Universidad Nacional Autónoma de Nicaragua-León
Facultad de Ciencias

Departamento de Computación

Monografía para optar al título de Ingeniería en Sistemas de Información:

Switching y Enrutamiento con Tecnología CISCO
Teoría e Implementación

Autores

Br. Alicia Esmeralda Larios Acuña
Br.Irayda Rosa Mayorga Castellón
Br. Bruna Mercedes Moreira Cárcamo

Tutor
Msc. Aldo René Martínez

León, Nicaragua, 04 julio del 2008.

Agradecimientos

Agradecemos:

A Dios:

Por habernos dado la oportunidad de vivir, brindarnos fuerza, esperanza, sabiduría y deseos de superación en cada momento de nuestras vidas.

A Nuestros Padres:

Por habernos apoyado día a día, siempre dándonos ánimo, confianza, amor y fortaleza, siendo nuestro mayor apoyo en la lucha por graduarnos como Ingenieras en Sistemas de Información.

A todo el claustro de profesores del Departamento de Computación:

Por su empeño y dedicación por transmitirnos todos y cada uno de los conocimientos que hoy son nuestros y que pondremos en práctica de aquí en adelante.

A todas aquellas personas que de una u otra manera colaboraron para que nos fuese posible terminar nuestro trabajo.

Indice

Introducción

La necesidad de compartir recursos computacionales existentes, así como permitir el acceso a grandes volúmenes de información situados en puntos geográficamente distantes, hizo surgir la necesidad de interconectar los sistemas informáticos disponibles.

En términos más básicos, la interconexión de redes no es nada más que enlazar máquinas y personas a través de un laberinto de líneas de telecomunicación intermediarias y de dispositivos de computación. Esto nos conduce al enrutamiento, que en esencia solo tiene dos misiones fundamentales: determinar una trayectoria a lo largo de la que se puede realizar un enlace y transmitir paquetes a lo largo de dicha trayectoria, debido a esto los enrutadores usan las direcciones IP para enviar mensajes a través de las redes, complementado con la conmutación encargada de llevar las tramas de extremo a extremo.

En el presente documento se abordan una serie de temas relacionados con la conmutación y enrutamiento con Tecnología CISCO, cada uno con su respectivo desarrollo Teórico e Implementación con los cuales se ampliarán los conocimientos teóricos y se mejorará la calidad de los aspectos prácticos del área de redes.

Este documento aborda la implementación práctica de cada uno de los temas, especificando la temporización de las prácticas, plasmando como parte del desarrollo de cada una de ellas un tema, diagrama de red, objetivos, introducción, requerimientos, enunciados y solución de la práctica misma con resultados comentados y bibliografía referente a cada una de ellas.

El desarrollo teórico del documento contiene temas relacionados con la conmutación y enrutamiento, tales como: Configuración de enrutadores, direccionamiento IP, Diagnóstico de fallas, conmutación de la capa de enlace de datos, conceptos informáticos de seguridad, soluciones para el direccionamiento IP y Protocolos de enrutamiento interno y externo.

El documento esta dividido básicamente en dos partes. La primera parte del documento consta del desarrollo teórico, que hay que tener como conocimiento base para el desarrollo de las prácticas. La segunda parte abarca la implementación práctica.

Para la realización de las prácticas se ha contado como recurso primario, la utilización de los simuladores Cisco Boson NetSimV6 y Packet Tracer 4.0, los cuales se han instalado en una computadora con sistema operativo Windows XP, así como también de la utilización de enrutadores físicos Cisco de la serie 1800.

Antecedentes

La Universidad Nacional Autónoma de Nicaragua en la Facultad de Ciencias, el Departamento de Computación ofrece dos carreras: Ingeniería en Sistemas de Información e Ingeniería en Telemática, cada una tiene su propio plan de estudio, los cuales contienen asignaturas relacionadas con el área de Redes en las que se abordan temas de Conmutación y Enrutamiento.

En ambas carreras las asignaturas tienen su propio plan académico donde desarrollan todo el temario a abordar en la asignatura.

En la carrera de Ingeniería en Sistemas, para la asignatura de Redes de Ordenadores la actualización mas reciente en el plan docente fue realizada en el año 2002, elaborado por Nestor Germán Castro Araúz como proyecto de fin de carrera, requisito para la culminacion de estudios complementarios a la Licenciatura en Computación de la UNAN-León, dicho proyecto consistía en realizar un plan docente para las asignaturas de Redes de Ordenadores I y Redes de Ordenadores II. Este plan docente contiene algunas prácticas de Conmutación y Enrutamiento, pero no enfocadas al desempeño de un Administrador de Red.

En cambio para la carrera de Ingeniería en Telemática no existe ningún antecedente de trabajos relacionados con las asignaturas de Redes de esa carrera.

Por lo que podemos decir que en ambas carreras para las asignaturas relacionadas con Conmutación y Enrutamiento no existe conocimiento de trabajos realizados que aborde en su contenido Conmutación y Enrutamiento con Tecnologías CISCO, por lo que nuestro trabajo sería el primero en brindar ese apoyo teórico y práctico al alumno y profesores de las asignaturas.

Justificación

La conmutación y enrutamiento son los conceptos en redes más importantes para las transferencias de información por todo el mundo, para su logro se hace necesaria una serie de configuraciones que todo administrador de redes debe conocer. Es por ello que en este trabajo se escogieron los temas más importantes y relevantes con respecto a la utilidad práctica en las redes corporativas, educativas y de gobierno en el mundo sobre conmutación y enrutamiento.

Este trabajo servirá como complemento y/o apoyo para las asignaturas relacionadas a redes. En cada tema se presenta un desarrollo teórico e implementaciones prácticas. En la parte teórica se pretende introducir al alumno sobre el tema desde un nivel básico hasta un nivel medio, en la práctica se reforzará la teoría mediante situaciones y planteamientos simulados sobre funcionamiento y administración de redes reales, creando una base más fuerte en el alumno para su desempeño competitivo como Administrador de Redes.

Se usarán tecnologías CISCO por el simple hecho de que Cisco System es el líder mundial en redes para internet y abastece más del 80% del mercado global en redes, siendo el router el producto que lo ha puesto en la posición donde se encuentra, complementando su línea de productos con switches.

Objetivo General

- Desarrollar temas con fundamento en conmutación y enrutamiento tanto en el aspecto teórico como práctico, implementados con Tecnologías CISCO para apoyar y/o complementar a las asignaturas de Redes de Computadores.

Objetivos Específicos

- Elegir un temario enfocado en la conmutación y enrutamiento.
- Desarrollar prácticas relacionadas con la configuración y administración de routers, direccionamiento, seguridad en redes, protocolos de enrutamiento.
- Utilizar simuladores (Boson y Packet Tracer 4.0) y enrutadores físicos (Serie CISCO 1800).
- Elaborar un documento que contenga el desarrollo teórico y se especifique la temporización de las prácticas, y por cada práctica plasmar un tema, diagrama de red, objetivos, introducción, requerimientos, enunciados y otro documento que contendrá la solución de las prácticas.

Planificación Temporal

Para realizar una planificación objetiva de la realización de las prácticas a lo largo del semestre se debe analizar la duración del período lectivo y obtener el número de horas del que se dispone.

Partiendo del año académico del año lectivo 2008 propuesto por la UNAN-León y tomando en cuenta que las prácticas serán impartidas en el segundo semestre, se tienen 16 semanas exactas para cumplir con el desarrollo de las prácticas.

Para el desarrollo de la parte práctica de la asignatura se cuenta con dos sesiones semanales de dos horas cada una, por lo tanto se tiene un total de 64 horas, se tomó en cuenta algunas pérdidas de sesiones, lo cual resulta en 15 semanas para un total de 60 horas.

El número de sesiones asignadas para cada tema se presenta en la siguiente tabla.

Nº	NOMBRE DE LA PRÁCTICA	NÚMERO DE SESIONES
1	Aspectos fundamentales de la línea de comandos	1
2	Modos de comando y configuración de contraseñas del router	1
3	Comando Show	1
4	Configuración de las interfaces Serial y Ethernet	1
5	Configuración de las descripciones de Interfaz y del Mensaje del día (MOTD)	1
6	RIP (Protocolo de información de enrutamiento)	2
7	Telnet, Ping y Tracerout	2
8	Descubrimiento de vecinos: Protocolo CDP	1
9	Verificación y Respaldo del IOS	1
10	Diagnóstico de fallas y recuperación de contraseñas	2
11	ACL (Listas de Acceso)	2
12	Configuración de VLAN	2
13	NAT – Network Address Translation-	3
14	Protocolo de enrutamiento: Configuración de OSPF	3
15	OSPF (Open Short Path First)	2
16	IS-IS (Integrated System – Integrated System)	2
17	Protocolo de enrutamiento externo: BGP	2

El número de sesiones de cada una de las prácticas realizadas en los simuladores, fue planteado para un tamaño de grupo de tres estudiantes y para las prácticas en las que se utilizaron routers físicos, deben de haber como máximo dos estudiantes.

Estructura y representación del trabajo final

- Cada tema presenta una teoría lo mas ampliamente desarrollada que va desde lo más básico hasta los aspectos más avanzados, cada tema refuerza sus simientos teóricos con la práctica, algunos llevan dos prácticas para un mismo tema como sigue:

Nº CAP.	TEMAS TEÓRICOS	Nº DE PRÁCTICAS
1	Aspectos Fundamentales de la línea de comandos	Pract. 1 y Pract. 2
2	Comando SHOW	Pract. 3
3	Configuración de las interfaces	Pract. 4
4	Configuración del BANNER y descripción de las interfaces	Pract. 5
5	RIP	Pract. 6
6	Información básica de Telnet, Ping y Traceroute	Pract. 7
7	CDP	Pract. 8
8	Verificación, respaldo del IOS, recuperación de contraseña	Pract. 9 y Pract. 10
9	ACL –Listas de Acceso-	Pract. 11
10	VLAN	Pract. 12
11	NAT (Network Address Translation)	Pract. 13
12	Protocolo de enrutamiento OSPF	Pract. 14 y Pract. 15
13	IS-IS	Pract. 16
14	BGP	Pract. 17

- Existen dos documentos impresos, el primero con la estructura de la monografía en el que se encuentra la teoría e implementación de cada tema y el segundo con la solución de las prácticas, para este último el uso es sólo autorizado para profesores.

- Todo el documento impreso se encuentra en un CD en formato PDF. Se les proporciona tambien los ejecutables de los simuladores usados para la realización de las prácticas los cuales son requerimientos para su desarrollo.

- En otro CD la estructura del documento se presenta en forma de libro con formato PDF, donde el primer libro “Conmutación y Enrutamiento con tecnología CISCO – Teoría e Implementación” presenta la teoría y los enunciados de las prácticas.

- Otro CD con un segundo libro “Conmutación y Enrutamiento con tecnologías CISCO – Solucion de Prácticas” restringido a estudiantes.

DESARROLLO TEÓRICO

CAPÍTULO 1

ASPECTOS FUNDAMENTALES DE LA LÍNEA DE COMANDOS Y CONFIGURACIÓN DE CONTRASEÑAS.

1. ASPECTOS FUNDAMENTALES DE LA LÍNEA DE COMANDOS

1.1. Introducción a los modos de router

Los enrutadores Cisco pueden estar en cualquiera de los siete modos operativos, que se muestran en la Figura 1.1. Tres de ellos son modo de inicio. En los otros cuatro, los administradores de red están en modo EXEC de usurario o en modo EXEC privilegiado (habilitar). Debe pasar por el símbolo de sistema de contraseña en el EXEC de usuario para entrar al EXEC privilegiado. Una vez dentro del EXEC privilegiado, se pueden realizar los cambios de configuración a todo el dispositivo o a una interfaz de red específica.

Debe realizar un seguimiento del modo de enrutador en que se encuentra en todo momento. Muchos comandos IOS sólo se ejecutan desde un modo específico. Como puede verse en la Figura 1.1, los modos de enrutador son más específicos, y potentes, conforme el usuario se desplaza hacia el centro del IOS. Conviene estar atentos a la línea de comandos IOS porque siempre indica en qué modo está.

