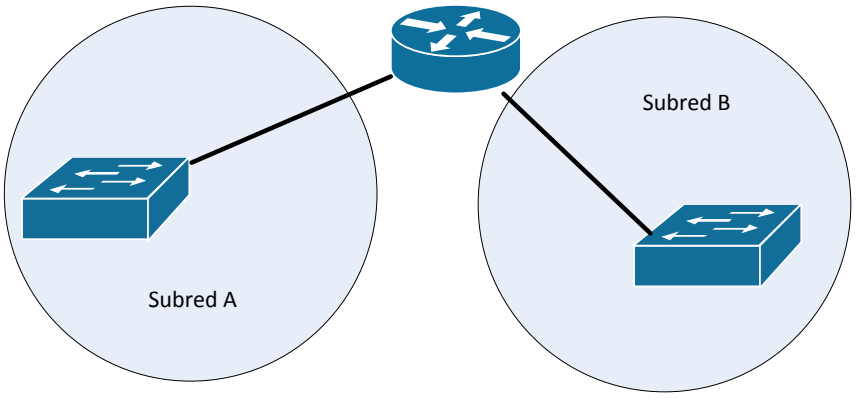


Figura 2. 1: Comunicación de 2 subredes a través de un router.

Subneteo básico

Para comenzar vamos a ver un par de fórmulas sencillas, que nos explicaran el número de direcciones existentes en una red o subred, recordemos como

dividíamos nuestras direcciones IPv4, la dirección la segmentábamos en 2 partes una llamada porción de RED y otra porción de HOST. Pues bien comencemos con decir que el número de bits en la porción de host determinara las direcciones disponibles o asignables. Observe la siguiente formula.

$$direcciones\ asignables = 2^n - 2$$

Donde n es el número de bits en la porción de host. La parte de la formula donde se restan 2, es debido a que siempre que dividamos una red deben haber 2 direcciones reservadas, la primera del bloque de direcciones siempre será la dirección de RED y la última será la dirección de BROADCAST.

Prestando bits

Supongamos que se nos asigna cualquier bloque de direcciones clase C, en concreto el 192.168.1.0/24, podemos dividir este bloque en bloques más pequeños, prestando bits de la porción de HOST a una nueva porción que la llamaremos "porción de Subred" (observe la figura 2.2).

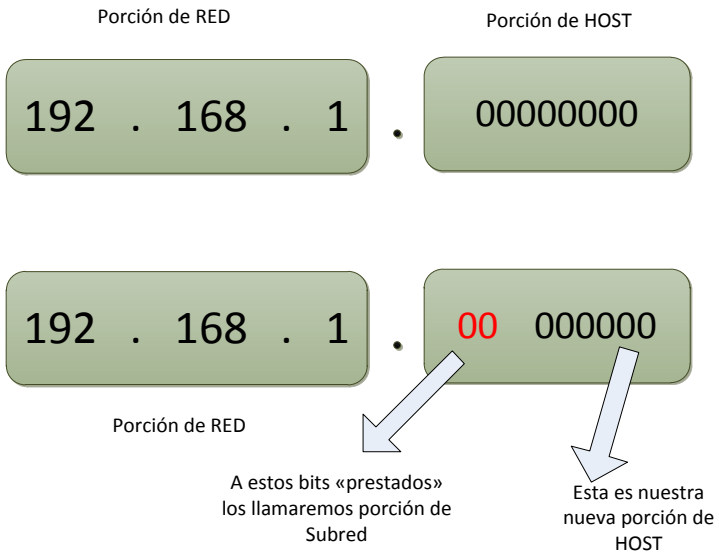


Figura 2. 2: Proceso de subneteo.

Pues bien ahora nosotros podemos crear subredes con los bits en la porción de Subred, el número de subredes estará dado por:

$$\#subredes = 2^S$$

Donde S es el número de bits en la porción de Subred, y al igual que antes el número de direcciones asignables en esas subredes estará dado por los bits en la nueva porción de HOST. En el ejemplo anterior solo tomamos prestados 2 bits, por lo que seremos capaces de crear 4 subredes con 62 direcciones asignables cada una.

Estas subredes tendrán una nueva mascara de subred, sabemos que la máscara de subred tiene la porción de HOST en ceros y la porción de RED en unos, pues lo único que hay que hacer es cambiar los bits de la porción de Subred en unos y contarlos como parte de la porción de RED, como se hizo en la figura 2.3.

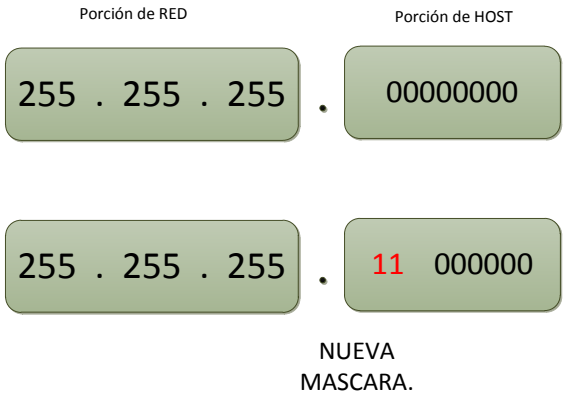


Figura 2. 3: Mascara de subred nueva después del subneteo.

La máscara anterior la podemos escribir como /26 ó 255.255.255.192.
Podemos listar las direcciones de RED de cada una de las subredes que hemos creado, esto se hace con todas las combinaciones posibles de los bits en la porción de Subred, la cuales son 4; 00, 01, 10 y 11. Si sustituimos y convertimos estos valores tendremos lo que se muestra en la siguiente figura.

	Dirección de RED con binarios	**Dirección de RED decimal.**
Subred A	172.168.1. 00 00000	172.168.1.0/26
Subred B	172.168.1. 01 00000	172.168.1.64/26
Subred C	172.168.1. 10 00000	172.168.1.128/26

Subred D	172.168.1. 11 00000	172.168.1.192/26

Figura 2. 4: Resumen de las nuevas subredes creadas.

Es así como pidiendo prestados bits podemos crear nuevas redes que se ajusten a las necesidades que tengamos, con diferentes cantidades de direcciones asignables, es importante resaltar la importancia de incluir la máscara de subred correcta en las nuevas subredes.

Podemos pedir el número de bits prestados que queramos, mientras la porción de HOST no se quede sin ninguno, también podemos basar nuestros diseños en el número de direcciones asignables que necesitemos. Al final con las nuevas direcciones de RED y la nueva mascara de subred podemos obtener también las direcciones de BROADCAST y el rango asignable de direcciones HOST.

VLSM

Variable Length Subnet Mask es un método de asignación de direcciones usando mascaras de subred variables, es decir usando subredes de diferentes tamaños, que se ajusten muy específicamente a las redes que formemos con nuestros dispositivos. En el ejemplo anterior solo dividimos una red con mascara /24 en cuatro redes de mascara /26, pero VLSM va más allá de esto, ya que trata de ajustar lo mejor posible el tamaño de los bloques de direcciones, esto conlleva un esfuerzo más grande a la hora del diseño de direccionamiento de nuevas redes, pero si se aplica bien puede traer grandes ventajas.

VLSM al igual que en el ejemplo anterior trata de evitar el desperdicio de direcciones IP, para hacer esto permite dividir el espacio de red en partes desiguales, dando como resultado diferentes máscaras de subred, que variaran dependiendo de los bits que se pidan prestados, lo anterior se logra subneteando una red de manera iterativa de tal manera que creemos redes de diferentes tamaños.

Vamos a dar unos pasos sencillos para aplicar VLSM, seguidamente usaremos estos pasos en un ejemplo para que dé mayor claridad al concepto.

1. Ordenar las subredes que se necesitan de mayor a menor.

2. Identificar los bits que se necesitan para cubrir las direcciones asignables a HOST.
3. Identificar la mascar de subred necesaria.
4. Aplicar subneteo.

Supongamos que tenemos la tarea de diseñar el direccionamiento de la siguiente red (figura 2.5), y se nos proporciona el bloque de direcciones 172.16.0.0/16.

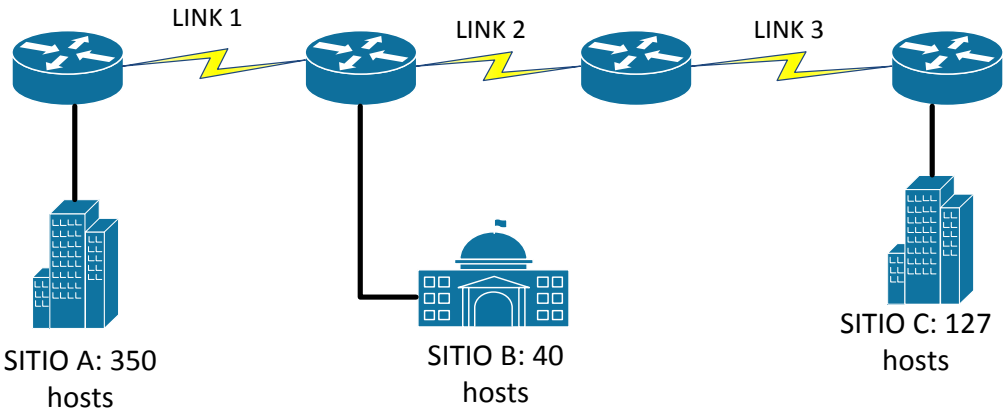


Figura 2. 5: Ejemplo de subneteo.

Comencemos aplicando los pasos que antes plantemos.

1. Tenemos 6 subredes, tres de sitio y tres más que se asignan a los links de los routers, ya que estas interfaces también necesitan una dirección, para estas subredes de los links solo necesitamos 2 direcciones. Muy bien solo las tenemos que ordenar de la siguiente manera:
    - Subred 1: 350 hosts.
    - Subred 2: 127 hosts.
    - Subred 3: 40 hosts.
    - Subred 4: 2 hosts.
    - Subred 5: 2 hosts.
    - Subred 6: 2 hosts.

2. Ahora pasamos a identificar los bits necesarios (bits en la porción de HOST) para satisfacer las necesidades de cada subred.
    - Subred 1:$direcciones\ asignables = 2^9 - 2 = 510$, esto quiere decir que necesitamos 9 bits en la porción de HOST a la hora de crear esta subred.

- Subred 2: $direcciones\ asignables = 2^8 - 2 = 254$, esto quiere decir que necesitamos 8 bits en la porción de HOST a la hora de crear esta subred.
- Subred 3: $direcciones\ asignables = 2^6 - 2 = 62$, esto quiere decir que necesitamos 6 bits en la porción de HOST a la hora de crear esta subred.
- Subred 4: $direcciones\ asignables = 2^2 - 2 = 4$, esto quiere decir que necesitamos 2 bits en la porción de HOST a la hora de crear esta subred.
- Subred 5: $direcciones\ asignables = 2^2 - 2 = 4$, esto quiere decir que necesitamos 2 bits en la porción de HOST a la hora de crear esta subred.
- Subred 6: $direcciones\ asignables = 2^2 - 2 = 4$, esto quiere decir que necesitamos 2 bits en la porción de HOST a la hora de crear esta subred.

3. Pasamos a identificar las máscaras de subred necesarias para los requerimientos que obtuvimos en el paso anterior. Sabemos que la dirección IPv4 tiene solo 32 bits, de los cueles ya identificamos cueles forman la parte de la porción de HOST, para identificar la mascar solo restamos los resultados del paso anterior a 32.
    - Subred 1: 32 bits (dirección IP) – 9 bits (porción de HOST) = 23. Para esta subred la máscara correspondiente es /23.
    - Subred 2: 32 bits (dirección IP) – 8 bits (porción de HOST) = 24. Para esta subred la máscara correspondiente es /24.
    - Subred 3: 32 bits (dirección IP) – 6 bits (porción de HOST) = 26. Para esta subred la máscara correspondiente es /26.
    - Subred 4: 32 bits (dirección IP) – 2 bits (porción de HOST) = 30. Para esta subred la máscara correspondiente es /30.
    - Subred 5: 32 bits (dirección IP) – 2 bits (porción de HOST) = 30. Para esta subred la máscara correspondiente es /30.
    - Subred 6: 32 bits (dirección IP) – 2 bits (porción de HOST) = 30. Para esta subred la máscara correspondiente es /30.

4. Finalmente solo tenemos que aplicar subneteo. Para ello tenemos que tomar el bloque de direcciones que nos fue asignado que es 172.16.0.0/16, comenzaremos dividiendo este bloque en subredes con mascara /23.

Necesitamos pedir prestados 7 bits de nuestro bloque original, lo que nos resultara en 128 bloques de direcciones con mascara /23.

Tomaremos el primer bloque que es 172.16.0.0/23, y se lo asignaremos a la subred 1. Vamos con la siguiente subred para ello vamos a subnetear el segundo bloque con mascara /23, el cual es 172.16.2.0/23. Lo que necesitamos ahora es una subred con mascara /24, esta vez solo pedimos prestado 1 bit, lo que nos resulta en 2 bloques de mascara /24, estos bloques son: 172.16.2.0/24, 172.16.3.0/24.

Al igual que antes asignamos el bloque 172.16.2.0/24 ala subred 2. Continuamos con la siguiente subred, la cual es de /26, pedimos prestados 2 bits, lo que nos resulta en 4 subredes con mascara /26 las cuales son: 172.16.3.0/26, 172.16.3.64/26, 172.16.3.128/26, 172.16.3.192/26.

Le asignaremos el bloque 172.16.3.0/26 a la subred 3. Solo nos quedan los enlaces que conectan los routers, para ello pedimos prestados 4 bits del bloque 172.16.3.64/26, lo que nos permite crear 16 subredes con mascara /30, elegiremos las primeras tres para asignarlas a los enlaces, estas subredes son: 172.16.3.64/30, 172.16.3.68/30, 172.16.3.72/30. Con esto finalizamos el direccionamiento, la siguiente figura resume todo lo que hicimos.

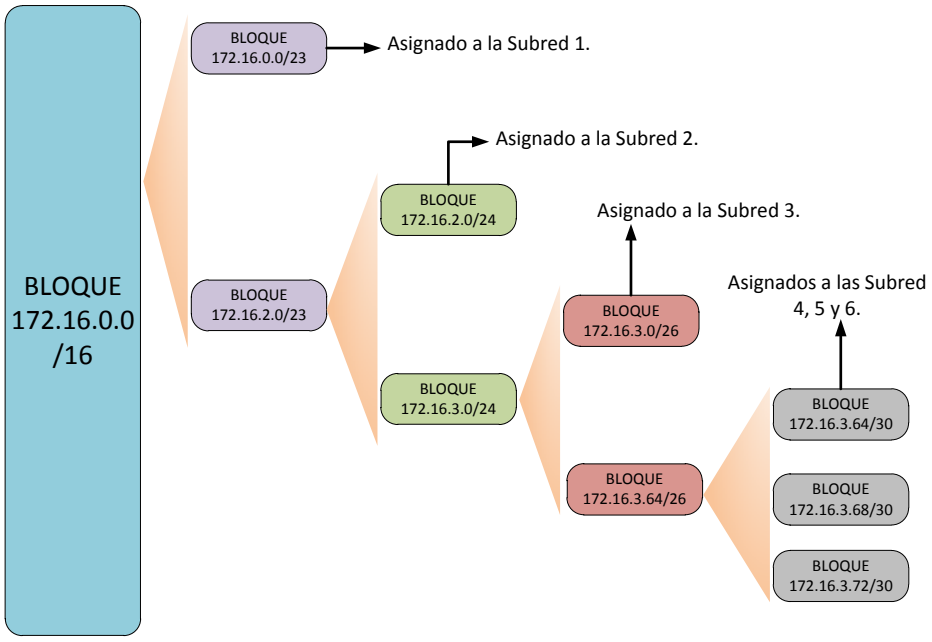


Figura 2. 6: Asignación y subneteo de subredes.

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.
A. Tanenbaum and D. Morales Peake, Redes de computadoras. México: Prentice-Hall Hispanoamericana, 1997.

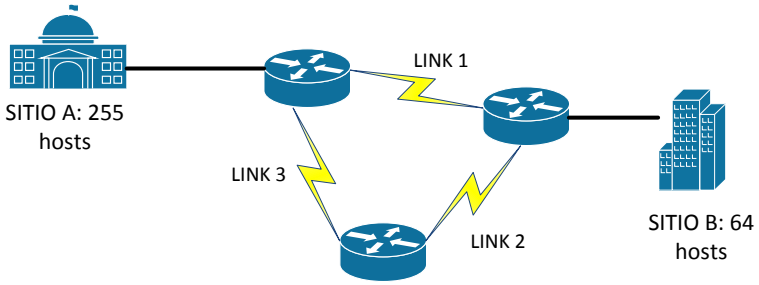
Desarrollo

Actividad 1

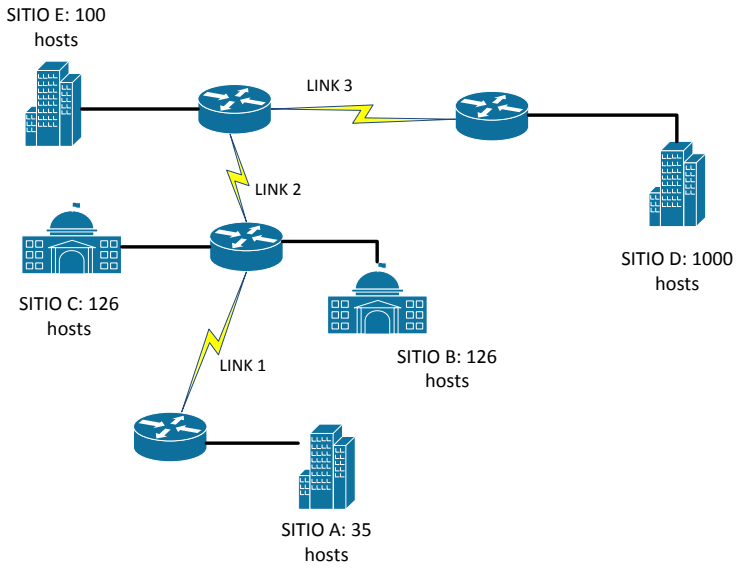
1. Divida los siguientes bloques de direcciones como se indica, anotando la dirección de RED de cada nuevo bloque.
    a. 192.168.1.0/27 en 2 bloques de igual tamaño.
    b. 172.16.0.0/16 en 4 bloques de igual tamaño.
    c. 172.16.32.0/20 en 8 bloques de igual tamaño.

Actividad 2

1. Aplique VLSM a las siguientes redes con el bloque asignado.
    a. Bloque asignado: 10.0.8.0/22



    b. Bloque asignado: 172.16.0.0/20



Conclusiones

En esta práctica logramos analizar la importancia del subneteo, entendimos la principal ventaja que este tiene, también logramos explicar un método sencillo para aplicar VLSM, si usted desea comprender por completo este tema, le sugerimos que practique con muchos ejercicios, le recomendamos los ejercicios que vienen en la referencia de esta práctica.

- Recuerde que para dividir una red en segmentos más pequeños, lo que hacemos es pedir prestados bits a la porción de HOST.
- El número de subredes que obtenga dependerá de los bits que haya tomado de la porción de HOST.
- Practique los 4 pasos que aplicamos para poder hacer VLSM.
- Mantenga en mente el porqué del VLSM y que su principal ventaja es evitar el desperdicio de direcciones.

Cuestionario

1. Si deseas dividir la red 172.16.8.0/21 en 16 subredes iguales ¿Cuál será la nueva mascara de subred?

   A. 255.255.255.0

B. 255.255.0.128
C. 255.255.255.128
D. 255.255.0.0

2. Se le solicita dividir la red 192.168.1.0/24 en al menos 12 redes iguales ¿Cuál será la nueva mascara de subred de esas 12 redes?