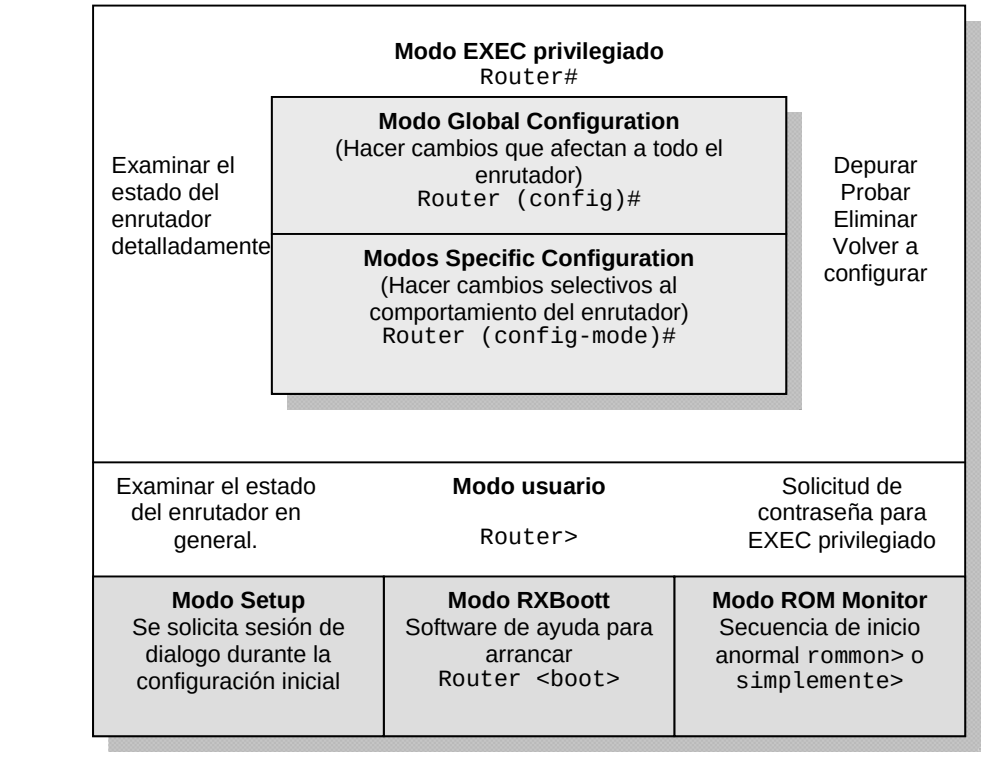


Figura 1.1 *Los siete posibles modos de operación de los enrutadores de Cisco*

1.1.1. Tres tipos de modos de operación

Los modos operativos de enrutador de Cisco existen para manejar tres condiciones generales:

- Iniciar un sistema.
- Definir qué comandos se pueden usar.
- Especificar qué partes de un enrutador se verán afectadas por los cambios realizados al archivo de config.

La Tabla 1.1 muestra los diferentes modos IOS y para que se usan. A medida que se familiarice con la interconexión de redes de Cisco en general, y con el software IOS en particular, verá que la mayoría de la acción se produce dentro de los diferentes modos de configuración.

Tabla 1.1 *Tres formas generales de modos software del IOS*

Tipo de modo	Propósito
Inicio	El *modo Setup* se usa para realizar un archivo básico de trabajo de configuración. El *modo RXBoot* ayuda en el inicio de los enrutadores a un estado rudimentario cuando no es posible encontrar en la memoria Flash una imagen operativa del IOS. El *modo ROM monitor* lo usa el enrutador si no es posible encontrar la imagen del IOS o si se interrumpió la secuencia normal de inicio.
Usuario	El *modo EXEC de usuario* es el primer <<lugar>> donde accede el usuario después de iniciar una sesión; limitada a los usuarios a examinar el estado del enrutador. Se entra al *modo EXEC privilegiado* utilizando una contraseña Enable; permite a los usuarios modificar el archivo de configuración, borrar memoria, etc.
Configuración	El *modo Global config* cambia parámetros de todas las interfaces. El *modo Config-command* <<realiza>> en interfaces concretas.

1.1.2. Modos de Configuración

Los modos de configuración se diferencian de los modos de usuario por naturaleza. Los dos <<modos de usuario>> EXEC definen el nivel de comandos IOS que puede utilizar el usuario. Por el contrario, los modos de configuración se usan para apuntar a interfaces de red específica, física o virtual, a las que se aplican los cambios de configuración. Por ejemplo, el usuario entrará en el modo de configuración de la interfaz, identificado por la línea de comandos (config-if), para configurar un modulo de interfaz Ethernet específico. Hay ocho modos de configuración en total, cada uno destinado a diferentes partes del archivo de configuración, como se muestra en la Tabla 1.2.

Si echa un vistazo a la Tabla 1.2, verá que el modo de configuración es la forma de indicar al IOS que hacer con los paquetes que fluyen a través del dispositivo. Algunos modos se aplican a paquetes que pasan a través de puntos de conexión específicos, como interfaces, líneas y puertos. Los demás modos de configuración IOS manejan protocolos y tablas de enrutamiento necesarias para manejar dicho flujo.

Los dos tipos de archivo de configuración

Hay dos tipos de archivos de configuración para cualquier enrutador:

- Archivo de configuración de ejecución.
- Archivo de configuración de inicio.

La diferencia básica es que el archivo de configuración de ejecución está <<vivo>> en el sentido de que su imagen está en RAM. Cualquier cambio que se realice al archivo de configuración en ejecución se aplica inmediatamente. El archivo de configuración de inicio se almacena en la NVRAM del enrutador, donde la secuencia de inicio del IOS busca los parámetros de configuración de ejecución del enrutador cuando se inicia.

Tabla 1.2 *Cada modo de configuración está destinado a una parte del enrutador*

Modo de Configuración	Puerto de enrutador destino	Se aplica a
Global	Router(config)#	Todo el archivo de configuración.
Interface	Router(config-if)#	Modulo de interfaz (físico).
Subinterface	Router(config-subif)#	Subinterfaz (Virtual).
Controller	Router(config-contoller)#	Controlador (físico).
Line	Router(config-line)#	Líneas de Terminal (virtual).
Router	Router(config-router)#	Enrutamiento IP (protocolo).
IPX-Router	Router(config-ipx-router)#	Enrutamiento IPX (protocolo).
Route-Map	Router(config-route-map)#	Tablas de enrutamiento.

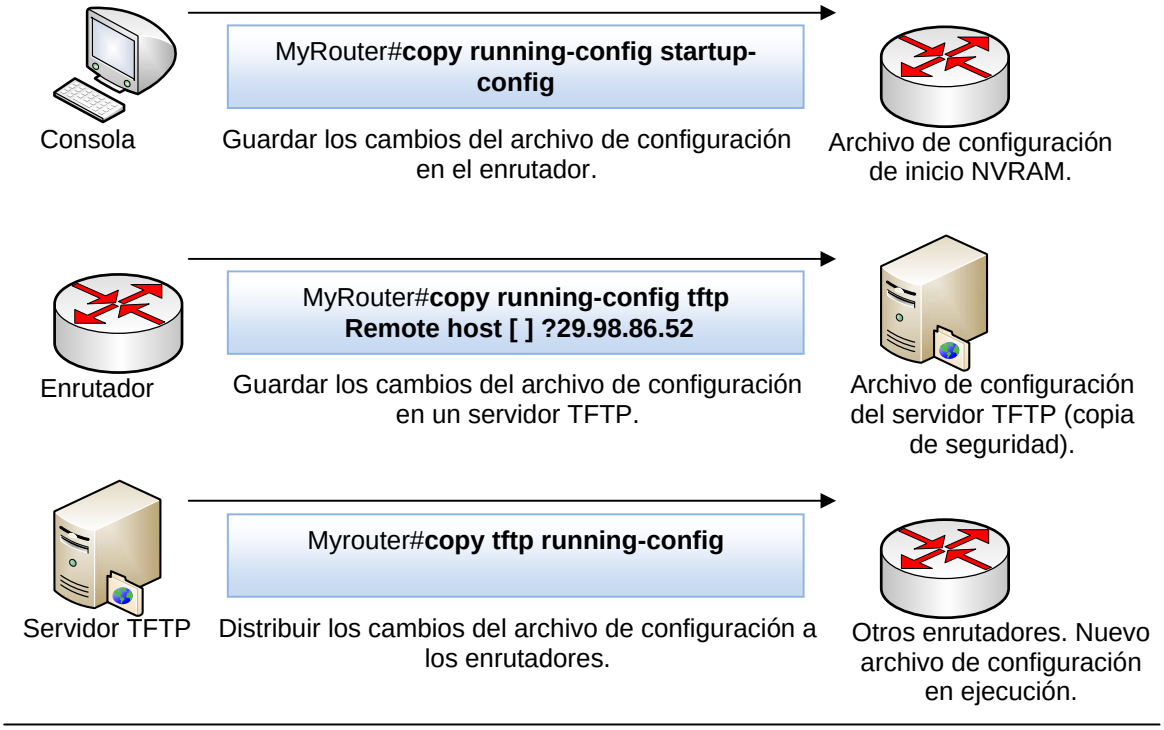


Figura 1.2 *Cada modo de configuración está destinado a una parte del enrutador.*

El comando `copy` se usa para guardar y distribuir cambios en el archivo config. Como puede ver en la parte inferior de la Figura 1.2, se puede distribuir un archivo config maestro a otros enrutadores mediante un servidor TFTP.

1.2. Como recorrer el IOS con el sistema de ayuda

IOS tiene incorporado un sistema de ayuda sensible al contexto. *Sensible al contexto* significa que el sistema de ayuda responde con información basándose en el lugar del sistema donde esté situado el usuario en ese momento. Puede conseguir la mejor ayuda sensible al contexto introduciendo simplemente una interrogación en la línea de comandos. Aquí, por ejemplo, tiene un listado de todos los comandos raíz, disponibles en el nivel EXEC de usuario de IOS:

```
Router>?
Exec commands:
   <1-99>           Session number to resume
   access-enable    Create a temporary Access-List entry
   access-profile   Apply user-profile to interface
   connect          Open a terminal connection
   disable          Turn off privileged commands
```

```
   disconnect        Disconnect an existing network connection
   enable            Turn on privileged commands
   exit              Exit from the EXEC
   help              Description of the interactive help system
   lock              Lock the terminal
   login             Log in as a particular user
   logout            Exit from the EXEC
   mtrace            Trace reverse multicast path from destination to
   source
   .
   .
   .
```

También puede conseguir lo que algunos llaman <<ayuda de palabra>> introduciendo parte del comando, que no conoce, seguido inmediatamente de una interrogación:

```
Router>sh?
show
```

La ayuda de palabra es una gran forma de conseguir definiciones y es especialmente práctica para averiguar lo que significan los comandos truncados, como con *show* en el ejemplo anterior. Otra forma de conseguir ayuda acerca de un comando parcial es simplemente introducirlo, con lo cual el sistema devolverá una instrucción sobre como obtener ayuda completa sobre el comando:

```
Router>sh
% Type "show ?" for a list of subcommands
```

Tenga en cuenta que en la ayuda que sugirió el comando show ? Hay un espacio entre el comando y la interrogación. Como se habrá dado cuenta, siempre hay un espacio entre un comando y su modificador (llamado *argumento*). Hacer esto en una solicitud de ayuda es la forma de solicitar una lista de argumentos disponible para el comando. En el siguiente ejemplo, la interrogación solicita todos los argumentos disponibles para show:

```
Router>show ?
   access-lists            List access lists
   arp                     ARP table
   cdp                     CDP information
   clock                   Display the system clock
   controllers             Interface controller status
   configuration           Contents of Non-Volatile memory
   history                 Display the session command history
   hosts                   IP domain-name, nameservers, and host isdn
   ISDN information
   ip                      IP information
   interfaces              Interface status and configuration
   .
   .
   .
```

Algunas veces, usar la ayuda de esta forma se llama ayuda de *sintáxis de comandos*, ya que ayuda a completar correctamente un comando con varias partes. La ayuda de sintáxis

de comandos es una herramienta potente de aprendizaje porque lista las claves o argumentos disponibles para el usuario en, prácticamente, cualquier momento de las operaciones de comandos IOS. Recuerde, es necesario insertar un espacio entre el comando y la interrogación para usar la ayuda de sintáxis de comandos.

En IOS, la ayuda juega un papel más importante que el sistema de ayuda de los paquetes de aplicaciones de software de negocios o de un PC normal. Estos sistemas de ayuda, también sensibles al contexto, son esencialmente manuales en línea que intentan ayudarle a aprender toda la subsección de la aplicación. La ayuda de IOS es escueta; sólo pretende ayudarle a llegar hasta la siguiente línea de comandos. Esto es alentador. La mayoría de los sistemas de ayuda actuales parecen asumir que el usuario está ansioso por pasar horas leyendo todo sobre un subsistema cuando, de hecho, sólo quiere saber qué hacer a continuación.

Nota: No se confunda por el nombre del comando **show**. **Show** muestra información del sistema en ejecución. No es un comando de propósito general para <<mostrar>> información de ayuda; el comando **?** hace eso. El comando show se usa para examinar el estado de los enrutadores.