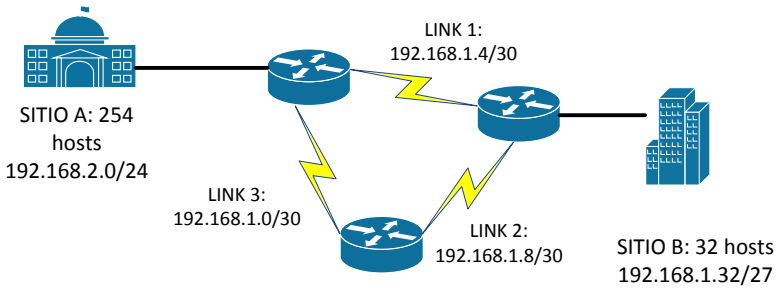
A. 255.255.255.128
B. 255.255.255.224
C. 255.0.0.0
D. 255.255.255.240

3. Mencione los 4 pasos para aplicar VLSM.

4. ¿Cuántos bits se necesitan en la porción de HOST para crear una subred con 512 dispositivos?

A. 10.
B. 9.
C. 12.
D. 8.

5. Un compañero hizo el diseño en la figura. Identifica cual es el problema con su esquema.



A. El sitio B no tiene suficientes direcciones asignables.
B. El sitio A no tiene suficientes direcciones asignables.
C. El direccionamiento en los enlaces de los routers es incorrecto.

6. Se le ordena dividir el bloque 192.168.0.0/20 en 4 redes del mismo tamaño, ¿Cuáles de las siguientes opciones son parte de las 4 subredes?

   A. 192.168.0.0/24
   B. 192.168.8.0/24
   C. 192.168.4.0/22
   D. 192.168.2.0/22
   E. 192.168.12.0/22
   F. 192.168.1.0/24

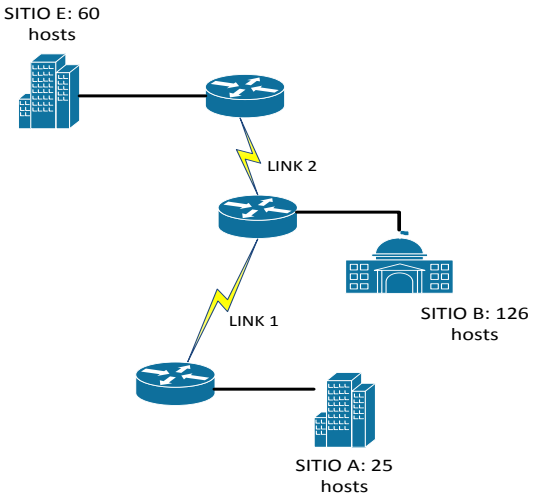
7. El administrador de red le ordena tomar la segunda dirección asignable de la tercera subred del ejercicio anterior ¿Qué dirección tomaría?

   A. 192.168.0.1
   B. 192.168.0.2
   C. 192.168.12.1
   D. 192.168.8.2
   E. 192.168.1.2
   F. 192.168.8.1
   G. 192.168.12.2

8. ¿Qué representa una máscara de subred /32?

   A. Un error.
   B. La dirección de un solo host.
   C. La dirección de una subred.
   D. La dirección de muchos hosts.

9. Aplique VLSM al diagrama siguiente con el bloque asignado 172.16.1.0/24.



10. Se le da un bloque de direcciones con mascara /20. Después se le solicita dividir dicho bloque en 5 subredes:
    2 que puedan contener 256 hosts.
    3 que sean de igual tamaño.
    ¿Cuáles son las máscaras de las 3 subredes de igual tamaño y de las 2 que pueden albergar 256 hosts que cumplen con lo anterior?

    A. /24 para albergar 256 hosts y /23 para las demás subredes.
    B. /23 para albergar 256 hosts y /21 para las demás subredes.
    C. /23 para albergar 256 hosts y /20 para las demás subredes.
    D. /23 para albergar 256 hosts y /22 para las demás subredes.
    E. /26 para albergar 256 hosts y /23 para las demás subredes.

Capítulo III: OSPFv2

Introducción

OSPF (Open Shortest Path First) es un protocolo de estado de enlace que pertenece a un grupo de protocolos de Gateway interior, los protocolos de estado de enlace usan una filosofía diferente a los protocolos de vector-distancia, en los protocolos de estado de enlace cada nodo en la red tiene información acerca de toda la topología de la red, incluyendo la forma en que están conectados los demás nodos y el tipo de enlace que usan para esta conexión.

Conceptos previos

Interior Gateway Protocols (IGP's): Protocolos de ruteo que se usan al interior de una Sistema Autónomo (AS) para comunicar las diferentes redes existentes.
Sistema Autónomo (AS): Un sistema autónomo es un grupo de redes o routers bajo la autoridad o administración de una sola entidad.

Características generales de OSPF

Como ya se mencionó antes, OSPF es un protocolo de estado de enlace, donde cada nodo conoce la topología entera de la red, con esto puede usar algoritmos de cálculo de la ruta más corta para llegar a un destino, el algoritmo que usa OSPF es Dijkstra. Con ello pude hacer un cálculo rápido de cuál es la mejor ruta dependiendo de la métrica resultante del algoritmo.

La métrica utilizada en OSPF se llama costo, el costo dependerá de varios o un solo factor, como lo es el ancho de banda, el retardo, etc. El cálculo del costo entonces variara dependiendo de los dispositivos utilizados así como de los fabricantes, para los productos de Cisco, por defecto, el costo se calcula de la siguiente manera:

$$Costo = {}^{10^8}/_{BW}$$

Donde BW es el ancho de banda.
OSPF es uno de los protocolos más preferidos a la hora de la implementación, lo anterior se debe a diferentes características que ofrecen una ventaja sobre otros protocolos, entre las cuales podemos listar las siguientes:

- Eficiencia.
- Permite la creación de áreas y sistemas autónomos.
- Minimiza el tráfico de actualización (updating).
- Protocolo Classless.
- Es altamente flexible, versátil y escalable.
- Estabilidad.
- Ofrece un conteo ilimitado de saltos.
- Es un protocolo abierto.
- Tiene una convergencia rápida.
- En el diseño pude confinar la inestabilidad de algunas redes a áreas únicas.
- Distancia administrativa de 110.

Áreas y tipos de routers en OSPF

OSPF organiza a un sistema autónomo en distintas áreas, estas áreas son agrupaciones lógicas de routers cuya información se puede resumir para las demás áreas en el AS, esta es una gran característica de OSPF que entre otras cosas evita una sobrecarga en el tráfico de actualización, manteniendo la misma información topológica en las bases de datos de los routers que pertenecen a una misma área.
OSPF define 2 tipos distintos de roles en los routers que ayudan a direccionar el tráfico entre distintas áreas así como en diferentes AS, estos roles se describen de la siguiente manera.

- Routers fronterizos de área o ABRs (Area Border Routers): Estos routers son los encargados de conectar 2 áreas, su base de datos mantiene información sobre las rutas en ambas áreas, es decir que este router

seguramente tendrá interfaces pertenecientes a un área y otras interfaces pertenecientes a un área distinta, permitiendo encaminar el tráfico entre las diferentes áreas. A este direccionamiento de tráfico se le conoce como inter-area routing.

- Routers fronterizos del AS o ASBRs (Autonomous System Border Routers): Estos routers se encargan de conectar 2 AS, permitiendo encaminar la información hacia otros AS, generalmente permitiendo la comunicación con Internet (vea la figura 3.2). A este direccionamiento de tráfico se le conoce como external routing.

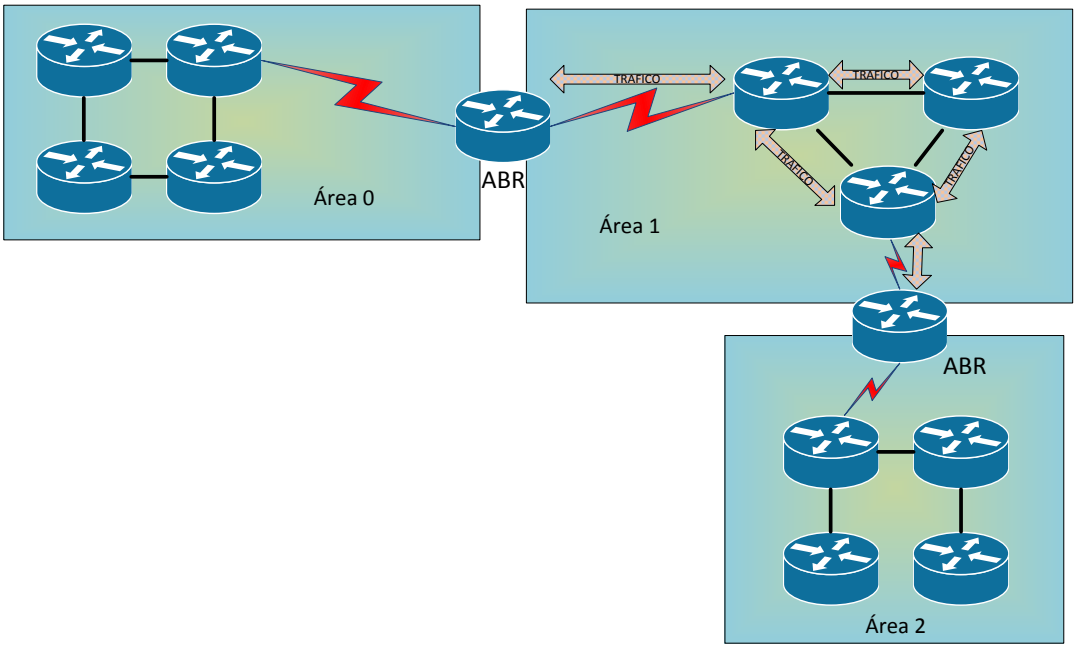


Figura 3. 1: División de áreas y la forma en que OSPF propaga información.

En la figura se muestra como se propaga el trafico OSPF en una sola área, sin afectar a las demás.

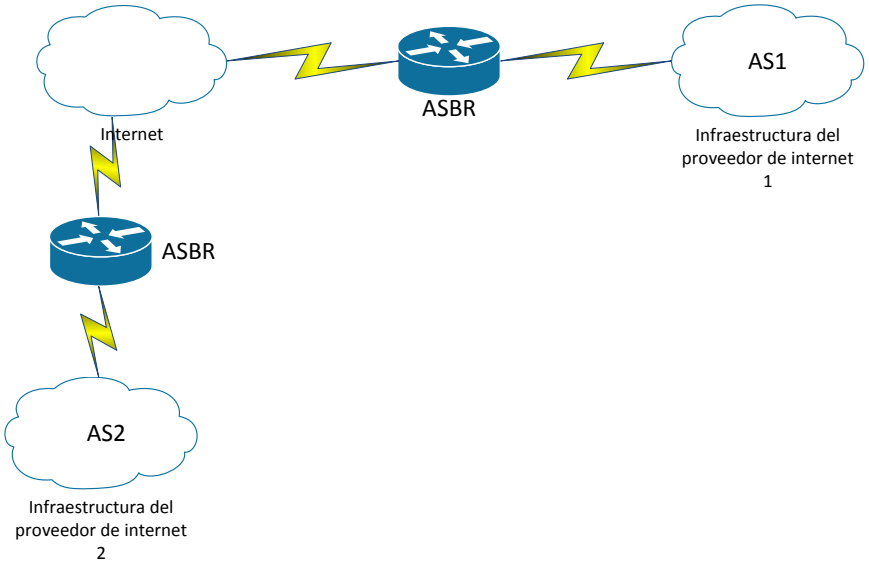


Figura 3. 2: Sistemas autónomos conectados por un ASBR.

Operación de OSPF

En primera instancia el router habilitado con OSPF intentara establecer una relación de adyacencia con sus vecinos más cercanos a través de los mensajes Hello. Tenemos que resaltar que para que suceda lo anterior los routers vecinos deben tener configurados los siguientes parámetros de la misma forma:

- Área ID.
- Intervalos Hello y Dead.
- Password de autenticación.
- La bandera “stub area”.

Después de haberse formado la adyacencia, los routers comenzaran a inundar la red con paquetes LSA (Link State Advertaisment), los cuales contienen el estado y costo de cada enlace directamente conectado, los routers que reciben los LSA inmediatamente inundan esos LSA a otros vecinos con los que hayan formado la adyacencia, esto se hace hasta que todos los routers OSPF del área tengan todos los LSA. Finalmente con los LSA recibidos se construye una tabla topológica en cada router, donde esta base de datos mantiene toda la información acerca de la topología de la red, después se aplica el algoritmo de cálculo de la ruta más corta,

obteniendo como resultado las mejores rutas hacia cualquier red, estas rutas son insertadas en la tabla de ruteo del dispositivo.

Tipos de paquetes OSPF

Para su correcto funcionamiento OSPF hace uso de cinco tipos de paquetes cuya función describiremos brevemente a continuación:

- Hello: Este paquete sirve para descubrir vecinos y construir adyacencias entre los diferentes routers OSPF.
- Database Description: Este paquete sirve para intercambiar información de la topología, y sincronizar esta información en las bases de datos de todos los routers.
- Link State Request: Este paquete sirve para hacer una petición de información sobre un enlace en específico de router a router.
- Link State Update: Este paquete es la respuesta a las peticiones que se hacen a través de los paquetes Link State Request.
- Link State Acknowledgment: Este paquete cumple la función de acuse de recibo para los otros tipos de paquetes.

La siguiente figura resume la información anterior.

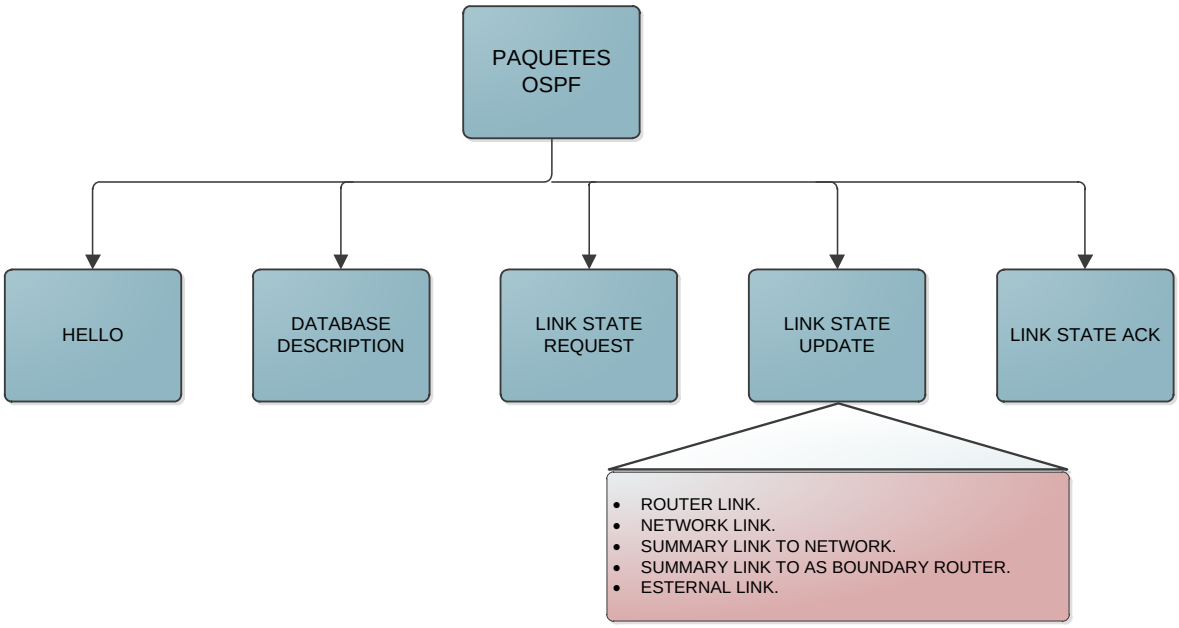


Figura 3. 3: Tipos de paquetes usados por OSPF.

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.
A. Tanenbaum and D. Morales Peake, Redes de computadoras. México: Prentice-Hall Hispanoamericana, 1997.
RFC 2328.
RFC 1247.
RFC 4577.

Tabla de comandos

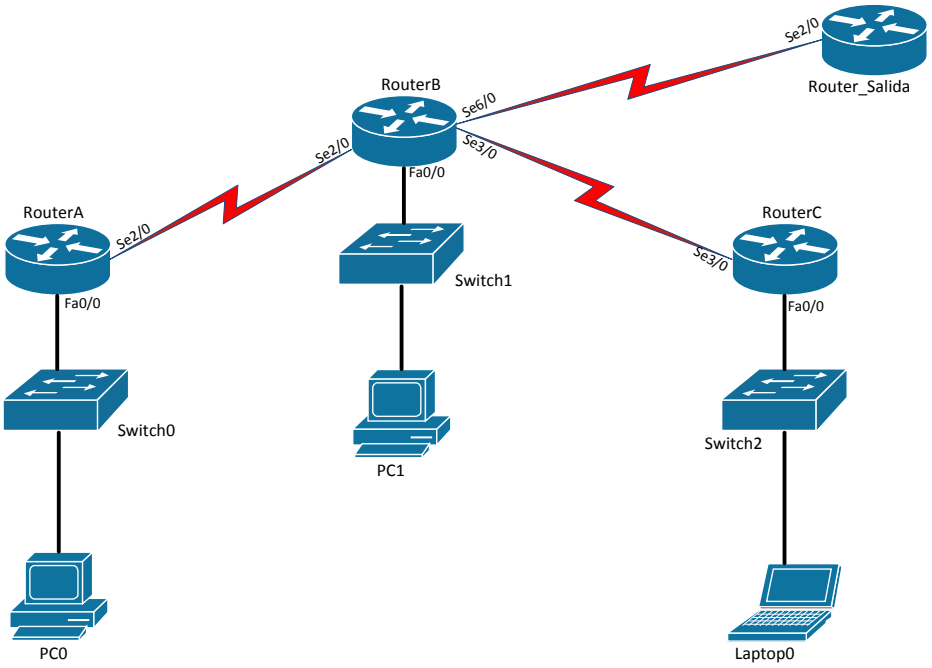
COMANDO	DESCRIPCIÓN.
#configure terminal	Habilita el modo EXEC privilegiado
(config)#router ospf ***[ID process]***	Inicia un proceso OSPF con el numero identificador “ID process”.
(config-router)# network ***[ip address] [wildcard mask]*** **area** ***[área ID]***	Habilita OSPF en las interfaces indicadas por la dirección IP y la máscara Wildcard.
(config)#interface ***[type X/X]***	Cambia al modo de configuración de interfaz, donde “type X/X” indica la interfaz que se desea configurar.
(config-if)#bandwidth ***[bandwidth]***	Modifica el ancho de banda de la interfaz, obligando a OSPF a recalcular las rutas con el nuevo valor. La unidad de medida son kbps.
(config-if)#ip ospf cost ***[cost]***	Establece un valor deseado como costo OSPF de la interfaz.
(config-router)#auto-cost reference-bandwidth ***[autocost]***	Establece un nuevo valor al costo de referencia usado para el cálculo de la métrica en OSPF. La unidad de medida es Mbps
	Recuerde que el costo de referencia por default es de 10^8, que serían 100 Mbps. Si

	usted hace esta configuración asegúrese de que todos los routers tengan el mismo valor de auto referencia ya que de lo contrario esto puede ocasionar problemas.
(config-if)#ip ospf hello-interval *[time]*	Modifica el intervalo Hello. La unidad de medida es en segundos.
(config-if)#ip ospf dead-interval *[time]*	Modifica el intervalo Dead. La unidad de medida es en segundos.
(config-router)#default-information originate	Propaga la ruta por defecto a todos los routers OSPF.

Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de subred
RouterA	Fa0/0	172.16.1.254	255.255.255.0
	Se2/0	172.16.2.1	255.255.255.252
RouterB	Fa0/0	172.16.3.254	255.255.255.0
	Se2/0	172.16.2.2	255.255.255.252
	Se3/0	172.16.5.1	255.255.255.252
	Se6/0	172.16.6.1	255.255.255.252
RouterC	Fa0/0	172.16.4.254	255.255.255.0
	Se3/0	172.16.5.2	255.255.255.252
Router_Salida	Se2/0	172.16.6.2	255.255.255.252

Topología



Desarrollo

Actividad 1

1. Pase al modo de simulación y edite los filtros para que solo pueda ver paquetes OSPF v2.
2. En ***RouterA*** habilite un proceso OSPF con el número identificador de 100.
3. Habilite las interfaces activas del ***RouterA*** para que envíen paquetes OSPF y puedan descubrir posibles vecinos.
4. Simule el envío de paquetes con el botón ***Capture/Forward***. ¿Hay alguna respuesta de los dispositivos hacia el ***RouterA***?
5. En ***RouterB*** habilite un proceso OSPF con el número identificador de 100.
6. Habilite las interfaces activas del ***RouterB*** para que envíen paquetes OSPF y puedan descubrir nuevos vecinos. Haga lo anterior con solo un comando network.
7. Corra de nuevo la simulación y note como se da el intercambio de paquetes entres los routers. Además puede ver el contenido de estos paquetes haciendo clic sobre el mensaje en específico.

Actividad 2

1. Habilite en ***RouterC*** un proceso OSPF con el numero identificador 99. Después habilite las interfaces activas del router para enviar paquetes OSPF.
2. Habilite en ***Router_Salida*** un proceso OSPF con el numero identificador 85. Después habilite las interfaces activas del router para enviar paquetes OSPF.
3. Haga pruebas de conectividad entre los routers de la topología y revise que entre todos se pueden comunicar.
4. Haga uso del comando necesario para poder ver la tabla de ruteo en ***RouterB***. ¿Cuantas entradas OSPF puede ver en la tabla?
5. Identifique y liste los costos y distancia administrativa de cada ruta que hay en la tabla de ruteo.
6. Utilice el comando ***show ip protocol*** en ***RouterB*** para ver los protocolos de ruteo que está corriendo. ¿Qué información importante podemos recatar de este comando?
7. En ***RouterB*** utilice el comando ***show ip ospf inteface***. Liste los costos que tiene cada interfaz activa. ¿Cuáles son los tiempos por default de los intervalos Hello y Dead?
8. Utilice el comando ***show ip ospf neighbor*** en ***RouterB.*** ¿Cuántos vecinos tiene registrado el router? ¿Cuáles son sus ID?

Actividad 3

1. ¿Cómo se calcula el costo de una interfaz?
2. ¿Cuál es ancho de banda de referencia que por default viene configurado en los routers Cisco?
3. Utilice el comando necesario para poder ver el costo de la interfaz Fa0/0 en ***RouterA.***
4. En ***RouterA*** vaya al modo de configuración del proceso “OSPF 100” y emplee el comando ***auto-cost reference-bandwidth 1000*** para cambiar el ancho de banda de referencia a 1 Gbps. Observe los cambios en el costo

de la interfaz Fa0/0. ¿Cuál es el nuevo costo de la interfaz?¿Cuál era el anterior?

5. Regrese el ancho de banda de referencia a su valor por defecto de 100 Mbps.
6. En ***RouterA*** vaya al modo de configuración de interfaz Fa0/0 y utilice el comando ***bandwidth 1000*** para "cambiar el ancho de banda de la interfaz". Observe los cambios en el costo de la interfaz Fa0/0.
7. En ***RouterA*** vaya al modo de configuración de interfaz Fa0/0 y utilice el comando ***ip ospf cost 75*** para cambiar el costo de la interfaz. Observe los cambios con el comando ***show ip ospf interface fa0/0***.

Conclusiones

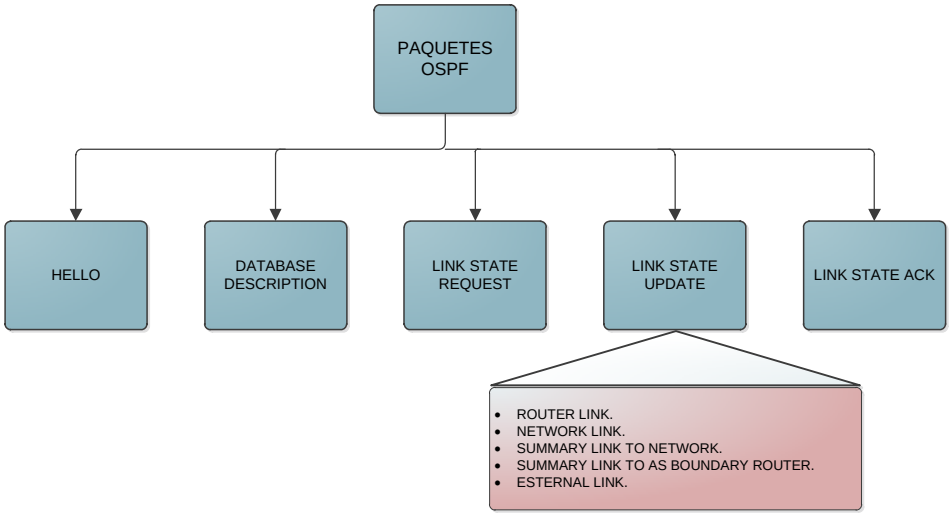
En esta práctica logramos ver el funcionamiento básico de OSPFv2, sus características y ventajas que le han permitido ser uno de los protocolos de ruteo más importantes en la actualidad, le sugerimos mantener los siguientes conceptos en mente que le serán útiles para entender mejor OSPFv2.

- OSPF utiliza el concepto de Sistema Autónomo (AS) y de áreas, recuerde que un sistema autónomo es un grupo de dispositivos bajo la administración de una misma entidad. Al dividir en áreas al sistema autónomo, OSPF mejora el rendimiento de la red evitando sobrecargarla con tráfico de actualización entre otras ventajas.
- OSPF hace uso de un algoritmo de cálculo de la ruta más corta llamado Dijkstra. La métrica implementada por el protocolo se le llama costo, la cual puede depender de varios factores, en routers Cisco por defecto el costo se calcula con la siguiente formula.

$$Costo = {10^8}/{BW}$$

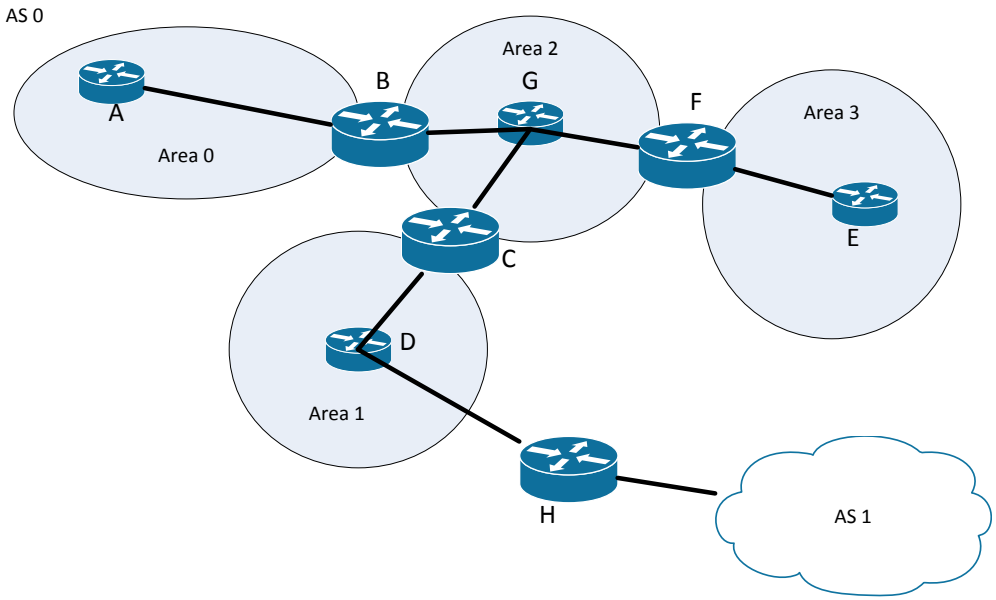
- Entre las características más apreciadas de OSPF podemos nombrar las siguientes; eficiencia, protocolo Classless, flexible, versátil, escalable, estable y tiene una rápida convergencia.
- OSPF también define dos roles especiales entre los routers, el primero de ellos es router fronterizo (ABR) que se encarga de conectar y comunicar 2 áreas, el segundo de ellos es router fronterizo de AS (ASBR) el cual se encarga de comunicar sistemas autónomos diferentes.

- El protocolo hace uso de diferentes tipos de mensajes, cada uno cumple con una función específica, estos mensajes se resumen en la siguiente figura.



Cuestionario

1. En la figura que se muestra a continuación, marque los routers que cumplen el rol de ABR's.



A. A
B. B
C. C

D. D
E. E
F. F
G. G
H. H

2. Un router aprende una ruta a cierta dirección de tres maneras distintas, la primera es a través de OSPF con una métrica de 68, la segunda es una ruta estática configurada por el administrador, y la última es una ruta aprendida de RIPv2 con una métrica de 6. ¿Cuál de las siguientes opciones tomara el router a la hora de instalar una ruta en su tabla de ruteo?

   A. La ruta aprendida a través de OSPF
   B. La ruta aprendida a través de RIPv2
   C. Las tres rutas.
   D. La ruta estática.

3. ¿Cuáles de los siguientes parámetros deben coincidir en la configuración de un router para que se conviertan en vecinos?

A. Area ID.
B. Router ID.
C. Stub area flag.
D. Intervalos Hello y Dead.

4. Escribe el nombre de los 5 mensajes principales de los cueles hace uso OSPFv2.

5. Un administrador de red te dice que ha insertado los siguientes comandos en su router.

```
Router1(config)#router ospf 100
Router1(config-router)#network 192.168.1.0 255.0.0.0 area 0
Router1(config-router)#
```

   ¿Cuál es el error en su configuración?

   A. El identificado de proceso “100”
   B. La máscara Wildcard

C. La dirección 192.168.1.0
D. Ninguno. Su configuración es correcta.

6. ¿Cuál es la distancia administrativa de OSPF?

A. 120
B. 110
C. 90
D. 1

7. Observe la información de la siguiente figura ¿Cuál es el ancho de banda BW de la interfaz Serial2/0 si el router tiene las configuraciones por defecto?

```
Serial2/0 is up, line protocol is up
  Internet address is 172.16.2.1/30, Area 0
  Process ID 100, Router ID 172.16.2.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
```

A. 10 Mbps.
B. 1 Gbps.
C. 1.5625 Mbps.
D. 100 Mbps.

8. Suponga que está trabajando con el mismo router del ejercicio anterior. Uno de sus compañeros decide insertar los siguientes comandos.

```
Router0(config)#router ospf 100
Router0(config-router)#auto-cost reference-bandwidth 10
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
Router0(config-router)#
```

¿Cuál será el nuevo costo de la interfaz Serial2/0?
Nota: Por facilidad redondee los números decimales del costo.

A. 7.

B. 10.
C. 64.
D. 6.

9. Uno de sus compañeros le pide ayuda con un problema. Él ha configurado ***Router0*** y ***Router1*** para que se conviertan en vecinos, desafortunadamente esto no sucede. Usted revisa la configuración en ambos routers y observa lo siguiente.

Router0.

```
Serial2/0 is up, line protocol is up
  Internet address is 172.16.2.1/30, Area 0
  Process ID 100, Router ID 172.16.2.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 50, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:15
```

Router1.

```
Serial3/0 is up, line protocol is up
  Internet address is 172.16.4.1/30, Area 0
  Process ID 100, Router ID 172.16.4.1, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
```

¿Cuál es el problema por el cual los routers no pueden ser vecinos?

A. El área OSPF no está configurada apropiadamente.
B. El process ID no está configurado correctamente.1
C. Los intervalos Hello y Dead no están configurados correctamente.
D. La prioridad está configurada incorrectamente.

10. ¿Cuál de los siguientes comandos habilitara OSPF área 0, en la interfaces que tengan direcciones en la red 192.168.1.0/27.

A. network 192.168.1.0 255.255.255.0 area 0.
B. network 192.168.1.0 255.255.255.224 area 0.

C. network 192.168.1.0 0.0.0.31 area 0.
D. network 192.168.1.0 255.255.255.0 area 1.

Capítulo IV: Listas de Control de Acceso

Introducción

En esta práctica revisaremos lo que son las Listas de Control de Acceso (ACL), su funcionamiento, la importancia que tienen en el filtrado de paquetes e implementación de medidas de seguridad básica. Analizaremos las mejores prácticas a la hora de programar una ACL e implementarla en nuestra red.

Conceptos previos

Que son las ACL y para que nos sirven

Por defecto un router no está configurado para filtrar el tráfico de datos, el tráfico que entra al router se direcciona únicamente basado en la información contenida en la tabla de enrutamiento.
Para un administrador de red probablemente lo anterior se pueda convertir en un problema, debido a que hay tráfico “sensible” que no queramos que sea enrutado fuera de una red, por ejemplo información acerca de los empleados en una empresa, también se puede dar la posibilidad de que no queramos recibir cierto tipo de información en nuestra red, es por ello que se ha vuelto una tarea de gran relevancia, el hecho de implementar medidas que protejan las redes y nuestros datos sensibles.

Se han desarrollado muchas tecnologías que nos ayudan a evitar el problema anterior, entre las cuales podemos destacar, los firewalls, sistemas de prevención y detección de intrusos, así como complejos programas de antivirus y antispyware, pero a un nivel básico de administración de red, nosotros podemos hacer uso de las ACL, cuya principal tarea es el filtrado de tráfico en los routers.

Una ACL es una lista secuencial de sentencias “permit” y “deny”, que esencialmente nos sirve para categorizar los paquetes IP en un router, y después tomar una decisión, en este caso descartar el paquete o permitir que el paquete continúe su ruta. Las ACL son de mucha utilidad a la hora de manejar y controlar el tráfico de una red, ya que podemos categorizar todos los paquetes y tomar una decisión en base a la información que deseemos filtrar.

Las ACL categorizan los paquetes IP basándose en información de capa 3 y 4, en específico en la dirección IP destino y fuente de los dispositivos, en capa 4 identifican el protocolo para filtrar los paquetes.

Crear un ACL es realmente sencillo, si alguna vez ha programado, en realidad es muy similar a ese proceso, ya que solo hay que redactar bien las sentencias que conforman la ACL, y finalmente aplicarla a la interfaz de un router. Para ello antes debemos entender cómo es que un paquete es “analizado” por la ACL, es muy simple solo debe recordar estas tres reglas:

- El paquete siempre es comparado con cada línea de la ACL en orden secuencial.
- El paquete será comparado con las sentencias que conforman la ACL, solo hasta que una de ellas se cumpla.
- Hay una sentencia “deny” (descartar) implícita al final de cada ACL, esto significa que al final si el paquete es comparado con todas las líneas anteriores y no se haya coincidencia, el paquete será descartado.

Tipos de ACL

En dispositivos Cisco podemos crear diferentes tipos de ACL, las cuales tienen diferencias que nos pueden ayudar a hacer un filtrado de paquetes de una mejor manera, vamos a hacer una descripción breve de estos tipos de ACL en la siguiente sección:

- Standard ACL (listas de control de acceso estándares): estas ACL usan solo la IP fuente en el paquete como condición de prueba, es decir solo comparan la IP fuente con las sentencias en la ACL, todas las decisiones son hechas basadas en esta IP.
- Extended ACL (listas de control de acceso extendidas): estas ACL pueden evaluar otros campos en capa 3 y 4, pueden evaluar tanto la IP fuente como destino en capa 3, el campo de protocolo en el encabezado IP y el número de puerto en el encabezado de la capa de trasporte.

También tenemos las Named ACL, pero no listaremos esta como parte de los tipos de ACL, debido a que en realidad se comportan igual que alguno de los otros 2 tipos, lo único que cambia es la forma en la que nos referenciamos a la ACL, en este caso a partir de un nombre y no de un numero como en los casos listados.

Después de crear una ACL vamos a tener que aplicarla en la interfaz de un router, donde se quiere que el tráfico sea filtrado, se va a tener que decidir la dirección en que la ACL es aplicada, para lo cual solo existen 2 posibles opciones:

Inbound ACL: cuando una ACL es aplicada de manera Inbound (entrante) en una interfaz, los paquetes son procesados a través de ACL antes de ser enrutados a la interfaz de salida.

Outbound ACL: cuando una ACL es aplicada de manera Outbound (saliente) en una interfaz, los paquetes son enrutados a la interfaz de salida y luego procesados por ACL.

Lineamientos generales para crear una ACL

Existen algunos lineamientos que se sugieren seguir a la hora de crear una ACL, manténgalos en mente cada vez que configure una:

- Se puede asignar solo una ACL por interfaz.
- Se puede asignar solo una ACL por dirección, es decir si se desea controlar el tráfico saliente y entrante se necesitaran 2 ACL.

- Se puede asignar solo una ACL por protocolo.
- Organice la ACL de manera que las condiciones más específicas estén al principio de la lista.
- Cada vez que una nueva condición es agregada esta se coloca al final de la ACL.
- No se pude remover 1 sola línea de la ACL, para ello se tendría que remover toda la ACL y volver a crearla. Esto ocurre a excepción de las Named ACL que permite remover una sola línea
- A menos que la ACL termine con el comando "***permit any***" todos los paquetes serán descartados si no cumplen con las condiciones anteriores.
- Las ACL están diseñadas para filtrar el tráfico que pasa a través del router, estas no están diseñadas para filtrar tráfico generado por el router.
- Coloque una ACL estándar tan cerca como sea posible del destino.
- Coloque una ACL extendida tan cerca como sea posible de la fuente de tráfico a filtrar.

Manejo de la máscara Wildcard

Antes de seguir avanzando con el tema, es necesario aprender a manejar bien la máscara Wildcard, está al igual que la máscara de subred, es de vital importancia a la hora de configurar un router, en especial cuando estamos creando una ACL.

Recordemos que una de las tantas funciones de la máscara de subred, es la de ayudar al router a identificar si una dirección pertenece a un bloque o rango de direcciones, pues la máscara Wildcard también tiene la misma función, esta nos ayudara a encontrar coincidencias para identificar si una dirección IP está dentro de cierto bloque, existe una manera sencilla de calcular una máscara Wildcard y es usando la siguiente formula.

$$Wildcard = Dirección\ de\ broadcast\ (255.255.255.255) - Mascara\ de\ Subred$$

Lo anterior se hace octeto a octeto de manera decimal. Es decir si deseamos encontrar la máscara Wildcard correspondiente a la máscara de subred /24, haríamos lo siguiente:

$$\begin{matrix}255 & 255 & 255 & 255\\ 255 & 255 & 255 & 0\end{matrix} = 0.0.0.255$$

Esta máscara la podemos incluir en una ACL en concreto, dictándole que solo deje pasar paquetes que contengan una dirección IP fuente proveniente del rango de direcciones 192.168.1.0, con mascara Wildcard 0.0.0.255. Lo anterior quiere decir que el router filtrara los paquetes, dejando pasar a aquellos que provengan de la red 192.168.1.0/24.

Es muy importante que aprenda a visualizar el rango de direcciones IP que conlleva un mascara Wildcard, lo más recomendable es que practique obteniendo las máscaras Wildcard de las máscaras de subred que se usan de manera común, como por ejemplo las máscaras usadas para los enlaces entre los routers que son mascara /30, cuya mascara Wildcard seria 0.0.0.3.

ACL estándar

Ahora vamos a ver cómo crear una ACL estándar, como sería la sintaxis de las instrucciones, así como la interfaz del router en la cual aplicaríamos esta ACL. Para ello usaremos un ejemplo.

Ejemplo: Se le pide crear una forma de limitar el tráfico proveniente de la PC hacia el servidor FTP, además debe evitar que el servidor FTP no se comunique con el servidor web (observe la figura 4.1).

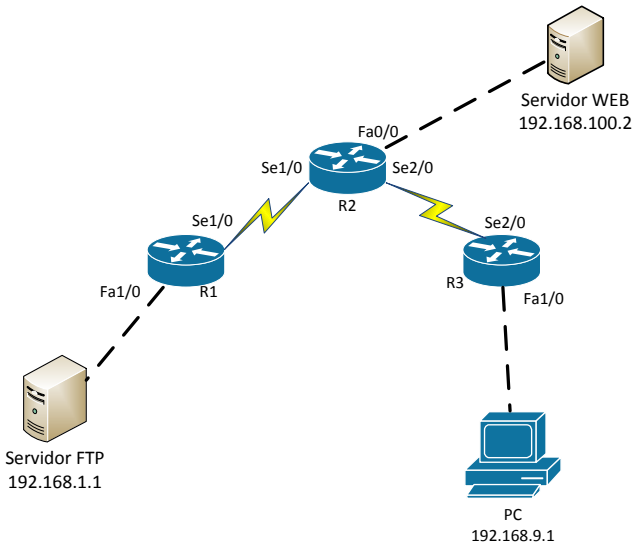


Figura 4. 1: Ejemplo de implementación de una ACL estándar.

En este ejemplo, usaremos una ACL estándar la cual nos puede ayudar a hacer el trabajo, antes que nada debemos tener claro los enunciados, entender perfectamente que tipo de trafico va a filtrar la ACL es crucial, en esencia se nos pide bloquear el tráfico que fluye de las siguientes maneras (vea la figura 4.2).

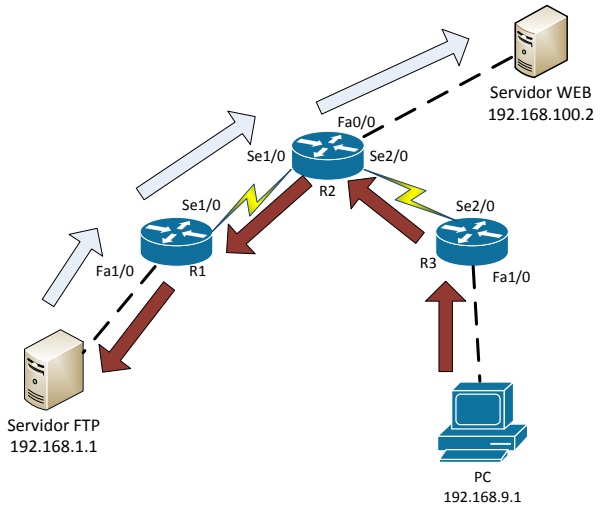


Figura 4. 2: Dirección del tráfico de datos.

En la figura 4.2 podemos ver que en azul tenemos el tráfico del servidor FTP al servidor web, y en rojo de la PC hacia el servidor FTP. Si seguimos las recomendaciones vamos a colocar una ACL estándar, tan cerca cómo se pueda del destino, aquí tenemos 2 destinos que están en diferentes subredes por lo que conviene crear 2 ACL. La primera estará cerca del servidor FTP (en R1), la segunda estará cerca del servidor web (R2).

Ahora vamos a decidir en qué interfaz colocaremos las ACL, en R1 podemos colocar la ACL en la interfaz Se1/0 ó en la interfaz Fa1/0, pero siguiendo la recomendación anterior, colocaremos la ACL en la interfaz Fa1/0. Como el tráfico que vamos a bloquear sigue la ruta roja, cuando pase por la interfaz Fa1/0 estará "saliendo" de dicha interfaz por lo que la ACL será Outbound.
Lo anterior lo podemos aplicar a R2, donde elegiremos colocar la ACL en la interfaz Fa0/0, si observamos el trafico azul que es el que bloquearemos, vemos que cuando pasa por Fa0/0 estará "saliendo" por lo que dicha interfaz será también Outbound.

Finalmente lo único que debemos hacer es crear las ACL y aplicarlas, siguiendo la sintaxis descrita en la tabla de comandos más adelante, podemos crear ambas ACL con un solo par de comandos:

En R1
(config)#access-list 10 deny host 192.168.9.1 (config)#access-list 10 permit any (config)#interface Fa1/0 (config-if)#ip access-group 10 out

En R2
(config)#access-list 5 deny 192.168.1.1 0.0.0.0 (config)#access-list 5 permit any (config)#interface Fa0/0 (config-if)#ip access-group 5 out

Figura 4. 3: Sentencias para la configuración de la ACL.

En la configuración anterior, vale la pena notar las 2 formas diferentes en la cuales se puede referir a un host, la primera de ellas es usando la palabra host en la instrucción para indicar que solo bloquearemos esa dirección, en la segunda dirección se hace uso de la máscara Wildcard, como sabemos la máscara de subred que hace referencia a una sola dirección es 255.255.255.255, por lo que la máscara Wildcard asociada será 0.0.0.0. También note que al final de cada ACL, se colocó una instrucción que permite cualquier tráfico, esto con la intención de anular el efecto del “deny” implícito, ya que de lo contrario, afectaríamos tráfico de otras fuentes que puede llegar hacia cada dispositivo.

ACL extendida

Vamos a estudiar como creamos una ACL extendida y para que nos puede servir, la diferencia que tienen estas ACL con las estándar, es que en estas ACL podemos crear criterios de filtrado más amplios, debido a que se analizan más campos además de la dirección IP fuente, también podemos usar como criterios la IP destino, algún protocolo de capa 3 como ICMP, protocolos de capa 4 (UDP y TCP), así como ciertas aplicaciones o puertos de capa 4.

Debido a que tenemos más opciones de filtrado, la estructura de las sentencias que conforman las ACL es un poco más compleja. Esta estructura la podrá encontrar en la tabla de comandos, pero trataremos de explicarla aquí mientras aplicamos un ejemplo.

Ejemplo:
Se le encomienda diseñar una ACL que; no permita que PC2 reciba tráfico web de ninguna fuente, que el trafico FTP sea enviado solo a la PC1, y que además evite que PC2 pueda hacer ping hacia PC1 o el servidor web (figura 4.4).

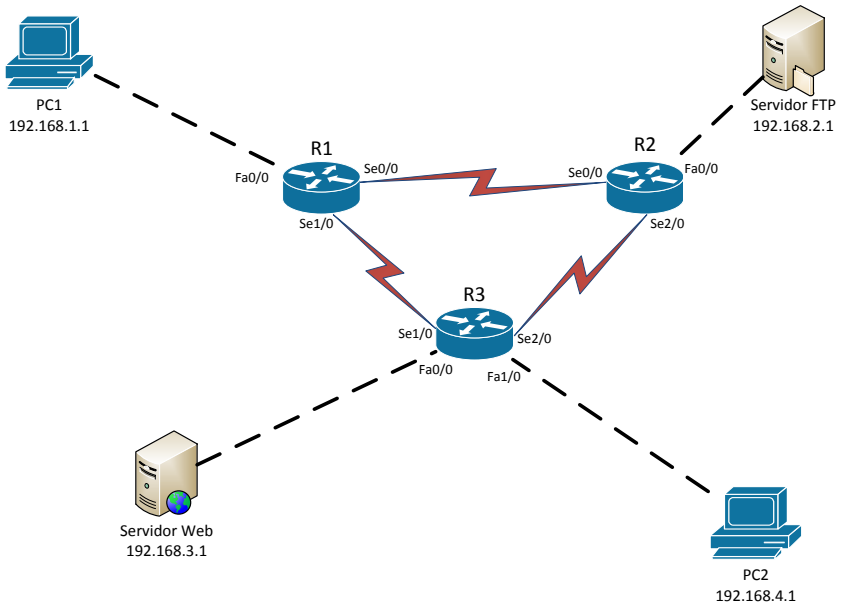


Figura 4. 4: Ejemplo de ACL extendida.

Como en el ejercicio anterior es muy importante leer detenidamente y entender lo que se nos pide, luego solo tenemos que seguir las recomendaciones antes explicadas, primero hay que recordar que una ACL extendida se debe colocar lo más cerca de la fuente de tráfico a filtrar, por lo que identificaremos las fuentes de tráfico que debemos filtrar en la topología.

- Tenemos que filtrar el tráfico web hacia PC2, por lo que es conveniente crear una ACL en R3.
- Tenemos que filtrar el trafico FTP, de tal forma que solo llegue a PC1, por lo que es conveniente crear una ACL en R2.

- Tenemos que denegar a PC2 la posibilidad de hacer ping hacia PC1 o hacia el Servidor web, por lo cual conviene crear la ACL en R3.

Ahora que hemos identificado las fuentes de tráfico hay que identificar las interfaces y la dirección en la cual colocaremos la ACL. Para ello hemos ilustrado en la figura 4.5 la dirección de dicho tráfico.

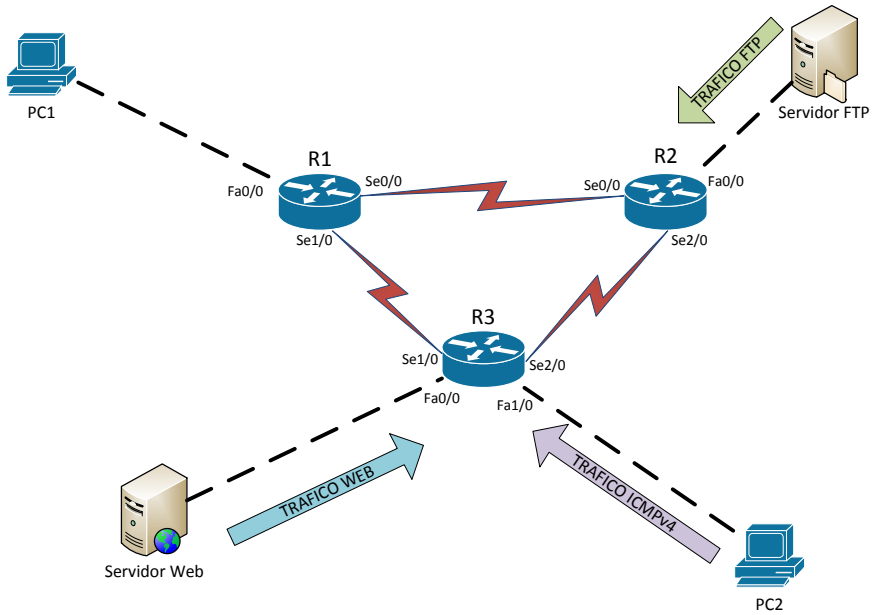


Figura 4. 5: Dirección del tráfico en la red.

De la figura anterior podemos concluir las direcciones e interfaz donde colocaremos las ACL:

- ACL 110 en la interfaz Fa0/0 de R3 de manera Inbound.
- ACL 120 en la interfaz Fa1/0 de R3 de manera Inbound.
- ACL 130 en la interfaz Fa0/0 de R2 de manera Inbound.

Ahora solo queda construir las ACL a través de las sentencias necesarias, como antes se hizo primero se construye la ACL y luego se aplica a una interfaz. Para ello vamos a mostrar cómo es la sintaxis en los routers Cisco para poder armar las sentencia de una manera correcta.

En modo de configuración global escribimos las sentencias con el siguiente formato:

access-list [numero] [deny/permit/remark] [protocolo] [IP fuente] [Wildcard] [operador] [numero de puerto TCP/UDP ó nombre] [IP destino] [Wildcard] [operador] [numero de puerto TCP/UDP ó nombre]

- [numero]: numero entre 100 y 199 ó 2000 y 2699.
- [deny/permit/remark]: parte de la sentencia que permite o deniega el tráfico, la opción remark sirve para añadir comentarios.
- [protocolo]: protocolo que se lee en el encabezado de capa 3, puede ser TCP, UDP o ICMP, entre otros.
- [IP fuente]: dirección o direcciones fuente.
- [IP Destino]: dirección o direcciones Destino.
- [Wildcard]: Mascara Wildcard asociada al IP fuente o destino dependiendo del caso.
- [operador]: puede tener 3 valores; “eq” que quiere decir igual a, “gt” que quiere decir más grande que y “lt” que quiere decir menores que.
- [numero de puerto TCP/UDP ó nombre]: puerto de los protocolos más usuales, o los llamados “well-known port numbers”. A continuación una tabla de los puertos y protocolos usados por ciertas aplicaciones.

TCP	UDP
Telnet 23	SNMP 161
SMTP 25	TFTP 69
HTTP 80	DNS 53
FTP 20, 21	BooTPS/DHCP 67
DNS 53	
HTTPS 443	
SSH 22	
POP3 110	
NTP 123	
IMAP4 143	

Figura 4. 6: Lista de puertos y aplicaciones TCP/UDP.

Ahora que sabemos el formato de la sentencias debemos crear las ACL, las cueles ya tenemos numeradas, después solo habrá que aplicarlas a las interfaces.

En R3 para la ACL 110
(config)#access-list 110 deny tcp 192.168.3.1 255.255.255.255 192.168.4.1 255.255.255.255 eq 80 (config)#access-list 10 permit any any (config)#interface Fa0/0 (config-if)#ip access-group 10 in

En R3 para la ACL 120
(config)#access-list 120 deny icmp 192.168.4.1 255.255.255.255 192.168.1.1 255.255.255.255 (config)#access-list 120 deny icmp 192.168.4.1 255.255.255.255 192.168.3.1 255.255.255.255 (config)#access-list 10 permit any any (config)#interface Fa1/0 (config-if)#ip access-group 10 in

En R2 para la ACL 130
(config)#access-list 130 permit tcp 192.168.2.1 255.255.255.255 192.168.1.1 255.255.255.255 eq 20 (config)#access-list 130 permit tcp 192.168.2.1 255.255.255.255 192.168.1.1 255.255.255.255 eq 21 (config)#interface Fa0/0 (config-if)#ip access-group 10 in

Figura 4. 7: Sentencias para la configuración de la ACL extendida.

Referencias

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 2086.
RFC 4314.

Tabla de comandos

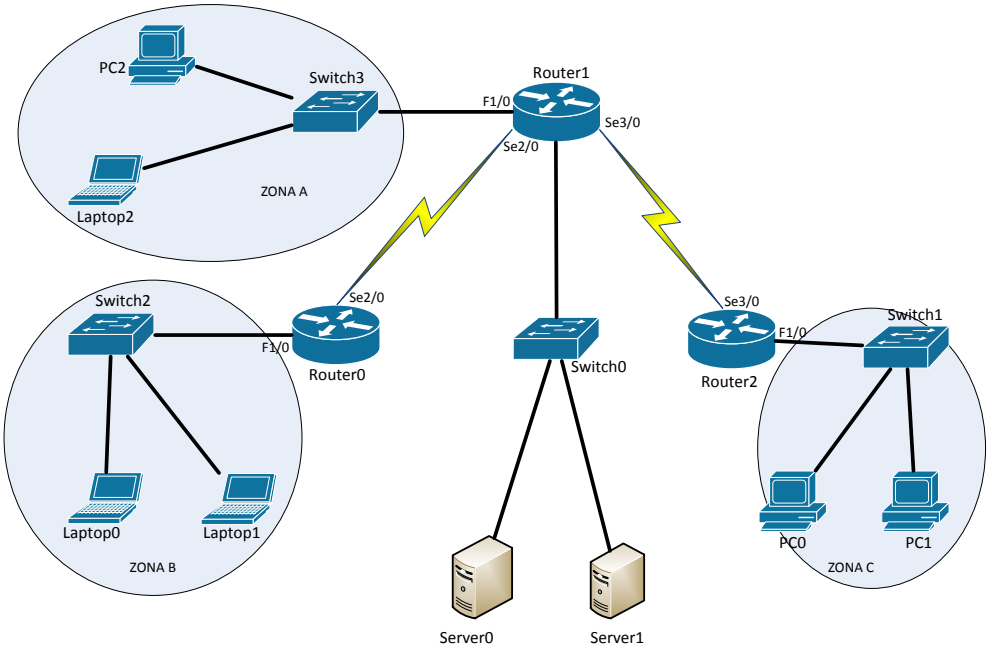
COMANDO	DESCRIPCIÓN.
(config)#access-list ***[número de ACL] [permit/deny/remark] [IP fuente] [mascara Wildcard]***	Crea o añade una sentencia a la ACL estándar indicada.
(config)#access-list ***[numero de ACL] [permit/deny/remark] any***	Usa la palabra especial “any” en lugar de una IP y una mascara, esto para especificar que deja pasar cualquier trafico. Es similar si usaramos cualquier IP y la Wildcard 255.255.255.255.
(config)#access-list ***[numero de ACL] [permit/deny/remark] host [IP del host]***	Usa la palabra especial “host” para indicar solo una dirección IP. Es similar si usamos la Wildcard 0.0.0.0.
(config)# no access-list ***[número de ACL]***	Remueve o quita una ACL.
(config)# access-list ***[número de ACL] [deny/permit/remark] [protocolo] [IP fuente] [Wildcard] [operador] [número de puerto TCP/UDP o nombre] [IP destino] [Wildcard] [operador] [número de puerto TCP/UDP o nombre]***	Crea o añade sentencias a una ACL extendida.
(config)# interface ***[tipo y nombre]***	Accede al modo de configuración de interfaz para la interfaz indicada.

(config-if)#ip access-group *[número de ACL] [in/out]*	Aplica o activa una ACL en una interfaz ya se manera “Inbound” ò “Outbound”.
#show ip interface	Muestra las ACL activas en la interfaz.
#show access-lists	Muestras todas las ACL configuradas.
#show access-list *[número de ACL]*	Muestra información de una ACL en específico.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Router0	Fa1/0	172.16.5.254	255.255.255.0
	Se2/0	172.16.2.1	255.255.255.252
Router1	Fa0/0	172.16.1.254	255.255.255.0
	Fa1/0	172.16.4.254	255.255.255.0
	Se2/0	172.16.2.2	255.255.255.252
	Se3/0	172.16.3.2	255.255.255.252
Router2	Fa1/0	172.16.6.254	255.255.255.0
	Se3/0	172.16.3.1	255.255.255.252
Server0	Fa0	172.16.1.1	255.255.255.0
Server1	Fa0	172.16.1.2	255.255.255.0
Zona A	NA	172.16.4.0	255.255.255.0
Zona B	NA	172.16.5.0	255.255.255.0
Zona C	NA	172.16.6.0	255.255.255.0

Topología



Desarrollo

Actividad 1

1. Cree las ACL necesarias para que se cumplan los siguientes requerimientos: El tráfico de PC1 y la zona A hacia los servidores debe de ser bloqueado, el tráfico entre Laptop0 y la zona A debe ser bloqueado, pero el tráfico de Laptop1 hacia la zona A debe ser permitido. Permita solo que el tráfico de la zona B entre hacia la zona C.
2. Revise las ACL que ha creado y haga pruebas de conectividad para verificar los resultados.

Actividad 2

1. Remueva todas las ACL que haya creado con anterioridad.
2. Configure las siguientes medidas de seguridad donde crea necesario:

Se desea evitar que se rastree la ruta hacia los servidores, por lo que debe negar cualquier trafico ICMP que tenga como destino los servidores. La zona A y C tienen como servidor web a Server1, en este servidor están alojadas páginas web que solo dichas zonas pueden ver, tome medidas para evitar que otros dispositivos vean estas páginas web.

3. Agregue una PC en la zona C y configúrela para obtener su configuración IP a través de DHCP. En caso de que exista algún problema de solución a este.
4. Se le pide hacer una Backup (respaldo) del archivo de configuración en cada router, guarde dichas copias vía TFTP en Server1, cada copia debe ser guardada siguiendo el siguiente formato para los nombres, Config_[Nombre del Router], donde [Nombre del Router] debe ser sustituido por el nombre del dispositivo correspondiente. Si existiera un problema resuélvalo.
5. Haga las pruebas necesarias para verificar que sus configuraciones tengan el resultado deseado.