1.3. Como asignarle una identidad al enrutador

Tomarse el tiempo adecuado para nombrar y documentar correctamente cada enrutador ayuda a hacer las redes más fáciles de administrar. La información de identificación puede introducirse mediante:

- Dando al enrutador un nombre significativo.
- Documentando individualmente las interfaces del enrutador.
- Poniendo un MOTD (*Message-Of-The-Day*; Mensaje del día) en el enrutador.

Frecuentemente vera que se usa el nombre de ejemplo <<Router>> en los ejemplos de configuración. No deje que esto le confunda; <<Router>> no es una parte obligatoria de la línea de comandos de IOS Cisco. Un enrutador puede nombrarse simplemente de forma tan fácil como <<OficinaCentral>> o <<R23183>> o cualquier otro nombre. A los enrutadores se les dan nombres significativos que informan a los administradores de red donde están los enrutadores y que hacen. Debe estar en el modo de configuración global y usar el comando **hostname** para cambiar el nombre de dispositivo, como se muestra aquí:

```
Router(config)#hostname MyRouter
MyRouter(config)#
```

Como el nuevo nombre se ha introducido en el archivo de configuración en ejecución, el nuevo nombre del enrutador MyRouter se usa de inmediato en la siguiente línea de comandos. Sin embargo, amenos que se use el comando **write** o el comando **copy** para almacenar el nuevo nombre (o cualquier otro cambio) en la NVRAM, si el enrutador fuese reiniciado, IOS seguiría usando el nombre antiguo.

1.4. Volver a llamar al historial de comandos

IOS mantiene un registro en ejecución de los comandos recientemente introducidos.
Ser capaz de volver a llamar comandos es útil para:

- Evitar tener que escribir comandos que se introducen repetidamente.
- Evitar tener que recordar líneas de comandos largas y complicadas.

La utilidad **history** registrará cualquier cosa que se introduzca, incluso comandos erróneos. El único límite es la cantidad de búfer de memoria dedicado a mantener el historial. Aquí tiene un ejemplo:

```
Router# show history
         test
         tel
         exit
         enable
```

Los comandos introducidos más recientemente aparecen mas arriba en la lista **show history**. No se listan alfabéticamente.
También se pueden usar las teclas de flecha para mostrar comandos anteriores. El uso de las teclas de flecha ahorra tener que introducir el comando **show history**, pero sólo muestra los comandos anteriores de uno en uno. Pulse la tecla de FLECHA ARRIBA o (CTRL-P) para volver a llamar al primer comando mas reciente. Si está ya en algún lugar en la secuencia de comandos anteriores, pulse la tecla de FLECHA ABAJO (CTRL-N) para volver a llamar al primer comando menos reciente.

1.5. Seguridad del enrutador

Los enrutadores no son muy visibles en las redes, principalmente, porque no tienen *Uniform Resource Locators* (URL, Localizador uniforme de recurso) como tiene www.yahoo.com o www.amazon.com. Los enrutadores no necesitan tener direcciones descriptivas, ya que los usuarios normales de las redes nunca necesitan saber si un enrutador está allí: simplemente necesitan la conectividad que éste les proporciona.

Las únicas personas que necesitan iniciar una sesión directamente en un enrutador son los miembros del equipo de red, responsables de su mantenimiento. En las redes TCP/IP, el protocolo sobre el que funcionan la mayoría de las redes, los enrutadores se identifican a sí mismos a las redes sólo con sus direcciones IP. Por esta razón, para iniciar una sesión en un enrutador, primero debe conocer que existe y qué dirección IP tiene. Los administradores de red responsables del enrutador, por supuesto, conocerán esta información.

No obstante, todavía existe el peligro potencial de abuso por parte de los *hackers.* Los enrutadores se envían constantemente mensajes entre sí para actualizar y administrar las redes en las que operan. Con las capacidades adecuadas y suficiente determinación, un *hacker* puede descubrir una dirección IP de un enrutador e intentar luego establecer una conexión Telnet con él. Como los enrutadores son los enlaces que mantienen unidas las redes, es fácil de comprender por qué Cisco y otros fabricantes de equipos de redes

diseñan muchas medidas de seguridad dentro de sus productos. Como muestra la Figura 1.3, la seguridad debe restringir el acceso a áreas dentro de una red y a dispositivos individuales.

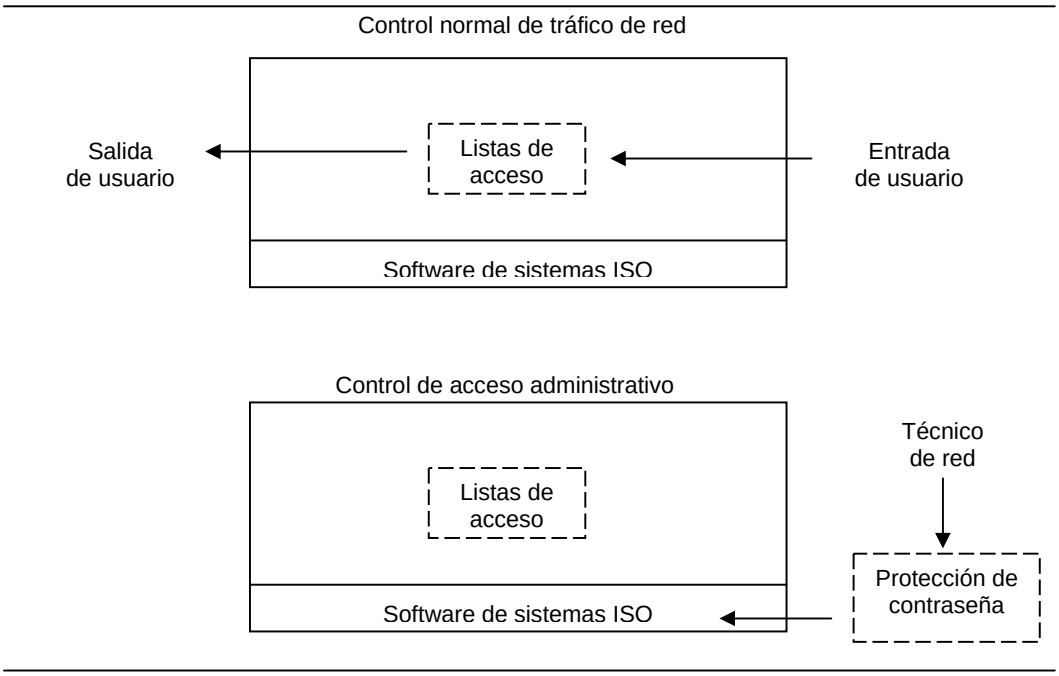


Figura 1.3. *Control de seguridad del tráfico de red frente al acceso administrativo.*

Nota: Las contraseñas del enrutador sólo controlan la entrada a los dispositivos de enrutador por sí mismas. No confunda las contraseñas de enrutador con las contraseñas que los usuarios normales de redes deben escribir para entrar a ciertos sitios Web o para poder acceder a intranets (redes privadas que utilizan los protocolos de Internet). Las restricciones que se exigen a los usuarios normales se administran mediante cortafuegos y listas de acceso.

1.6. Contraseñas de enrutador

La única intención de las contraseñas de enrutador es evitar el acceso de los *hacker*. La protección por contraseña se administra dependiendo del enrutador en particular. En la mayoría de los casos, las contraseñas para acceder a un enrutador se almacenan dentro del propio enrutador. Las grandes redes tienen docenas o incluso cientos de enrutadores, algunos más importantes que otros para operaciones de red, por lo que es una práctica común de los administradores de red permitir sólo a los miembros del equipo de red acceder a ciertos enrutadores, o incluso, a niveles de comandos dentro de los enrutadores. La Tabla 1.3, lista las contraseñas de enrutador y lo que hacen.

En los enrutadores de Cisco se utilizan las contraseñas para restringir el acceso a:

- El propio dispositivo de enrutador.
- La parte EXEC privilegiada (modo habilitar) del entorno del software IOS.
- El uso de comandos específicos del IOS.

Tabla 1.3 *Información básica de las contraseñas de enrutador y sus usos.*

Punto de control	Tipo de contraseña	¿Qué está restringido?
Puerto de consola	Línea	Iniciar una sesión mediante una línea local a través del puerto de consola.
Puerto AUX	Línea	Iniciar una sesión mediante una línea módem (o local) conectada al puerto auxiliar.
Inicio de sesión de red	Terminal virtual	Iniciar la sesión en el router mediante una conexión de red usando Telnet sobre una línea VTY
EXEC privilegiado	Enable o Enable Secret	Entrar al nivel más potente Privilegiado EXEC del entorno IOS.

1.6.1. Contraseñas de línea

Las contraseñas de línea se usan para controlar quien puede iniciar la sesión en un enrutador. Se usan para definir protección por contraseña en la línea Terminal de consola, la línea AUX (auxiliar) y en cualquiera de las cinco líneas (VTY) de Terminal virtual.
Es necesario establecer al menos una contraseña para las líneas VTY del enrutador. Si no se define una contraseña de línea, cuando intente iniciar la sesión en el enrutador mediante Telnet, aparecerá un mensaje de error *password required but none set* (es necesaria una contraseña, pero no ha escrito ninguna). Recuerde, cualquiera en Internet puede hacer un Telnet a cualquier enrutador, porque definir las contraseñas de línea detendrá a todos los *hacker*, excepto a los mejores, de conseguir una forma de introducirse. Por debajo, IOS solicita una contraseña:

```
User Access verification

Password:
Enrutador>
```

Cuando introduce contraseñas en el IOS, no aparecen asteriscos para enmascarar las letras escritas, algo a lo que la mayoría de nosotros estamos acostumbrados. En el ejemplo anterior, en la línea de comandos Enrutador> (el nombre de host del enrutador en este ejemplo), se ha introducido la contraseña correcta, se inicio la sesión en el enrutador del equipo, pero los asteriscos no aparecen a la derecha de la línea del

comando **Password**. Esto le puede sorprender en un principio, pero se acostumbrara a ello.

Nota: No siempre es posible tener un nombre de usuario con contraseñas de Enable y Enable Secret. Esto se debe a que las contraseñas de Enable y Enable Secret se almacenan en los archivos de configuración del enrutador. Los administradores de red, simplemente, encuentran más práctico definir contraseñas genéricas para evitar la pesadilla administrativa de mantener nombres de usuario/contraseñas en docenas o incluso cientos de enrutadores.

1.6.2. Contraseñas Enable y Enable secret

Una vez superada la contraseña de línea, inicia la sesión en el entorno del software IOS del enrutador. El IOS se divide en dos niveles de privilegio, EXEC y Privileged EXEC (modo habilitar).

El nivel EXEC contiene sólo comandos básicos, no destructivos. Estar en modo Enable permite acceder a más comandos. Los comandos del nivel EXEC, básicamente le permiten ver un enrutador. Los comandos del modo Enable son mas potentes en el sentido de que permiten volver a configurar el enrutador. Estos comandos son potencialmente destructivos, el comando **erase** es un buen ejemplo.

Se pueden usar dos tipos de contraseñas para restringir el acceso al Privileged EXEC (modo habilitar): la contraseña Enable y la contraseña Enable Secret. La idea de una <<contraseña secreta>> parece una tontería al principio. *Por supuesto* todas las contraseñas son secretas, o al menos lo deberían ser. A lo que se refieren los ingenieros de Cisco aquí es al nivel de cifrado que se utiliza para enmascarar las contraseñas a usuarios no autorizados.

***NIVEL PRIVILEGED EXEC DEL IOS*.** Las contraseñas Enable y Enable Secret hacen las dos lo mismo: restringen el acceso a Privileged EXEC (modo habilitar). La diferencia entre las dos esta en el nivel de cifrado que soportan. El *cifrado* es una técnica que se utiliza para codificar los datos, haciéndolos incomprensibles a aquellos que no tienen una clave para leerlos. Las contraseñas Enable Secret son enrevesadas y utilizan un complejo algoritmo de cifrado basado en 128 bits para el que no hay técnica conocida de decodificación. El cifrado para la contraseña Enable se basa en un algoritmo menos potente. Cisco recomienda encarecidamente que se use la contraseña Enable Secret en lugar de la contraseña Enable.

La contraseña Enable Secret se introdujo en 1997, por lo que todavía se sigue utilizando mucho hardware y software que sólo soportan la contraseña Enable, y los servidores que guardan imágenes de copias de seguridad de IOS suelen dar servicio tanto a enrutadores nuevos como antiguos. Cuando se establecen los dos, la contraseña Enable Secret siempre precede a la contraseña Enable. IOS sólo utilizará la contraseña Enable cuando se ejecute una versión antigua del software IOS.