Conclusiones

En esta práctica logramos aprender los conceptos básicos de las listas de control de acceso, es muy importante saber cómo funcionan las ACL, ya que son una medida de seguridad, que en primera instancia ayudan a filtrar el tráfico, no se debe olvidar que esto se hace en base a las direcciones IP, tanto de origen como de destino, a protocolos que están en el encabezado de capa 3, como el TCP o UDP, y los puertos que usan ciertas aplicaciones en capa 4. Recuerde bien que la diferencia entre una ACL estándar y una extendida es, que la primera usa solo como criterio de evaluación la IP destino, la segunda agrega más criterios, como la IP fuente y los protocolos de capa 3 y aplicaciones de capa 4. También recuerde la dirección en que se deben aplicar las ACL ya sea “Inbound” o “Outbound”, es importante que siga los consejos que se describieron al monumento de crear una ACL.

Cuestionario

1. ¿Cuál de los siguientes rangos es usado para las ACL extendidas?

   A. 1 – 99.
   B. 200 – 299.
   C. 100 – 199.
   D. 1000 – 1099.

2. Un compañero tuyo ha configurado la ACL mostrada a continuación, tratando de negar el tráfico proveniente de la red 192.168.1.0/24.

   (config)#ip access-list 10 deny 192.168.1.0 0.0.0.255
   (config-if)#ip access-group 10 in

   Pero se dan cuenta de que ahora ningún tipo de tráfico es permitido ¿Cuál es la razón más probable?

   A. Es debido a “deny” implícito en la ACL.
   B. La ACL fue aplicada en una interfaz errónea.
   C. La ACL debe tener “permit” en lugar de la palabra “deny”.
   D. La ACL no se habilito en la interfaz.

3. ¿Qué tipo de ACL te permite filtrar tráfico basándose solo en la IP fuente?

   A. ACL extendida.
   B. ACL básica.
   C. ACL estándar.
   D. ACL avanzada.

4. Se ha configurado la ACL mostrada a continuación.

   (config)#access-list 110 deny tcp 192.168.3.1 255.255.255.255 192.168.4.1 255.255.255.255 gt 23

   Usted se da cuenta que el trafico web no puede pasar. ¿Qué solucionaría el problema, si originalmente lo que trata de evitarse es el acceso vía telnet?

   A. Cambiar la parte de la sentencia “gt” por “eq”.
   B. Cambiar la parte de la sentencia “tcp” por “udp”.
   C. Cambiar el número de la ACL por 10.
   D. Borrar la ACL.

5. ¿Qué puertos TCP utiliza FTP?

   A. 20 y 21
   B. 80 y 81.
   C. 67 y 68.
   D. 22 y 23.

6. Se está configurando una ACL para negar tráfico TCP de la red 172.16.4.0/28 hacia la red 172.16.8.0/22 ¿Cuáles son las máscaras Wildcard que se deben introducir?

   A. 255.255.255.0
   B. 0.0.0.0
   C. 0.0.0.15
   D. 0.0.0.3
   E. 0.0.3.255
   F. 0.3.3.255

7. ¿Cuál de los siguientes rangos es usado para las ACL estándares?

   A. 1 – 99.
   B. 200 – 299.
   C. 100 – 199.

D. 1000 – 1099.

8. ¿Qué palabra clave sustituye una máscara Wildcard de 255.255.255.255?

   A. Any.
   B. Host.
   C. Eq.
   D. Deny.

9. ¿Qué comandos en el router te permite saber si una ACL está activa en cierta interfaz?

A. show ip route.
B. show access-lists.
C. show ip interface.
D. show access-list [numero de ACL].

10. ¿Cuál de las siguientes sentencias va a negar el trafico vía telnet a la PC con dirección 172.16.15.30?

    A. (config)#access-list 110 deny tcp 192.168.3.1 255.255.255.255 192.168.4.1 255.255.255.255 eq 23
    B. (config)#access-list 110 deny tcp 192.168.3.1 255.255.255.255 172.16.15.30 255.255.255.255 eq 23
    C. (config)#access-list 110 deny tcp any 172.16.15.30 255.255.255.255 gt 23
    D. (config)#access-list 110 deny tcp any host 172.16.15.30 eq 23

Capítulo V: Traducción de Direcciones de Red

Introducción

En esta práctica estudiaremos un concepto muy importante, NAT (Network Address Traslation), el cual ha tenido una tarea importante como método para lidiar con el problema de la insuficiencia de direcciones IPv4, como veremos es una solución parcial, que pretende hacer eficiente el uso de direcciones publicas en los diseños de red.

Conceptos previos

Que es NAT y para qué sirve

NAT (Network Address Traslation) es una solución parcial, que nos permite enfrentar el problema del uso eficiente de direcciones públicas, como recordatorio usted sabe que un dispositivo debe tener una dirección IP única, estas direcciones las podemos clasificar como privadas y públicas. Las direcciones públicas son las que nos permiten comunicarnos con todo Internet, mientras que las direcciones privadas están diseñadas solo para un direccionamiento interno. A medida que la cantidad de dispositivos, que necesitan conectarse con internet creció, tener una dirección pública exclusiva para cada aparato se volvió un problema, esto fue creciendo cada vez más y más con la expansión de internet.

Llego el punto en el que las direcciones IPv4 públicas se terminaron, y nació lo que es IPv6, pero antes de ello NAT era la solución viable para lidiar con esta insuficiencia, en concreto ***NAT lo que permite es que varias direcciones privadas, puedan ser representadas a través de pocas direcciones publicas***, de esta manera podemos comunicar muchos dispositivos a internet, usando el mínimo de direcciones publicas posible.

Direccionamiento privado (RFC 1918)

El direccionamiento privado es importante a la hora de implementar NAT, debido a que las direcciones privadas son las direcciones que vamos a traducir. Este tema ya lo tocamos con anterioridad en prácticas pasadas de direccionamiento IPv4, como pequeño recordatorio a continuación dejaremos la tabla de direcciones privadas.

Clase	Bloque	Rango
A	10.0.0.0/8	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0/12	172.16.0.0 hasta 172.31.255.255
C	192.168.0.0/16	192.168.0.0 hasta 192.168.255.255

Figura 5. 1: Bloques de direcciones privadas.

Recuerde que las direcciones privadas son aquellas que no son ruteables por un router en Internet. Es decir que un dispositivo con una dirección privada no va a poder comunicarse con Internet, es por ello que es necesario NAT para que éste traduzca las direcciones en direcciones públicas.

El uso principal de NAT es la traducción de direcciones públicas, esto permite que las redes utilicen direcciones privadas internamente, y sólo se traduce a direcciones públicas cuando sea necesario. A los dispositivos dentro de la organización se les asigna direcciones privadas y funcionarán con direcciones locales únicas.

Tipos de NAT

Existen diferentes tipos de NAT con los que nos vamos a encontrar, a continuación vamos a explicar brevemente cada uno de ellos:

- NAT estático: este tipo de NAT está diseñado para permitir un mapeo uno a uno entre las direcciones local y global. Mantenga en mente que la versión estática requiere que usted tenga una dirección pública para cada uno de sus dispositivos en la red. Lo anterior quiere decir que una dirección privada se va mantener enlazada de manera fija con una dirección pública.

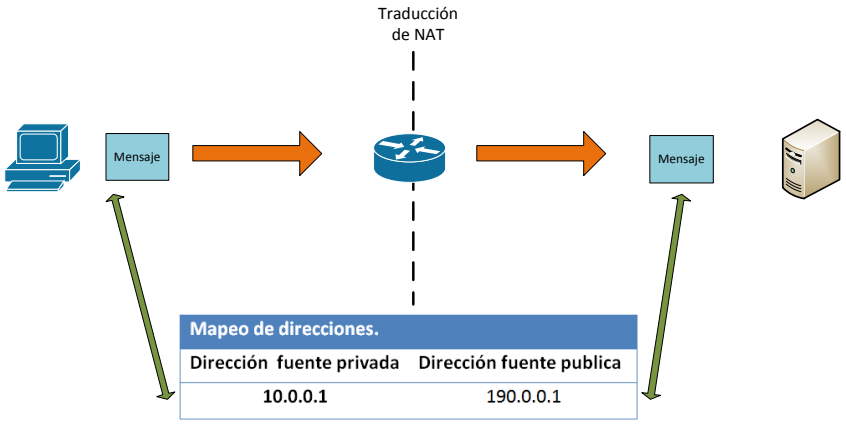


Figura 5. 2: Uso de NAT estático.

- NAT dinámico: A diferencia del anterior, este tipo de NAT permite hacer un mapeo de varias direcciones globales, por ejemplo si tenemos disponibles 3 direcciones públicas, podemos mapear estas tres direcciones a un grupo de direcciones privadas, donde NAT se encarga de usar las direcciones publicas conforme los equipos con direcciones privadas lo necesiten, para después desocupar dichas direcciones públicas y permitir a otros equipos usarlas.

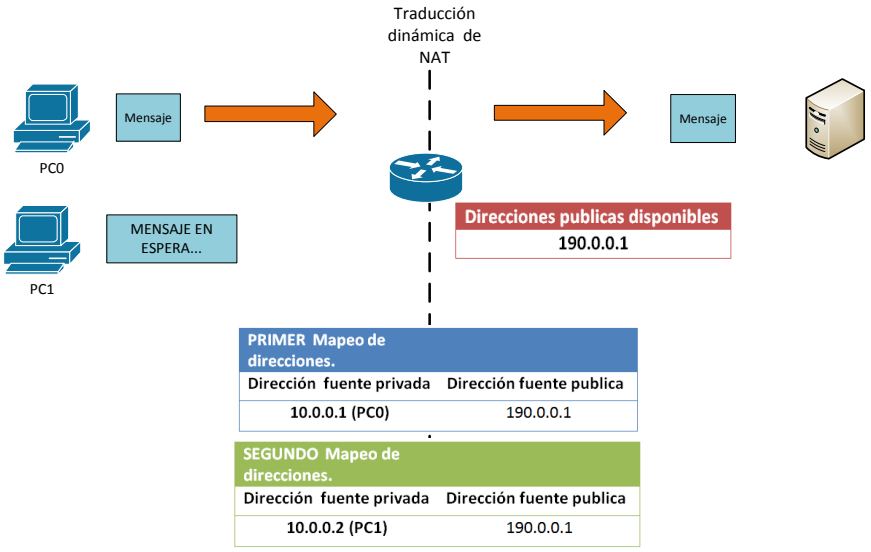


Figura 5. 3: Uso de NAT dinámico.

- PAT (Port Address Traslation) ó NAT sobrecargado: en esta versión nos encontraremos con el uso de los puertos TCP/UDP, dichos puertos son usados como identificadores únicos para los dispositivos con una dirección privada, de tal manera que el mapeo se realiza de dirección privada a puerto, permitiendo tener una traducción de 2^{16} direcciones privadas usando solo una dirección publica.

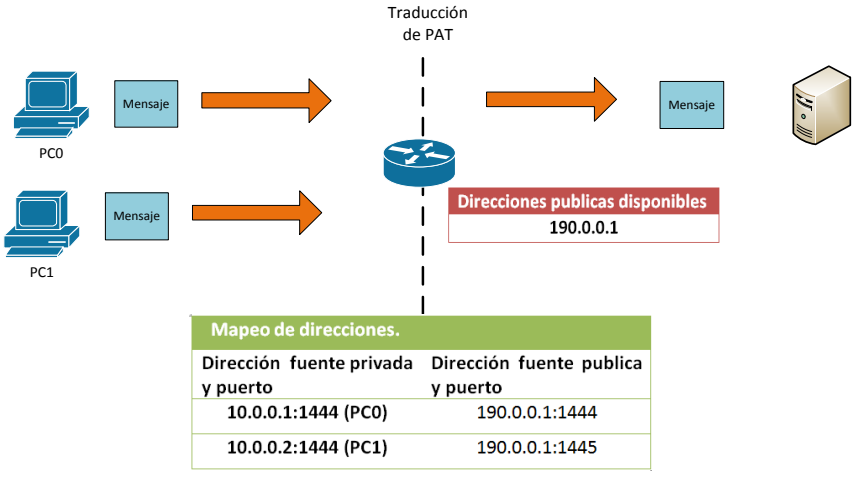


Figura 5. 4: Uso de PAT.

Terminología

Existen diferentes términos usados en tema de NAT, principalmente para identificar las direcciones en el proceso de traducción, es por ellos que vamos a explicar cuáles son estos términos.

- Inside local: Con este término nos vamos a referir a las direcciones dentro de la red local antes de la traducción (generalmente estas direcciones son privadas)
- Outside local: Con este término nos vamos a referir a la dirección que el host dentro de la red privada usa como destino en el encabezado del paquete IP.
- Inside global: Con este término nos vamos a referir a las direcciones públicas usadas para representar a un host después de la traducción.
- Outside global: Con este término nos vamos a referir a la dirección especifica de host destino.

Configuración de NAT dinámico

A continuación vamos a describir los pasos para hacer la configuración de NAT dinámico.

1. Definir un pool o grupo de direcciones públicas en el router que ejecutara la traducción.
2. Crear una ACL que identifique que direcciones privadas serán traducidas.
3. Enlazar la ACL hacia el pool de direcciones.
4. Definir que interfaces son “Inside” (interfaces contenidas dentro de la red local privada).
5. Definir que interfaces son “Outside” (interfaces contenidas en internet las cuales tienen una dirección pública).

Configuración de NAT sobrecargado (PAT)

Al igual que antes se hará una lista de pasos para configurar PAT, existe solo una ligera diferencia entre la configuración de NAT dinámico y PAT, cabe resaltar que a NAT dinámico se conoce como una traducción de “una dirección privada a una dirección pública”, mientras que PAT se le conoce como “muchas direcciones

privadas a una dirección pública", esto debido a que PAT usa los puertos de capa 4, para identificar de manera única cada dirección privada, permitiendo mapear muchas direcciones privadas en una pública.

1. Definir un pool o grupo de direcciones públicas en el router que ejecutara la traducción.
2. Crear una ACL que identifique que direcciones privadas serán traducidas.
3. (Opción 1) enlazar la ACL hacia el pool de direcciones sin olvidar teclear la palabra clave "overload".
4. (Opción 2) enlazar la ACL con una interfaz de salida que tenga una dirección pública, de esta manera esta única dirección pública será usada en el mapeo.
5. Definir que interfaces son "Inside" (interfaces contenidas dentro de la red local privada).
6. Definir que interfaces son "Outside" (interfaces contenidas en internet las cuales tienen una dirección pública).

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.
A. Tanenbaum and D. Morales Peake, Redes de computadoras. México: Prentice-Hall Hispanoamericana, 1997.
RFC 2086.
RFC 4314.

Tabla de comandos

COMANDO	DESCRIPCIÓN.
(config)#ip nat pool *[nombre del pool]* *[dirección de inicio] [dirección final]*	Crea un grupo o pool de direcciones públicas, las cuales

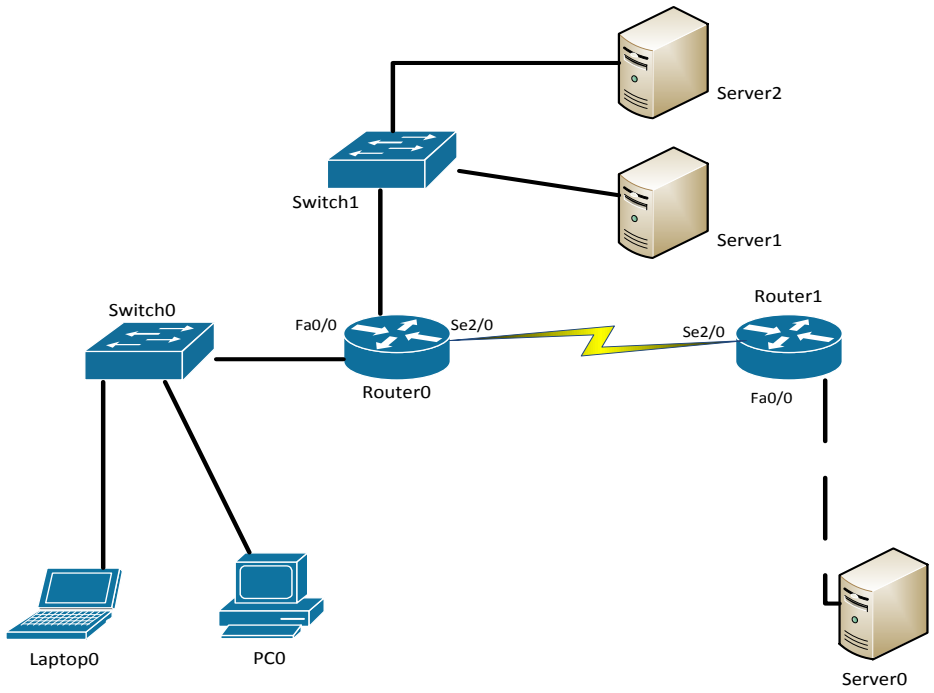
netmask *[mascara de subred]*	serán usadas a la hora de la traducción.
(config)#access-list *[número de ACL]* permit *[dirección de subred privada] [mascara Wildcard]*	Crea una ACL dónde se especifica las direcciones privadas que serán traducidas.
(config)#ip nat inside source list *[número de ACL]* pool *[nombre del pool]*	Enlazamos la ACL que contiene las direcciones privadas con el pool de direcciones públicas.
(config)#ip nat inside source list *[numero de ACL]* interface *[interfaz]* overload	Enlazamos la ACL que contiene las direcciones privadas con una sola dirección IP la cual es la de la interfaz especificada.
(config)#ip nat inside source list *[número de ACL]* pool *[nombre del pool]* overload	Enlazamos la ACL que contiene las direcciones privadas con varias direcciones IP, esto utilizando PAT.
(config)# interface *[tipo y nombre]*	Accede al modo de configuración de interfaz para la interfaz indicada.
(config-if)#ip nat inside	Define que interfaz es “inside” (interfaz que está contenida dentro del direccionamiento privado).
(config-if)#ip nat outside	Define que interfaz es “outside” (interfaz que está contenida dentro del direccionamiento público).
#show access-lists	Muestras todas las ACL configuradas.
# show ip nat translations	Muestra información de las traducciones que se han hecho.

Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Router0	Fa0/0	10.0.0.254	255.255.255.0
	Se2/0	190.1.1.1	255.255.255.252
Router1	Fa0/0	190.1.2.254	255.255.255.0

	Se2/0	190.1.1.2	255.255.255.252
Server0	Fa0	190.1.2.1	255.255.255.0
Laptop0	Fa0	10.0.0.2	255.255.255.0
PC0	Fa0	10.0.0.1	255.255.255.0

Topología



Desarrollo

Actividad 1

1. Configure NAT Dinámico en Router0, para que PC0 y Laptop0 puedan comunicarse con Server0, siguiendo los pasos descritos en los conceptos

previos, usando como direcciones públicas las siguientes: 191.1.1.1 y 191.1.1.1.2.

2. Configure una ruta estática en Router1 que indique hacia donde hay que enviar los paquetes dirigidos a las direcciones 191.1.1.1 y 191.1.1.2
3. Revise los resultados de su configuración en el modo se simulación y vea el contenido de la cabecera IP en los mensajes enviados hacia Server0
4. Agregue una PC al Switch0 y haga ping de manera simultánea hacia Server0 en todos los dispositivos conectados a Switch0.

Actividad 2

1. Configure PAT en Router0, para que Server1 y Server2 puedan comunicarse con Server0, siguiendo los pasos descritos en los conceptos previos, usando como dirección publica la dirección de la interfaz Se2/0.
2. Revise los resultados de su configuración en el modo se simulación y vea el contenido de la cabecera IP en los mensajes enviados hacia Server0

Conclusiones

En esta práctica logramos aprender la importancia que ha tenido NAT a lo largo de la historia, explicamos su esencial papel a la hora de lidiar con el problema de la insuficiencia de direcciones IPv4, ya que esto mejora el rendimiento de dicho direccionamiento, vimos los conceptos básicos de NAT, la diferencia entre las formas de etiquetar las direcciones en los mensajes, le sugerimos que no olvide dichos conceptos, y hacemos un hincapié especial en recordar los pasos descritos para configurar NAT dinámico y PAT.

Cuestionario

1. ¿Cuál de los siguientes nombres hace referencia a la implementación de NAT sobrecargado?

   A. PAT
   B. SNAT
   C. JAT
   D. FAT

2. ¿Qué implementación de NAT hace un mapeo de direcciones de manera fija, es decir uno a uno?

   A. PAT
   B. NAT estático.
   C. JAT
   D. NAT dinámico.

3. Un compañero suyo está configurando NAT dinámico en un router, le pide ayuda ya que tiene problemas al crear un ACL que le permita mapear una red de mascara /28. ¿Cuál de las siguientes instrucciones usaría usted para crear dicha ACL?

   A. (config)#access-list 10 permit any any.
   B. (config)#access-list 10 permit 191.0.0.0 0.0.0.15.
   C. (config)#access-list 10 permit 10.0.0.0 255.255.0.0
   D. (config)#access-list 10 permit 10.0.0.0 0.0.0.15.

4. ¿Qué implementación de NAT hace un mapeo de direcciones de manera dinámica usando los puertos de capa 4, es decir una a varias?

   A. PAT
   B. NAT estático.

C. JAT
D. NAT dinámico.

5. Se le da un router para que configura NAT en el, este tiene un puerto serial conectado a un enlace WAN, además tiene un puerto FastEthernet conectado a una LAN ¿Cómo configuraría el puerto serial?

   A. (config)#ip nat inside
   B. (config-if)#ip nat inside
   C. #ip nat outside
   D. (config-if)#ip nat outside

6. Escriba los pasos necesarios para configurar NAT dinámico.

7. ¿Qué es una dirección Outside local?

   A. Direcciones dentro de la red local antes de la traducción (generalmente estas direcciones son privadas)
   B. Dirección que el host dentro de la red privada usa como destino en el encabezado del paquete IP.
   C. Direcciones publicas usadas para representar a un host después de la traducción.

8. Escriba los pasos necesarios para configurar NAT dinámico sobrecargado.

9. ¿Qué es una dirección inside global?

10. ¿Cuáles de las siguientes sentencias serian una buena razón para implementar NAT? (escoge 2)

A. Se necesita conectares a Internet y los hosts no tienen un IP pública.

B. No quieres que ningunos de tus dispositivos se conecte a Internet.
C. Tienes una Intranet con direcciones duplicadas en otro sitio.

Capítulo VI: Seguridad

Introducción

En esta práctica analizaremos algunos principios y métodos básicos para darle seguridad a nuestra red. En la primera parte estudiaremos los diferentes tipos de amenazas comunes, continuaremos con prácticas básicas para asegurar nuestros dispositivos.

Tipos de amenazas

Existen muchos tipos de amenazas a los sistemas de información. Las redes no quedan exentas de ataques, pero normalmente muchas personas se imaginan que los ataque y amenazas se limitan solo a los virus de computadora y ataques por software, lo cual no es verdad.
Es por ello que es importante ir dilucidando que tipos de amenazas podemos encontrar. Primero vamos a definir lo que es una amenaza, una amenaza es un evento que pude causar alteraciones malintencionadas de la información y los equipos, que puedan causar pérdidas o afectaciones de algún tipo. Estas amenazas vienen de ciertas vulnerabilidades, como son:

- Vulnerabilidades tecnológicas.
- Vulnerabilidades en la configuración y diseño.
- Vulnerabilidades en las políticas de seguridad.

Dentro de las vulnerabilidades tecnológicas podemos incluir vulnerabilidades físicas y de hardware. Profundicemos primero con algunas vulnerabilidades físicas: dentro de estas podemos listar problemas ambientales, por ejemplo

tormentas eléctricas, problemas eléctricos como una mala instalación o fallas eléctricas, problemas de mantenimiento como revisión y remplazo de algunos componentes.
Las vulnerabilidades de configuración y diseño se dan normalmente dentro de redes pequeñas de hogares u oficinas, esto se refiere a una mala implementación de conceptos o políticas de seguridad, donde la inexperiencia de los diseñadores o administradores hace que haya puertas y hoyos en la configuración.

Vulnerabilidades en las políticas de seguridad, tiene que ver con todas las medidas de prevención de desastres y protocolos diseñados para la contención de los mismos, es responsabilidad de la organización y del administrador revisar implementar y actualizar sus políticas y prácticas de seguridad, así también como auditar dichas políticas de manera constante y regular, para poder parchar fallos u agujeros en los sistemas de seguridad.

Ataque comunes

Ahora listaremos algunos taques que suceden de manera común y a los cuales los administradores de redes se tienen que enfrentar:

Reconocimiento: un ataque de reconocimiento se refiere al descubrimiento y la asignación no autorizada de sistemas servicios o vulnerabilidades. Aquí los agresores pueden usar herramientas de Internet como nslookup para determinar fácilmente el espacio de direcciones IP. Una vez determinado el espacio IP, el agresor puede hacer uso de ping para determinar que direcciones están activas, después de esto puede usar otras herramientas para verificar que puertos están activos en las direcciones IP que detecto anteriormente y así poder atacar.

Acceso: esto se refiere a la capacidad del intruso de entrar a los dispositivos sin tener una cuenta y contraseña. Existen varias formas de que esto ocurra, lo más común es explotar el hecho de creación de contraseñas débiles por parte de usuarios, donde el atacante puede usar programas para probar las contraseñas más probables en base a cierta información estadística.

Denegación de servicio: la denegación de servicio (DoS) se lleva acabo cuando un agresor desactiva o daña redes, sistemas o servicios con el propósito de denegar

servicios a los usuarios a quienes están dirigidos. Entre este tipo de ataques podemos mencionar, el ping de la muerte, la saturación SYN, el ataque Smurf.

Seguridad básica para dispositivos de red (Routers y Switches)

Como primeras medidas de seguridad un administrador de red; se tiene que asegurar de no permitir ataques de acceso a los dispositivos de red. Esto se hace como en cualquier otro sistema operativo, a través del uso de contraseñas y cuentas de usuario para acceder a los diferentes recursos del dispositivo.

Antes de continuar tenemos que hablar de los diferentes modos, a los cuales podemos tener acceso en los dispositivos Cisco. No profundizaremos en ello pero es importante para el establecimiento de contraseñas, a continuación damos una breve descripción de estos modos:

Modo usuario: permite consultar la información relacionada al dispositivo sin poder modificarla, el símbolo que se muestra en el prompt es >.

Modo usuario privilegiado: permite visualizar el estado del dispositivo e importar o exportar imágenes del IOS (Internetwork Operating System), el símbolo que se muestra en el prompt es #.

Modo de configuración global: permite el uso de comandos de configuración generales del dispositivo, lo que se muestra en el prompt es (config)#.

Ahora tenemos que abordar las formas de tener acceso al dispositivo, estas se resumen en tres formas básicas. La primera es usando el puerto de consola, para lo cual se necesita una conexión física directa al dispositivo, la segunda es vía el puerto auxiliar que básicamente necesita lo mismo que la forma anterior y la ultima es vía VTY o líneas virtuales, estas son usadas para conexiones Telnet o SSH, los cuales son protocolos de acceso remoto, donde podemos usar una conexión vía Internet.

Comenzaremos por decir que hay 5 passwords que deben ser configuradas para establecer una forma segura de acceso al dispositivo y a los modos del mismo. Estos 5 passwords son:

Password de consola.
Password de líneas VTY.
Password de línea auxiliar.
Password de acceso al modo privilegiado.
Password encriptado de acceso al modo privilegiado.

Por defecto los dispositivos Cisco no tienen configurada una contraseña ni usuarios. Es por ello que la primera tarea que debemos hacer al instalar un nuevo dispositivo es establecer dichas configuraciones. Vamos a dar una breve explicación de cómo establecer las contraseñas básicas anteriores.

Password de consola: para esto necesitamos acceder al modo de configuración global y después al modo de configuración de línea de consola, dentro de este modo solo tiene que configurar la clave usando el comando password, y después el comando login. Este password será solicitado cuando alguien desee acceder vía puerto de consola al dispositivo.

Password de línea auxiliar: para esto necesitamos acceder al modo de configuración global y después al modo de configuración de línea auxiliar, dentro de este modo solo tiene que configurar la clave usando el comando password, y después el comando login. Este password será solicitado cuando alguien desee acceder vía puerto auxiliar.

Password de acceso al modo privilegiado: para establecer este password solo se necesita acceder al modo de configuración global y usar el comando correspondiente, esta clave será solicitada cuando se intente acceder al modo privilegiado, existen 2 formas de establecer dicha clave, la primera es usando texto plano y la segunda estableciendo una clave encriptada. Es recomendable usar la clave encriptada por razones de seguridad.

Conexión vía SSH o Telnet

La conexión remota es algo importante de configurar en los dispositivos, ya que es uno de los métodos de acceso mas comunes y uno de los mas vulnerables, debido a que generalmente la información de la conexión pasara a través de la red o de internet.

Existen 2 métodos para acceder de manera remota a nuestros dispositivos el primero es usando Telnet, que es un protocolo no segura ya que envía toda la información en texto plano. Aun así podemos proteger el inicio de sesión con este protocolo estableciendo las contraseñas básicas en las líneas vty.

Lo mas recomendable es usar SSH, protocolo que encripta la información antes de enviarla, también podemos proteger el acceso a remoto con un par de listas de control de acceso, de esta manera tendremos una mejor configuración de seguridad.

A continuación vamos a describir los pasos necesarios para configurar SSH en un dispositivo:

1. Establezca un “hostname” (se recomienda cambiar el que viene configurado por defecto).
2. Establezca un nombre de dominio.
3. Establezca un nombre de usuario y una contraseña.
4. Genere una clave para la encriptación.
5. Habilite SSH versión 2.
6. Configure los protocolos permitidos en el acceso remoto.
7. Indique al dispositivo revisar los nombres de usuario y contraseñas.

Seguridad de puertos en un Switch

Es importante hablar sobre la seguridad alrededor de los puertos de acceso en un Switch, no podemos dejar que cualquiera pueda llegar y usar a nuestro dispositivo con solo quitar y conectar un cable de red. Es por ello que la seguridad en los puertos de un Switch es tan importante como las otras medidas que podemos tomar. Para ello tenemos a nuestra disposición varias herramientas de configuración básica en el dispositivo.

Todos los puertos de un Switch están habilitados por defecto, es esto lo que los hace un poco inseguros, así que nos tenemos que asegurar de nadie puada conectar un host, switch o punto de acceso a nuestro dispositivo. Para ello vamos a usar la dirección MAC de cada dispositivo y los modos en que puede operar el puerto de un switch.

Un Switch puede asociar desde 1 hasta 8192 direcciones MAC a un puerto, nosotros podemos configurar estas MAC de manera manual o hacer que el Switch las aprenda de forma dinámica.

A continuación vamos a describir los pasos que debe seguir para poder configurar un filtrado MAC en los switches y otorgarle más seguridad a estos dispositivos:

1. Configure el Switch como puerto de acceso.
2. Habilite la seguridad del puerto.
3. Defina la forma en que el Switch aprenderá las direcciones MAC (Estática/ Dinámica).
4. Defina el límite de direcciones MAC permitidas en el puerto.
5. Defina el modo de restricción que tomara el puerto en caso de violación.

Los pasos donde debe tener algunas consideraciones son en los 3 y 5, los demás si los ejecuta bien no habrá ningún problema. Todas las configuraciones anteriores se hacen en el modo de configuración de interfaz.

En el paso 3 el administrador de red debe elegir un modo para que el dispositivo aprenda las MAC permitidas en la red. Esto se puede hacer de manera manual indicando que direcciones MAC están permitidas, desafortunadamente esto nos es escalable cuando tenemos redes grandes y más dispositivos. Por lo que existe un modo dinámico llamado “sticky”, donde si fijamos el límite de direcciones en n, el dispositivo va aprender las primeras n direcciones MAC que entren en su puerto. Sin necesidad de introducirlas de manera manual.

Servicio AAA

Existen otras herramientas avanzadas que nos permiten mejorar nuestras condiciones de seguridad, de manera breve vamos a hablar de un conjunto de protocolos referidos con el acrónimo AAA. Esto quiere decir Autenticación, Autorización y Auditoria. Describiremos las funciones principales de estas herramientas a continuación:

Autenticación: Es le proceso de identificación de individuos normalmente mediante un usuario y una contraseña.

Autorización: Este servicio se refiere a la concesión, denegación de permisos y acceso a determinadas aplicaciones. Es aquí donde nos encargamos de limitar el acceso a ciertos datos también, esto dependiendo del nivel de autorización que tenga el usuario.

Auditoria: Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red. Incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede, así como los datos transferidos durante la sesión.

Existen 2 protocolos AAA muy usados en la industria, estos son RADIUS y TACACS. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos. TACACS es un protocolo propietario de cisco, que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Referencias

W. Odom, Official cert guide Cisco CCENT, CCNA ICND1 200-101. Indianapolis, In.: Cisco Press, 2013.
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 2903.
RFC 2904.
RFC 2905.
RFC 2906.

Tabla de comandos

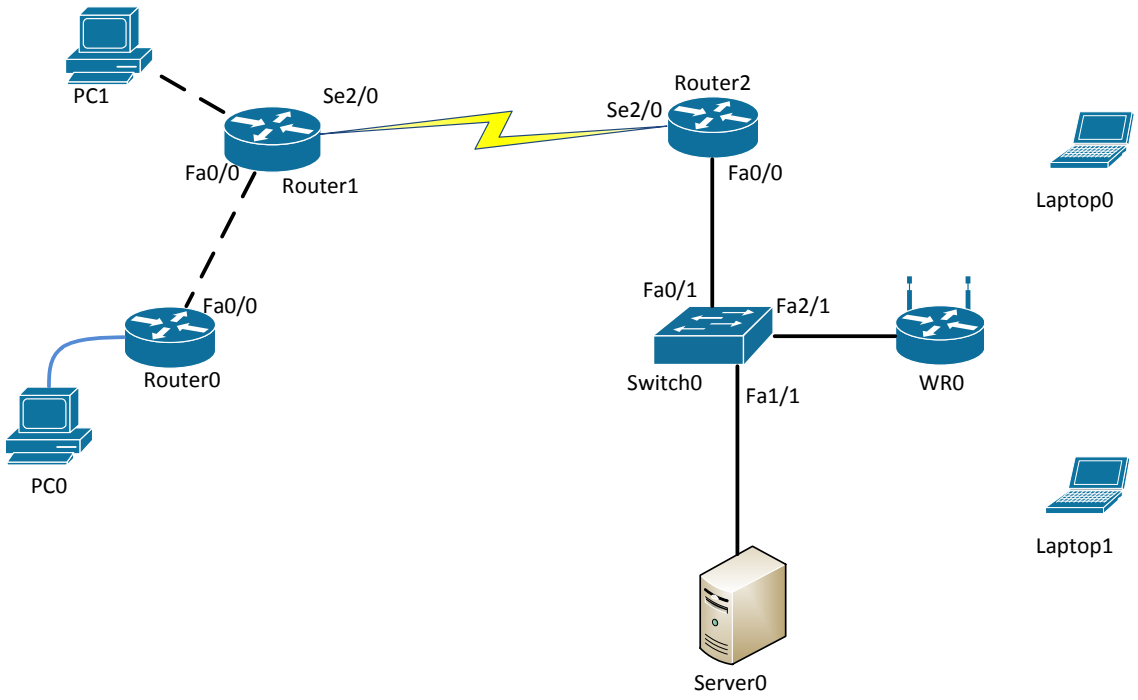
COMANDO	DESCRIPCIÓN.
(config)#interface fax/x	Pasa al modo de configuración de interfaz.
(config-if)# switchport mode access	Define la interfaz como puerto de acceso.
(config-if)# switchport port-security mac-address sticky	Activa el aprendizaje de direcciones MAC estáticas (seguras) en el puerto.
(config-if)# switchport port-security maximum [número de direcciones MAC]	Establece el límite de direcciones MAC estáticas para el puerto.
(config-if)# switchport port-security violation [modo]	Establece el modo de violación, es decir lo que el dispositivo hará si se comete alguna violación.
(config-if)#switchport port-security	Activa la seguridad en el puerto.
# sh mac-address-table	Muestra la tabla MAC.
#sh port-security int [interfaz]	Muestra las configuraciones de seguridad para una interfaz.
(config-if)#shut	Deshabilita de manera administrativa una interfaz.
(config-if)#no shut	Habilita una interfaz.
(config)# line console 0	Pasa al modo de configuración de la línea de consola.
(config-line)# password [clave]	Establece un password.
(config-line)# login	Establece una petición de password para el usuario.
(config)# enable secret [clave]	Establece una contraseña encriptada para acceder al modo privilegiado.
(config)#ip domain-name [nombre de dominio]	Estable un nombre de dominio.
(config)#username [ususario] password [clave]	Configura un usuario y contraseña permitidos, para las conexiones SSH.
(config)# crypto key generate rsa	Habilita SSH para una

	autenticación local o remota, además genera un clave encriptada.
(config)# ip ssh version 2	Habilita SSH versión 2.
(config)# line vty 0 15	Pasa al modo de configuración de las líneas VTY 0 a 15.
(config-line)# transport input [protocolo]	Establece el protocolo de acceso remoto, ya sea Telnet o SSH. Sus opciones son: ssh, telnet, all, none.
(config-line)# login local	Le indica al router revisar que los nombre de usuarios y contraseñas habilitados estén correctos.
(config)#access-list [número de ACL] permit [dirección de red] [mascara wildcard]	Crea una lista de control de acceso estándar.
(config-line)# access-class [número de ACL in	Enlaza la lista de control de acceso con las líneas VTY, de esta manera solo se permitirá las conexiones remotas a los hosts permitidos dentro de la ACL.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Mascara de subred
Router0	Fa0/0	192.168.1.1	255.255.255.0
Router1	Fa0/0	192.168.1.2	255.255.255.0
	Fa1/0	192.168.4.254	255.255.255.0
	Se3/0	192.168.2.1	255.255.255.0
Router2	Fa0/0	192.168.3.254	255.255.255.0
	Se3/0	192.168.2.2	255.255.255.0
PC1	Se2/0	192.168.4.1	255.255.255.0
Server0	Se2/0	192.168.3.1	255.255.255.0

Topología



Desarrollo

Actividad 1

1. Configure WR0 (en la pestaña Config>LAN) para que cree una WLAN con dirección de red 192.168.20.0/24, en la cual WR0 tenga como dirección IP la dirección 192.168.20.254.

2. Configure la interfaz Internet de WR0 (en la pestaña Config>Internet) con la dirección IP 192.168.3.253, Default Gateway de 192.168.3.254 y una máscara de red /24.
3. Conecte la interfaz Internet de WR0 al puerto Fa2/1 de Switch0.

4. Vaya a la interfaz gráfica de WR0 (pestaña GUI) y verifique las configuraciones anteriores. Además establezca a WR0 como servidor DHCP para la red 192.168.20.0/24, de tal manera que otorgue las primeras 50 direcciones (No olvide guardar las configuraciones).