Las contraseñas IOS se almacenan en el archivo de configuración del enrutador. Los archivos de configuración viajan a través de las redes de forma rutinaria cuando se actualizan los enrutadores o se hace una copia de seguridad. Tener una contraseña

Enable significa que un *hacker* que use un analizador de protocolo (un dispositivo de prueba que puede leer paquetes) tardará mucho más en decodificar su contraseña. El siguiente ejemplo de archivo de configuración muestra esto:

```
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Enrutador
enable secret 5 $sdf$6978yhg$jnb76sd
enable password cisco
!
```

Tenga en cuenta que la máscara de cifrado de la contraseña Enable en la última línea es mucho mas corta que la máscara de cifrado de la contraseña Enable Secret (en la penúltima línea).

EL COMANDO SERVICE PASSWORD-ENCRYPTION. Ciertos tipos de contraseñas, como las contraseñas de línea, aparecen por defecto en texto legible en el archivo de configuración. Puede usar el **service password-encryption** para hacerlas más seguras. Una vez que se introduce este comando, cualquier contraseña que se haya definido se cifra automáticamente, por lo que se escribe de forma no legible dentro del archivo de configuración (casi igual que las contraseñas Enable/Enable Secret). La seguridad mediante contraseñas de línea es doblemente importante en las redes en las que se usan servidores TFTP, ya que la copia de seguridad del TFTP implica el movimiento rutinario de archivos de configuración entre redes, y los archivos de configuración, por supuesto, contienen las contraseñas de línea.

1.6.3. Ejemplo de configuración de contraseñas “Enable Secret” y “Enable password”:

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# enable secret contraseña (configura la contraseña
Enable Secret)
RouterA(config)# enable password contraseña * (configura contraseña
Enable Password)
RouterA(config)#
```

1.6.4. Ejemplo de configuración de la contraseña de consola:

```
RouterA> enable
RouterA# config Terminal
RouterA(config)# line con 0 (ingresa a la Consola)
RouterA(config-line)# password contraseña (configura contraseña)
RouterA(config-line)# login (habilita la contraseña)
RouterA(config-line)# exit
```

```
RouterA(config)#
```

1.6.5. Ejemplo de configuración de la contraseña VTY (TELNET):

```
RouterA> enable
RouterA# config Terminal
RouterA(config)# line vty 0 4 (crea las 5 líneas VTY, pero podría ser una sola. Ej: line vty 0)
RouterA(config-line)# password contraseña (contraseña para las 5 líneas en este caso)
RouterA(config-line)# login (habilita la contraseña)
RouterA(config-line)# exit
RouterA(config)#
```

CAPÍTULO 2

COMANDO SHOW

2. COMANDO SHOW

Los numerosos comandos show se pueden utilizar para examinar el contenido de los archivos en el router y para diagnosticar fallas. Tanto en el modo EXEC privilegiado como en el modo EXEC de usuario, el comando **show ?** muestra una lista de los comandos show disponibles. La lista en el modo EXEC privilegiado es considerablemente más larga que en el modo EXEC de usuario. A continuación se muestra una pequeña lista de los sub-comandos de show

- **show interfaces:** Muestra las estadísticas completas de todas las interfaces del router. Para ver las estadísticas de una interfaz específica, ejecute el comando **show interfaces** seguido de la interfaz específica y el número de puerto. Por ejemplo:

```
Router#show interfaces serial 0/1
```

- **show controllers serial:** muestra información específica de la interface de hardware. El comando debe incluir el número de puerto y/o de ranura de la interfaz. Por ejemplo:

```
Router#show controllers serial 0/1
```

- **show clock:** Muestra la hora fijada en el router
- **show hosts:** Muestra la lista en caché de los nombres de host y sus direcciones
- **show users:** Muestra todos los usuarios conectados al router
- **show history:** Muestra un historial de los comandos ingresados
- **show flash:** Muestra información acerca de la memoria flash y cuáles archivos IOS se encuentran almacenados allí
- **show version:** Despliega la información acerca del router y de la imagen de IOS que esté corriendo en la RAM. Este comando también muestra el valor del registro de configuración del router
- **show ARP:** Muestra la tabla ARP del router
- **show protocols:** Muestra el estado global y por interface de cualquier protocolo de capa 3 que haya sido configurado
- **show startup-configuration:** Muestra el archivo de configuración almacenado en la NVRAM
- **show running-configuration:** Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica o información de un map class

CAPÍTULO 3

CONFIGURACIÓN DE LAS INTERFACES

3. CONFIGURACIÓN DE LAS INTERFACES

Las interfaces de un router forman parte de las redes que están directamente conectadas al dispositivo. Estas interfaces activas deben llevar una dirección IP y su correspondiente máscara, como un host perteneciente a esa red. El administrador debe habilitar administrativamente la interfaz con el comando **no shutdown**, si fuera necesario la interfaz podrá deshabilitarse con el comando **shutdown**.

3.1. Configuración de una interfaz Ethernet

Se puede configurar una interfaz Ethernet desde la consola o a través de una línea de terminal virtual. A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

Para configurar una interfaz Ethernet, siga estos pasos:

- Ingrese al modo de configuración global
- Ingrese al modo de configuración de interfaz
- Especifique la dirección de la interfaz y la máscara de subred
- Active la interfaz

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 183.8.126.2  255.255.255.0
Router(config-if)#no shutdown
```

El estado predeterminado de las interfaces es APAGADO, es decir están apagadas o inactivas. Para encender o activar una interfaz, se ejecuta el comando **no shutdown**. Cuando resulte necesario inhabilitar administrativamente una interfaz a efectos de mantenimiento o diagnóstico de fallas, se utiliza el comando **shutdown** para desactivarla.
La siguiente captura muestra una configuración de una interfaz Ethernet:

```
MADRID>enable
Password:*******
MADRID#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MADRID(config)#interface ethernet 0
MADRID(config-if)#ip address 192.168.1.1 255.255.255.0
MADRID(config-if)#no shutdown
MADRID(config-if)#description INTERFAZ_DE_LAN
```

El comando **show interfaces ethernet 0,** muestra en la primer línea como la interfaz esta **UP** administrativamente y **UP** físicamente. Recuerde que si la interfaz no estuviera conectada o si existen problemas de conectividad el segundo UP aparecería como down.

La tercera línea muestra la **descripción** configurada a modo de comentario puesto que solo tiene carácter informativo y **NO** afecta al funcionamiento del router, la cual puede tener cierta importancia para los administradores a la hora de solucionar problemas.

Mas abajo aparece la dirección IP, encapsulación, paquetes enviados, recibidos, etc.

```
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0000.0cfb.6c19 (bia 0000.0cfb.6c19)
  Description: INTERFAZ_DE_LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 183/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     188 packets output, 30385 bytes, 0 underruns
     188 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     188 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Si el administrador deshabilita la interfaz se vera:

```
Ethernet0 is administratively down, line protocol is down
   Hardware is Lance, address is 0000.0cfb.6c19 (bia 0000.0cfb.6c19)
   Description: INTERFAZ_DE_LAN
   Internet address is 192.168.1.1/24
 . . . . . . . . . . . . . . . . . .
```

3.2. Configuración de una interfaz Serial

Las interfaces seriales se configuran siguiendo el mismo proceso que las ethernet, se debe tener especial cuidado para determinar quien es el **DCE** (equipo de comunicaciones) y quien el **DTE** (equipo Terminal del abonado) debido a que el DCE lleva el sincronismo de la comunicación, este se configurará solo en la interfaz serial del DCE, el comando **clock rate** activará el sincronismo en ese enlace.

La interfaz entre el DTE y el DCE se halla en un conector, que es el punto de enlace entre estas dos clases de equipos. Se pueden utilizar conectores separados para los circuitos de enlace asociados con el equipo conversor de señales u otro similar y con el equipo de llamada automática paralelo. Con relación a las características mecánicas de la interfaz se pueden consultar las publicaciones ISO 2110 o ISO 4902, según proceda.

Normalmente, con el DTE se suministran uno o varios cables de interconexión. Se recomienda el empleo de cables cortos, cuya longitud esté limitada únicamente por la capacidad de la carga y otras características eléctricas especificadas en la Recomendación pertinente sobre las características eléctricas.

Clock rate Vs ancho de banda: Recuerde que existe un comando **bandwidth** para la configuración del ancho de banda, el router solo lo utilizará para el cálculo de costes y métricas para los protocolos de enrutamiento, mientras que el clock rate brinda la verdadera velocidad del enlace.

A continuación se observa la configuración de un enlace serial como DCE:

```
MADRID(config)#interface serial 0
MADRID(config-if)#ip address 170.16.2.1 255.255.0.0
MADRID(config-if)#clock rate 56000
MADRID(config-if)#bandwidth 100000
MADRID(config-if)#description RED_SERVIDORES
MADRID(config-if)#no shutdown
```

Algunos router llevan incorporados slots o ranuras para ampliar la cantidad de puertos, en ese caso las interfaces se identificaran con 0/0, esto hace referencia al slot 0, interfaz 0.

3.2.1. Diagnóstico de fallas en una interfaz serial

- Serial x is up, line protocol is up (looped): es la condición adecuada
- Serial x is down, line protocol is down: el router no detecta señal de DCE. Línea inactiva, cable defectuoso o incorrecto o fallo de hardware.
- Serial x is up, line protocol is down: el router no envía mensajes de actividad. Router local o remoto mal configurado, problema de temporización, falta clock rate, fallo de portadora o de hardware.
- Serial x is up, line protocol is down (disabled): Errores en el proveedor de servicios WAN o error de hardware, interface dañada.
- Serial x is administratively down, line protocol is down: Configuración del router, interfaz no operativa o problema de dirección IP duplicada.

CAPÍTULO 4

CONFIGURACIÓN DEL BANNER Y DESCRIPCIÓN DE LAS INTERFACES

4. CONFIGURACIÓN DEL BANNER Y DESCRIPCIÓN DE LAS INTERFACES

4.1. Banner o Mensajes de inicio de sesión

El mensaje de inicio de sesión se muestra al usuario al momento de hacer login en el router, y se usa para comunicar información de interés a todos los usuarios de la red, tales como avisos de próximas interrupciones del sistema.
Con el fin de brindar mensajes ante posibles averías o intrusos existen varios tipos de banners.

```
MADRID(config)#banner
LINE      c banner-text c, where ‘c’ is a delimiting character
exec      Set EXEC process creation banner
incoming  Set incoming terminal line banner
login     Set login banner
motd      Set Message of the Day banner
```

El banner **motd** ofrece la posibilidad de un mensaje diario, el banner **login** será visto al establecer una sesión de telnet, el **banner exec** al pasar la password al modo privilegiado. Un mensaje de inicio de sesión debe advertir que sólo los usuarios autorizados deben intentar el acceso. . Evite un mensaje del estilo “¡bienvenido!” por el contrario introduzca un mensaje del estilo "¡Este es un sistema protegido, ingrese únicamente si está autorizado!", de esta manera advertirá a los visitantes que el ir más allá está prohibido y es ilegal.

En la configuración de un banner diario, el texto debe ir entre caracteres similares al comenzar y al terminar:

```
MADRID(config)#banner motd * Usted intenta ingresar en un sistema
protegido*
```

4.2. Descripción de una Interfaz

La interfaz de un enrutador puede documentarse específicamente usando el comando **description**. Usar descripciones es una gran forma de hacer un seguimiento de la red (y usuarios) a la que da servicio una interfaz. Puede que esto no parezca muy importante, pero las grandes redes tienen miles interfaces y se reconfiguran frecuentemente. Para introducir una descripción de una interfaz específica, debe ir primero a esa interfaz, en este ejemplo ToKenRing0:

```
MADRID(config)#interface ToKenRing0
MADRID(config-if)#
Introduzca luego el comando description  seguido por la descripción:
MADRID(config-if)#descripcion ToKenRing for finance departament
MADRID(config-if)#
```

Las descripciones pueden tener hasta 80 caracteres de longitud. Para cerrar el ciclo, es posible ver la descripción en la parte del archivo config dedicada a la interfaz:

```
MADRID(config-if)#
MADRID#show running-config
.
.
.
Iterface ToKenRing0
 description TokenRing0 for finance departament
```

Los nombres de enrutador y las descripciones de interfaz sólo las ven los administradores de red.

CAPÍTULO 5

RIP
(ROUTING INFORMATION PROTOCOL)

5. RIP

El Protocolo de Información de Enrutamiento (RIP) es un protocolo de vector-distancia que utiliza un contador de saltos como métrica. RIP es muy usado para enrutar tráfico en redes globales como un protocolo de gateway interior (IGP), lo que significa que realiza el enrutamiento en sistemas autónomos. Los protocolos de gateway exterior, como el BGP (Border Gateway Protocol), realizan el enrutamiento entre dos sistemas autónomos. El origen del RIP fue el protocolo de Xerox, el GWINFO. Una versión posterior, fue conocida como Routed, distribuida con Berkeley Standard Distribution (BSD) Unix en 1982. RIP evolucionó como un protocolo de enrutamiento de Internet, y otros protocolos propietarios utilizan versiones modificadas de RIP. El protocolo Apple Talk Routing Table Maintenance Protocol (RTMP) y el Banyan VINES Routing Table Protocol (RTP), por ejemplo, están los dos basados en una versión del protocolo de enrutamiento RIP. La última mejora echa al RIP es la especificación RIP 2, que permite incluir mas información en los paquetes RIP y provee un mecanismo de autenticación muy simple.

IP RIP es formalmente definido en dos documentos: Request For Comments (RFC) 1058 y 1723. En el RFC 1058 (1988) describe la primera implementación del protocolo RIP, mientras que la especificación RFC 1723 (1994) actualiza a la RFC 1058. En la RFC 1723 posibilita adjuntar mayor información en los mensajes RIP e implementa algún nivel básico de seguridad.

5.1. Funcionamiento de RIP

RIP utiliza UDP para enviar sus mensajes y el puerto 520.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo Vector distancia. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.

RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado) RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. Las métricas se actualizan sólo en el caso de que la

métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea.

RIP envía mensajes de actualización de enrutamiento a intervalos regulares. Cuando un router recibe una actualización de enrutamiento que incluya cambios a una entrada de su tabla de enrutamiento, actualiza dicha tabla para reflejar la nueva ruta. El valor recibido de la métrica de la ruta aumenta en 1 y la interfaz de origen de la actualización se señala como el salto siguiente en la tabla de enrutamiento. Los routers RIP conservan sólo la mejor ruta hacia un destino pero pueden conservar más de una ruta al mismo destino si el costo de todas es igual.

La mayoría de los protocolos de enrutamiento usan una combinación de actualizaciones causadas por eventos (event-driven) o por tiempo (time-driven). RIP es time-driven, pero la implementación Cisco de RIP envía actualizaciones tan pronto se detectan cambios. Cambios en la topología también originan actualizaciones inmediatas en routers IGRP, independientes del valor del temporizador de actualización. Sin actualizaciones event-driven RIP e IGRP no funcionarían adecuadamente. Una vez que se haya actualizado la tabla de enrutamiento por cambios en la configuración, el router comienza inmediatamente a transmitir las actualizaciones de enrutamiento, a fin de informar de estos cambios a los otros routers. Estas actualizaciones, denominadas **Actualizaciones generadas por eventos**, se envían independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares.

Los routers RIP dependen de los routers vecinos para obtener la información de la red que no conocen de primera mano. Un término común empleado para describir esta funcionalidad es **Enrutamiento por rumor**. El protocolo RIP usa un algoritmo de enrutamiento por vector-distancia. Todos los protocolos de enrutamiento por vector-distancia tienen detalles importantes que son producto principalmente de una convergencia lenta. La convergencia ocurre cuando todos los routers de una red tienen la misma información de enrutamiento.

Entre estos detalles se encuentran los bucles de enrutamiento y la cuenta al infinito. Éstos generan incongruencias debido a la propagación por la red de actualizaciones de enrutamiento con información obsoleta.

Para reducir los bucles de enrutamiento y la cuenta al infinito, RIP emplea las siguientes técnicas.

- Horizonte dividido
- Actualización inversa
- Temporizadores de espera
- Actualizaciones generadas por eventos

Algunos de estos métodos pueden requerir hacer algunas configuraciones, mientras que otros no lo requieren o rara vez lo requieren.

Otro detalle de los protocolos de enrutamiento es la publicación indeseada de actualizaciones del enrutamiento desde una interfaz en particular. Cuando se ejecuta un comando **network** para una red dada, RIP comenzará inmediatamente a enviar publicaciones hacia todas las interfaces dentro del ámbito de direcciones de red especificado. Para controlar cuáles serán las interfaces que harán intercambio de actualizaciones de enrutamiento, el administrador de redes puede inhabilitar el envío de actualizaciones desde las interfaces que escoja. Para ello se usa el comando **passive-interface.**

Como RIP es un protocolo de tipo broadcast, el administrador de la red podría tener que configurar RIP para que intercambie información de enrutamiento en redes no broadcast, como en el caso de las redes Frame Relay. En este tipo de redes, RIP necesita ser informado de otros routers RIP vecinos. Para esto se utiliza el comando **neighbor ip address.**

5.2. Problemas

5.2.1. Bucles en el enrutamiento por vector-distancia.

Los bucles de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes, las cuales no se han actualizado debido a la lenta convergencia de una red sujeta a cambios. Figura 5.1.

- Antes de la falla de la red 1, todos los routers poseen información coherente y tablas de enrutamiento correctas. Se dice que la red ha logrado la convergencia. Supongamos, para el resto de este ejemplo, que la ruta preferida del router C hacia la red 1 es a través del router B y que la distancia del router C a la Red 1 es 3.

- En el momento en que la red 1 falla, el router E envía una actualización al router A. El router A deja de enrutar paquetes hacia la red 1, pero los routers B, C y D siguen haciéndolo porque todavía no se les ha informado acerca de la falla. Cuando el router A envía su actualización, los routers B y D detienen el enrutamiento hacia la red 1; sin embargo, el router C no ha recibido la actualización. Para el router C, la red 1 todavía se puede alcanzar a través del router B.

- El router C envía ahora una actualización periódica al router D, que señala una ruta hacia la red 1 a través del router B. El router D cambia su tabla de enrutamiento para introducir esta información buena pero errónea, y transmite la información al router A. El router A transmite la información a los routers B y E, etc. Cualquier paquete destinado a la red 1 ahora realizará un bucle desde el router C al B, de allí al A y luego al D, y volverá nuevamente al C.

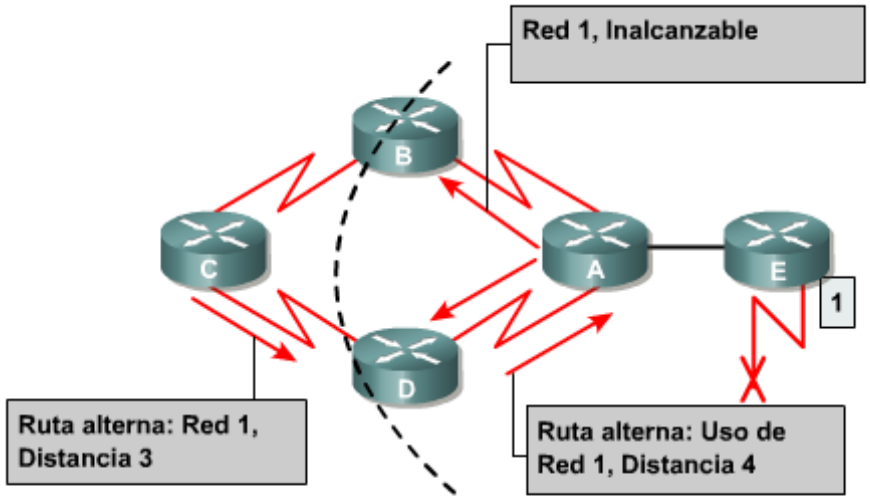


Figura 5.1. *Problema de bucles en el enrutamiento por vector distancia*

5.2.2. Definición de cuenta máxima

Las actualizaciones erróneas de la red 1 continuarán generando bucles hasta que algún otro proceso lo detenga. Esta condición, denominada cuenta al infinito, hace que los paquetes recorran la red en un ciclo continuo, a pesar del hecho fundamental de que la red de destino, la red 1, está fuera de servicio. Mientras los routers cuentan al infinito, la información errónea hace que se produzca un bucle de enrutamiento. Figura 5.2.

Si no se toman medidas para detener la cuenta al infinito, la métrica del vector-distancia del número de saltos aumenta cada vez que el paquete atraviesa otro router. Estos paquetes hacen un recorrido cíclico por la red debido a la información errónea en las tablas de enrutamiento.

Los algoritmos de enrutamiento por vector-distancia se corrigen automáticamente, pero un bucle de enrutamiento puede requerir primero una cuenta al infinito. Para evitar este problema, los protocolos de vector-distancia definen el infinito como un número máximo específico. Este número se refiere a una métrica de enrutamiento, la cual puede ser el número de saltos.

Con este enfoque, el protocolo de enrutamiento permite que el bucle de enrutamiento continúe hasta que la métrica supere el máximo valor permitido. El gráfico muestra que en este caso ya el valor alcanzó los 16 saltos. Esto supera la cifra máxima por defecto de 15 saltos del vector-distancia, de modo que el router descarta el paquete. En

cualquier caso, cuando el valor de la métrica supera el valor máximo, se considera que no se puede alcanzar la red 1.

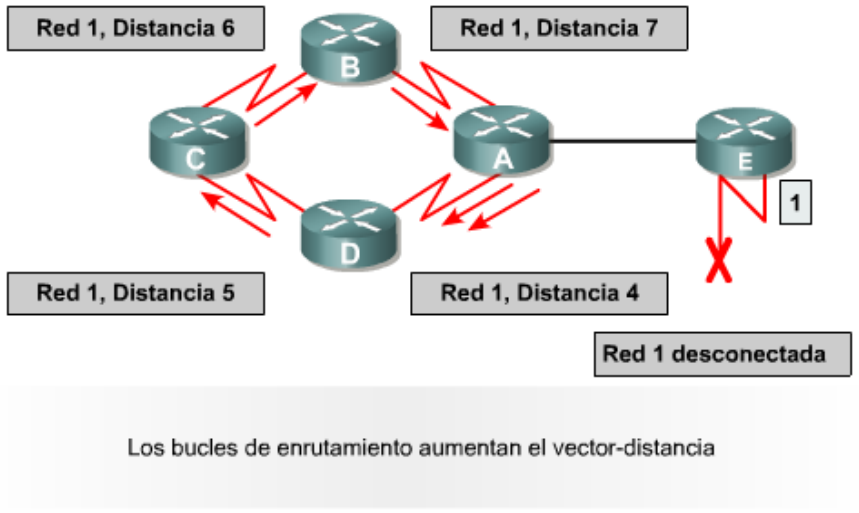


Figura 5.2. *Problema de la cuenta máxima en el enrutamiento por vector distancia*

5.3. Soluciones

5.3.1. Eliminación de los bucles de enrutamiento mediante el horizonte dividido.

Otra fuente posible de bucles de enrutamiento se presenta cuando se envía información incorrecta a un router, la cual contradice información correcta que este envió originalmente. Así es como se produce el problema:

- El router A transfiere una actualización al router B y al router D, la cual indica que la red 1 está fuera de servicio. El router C, sin embargo, transmite una actualización periódica al router B, que señala que la red 1 está disponible a una distancia de 4, a través del router D. Esto no rompe las reglas del horizonte dividido.

- El router B determina erróneamente que el router C todavía tiene una ruta válida hacia la red 1, aunque con una métrica mucho menos favorable. El router B envía una actualización periódica al router A la cual indica al router A la nueva ruta hacia la red 1.

- El router A ahora determina que puede enviar paquetes a la red 1 a través del router B, el router B determina que puede enviar paquetes a la red 1 a través del router C, y el router C determina que puede enviar paquetes a la red 1 a través del router D. Cualquier paquete introducido en este entorno quedará atrapado en un bucle entre los routers.

El horizonte dividido busca evitar esta situación. Si la actualización de enrutamiento relativa a la red 1 es enviada desde el router A, el router B o D no pueden enviar

información sobre la red 1 de vuelta hacia el router A. El horizonte dividido reduce así los errores de enrutamiento, y también disminuye el procesamiento de información de enrutamiento.

En algunas configuraciones de red, puede resultar necesario inhabilitar el horizonte dividido.

El siguiente comando se utiliza para inhabilitar el horizonte dividido:

```
GAD(config-if)#no ip split-horizon
```

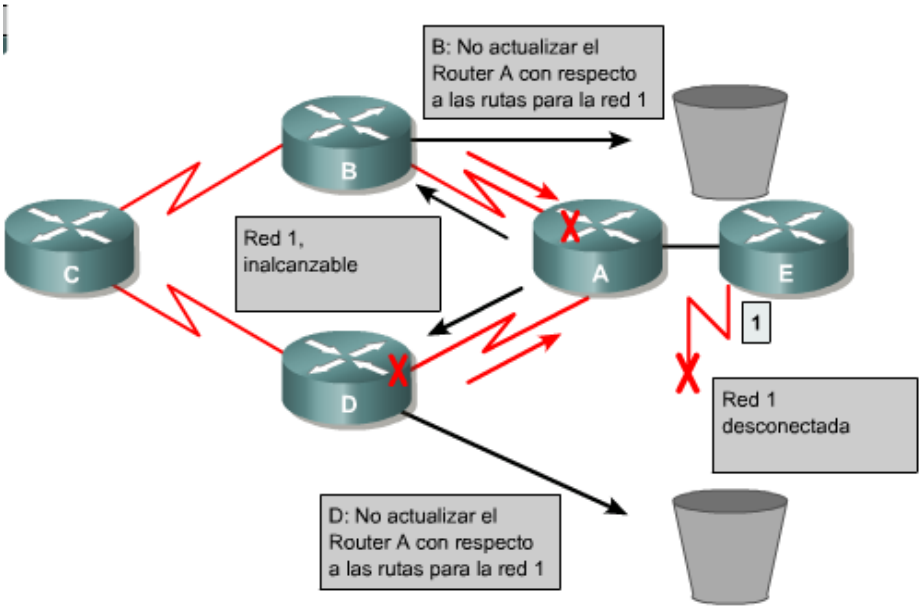


Figura 5.3. *Horizonte Dividido*

5.3.2. Envenenamiento de rutas.

El evenenamiento de rutas es utilizado por varios protocolos de vector de distancia para resolver grandes bucles de enrutamiento. A menudo, provee información explicita cuando no es posible el acceso a una subred o red. Esto se lleva a cabo normalmente mediante la configuración del número de salto en la cantidad máxima más uno.

Una forma de evitar actualizaciones incongruentes es el envenenamiento de rutas. Cuando la red cinco sale de fuera de servicio, el rotuer E inicia el envenenamiento de la ruta mediante una entrada de valor 16 para la red 5, es decir, fuera de alcance (figura 5.4.). Debido al envenamiento de la ruta hacia la red 5, el router C no es susceptible de efectuar actualizaciones incorrectas de la ruta hacia dicha red. Cuando el rotuer C recibe el envenenamiento de rutas desde el router E, envia una actualización llamada

actualización de envenenamiento inversa, devuelta al router E. Esto asegura que todas las rutas del segmento hayan recibido la información del envenenamiento de la ruta.

Cuando se combina el envenenamiento de ruta con las actualizaciones generadas por eventos, se agiliza el tiempo de convergencia ya que los router vecinos no tienen que esperar 30 seg antes de publicar la ruta envenenada.

El envenenamiento de ruta hace que el protocolo de enrutamiento publique rutas de métrica infinita para la ruta que esta fuera de servicio. El envenenamiento de rutas no rompe las reglas del horizonte dividido. El horizonte dividido con envenenamiento de rutas es en esencia un envenenamiento de rutas, pero, colocada en los enlaces, en los que el horizonte dividido no permitiría el paso de información de enrutamiento. En cualquiera de los casos, el resultado es que las rutas que están fuera de servicio se publican con métricas infinitas.

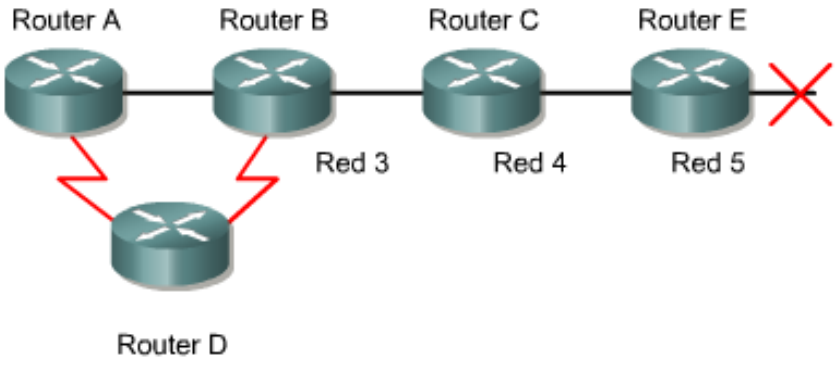


Figura 5.4. *Envenenamiento de rutas*

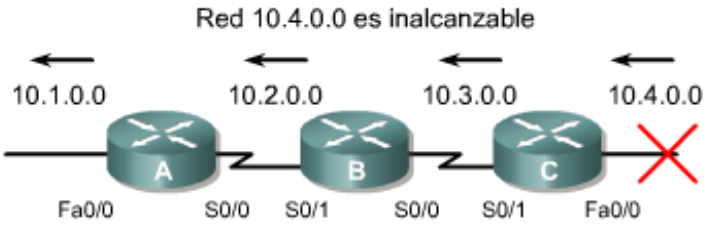
5.3.3. Prevención de bucles de enrutamiento mediante actualizaciones generadas por eventos

Los routers envían nuevas tablas de enrutamiento a los routers vecinos periódicamente. Por ejemplo, las actualizaciones en el protocolo RIP se producen cada 30 segundos. Sin embargo, una actualización generada por eventos es enviada de inmediato, en respuesta a algún cambio en la tabla de enrutamiento. El router que detecta un cambio de topología envía de inmediato un mensaje de actualización a los routers adyacentes, los cuales a su vez, generan actualizaciones a efectos de notificar el cambio a sus vecinos adyacentes. Cuando una ruta falla, inmediatamente se envía una actualización, sin esperar a que expiren los temporizadores de las actualizaciones. Las actualizaciones

generadas por eventos, cuando se usan en conjunto con el envenenamiento de rutas, aseguran que todos los routers conozcan de la falla en las rutas, aun antes de que se cumpla el lapso de tiempo para una actualización periódica.

Las actualizaciones generadas por eventos envían actualizaciones porque la información de enrutamiento ha cambiado, no porque se ha cumplido el lapso para una actualización. El router envía otra actualización de enrutamiento a sus otras interfaces, sin esperar a que expire el temporizador de las actualizaciones de enrutamiento. Esto causa que la información acerca del estado de la ruta que ha cambiado sea enviada, y activa más rápidamente los temporizadores de espera (holddown timers) en los routers vecinos. La ola de actualizaciones se propaga a través de la red.

Mediante la actualización generada por eventos que genera el router C, éste anuncia que la red 10.4.0.0 está inaccesible. Al recibir esta información, el router B anuncia a través de la interfaz S0/1 que la red 10.4.0.0 está fuera de servicio. A su vez, el router A envía una actualización desde la interfaz Fa0/0.



Con el método de actualización generada por eventos, los routers envían mensajes tan pronto como se dan cuenta de que se ha producido algún cambio en su tabla de enrutamiento.

Figura 5.5. *Actualizaciones generadas por eventos*

5.3.4. Prevención de bucles de enrutamiento mediante temporizadores de espera

El problema de la cuenta al infinito puede evitarse mediante los temporizadores de espera (holddown timers): Figura 5.6.

- Si un router recibe una actualización de un router vecino, la cual indique que una red previamente accesible está ahora inaccesible, el router marca la ruta como inaccesible y arranca un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del

mismo router, la cual indique que la red se encuentra nuevamente accesible, el router marca la red como accesible y desactiva el temporizador de espera.

- Si llega una actualización desde un router distinto, la cual establece una métrica más conveniente que la originalmente registrada para la red, el router marca la red como accesible y desactiva el temporizador de espera.

- Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un router distinto, la cual establece una métrica menos conveniente que la originalmente registrada para la red, la actualización no será tomada en cuenta. El descartar las actualizaciones con métricas menos convenientes mientras el temporizador de espera se encuentra activado, da más tiempo para que la información relativa a un cambio perjudicial sea transmitido a toda la red.

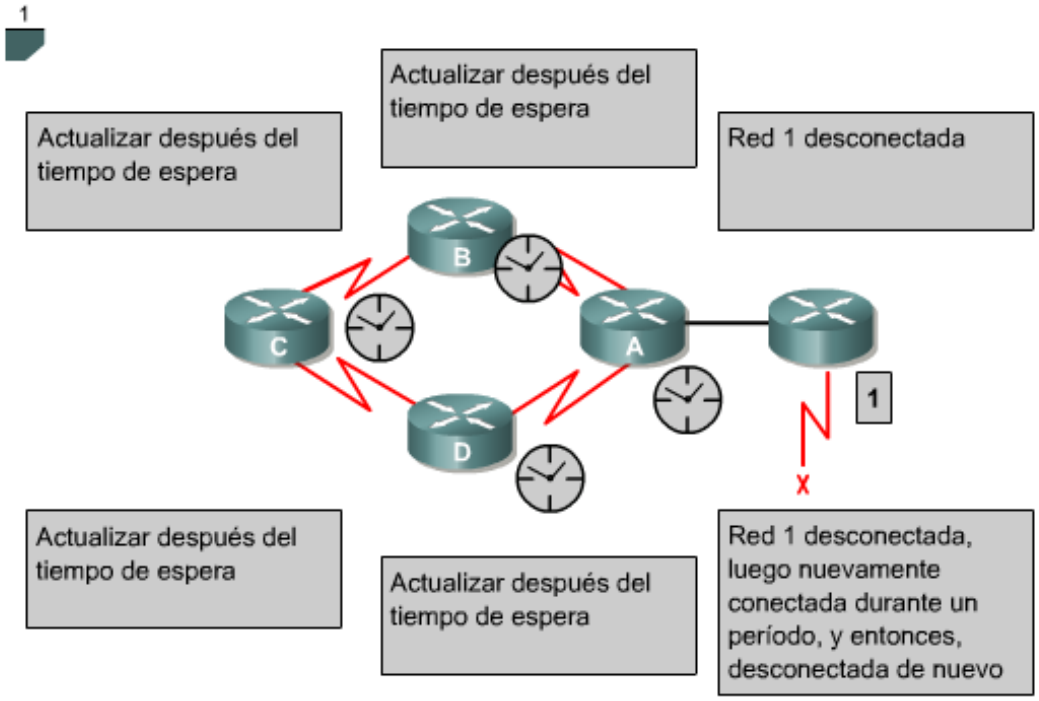


Figura 5.6. *Temporizadores de espera*

Los temporizadores de espera ayudan a prevenir la cuenta al infinito, pero también aumentan el tiempo de convergencia. La espera por defecto en el protocolo RIP es de 180 segundos. Esto evita que una ruta menos conveniente ingrese en la tabla de enrutamiento pero también puede evitar que se instale una ruta alternativa válida. Es posible reducir el lapso del temporizador de espera, para agilizar la convergencia pero esto se debe hacer con cautela. El ajuste ideal es el que fije el temporizador con una duración apenas mayor al lapso máximo de actualización posible de la red. En el ejemplo de la Figura 5.7, el bucle consta de cuatro routers. Si cada router tiene un lapso

de actualización de 30 segundos, el bucle más largo posible es de 120 segundos. Por lo tanto, el temporizador de espera debe ser apenas mayor a 120 segundos.

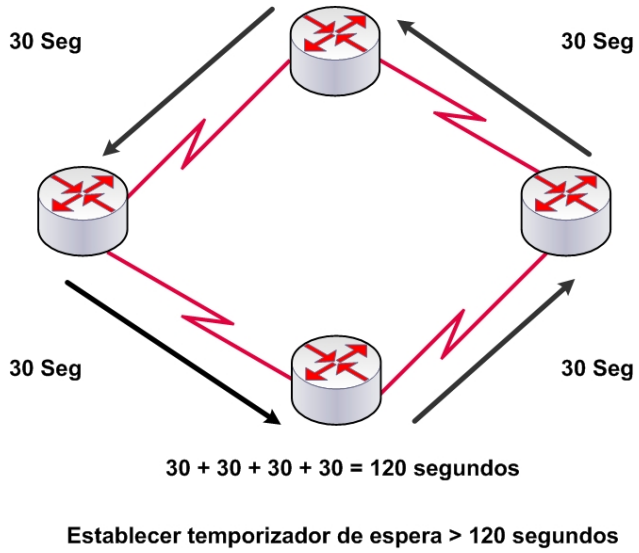


Figura 5.7 *Ejemplo de configuración de los temporizadores de espera*

Use el siguiente comando para cambiar el temporizador del contador de "**holddown**", así como el temporizador de actualizaciones, el intervalo de invalidez y el intervalo de desecho.