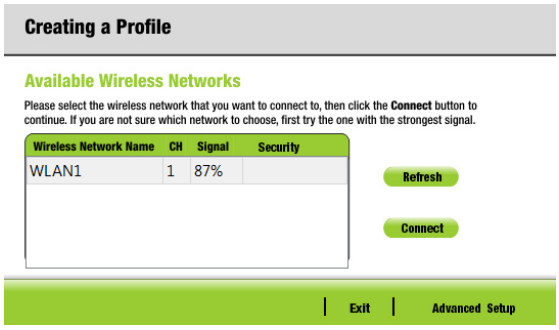
5. En la interfaz gráfica de WR0 vaya a la pestaña de Wireless y configure el nombre de la red inalámbrica como WLAN1 y establezca como método de autenticación WPA Enterprise. Con una encriptación AES, dirección del servidor RADIUS en 192.168.3.1 y clave “redes99” (No olvide guardar las configuraciones).

6. En Server0 active el servicio AAA, con los siguientes parámetros:
   - Client Name: WLAN1.
   - Client IP: 192.168.3.253.
   - Secret: redes99.
   - ServerType: RADIUS.

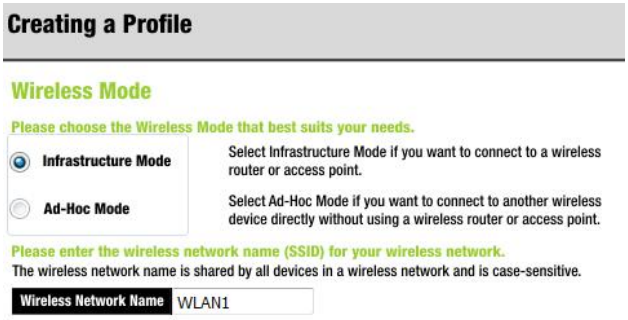
   No olvide dar clic en Add para que las configuraciones tengan efecto.

7. En la parte de User Setup, configure 2 usuarios con los siguientes nombres y contraseñas:
   - Username: admin.
   - Contraseña: cisco25.
   - Username: user1.
   - Contraseña: cisco50.
8. Agregue módulos WPC300N a las laptops para que tengan una tarjeta de red inalámbrica y puedan conectarse vía wireless.
9. Diríjase a la pestaña de Desktop>PC Wireless. En la interfaz de Linksys vaya a la pestaña de Profiles y Edite el perfil “Default” de la siguiente manera:

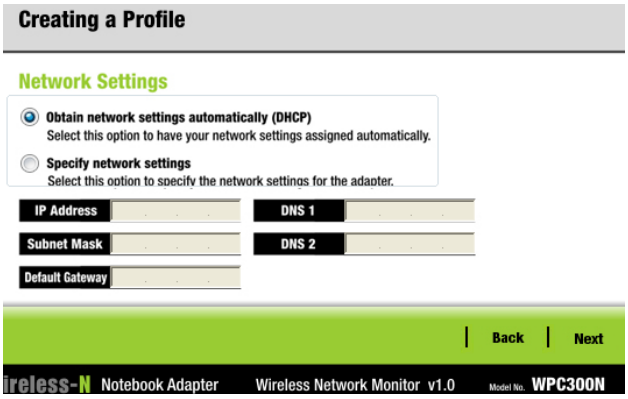
En esta pestaña de clic sobre Advanced Setup.



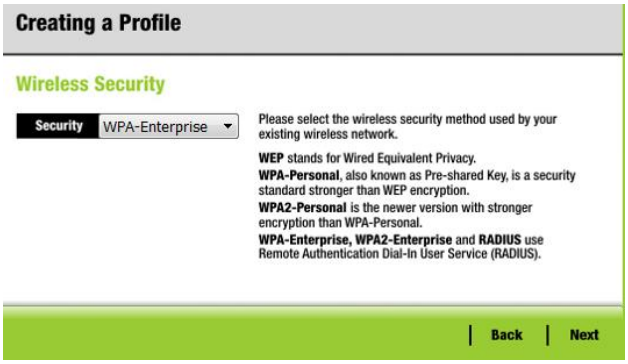
La siguiente pestaña se queda como esta.



En la siguiente pestaña elija la opcion de obtener direccion IP via DHCP.



En la siguiente pestaña elija la opcion de seguridad WPA Enterprise.



Use un nombre de usuario y contraseña, ya sea admin o user1, cambie la opción de encriptación a AES y de clic en next.

Finalmente guarde las configuraciones y conéctese a la red.

10. Pruebe su configuración enviando un ping de las laptops hacia Server0.

Actividad 2

1. Entre al modo de configuración en Switch0 y configure los puertos Fa1/1 y Fa2/1 como puertos de acceso.
2. Configure el puerto Fa2/1, para que aprenda direcciones MAC de manera dinámica (sticky). Además establezca el límite de direcciones MAC en 2, utilice como medida protección la deshabilitación (shutdown) y active la seguridad en el puerto.
3. Configure el puerto Fa1/1, para que aprenda direcciones MAC de manera dinámica (sticky). Además establezca el límite de direcciones MAC en 1, utilice como medida protección la deshabilitación (shutdown) y active la seguridad en el puerto.
4. Envié un ping desde las Laptops hacia Server1 y observe la tabla MAC en el Switch.
5. Sustituya a WR0 por una PC y conéctela al puerto Fa2/1, asigne la dirección IP 192.168.3.5 a esta PC y haga ping a Server0. ¿Qué sucede?
6. Sustituya a Server0 por una PC y conéctela al puerto Fa1/1, asígnele la dirección 192.168.3.6 y haga ping a la dirección 192.168.3.5. ¿Qué sucede? ¿Por qué?
7. Restablezca los dispositivos WR0 y Server0. Configure el Switch para que habilite de nuevo el puerto Fa1/1.

Actividad 3

1. Configure contraseñas para asegurar el puerto auxiliar y el de consola en Router0, use como password “telecomfi”.
2. Configure una contraseña encriptada para acceder en el modo privilegiado usando el password “telecomfi”.
3. Acceda a Router0 via consola con PC0 y compruebe sus configuraciones.
4. Configure las líneas VTY con un password “adminrouter” y habilite la solicitud de este password.
5. Usando Laptop0 inicie una sesión telnet en Router0 para comprobar sus configuraciones.
6. Desde Laptop0 configure a Router0 para usar solo SSH en vez de Telnet. Habilite un usuario llamado “user02” con password “redes02”. Además

proteja dichas sesiones SSH con una ACL para que solo los host en la red 192.168.3.0/24 puedan tener acceso vía SSH.

7. Compruebe sus configuraciones tratando de iniciar sesiones SSH a través de las laptops y de Server0.

Conclusiones

En esta práctica se logró comprender, que existe una gran variedad de amenazas para los dispositivos de red, que van desde amenazas físicas hasta los ya conocidos virus informático, es importante en primera instancia saber identificar cuáles son las amenazas a las que es propensa nuestra red, para poder tomar contramedidas que puedan protegernos de alguna manera.
Tenemos muchas herramientas a nuestra disposición para poder configurar medidas de seguridad básica en nuestros dispositivos, desde la configuración de usuarios y contraseñas, hasta el filtrado de direcciones MAC en los dispositivos de acceso, sin olvidarse de las muy utilice listas de control de acceso. El tema de seguridad es muy amplio y da pie para un estudio mas profundo y detallado pero mientas tanto trate de recordar las amenazas y medidas básicas que puede configurar en un dispositivo de red.

Cuestionario

1. Mencione los pasos necesarios para habilitar SSH en un dispositivo Cisco.

2. ¿Cuál de los siguientes comandos establece una contraseña (unamFI) encriptada para entrar al modo privilegiado?

    A. enable secret unamFI
    B. enable secret password unamFI
    C. enable password unamFI
    D. enable secret UNAMFI

3. ¿Cuál comando en la siguiente configuración es un requisito para que los demás comandos tengan efecto?

    A. (config)#int fa0/3
    B. (config-if)#switchport port-security
    C. (config-if)# switchport port-security mac-address sticky
    D. (config-if)#switchport port-security máximum 2
    E. (config-if)#switchport port-security violation shutdown

4. ¿Qué comando es usado para verificar la configuración de la seguridad de puerto en un Switch?

    A. Show interface port-security
    B. Show port-security interface
    C. Show ip interface
    D. Show interface switchport

5. Escribe los pasos a seguir para habilitar un puerto de un Switch que se ha “apagado”, después de una violación de seguridad.

6. ¿Qué utilizaría para proteger sus dispositivos, los cuales tiene acceso vía línea VTY?

    A. Usar Telnet.
    B. Usar una ACL.
    C. Usar SSH.
    D. Usar el comando enable secret.

7. ¿Qué tipo de vulnerabilidad sufre un equipo si una tormenta eléctrica lo daña?

    A. Vulnerabilidad tecnológica.
    B. Vulnerabilidad de configuración.
    C. Vulnerabilidad en las políticas de seguridad.

8. ¿A qué se refiere una ataque DoS?

9. ¿Qué significa AAA?

10. Mencione los pasos para configurar un filtrado MAC en un Switch.

Capítulo VII: Principios de Routing en IPv6

Introducción

Esta práctica abordara conceptos básicos de ruteo en IPv6, hablaremos sobre la evolución de los conceptos aplicados en IPv4, las diferencias más notables que tienen estos 2 protocolos. Así también profundizaremos en la forma correcta de configurar IPv6 en una red, tocando el ruteo estático y la configuración de rutas por defecto, hablaremos de la configuración de OSPFv3 y RIPng, 2 protocolos dinámicos que son la "evolución" de sus similares en IPv4.

Conceptos Previos

Ventajas de migrar a IPv6

Antes que nada debemos comenzar mencionando las principales ventajas que tiene el hecho de migrar a IPv6, durante los últimos años con la expansión de internet, hemos tenido la oportunidad de implementar y mejorar las redes a través de IPv4, así también hemos aprendido de sus debilidades y fortalezas, es por ello que al empezar el diseño de IPv6 se decidieron hacer varias mejoras respecto a IPv4, las cuales podemos resumir de la siguiente manera:

- IPv6 soporta dos métodos de direccionamiento dinámico, el primero de ellos es DHCP y el segundo es SLAAC (Stateless Address Autoconfiguration).
- Soporte integrado para movilidad, lo que quiere decir que el host puede moverse alrededor de "internetworks" reteniendo su dirección IPv6 sin perder las sesiones activas de las aplicaciones.

- Elección de la dependencia o no de un proveedor, las organizaciones pueden recurrir a un proveedor de internet (ISP) para solicitar un espacio de direcciones IPv6, o pueden solicitar directamente dicho espacio a las organizaciones encargadas de regular el direccionamiento IPv6.
- Facilidad para la adición de nuevos bloques de direcciones en internet, haciendo más eficiente el ruteo en internet.
- No existe NAT/PAT lo que significa que no hay problemas inherentes a la implementación de dicho protocolo.
- Mejoras en el encabezado IPv6, existen varias mejoras que se han hecho en el encabezado de este protocolo, en especial podemos destacar el hecho de que los routers no tienen que calcular el “checksum” en cada paquete, esto reduce la carga de trabajo al router, además de que incluye una etiqueta especial para el control de flujo, lo cual facilita la identificación de paquetes en las sesiones TCP y UDP.
- IPv6 no utiliza mensajes de Broadcast, lo que reduce ciertos problemas inherentes a estos mensajes.
- Existen varias herramientas de transición entre IPv4 e IPv6, entre las cuales podemos nombrar “Dual stack” y el “Tunneling”.

Las anteriores ventajas nos dan la idea de lo que se pretende con IPv6, y es el hecho de que la mayoría de las redes que actualmente operan con IPv4 pronto vayan migrando a este nuevo protocolo, actualmente se tiene la expectativa de que para la década de 2030 este proceso de migración se complete, teniendo redes e internet operando totalmente en IPv6.

Direccionamiento dinámico en IPv6

Dynamic Host Configuration Protocol (DHCPv6)

DHCPv6 es la versión del protocolo para IPv6, al igual que su versión en IPv4 el proceso básico de funcionamiento es el mismo, existen diferencias en algunos formatos y campos en los mensajes, pero en esencia la obtención de direcciones es la misma, es decir el cliente envía un mensaje Multicast tratando de encontrar el servidor DHCP, después este responde a lo cual el cliente envía otro mensaje haciendo una solicitud de arrendamiento de una dirección IP, si no existe conflicto el servidor va a responder de manera satisfactoria otorgando la dirección IPv6.

DHCP en IPv4 es un protocolo “stateful”, es decir que el servidor retenía información de estado acerca de cada cliente, como por ejemplo la dirección IP otorgada y el tiempo con el que el cliente contaba para usar esta dirección. En IPv6 DHCP puede actuar como un protocolo “stateful” o “stateless”, dependiendo de las necesidades de la red y la configuración, ambos modos pueden ser útiles en distintas situaciones.

Stateless Address Autoconfiguration (SLAAC)

El Stateless Address Autoconfiguration (SLAAC) es un método automático de obtener la dirección IPv6 y junto con DHCPv6 son los únicos métodos de direccionamiento dinámico disponibles para IPv6.
SLAAC es una característica integrada en el protocolo IPv6, con la cual un host puede construir su información IP básica, como lo es su propia dirección IPv6, la dirección del Default Gateway y la dirección del servidor DNS, para hacer esto SLACC se vale de los siguientes pasos:

- Se usa un mensaje de IPv6 Neighbor Discovery Protocol (NDP), este protocolo permite el intercambio de información para que el host aprenda el prefijo de red (máscara en IPv4) y la dirección de su Default Gateway.
- El dispositivo implementa EUI-64, este proceso requiere solo un par de cálculos matemáticos, con los cuales a partir de la dirección MAC del dispositivo se construye su propia dirección IPv6.
- Stateless DHCPv6 permite que los hosts puedan aprender la dirección del servidor DNS.

Eui-64

Recordemos que EUI-64 toma la MAC del dispositivo para formar una dirección IPv6; 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: Se colocan los primeros 24 bits de la MAC seguidos de 16 bits propios de EUI-64, estos 16 bits siempre serán FF - FE, y finalmente se colocan los últimos 24 bits.

3. Después se invierte el séptimo bit de izquierda a derecha (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.

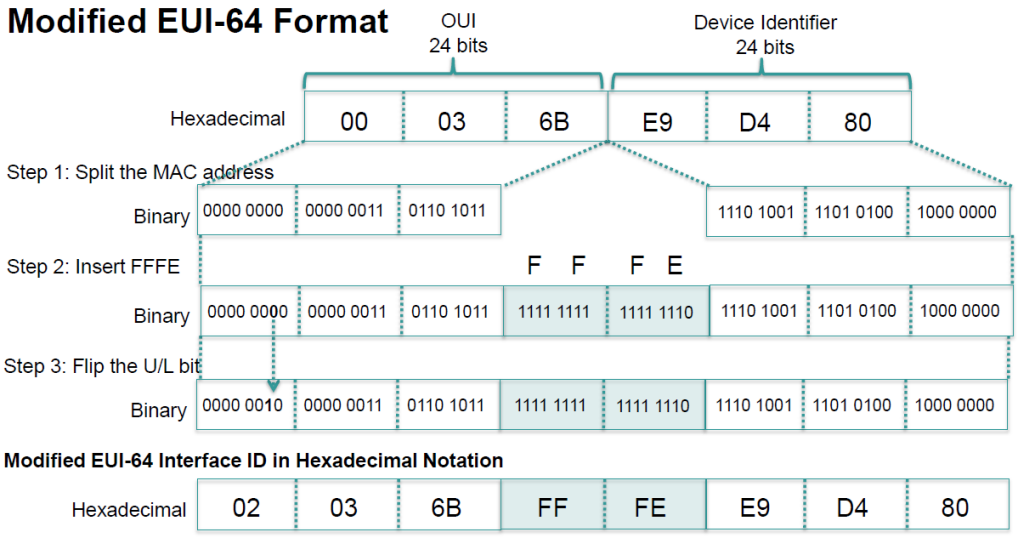


Figura 6. 1: Ejemplo del uso de EUI-64.

Configuración de IPv6 en routers Cisco

El ruteo y manejo de paquetes IPv6 no está habilitado por defecto en los routers Cisco, es por ello que para efectos de esta práctica daremos una explicación breve de la habilitación y asignación de direcciones IPv6 para dispositivos Cisco, hoy en día de manera general podemos decir que en muchos dispositivos debe de ser habilitado el protocolo IPv6, para que las maquinas puedan enviar paquetes de dicho protocolo. Tal vez en el futuro esta opción venga por defecto habilitada pero por el momento vamos a continuar con la explicación para los routers Cisco.

Al igual que muchos otros dispositivos, el manejo de paquetes IPv6 va a ser una característica, que dependerá tanto del hardware y del software que tenga el dispositivo, en el simulador propietario de Cisco Packet Tracer en específico, nos encontramos algunos dispositivos con versiones de IOS inferiores a la 15, el manejo de IPv6 no está permitido en dichos sistemas operativos. Es un hecho extraño ya que en dispositivos reales o versiones emuladas de IOS inferiores al 15 si tenemos disponible la capacidad de habilitar IPv6. Deberá tomar en cuanta esto a la hora de usar el simulador y elegir los dispositivos.

Para habilitar IPv6 solo necesitamos hacer uso de los comandos: ipv6 unicast-routing, ipv6 enable e ipv6 address. Los cuales vienen descritos en la tabla de comandos correspondiente a esta práctica.

Ruteo estático y dinámico

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

Vamos a encontrar que existen 2 tipos de enrutamiento, el enrutamiento estático que requiere la intervención directa de un administrador y el enrutamiento dinámico, donde los protocolos de ruteo se encargan de la mayor parte del trabajo.

- Ruteo Estático
  - Ventajas
    - ✓ Configuración manual.
    - ✓ Definición de una ruta explicita entre 2 dispositivos.
    - ✓ 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 manutención 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 manutención sea difícil.

- ✗ Necesita el 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.
  - ➢ Desventajas
    - ✗ Dedica parte de los recursos del router para el funcionamiento del protocolo, incluyendo ciclos de CPU y el ancho de banda del enlace de red

Entre los diversos protocolos de ruteo dinámico existentes, podemos denotar los siguientes:

- **EIGRPv6 –** Enhanced Interior Gateway Routing Protocol
- **OSPFv3 –** Open Shortest Path First
- **RIPng –** Routing Information Protocol

Distancia administrativa

Recordemos que la distancia administrativa, es la herramienta que tiene un router para elegir una ruta cuando este ha aprendido está a través de diferentes

protocolos. Es decir supongamos que un router ha aprendido como llegar al destino A usando RIP y OSPF. El router debe elegir alguna de las 2 rutas (OSPF o RIP) para colocar en la tabla de ruteo. Para ello hace uso de la distancia administrativa (AD), y elige la que más baja distancia tenga, en este caso OSPF tiene una distancia de 110 y RIP una de 120. Por lo que dará preferencia a OSPF. A continuación se presenta una tabla de distancias administrativas.

Origen de la ruta	Valores de distancia predeterminados
Interfaz conectada	0
Ruta estática	1
Protocolo de gateway de frontera externa (BGP)	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (zona desmilitarizada) externa	170
BGP interno	200
Desconocido*	255

Figura 6. 2: Tabla de distancias administrativas.

Proceso de configuración de rutas estáticas

El proceso de configuración de una ruta estática en IPv6 es el mismo que en IPv4, recuerde las ventajas y desventajas que esta acción puede conllevar en la práctica. En la tabla de distancias administrativas observamos que las rutas estáticas tienen un valor de 1. Este es uno de los parámetros que podemos manipular de tal manera que tenemos la posibilidad de crear rutas estáticas con

diferentes distancias administrativas. Para esto vamos a hacer uso del siguiente comando en el modo de configuración global.

ipv6 route [Red de destino especificando el prefijo] [Interfaz de salida/Dirección del siguiente salto] [Distancia Administrativa (Opcional)]

Por ejemplo si deseamos establecer una ruta hacia la red 2001:0:0:0/64 con distancia administrativa de 200 e interfaz serial 2/0, el comando seria el siguiente:

ipv6 route 2001:0:0:0/64 se2/0 200

Como puede darse cuenta en la estructura del comando hay 2 formas de establecer la ruta estática, la primera es usando la dirección IP del siguiente salto. La segunda es especificando la interfaz de salida por donde se envía el paquete, aquí es preciso hacer ver un detalle fino pero importante, cuando usamos la dirección del siguiente salto y no especificamos una AD, la distancia que vamos a poder ver en la tabla de ruteo será de 1. En cambio cuando usamos la interfaz de salida para indicar al dispositivo a donde enviar el paquete, vamos a ver una AD de 0 en la tabla de ruteo o en su caso una leyenda que nos indique que la subred está directamente conectada.

Rutas por defecto

Existe un tipo de ruta estática especial que podemos configurar en nuestra red, esta ruta nos sirve como ruta de último recurso, es decir si nuestro dispositivo no encontró ninguna ruta en su tabla, en vez de descartar el paquete podemos enviarlo a otro dispositivo que tenga mejores posibilidades de encontrar una ruta. Esta acción se va a tomar con todos los paquetes para los cuales el router no haya encontrado un resultado en su tabla de ruteo. Esta ruta especial se llama ruta por defecto o default, generalmente en las topologías de redes locales vamos a apuntar dicha ruta hacia internet, de esta manera todos los paquetes hacia un destino desconocido pueden ser direccionados por la infraestructura que mantiene internet. También podemos designar un router o una infraestructura especial que contenga las rutas hacia toda la red local, de esta manera se configuraría la ruta apuntando a dicha infraestructura.

Para crear una ruta por defecto vamos a utilizar el mismo formato que en la creación de rutas estáticas. Solo que en el campo de Red de destino vamos a colocar:

::/0

Lo que indica que estamos configurando una ruta por defecto, los demás campos se mantienen igual, a continuación mostraremos un comando que configura una ruta por defecto hacia el router con dirección 2001::1/64.

Ipv6 route ::/0 2001::1 2001::1/64

Proceso de configuración de OSPFv3 y RIPng

Vamos a explicar el proceso de configuración de los protocolos OSPF y RIP para IPv6, estos protocolos funcionan igual que en IPv4, hay ligeros cambios en algunos mensajes y direcciones, pero la esencia y el proceso básico de funcionamiento sigue siendo el mismo. Es por ello que no ahondaremos en las características de cada protocolo, para ello se le recomienda leer las practicas especificas en estos dos protocolos.

Configuración de RIPng

Para poder configurar el protocolo en los dispositivos Cisco solo necesitamos habilitarlo interfaz por interfaz. A diferencia de la configuración de RIP en IPv4 en donde primero creábamos un proceso y después indicábamos en que interfaces estaría activo, con RIPng esto cambia, aquí simplemente tenemos que entrar al modo de configuración de interfaz e ir habilitando RIPng interfaz por interfaz, esto se hace usando el siguiente comando:

ipv6 rip *[nombre del proceso]* enable

El nombre del proceso es elección del administrador, pero recuerde que este comando se ejecuta en el modo de configuración de interfaz. Cabe decir que aún sigue existiendo la opción de ingresar al modo de configuración del protocolo usando el comando *ipv6 router rip [Nombre del proceso]*, pero este modo solo se

usa para configurar algunas opciones adicionales del protocolo, no para habilitarlo en las interfaces.

Configuración de OSPFv3

De manera similar que RIPng, OSPFv3 sera habilitado interfaz por interfaz, solo que aquí es recomendable primero crear el proceso OSPF antes de activarlos en las interfaces, para ellos solo se hara uso del comando siguiente en modo de configuración global:

ipv6 router ospf *[número de proceso]*

Después de haber creado el proceso OSPF simplemente se tiene que entrar al modo de configuración de interfaz y activar el envió de paquetes OSPF con el siguiente comando:

ipv6 ospf *[número de proceso]* area *[área ID]*

Referencias

W. Odom, Official cert guide Cisco CCENT, CCNA ICND1 200-101. Indianapolis, In.: Cisco Press, 2013.
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 2373.
RFC 2460.
RFC 2461.
RFC 2462.

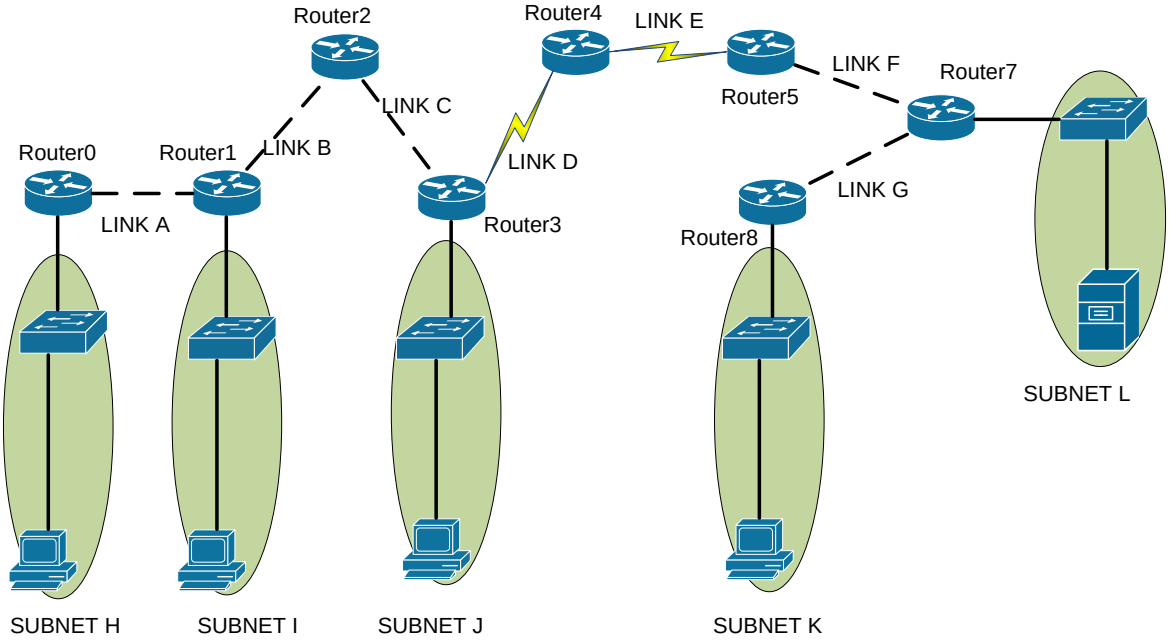
Tabla de comandos

COMANDO	DESCRIPCIÓN.
(config)#ipv6 unicast-routing	Habilita el envió de paquetes IPv6 en todo el router
(config-if)#ipv6 enable	Configura automáticamente una dirección tipo Link Local en la interfaz además de que habilita IPv6 en dicha interfaz.
(config-if)#ipv6 address *[prefijo de 64 bits]* eui-64	Configura una dirección IPv6 usando el proceso EUI-64 y el prefijo de red introducido.
(config-if)#no shutdown	Habilita la interfaz.
(config-if)#ipv6 rip *[nombre del proceso]* enable	Habilita el uso del protocolo RIPng en la interfaz, usando el nombre de proceso introducido.
(config-if)#ipv6 rip *[nombre del proceso]* default-information originate	Propaga una ruta por defecto usando RIPng.
(config)#ipv6 route *[Red de destino especificando el prefijo] [Interfaz de salida/Dirección del siguiente salto] [Distancia Administrativa (Opcional)]*	Establece una ruta estática hacia una red.
(config)#ipv6 route ::/0 *[Interfaz de salida/Direccion del siguiente salto]*	Establece un ruta por defecto.
#sh ipv6 route	Muestra la tabla de enrutamiento en IPv6
(config)#ipv6 router ospf *[número de proceso]*	Crea o abre un proceso OSPFv3 en el router.
(config-if)#ipv6 ospf *[número de proceso]* area *[área ID]*	Habilita la interfaz con OSPFv3 especificando el proceso y el área al que pertenece.
(config-router)#default-information originate	Habilita la propagación de rutas por defecto.

Tabla de direccionamiento

Subred/Link	Prefijo de red (64 bits)
LINK A	2000:0:0:0::/64
LINK B	2000:0:0:1::/64
LINK C	2000:0:0:2::/64
LINK D	2000:0:0:3::/64
LINK E	2000:0:0:4::/64
LINK F	2000:0:0:5::/64
LINK G	2000:0:0:6::/64
SUBRED H	2000:0:0:7::/64
SUBRED I	2000:0:0:8::/64
SUBRED J	2000:0:0:9::/64
SUBRED K	2000:0:0:10::/64
SUBRED L	2000:0:0:11::/64

Topología



Desarrollo

Actividad 1

1. Configure las direcciones IPv6 usando los prefijos señalados y el método EUI-64 en las interfaces indicadas y actívelas.

   Router0: Interface Fa0/1, prefijo de la subred H.
   Router1: Interface Fa1/0, prefijo de la subred I.
   Router3: Interface Fa0/1, prefijo de la subred J.
   Router7: Interface Fa0/0, prefijo de la subred L.
   Router6: Interface Fa1/0, prefijo de la subred K.
2. Configure todos los dispositivos terminales para que obtengan sus direcciones IPv6 vía SLAAC, en caso de existir un problema de solución a este.

Actividad 2

1. Configure todas las interfaces de Router6 y Router7 con un proceso RIPng llamado “sideA”, para que compartan información de ruteo.
2. Configure la interfaz Fa0/0 de Router5 con un proceso RIPng llamado “sideA”, para que compartan información de ruteo.
3. Configure las interfaces de Router0 y Router1 con un proceso OSPFv3 etiquetado con el número 100 y en el área 1, para que compartan información de ruteo.
4. Configure la interfaz Fa0/1 de Router2 con un proceso OSPFv3 etiquetado con el número 100 y en el área 1, además configure la interfaz Fa0/0 con un proceso similar al anterior excepto que esta vez utilice el área 0.
5. Configure la interfaz Fa0/0 de Router3 con un proceso OSPFv3 etiquetado con el número 100 y en el área 0.

Nota Importante: OSPFv3 utiliza una dirección de 32 bits como “Router ID” para el proceso, por lo que si no tiene configurada ninguna dirección IPv4 (dirección de 32 bits) en los routers donde active OSPFv3, tendrá que configurar un “Router ID” de manera manual.

Actividad 3

1. Configure Router4 con solo rutas estáticas, de tal manera que tenga forma de llegar a cualquier subred en la topología.
2. Configure en Router3 y Router5 una ruta por defecto que direccione el tráfico hacia Router4.
3. Configure a Router3 y Router5 para que propaguen la ruta por defecto, usando OSPFv3 y RIPng respectivamente.
4. Haga pruebas de conectividad para verificar que todos los dispositivos se pueden comunicar.

Conclusiones

En esta práctica se logró ver que no hay una gran diferencia entre el ruteo en IPv4 e IPv6, desde luego existen cambios inherentes al tipo de direcciones, pero de manera general los protocolos dinámicos siguen funcionando igual solo que ahora ha cambiado la forma de configurarlos, lo mismo sucede con el funcionamiento y configuración del direccionamiento estático. Vale la pena destacar los beneficios y cambios en el direccionamiento y la forma en que los hosts utilizan IPv6, ya que se resolvieron muchos problemas que había con IPv4, además de que se agregaron nuevas capacidades al protocolo IPv6. Entre los conceptos más importantes que se le sugiere recordar están las diferencias, ventajas y desventajas del direccionamiento estático y dinámico. El concepto y utilización de la distancia administrativa así como las diferencias en la configuración de los protocolos dinámicos en IPv4 e IPv6.

Cuestionario

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

   ipv6 route 3000:0:0:2::/64 serial 2/0

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. El comando se utiliza para establecer una red de conexión única.

2. ¿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

3. ¿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

4. Si una tabla de enrutamiento, aprendió una ruta mediante RIP, y mediante EIGRP a la misma red, ¿qué ruta se utilizará para enrutar paquetes?

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

5. Menciones los 2 protocolos usados por un host para obtener su dirección IPv6.

6. Mencioné 3 ventajas de migrar a IPv6.

7. ¿Cuántos bits tiene una dirección IPv6?

8. Un dispositivo está usando EUI-64 para construir su dirección IPv6 con un prefijo de red 2002:0:0:8::/64 y una MAC 00D0.BAD2.5501 ¿Qué dirección IPv6 tendrá el dispositivo?

9. ¿Cuál es la métrica usada por OSPF y como se calcula (por defecto) en dispositivos Cisco?

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

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

Respuestas a los Cuestionarios.

Practica 1.

1. C.
2. A y E.
3. ARIN, LAPNIC, ACNIC, AFRINIC, RIPE NCC.
4. A, D y G.
5. C.
6. A, C.
7. A.
8. A, D, F.
9. A.
10. Dirección de RED: 172.16.4.0
    Dirección de BROADCAST: 172.16.7.255.255
    Rango: 172.16.4.1 hasta 172.16.7.254

Practica 2.

1. C.
2. D.
   Debemos tomar 4 bits de la parte de Host y asignarlos a la parte de subred de esta manera tenemos $2^4 = 16$ subredes de igual tamaño.
3. Ordenar las subredes, identificar los bits de la porción de HOST, identificar las máscaras de subred y aplicar subneteo.
4. A.
5. A.
   Recordemos que podemos calcular las direcciones asignables de Host con la formula siguiente:

   $$2^n - 2$$

   Tenemos una máscara /27 en el sitio B por lo que tendremos $2^5 - 2 = 30$ direcciones asignables, lo cual no alcanza para los 32 hosts del sitio.

6. C, E.

7. D.
   Si identificamos las subredes de menor a mayor tenemos lo siguiente:

192.168.0.0/22	192.168.4.0/22	192.168.8.0/22	192.168.12.0/22

   La tercera subred es la 192.168.8.0/22, donde la 2ª dirección asignable a Host es 192.168.8.2.
8. B.
9. Sitio A: 172.16.1.192/27.
   Sitio B: 172.16.1.0/25.
   Sitio E: 172.16.1.128/26
   Link 1: 172.16.1.224/30.
   Link 2: 172.16.1.228/30.
10. D.

Practica 3.

1. B, C, F.
2. D.
   Una ruta estática tiene una distancia administrativa menor que OSPF y RIP por lo que el router elegirá esta ruta a la hora de insertarla en su tabla de ruteo.
3. A, C, D.
4. HELLO, DATABASE DESCRIPTION, LINK STATE REQUEST, LINK STATE UPDATE, LINK STATE ACK.
5. B.
   La máscara wildcard no coincide con ningún tipo de mascara de red, si calculáramos la máscara de red resultante de esta wildcard, tendríamos una máscara 0.255.255.255, la cual no tendría sentido.
6. B.
7. C.

De la fórmula del cálculo del costo solo despejamos el ancho de banda, el costo lo podemos ver en la figura.

$$BW = {}^{10^8}/_{costo} = {}^{10^8}/_{64} = 1.5625\ Mbps$$

8. D.
   Lo que hicimos con los comandos de la figura fue cambiar el costo de referencia en la fórmula original a 10 Mbps lo cual nos da el resultado siguiente.

$$costo = {}^{10\ Mbps}/_{1.5625\ Mbps} = 6.4 \approx 6$$

9. C.
10. C.
    Las respuestas A y B tienen mascaras Wilcard incorrectas y la respuesta D tiene el área mal configurada.

Practica 4.

1. C.
2. A.
   El “deny” implícito se refiere a la forma en la que las ACL procesan un paquete, el terminar de comparar todas las condiciones en la ACL, al final si ninguna coincide entonces el paquete se descarta.
3. C.
4. A.
   Al cambiar la parte del comando “gt” por “eq”, se ajusta la sentencia para que no permita el trafico tcp en el puerto 23, recuerde que “gt” significa más grande que, por lo que en la sentencia original no se permite el tráfico de los puertos más grandes que el 23.
5. A.
6. C, E.

$$-\begin{matrix}255 & 255 & 255 & 255\\ 255 & 255 & 255 & 240\end{matrix} = 0.0.0.15$$

$$\begin{matrix} 255 & 255 & 255 & 255 \\ - & & & \\ 255 & 255 & 252 & 0 \end{matrix} = 0.0.3.255$$

7. A.
8. A.
9. C.
10. D.

    La sentencia A no Deniega el tráfico a la PC. La sentencia B deniega el trafico telnet a la PC, pero lo hace solo para el tráfico que viene de la dirección 192.168.3.1. La sentencia C deniega el tráfico en los puertos mayores que 23. Por lo que la sentencia D cumple con la condición establecida.

Practica 5.

1. A.
2. B.
3. D.
4. A.
5. D.
6.

- Definir un pool o grupo de direcciones publicas en el router que ejecutara la traducción.
- Crear una ACL que identifique que direcciones privadas serán traducidas.
- Enlazar la ACL hacia el pool de direcciones.
- Definir que interfaces son “Inside” (interfaces contenidas dentro de la red local privada).
- Definir que interfaces son “Outside” (interfaces contenidas en internet las cuales tienen una dirección pública).

7. B.
8.

- Definir un pool o grupo de direcciones públicas en el router que ejecutara la traducción.
- Crear una ACL que identifique que direcciones privadas serán traducidas.

- (Opción 1) enlazar la ACL hacia el pool de direcciones sin olvidar teclear la palabra clave “overload”.
- (Opción 2) enlazar la ACL con una interfaz de salida que tenga una dirección publica, de esta manera esta única dirección publica será usada en el mapeo.
- Definir que interfaces son “Inside” (interfaces contenidas dentro de la red local privada).
- Definir que interfaces son “Outside” (interfaces contenidas en internet las cuales tienen una dirección publica).

9. Inside global: Con este termino nos vamos a referir a las direcciones publicas usadas para representar a un host después de la traducción.
10. A y C.
    NAT se utiliza cuando tus hosts o redes internas tienen un direccionamiento privado (que puede ser duplicado), y se desea comunicar con otras redes o con Internet.

Practica 6.

1.
   - Establecer un “hostname” (se recomienda cambiar el que viene configurado por defecto).
   - Establecer un nombre de dominio.
   - Establecer un nombre de usuario y una contraseña.
   - Generar una clave para la encriptación.
   - Habilitar SSH versión 2.
   - Configurar los protocolos permitidos en el acceso remoto.
   - Indicar al dispositivo revisar los nombres de usuario y contraseñas.

2. A.
3. B.
   Si no se introduce el comando switchport port-security no se está habilitando la seguridad en el puerto, por lo que los demás comandos no tienen efecto.
4. B.
5. Simplemente se debe deshabilitar el puerto de manera administrativa con el comando shutdown y después habilitarlo de nuevo.

6. C.
7. A.
8. Es cuando un agresor desactiva o daña redes, sistemas o servicios con el propósito de denegar servicios a los usuarios a quienes están dirigidos.
9. Autenticación, Autorización y Auditoria.
10.
    - Configurar los puertos de acceso.
    - Habilitar la seguridad del puerto.
    - Definir la forma en que el Switch aprenderá las direcciones MAC (Estática/ Dinámica).
    - Definir el límite de direcciones MAC permitidas en el puerto.
    - Definir el modo de restricción que tomara el puerto en caso de violación.

Practica 7.

1. A y B.
2. C.
3. A.
4. D.
   La distancia administrativa de EIGRP es menor que la de RIP.
5. DHCP Y SLAAC.
6. No existe NAT/PAT lo que significa que no hay problemas inherentes a la implementación de dicho protocolo. IPv6 no utiliza mensajes de Broadcast, lo que reduce ciertos problemas inherentes a estos mensajes.
7. 128 bits.
8. 2002::8:2D0:BAFF:FED2:5501.
9. Costo.
$$costo = {10^8}/{BW}$$
10. C.