```
Router(config-router)#timers basic update invalid holddown flush
[sleeptime]
```

Un punto adicional que afecta el tiempo de convergencia y que puede configurarse es el intervalo entre actualizaciones. El intervalo entre actualizaciones por defecto de RIP en el IOS de Cisco es de 30 segundos. Puede configurarse para intervalos más prolongados, a fin de ahorrar ancho de banda, o más cortos para disminuir el tiempo de convergencia.

5.4. Mensajes RIP

Los mensajes RIP pueden ser de dos tipos.

- **Petición:** Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.
- **Respuesta:** mensajes con la actualización de las tablas de enrutamiento.

Existen tres tipos:

- **Mensajes ordinarios:** Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos.

- **Mensajes enviados como respuesta a mensajes de petición**.

- **Mensajes enviados cuando cambia algún coste.** Se envía toda la tabla de routing.

5.5. Versiones RIP

En la actualidad existen tres versiones diferentes de RIP las cuales son:

- **RIPv1:** No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058.

- **RIPv2:** Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Su especificación está recogida en el RFC 1723-2453.

- **RIPng:** RIP para IPv6. Su especificación está recogida en el RFC 2080.

También existe un RIP para IPX; casualmente lleva el mismo acrónimo, pero no está directamente relacionado con el RIP para redes IP, ad-hoc.

5.5.1. RIP Versión 1

El protocolo RIPv1, al igual que sus antecesores propietarios es un protocolo de routing que fue diseñado para funcionar como protocolo vector distancia. RIPv1 fue diseñado para funcionar en redes pequeñas de pasarela interior. RIPv1 está basado según el autor del RFC en la versión 4.3 de la distribución de UNIX de Berkeley.

En cuanto al protocolo tenemos que tener en cuenta las tres limitaciones que C. Hedrick describe en la página 3 del RFC 1058:

- El protocolo no permite más de quince saltos, es decir, los dos routers más alejados de la red no pueden distar más de 15 saltos, si esto ocurriera no sería posible utilizar RIP en esta red.

- Problema del “conteo a infinito”. Este problema puede surgir en situaciones atípicas en las cuales se puedan producir bucles, ya que estos bucles pueden producir retardos e incluso congestión en redes en las cuales el ancho de banda sea limitado. El autor del RFC 1058 también comenta que en la realidad esto sólo puede ser un problema en redes lentas, pero el problema existe.

- El protocolo utiliza métricas fijas para comparar rutas alternativas, lo cual implica que este protocolo no es adecuado para escoger rutas que dependan de los parámetros a tiempo real como por ejemplo retardos o carga del enlace.

Además de los problemas que cita el autor del protocolo tenemos que tener en cuenta que el protocolo RIPv1 es un protocolo classfull, con lo que existe el problema de la discontinuidad de redes. El problema de la discontinuidad de redes se produce en el momento que tenemos una red dividida en varias subredes y no pueden ser sumarizadas en una misma ruta, ya que físicamente cada una de las subredes está ubicada en un lugar que depende de un interfaz distinto una subred de la otra. Pero claro, en la época en la que se escribió este RFC, que era en 1988 estos problemas no estaban contemplados y con el tiempo se detectó este problema, esta es una de las razones de la existencia de RIPv2.

Formato de los paquetes RIP

La Figura 5.8 que a continuación se ve muestra el formato de los campos de un paquete RIP

1-octeto Command field	1-octeto Version number field	2-octeto AFI field	2-octeto Zero field	4-octeto IP address field	4-octeto Zero field	1-octeto Command field	4-octeto Zero field	4-octeto Metric field

Figura 5.8. *Un paquete RIP esta formado por 9 campos*

A continuación describimos los campos de un paquete RIP:

- **Command:** Indica si el paquete es una solicitud o una respuesta. La solicitud le pide al router que envíe parte o toda su tabla de enrutamiento. La respuesta puede ser también una actualización de tablas de enrutamiento regular (puede no haber sido pedida explícitamente) o puede también ser la respuesta a una solicitud previa. Las repuestas contienen entonces entradas de tablas de enrutamiento.

- **Version Number:** Específica que versión del protocolo RIP estamos utilizando.

- **Zero:** No usado.

- **Address-Family Identifier (AFI):** Especifica la dirección utilizada. RIP esta diseñado para portar información de enrutamiento de diferentes protocolos. Cada entrada tiene una dirección de identificación que indica cual es el tipo de direcciones especificadas. El valor del campo de AFI para IP es 2.

- **Address:** Especifica la dirección IP para la entrada.

- **Metric:** Indica cuantos saltos o redes han sido traspasadas desde el destino. Este valor debe estar entre 1 y 15, si este valor es 16, se toma como ruta no valida o inalcanzable (unreachable).

5.5.2. RIP Versión 2

Diez años después de que se publicara la versión 1 de RIP se publicó la versión 2, por G.Malkin de la compañía Bay Networks en Noviembre de 1998 en el RFC 2453.

RIPv2 establece una serie de mejoras muy importantes con su antecesor que son las siguientes:

- Autenticación para la transmisión de información de RIP entre vecinos.
- Utilización de máscaras de red, con lo que ya es posible utilizar VLSM.
- Utilización de máscaras de red en la elección del siguiente salto, lo cual nos puede permitir la utilización de arquitecturas de red discontinuas.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9.
- Inclusión de RIPv2 en los bloques de información de gestión (MIB).

Por supuesto además de estas mejoras RIPv2 nos permite la redistribución de rutas externas aprendidas por otros protocolos de routing.

Pero RIPv2 aunque haya tenido una serie de mejoras muy importantes desde la versión 1 del protocolo sigue teniendo una serie de carencias muy importantes como:

- Limitación en el tamaño máximo de la red. Con RIPv2 sigue existiendo la limitación de 15 saltos como tamaño máximo de la red, lo cual implica que no nos permite la utilización de RIPv2 en redes de un tamaño más grande.
- Conteo a infinito, RIPv2 sigue sin solucionar el problema del conteo hasta el infinito si se forman bucles, aunque existen técnicas externas al protocolo como pueden ser la inversa envenenada y el horizonte dividido, técnicas brevemente descritas por William Stallings en su libro “Comunicaciones y Redes de Computadoras”, las cuales consisten básicamente en no anunciar una ruta por la interfaz por el que se ha recibido en algún momento.
- Métricas estáticas que pueden ser cambiadas por el administrador de la red, pero que no nos dan ninguna información del estado de la red.
- RIPv2 sólo permite al igual que su antecesor una ruta por cada destino, lo cual implica la imposibilidad de realizar balanceos de carga por ejemplo, lo que redunda en una pobre y poco óptima utilización de los enlaces.

RIPv2 es un protocolo que al igual que su antecesor genera muchísimo tráfico al enviar toda la tabla de routing en cada actualización, con la carga de tráfico que ello conlleva.

Formato de los paquetes RIPv2

La especificación de RIPv2 (descripta en el RFC 1723) permite incluir mayor cantidad de información en un paquete RIP y nos provee de un mecanismo de autenticación simple.

En la figura que se muestra a continuación vemos un esquema de los campos de un paquete RIPv2.

Figura 5.9. *Un paquete RIPv2 esta constituido por campos muy similares a los de uno RIP.*

A continuación describimos los campos de un paquete RIPv2:

- **Command:** Indica si el paquete es una solicitud o una respuesta. La solicitud le pide al router que envíe parte o toda su tabla de enrutamiento. La respuesta puede ser también una actualización de tablas de enrutamiento regular (puede no haber sido pedida explícitamente) o puede también ser la respuesta a una solicitud previa. Las repuestas contienen entonces entradas de tablas de enrutamiento.

- **Version number:** Específica que versión del protocolo RIP estamos utilizando.

- **Unused:** Valor establecido en cero.

- **Address-Family Identifier (AFI):** Especifica la dirección de familia utilizada. RIP esta diseñado para portar información de diferentes protocolos. Cada entrada tiene una dirección de identificación que indica cual es el tipo de direcciones especificadas. El valor del campo de AFI para IP es 2. Si la AFI para la primera entrada es 0xFFFF, significa que el resto de la entrada contiene información de autenticación. Actualmente, la información de autenticación es nada más simple que un password.

- **Route Tag:** Provee un método para distinguir entre rutas internas (reconocidas por RIP) y rutas externas (reconocidas por otros protocolos).

- **IP Address:** Especifica la dirección IP para la entrada.

- **Subnet Mask:** Contiene la máscara de subred para la entrada. Si este campo esta en cero, quiere decir que no se ha especificado ninguna máscara de subred para la entrada.

- **Next Hop:** Indica la dirección IP del próximo salto al cual el paquete debe ser enviado.

- **Metric:** Indica cuantos saltos o redes han sido traspasadas desde el destino. Este valor debe estar entre 1 y 15, si este valor es 16, se toma como ruta no valida o inalcanzable (unreachable).

5.6. Tabla de enrutamiento de RIP

Si continuamos la lectura detallada del RFC1058, podemos ver que el autor nos dice que la base de datos de routing de cada uno de los hosts de la red que están utilizando el protocolo de routing RIP tiene los siguientes campos:

- Dirección de destino
- Siguiente salto
- Interfaz de salida del router
- Métrica
- Temporizador

Para obtener esta tabla, el protocolo de routing RIP utiliza el siguiente procedimiento para mantener actualizada la tabla de enrutamiento de cada uno de los nodos o routers de la red:

- Mantener una tabla con una entrada por cada posible destino en la red. La entrada debe contener la distancia D al destino, y el siguiente salto S del router a esa red. Conceptualmente también debería de existir una entrada para el router mismo con métrica 0, pero esta entrada no existirá.

- Periódicamente se enviará una actualización de la tabla a cada uno de los vecinos del router mediante la dirección de broadcast. Esta actualización contendrá toda la tabla de routing.

- Cuando llegue una actualización desde un vecino S, se añadirá el coste asociado a la red de S, y el resultado será la distancia D'. Se comparará la distancia D' y si es menor que el valor actual de D a esa red entonces se sustituirá D por D'.

- El protocolo de routing RIP como ya hemos dicho mantiene una tabla de routing, como cualquier protocolo de routing, seguidamente pasamos a comentar cada uno de los campos de la tabla.

5.6.1. Dirección de destino

La dirección de destino en la tabla de routing de RIP será la red de destino, es decir, la red final a la que deseamos acceder, esta red en la versión 1 del protocolo RIP tendrá que ser obligatoriamente classfull, es decir tendrá que tener en cuenta la clase, es decir, no se permite el subneting en RIP versión 1, por ejemplo si la red de destino es la 192.168.4.0, sabemos que al ser RIP classfull la red de destino tiene 256 direcciones, de

las cuales 254 son útiles, una vez descontada la dirección de red y la dirección de broadcast, ya que la red 192.168.4.0 es de clase C, es decir que los 24 primeros bits de la dirección IP identifican la red y los 8 últimos identifican los hosts de dentro de la red.

5.6.2. Siguiente salto

El siguiente salto lo definimos como el siguiente router por el que nuestro paquete va a pasar para llegar a su destino, este siguiente salto será necesariamente un router vecino del router origen.

5.6.3. Interfaz de salida del router

Entendemos por interfaz de salida del router a la interfaz a la cual está conectado su siguiente salto.

5.6.4. Métrica

La métrica utilizada por RIP como ya hemos comentado consiste en el conteo de saltos, como métrica se considera cada salto como una única unidad, independientemente de otros factores como tipo de interfaz o congestión de la línea. La métrica total consiste en el total de saltos desde el router origen hasta el router destino, con la limitación que 16 saltos se considera destino inaccesible, esto limita el tamaño máximo de la red.

5.6.5. Temporizador

El temporizador nos indica el tiempo transcurrido desde que se ha recibido la última actualización de esa ruta. RIP utiliza dos tiempos importantes, el tiempo de actualización que se establece en 30 segundos, el tiempo de desactivación que se establece en 180 segundos y el tiempo de borrado se establece en 300 segundos.

El tiempo de actualización se considera el tiempo máximo a transcurrir entre el envío de los mensajes de actualización de los vecinos.

El tiempo de desactivación se considera el tiempo máximo que puede esperar un router sin recibir actualizaciones de vecino, una vez pasado este tiempo, el vecino que no ha enviado la actualización se considera que ha caído y con lo cual el router no está activo en la red, se establece la métrica a valor 16, es decir destino inalcanzable.

El tiempo de borrado implica que una vez transcurrido ese tiempo todas las rutas de ese router supuestamente caído son eliminadas de la tabla de routing.

5.7. Rutas Estáticas

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.

- Los paquetes se enrutan de acuerdo a la ruta estática.

Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando **ip route**. La sintaxis correcta del comando ip route se muestra en la Figura.5.10.

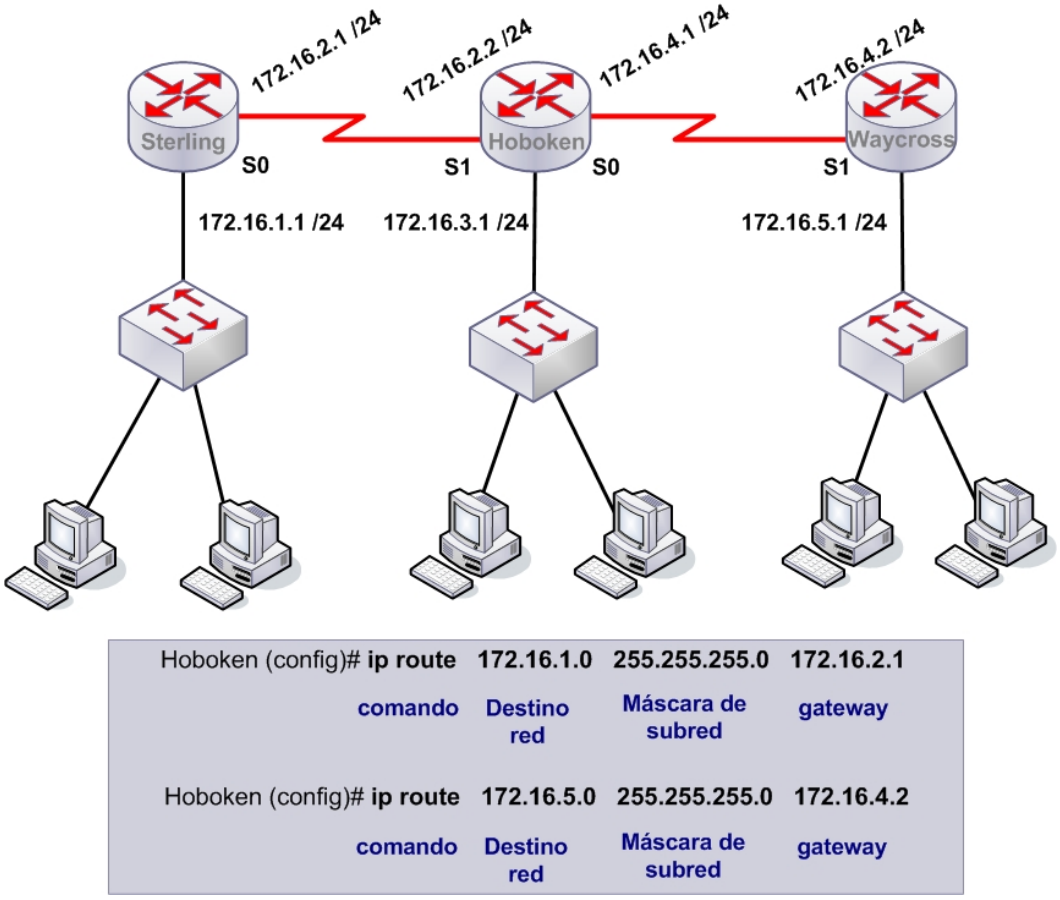


***Figura 5.10.**. Rutas estáticas*

En las Figuras 5.10, el administrador del router Hoboken necesita configurar las rutas estáticas cuyo destino son las redes 172.16.1.0/24 y 172.16.5.0/24. El administrador puede ejecutar uno de dos comandos posibles para lograr su objetivo. Se puede especificar la interfaz de salida. El método de la Figura 5.10 especifica la dirección IP del siguiente salto (hop) del router adyacente. Cualquiera de los comandos instalará una ruta estática en la tabla de enrutamiento del router Hoboken.
La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. Por lo tanto, es preferible instalar rutas de distancia administrativa menor antes que una ruta idéntica de distancia administrativa mayor. La distancia administrativa por defecto cuando se usa una ruta estática es 1. Cuando una interfaz de salida se configura como el gateway de una ruta estática, dicha ruta será desplegada en la tabla de

enrutamiento como si estubiera directamente conectada. Esto a veces confunde, ya que la redes directamente conectadas tienen distancia 0. Para verificar la distancia administrativa de una ruta en particular use el comando **show ip route address**, donde la dirección ip de dicha ruta se inserta en la opción address. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida o el siguiente salto, como se muestra a continuación:

```
Waycross (config) #ip route 172.16.3.0  255.255.255.0  172.16.4.1  130
```

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta.

A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

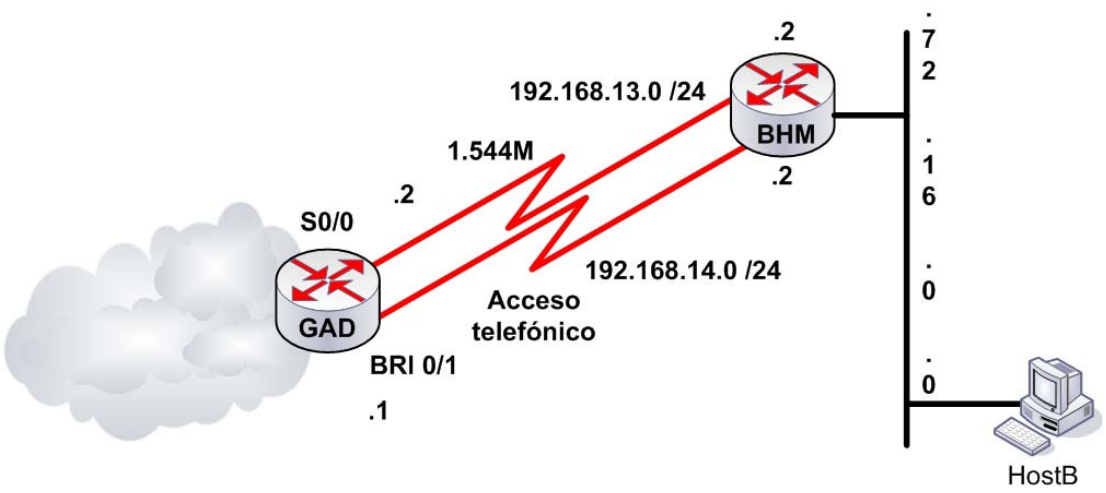
5.7.1. Rutas estáticas en RIP

Las rutas estáticas son rutas definidas por el usuario, que obligan a los paquetes a tomar una ruta determinada entre su origen y su destino. Las rutas estáticas adquieren importancia si el IOS de Cisco no aprende una ruta hacia un destino en particular. Son útiles también para especificar "un gateway de último recurso", el cual generalmente se conoce como una ruta por defecto. Si un paquete tiene como destino una subred que no aparece expresamente en la tabla de enrutamiento, el paquete es enviado a través de una ruta por defecto.

Un router que ejecuta el protocolo RIP puede recibir una ruta por defecto a través de una actualización de otro router que ejecuta RIP. Otra opción es que el router genere, por sí mismo la ruta por defecto.

Las rutas estáticas pueden eliminarse con el comando de configuración global **no ip route**. El administrador puede dejar de lado una ruta estática y dar prioridad a la información de enrutamiento dinámico mediante el ajuste de los valores de distancia administrativa. Cada protocolo de enrutamiento dinámico tiene una distancia administrativa (AD) por defecto. Es posible definir una ruta estática como menos conveniente que una ruta aprendida de forma dinámica, siempre que la AD de la ruta estática sea mayor que la de la ruta dinámica.

Note que después de configurar la ruta estática a la red 172.16.0.0 vía 192.168.14.2, la tabla de enrutamiento no la muestra. Se muestran únicamente las rutas dinámicas aprendidas mediante RIP. Esto se debe a que la AD es mayor (130) para las rutas estáticas, y al menos que la ruta RIP en S0/0 se pierda, no será instalada en la tabla de enrutamiento.




```
GAD(config)#ip route 172.16.0.0 255.255.0.0
192.168.14.2 130
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
          D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
          E 1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
          i - IS-IS, L1 - IS-IS level - 1, L2 -
IS-IS level -2, ia - IS-IS inter area
          * - candidate default, U - per -user
static route, o - ODR
          p - periodic downloaded static route
    Gateway of last resort is not set

     C      192.168.13.0/24 is directly connected,
Serial 0/0
          p - periodic downloaded static route
    Gateway of last resort is not set

     C      192.168.13.0/24 is directly connected,
Serial 0/0
     C      192.169.14.0/24 is directly connected,
BRI0/1
     R      172.16.0.0/16 [120/1] via 192.168.13.2,
00:00:24, Serial0/0
```

Figura 5.11. *RIP con rutas estáticas*

Las rutas estáticas que señalan una interfaz serán publicadas a través del router propietario de las rutas estáticas, y se propagarán por toda la red. Esto se debe a que las rutas estáticas que apuntan a una interfaz se consideran en la tabla de enrutamiento como conectadas, y por ello pierden su naturaleza estática en la actualización. Si se asigna una ruta estática a una interfaz que no está definida en el proceso RIP, mediante el comando network, RIP no publicará la ruta a menos que se especifique un comando **redistribute static** en el proceso de RIP.

Cuando una interfaz sale fuera de servicio, todas las rutas estáticas que apuntan a ella son eliminadas de la tabla de enrutamiento de paquetes IP. De igual forma, cuando el

IOS no puede encontrar un salto siguiente válido para la dirección especificada en la ruta estática, la ruta es eliminada de la tabla de enrutamiento de paquetes IP.

5.8. Tabla de host

La resolución de nombres de host es el mecanismo que utiliza un computador para relacionar un nombre de host con una dirección de IP.

Para poder usar nombres de host para comunicarse con otros dispositivos de IP, los dispositivos de red, como los routers, deben poder vincular los nombres de host con las direcciones de IP. Una lista de nombres de host y sus direcciones de IP asignadas se denomina tabla de host.

Los protocolos como Telnet utilizan nombres de host para identificar los dispositivos de red o hosts. Los dispositivos de red (por ejemplo, los routers) deben asociar nombres de host con direcciones IP para comunicarse con otros dispositivos IP.

Una tabla de host puede incluir todos los dispositivos de una red. Cada dirección de IP individual puede estar vinculada a un nombre de host. El software Cisco IOS mantiene un archivo de vínculos entre los nombres de host y las direcciones de IP, el cual es utilizado por los comandos EXEC. Este caché agiliza el proceso de conversión de nombres a direcciones.

Los nombres de host, a diferencia de los nombres DNS, sólo tienen vigencia en el router en el que están configurados. La tabla de host permite que el administrador de red pueda escribir tanto el nombre del host, como puede ser Auckland, como la dirección de IP, para conectarse por Telnet a un host remoto.

CAPÍTULO 6

INFORMACIÓN BÁSICA DE TELNET, PING, Y TRACEROUTE

6. INFORMACIÓN BÁSICA DE TELNET, PING Y TRACEROUTE

6.1. Telnet.

Cuando surgió Internet, la red (ARPANET) estaba compuesta de equipos cuyas configuraciones eran muy poco homogéneas (teclados, juegos de caracteres, resoluciones, longitud de las líneas visualizadas). Además, las sesiones de los terminales también tenían su propia manera de controlar el flujo de datos entrante/saliente.

Por lo tanto, en lugar de crear adaptadores para cada tipo de terminal, para que pudiera haber interoperabilidad entre estos sistemas, se decidió desarrollar una interfaz estándar denominada NVT (Terminal virtual de red). Así, se proporcionó una base de comunicación estándar, compuesta de:

- Caracteres ASCII de 7 bits, a los cuales se les agrega el código ASCII extendido.
- Tres caracteres de control.
- Cinco caracteres de control opcionales.
- Un juego de señales de control básicas.

Por lo tanto, el protocolo Telnet consiste en crear una abstracción del terminal que permita a cualquier host (cliente o servidor) comunicarse con otro host sin conocer sus características.

Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

El protocolo Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma Terminal virtual de red (NVT).
- El principio de opciones negociadas.
- Las reglas de negociación.

Éste es un protocolo base, al que se le aplican otros protocolos del conjunto TCP/IP (FTP, SMTP, POP3, etc.). Las especificaciones Telnet no mencionan la autenticación porque

Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet). Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada). Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.

Aparte de estos usos, en general telnet se ha utilizado (y aún hoy se puede utilizar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina. Es una forma muy usual de trabajar con sistemas UNIX.

Excepto por las opciones asociadas y las reglas de negociación, las especificaciones del protocolo Telnet son básicas. La transmisión de datos a través de Telnet consiste sólo en transmitir bytes en el flujo TCP (el protocolo Telnet específica que los datos deben agruparse de manera predeterminada esto es, sin ninguna opción que especifique lo contrario, en un búfer antes de enviarse. Específicamente, esto significa que de manera predeterminada los datos se envían línea por línea). Cuando se transmite el byte 255, el byte siguiente debe interpretarse como un comando. Por lo tanto, el byte 255 se denomina IAC (Interpretar como comando).

Las especificaciones del protocolo Telnet permiten tener en cuenta el hecho de que ciertos terminales ofrecen servicios adicionales, no definidos en las especificaciones básicas (pero de acuerdo con las especificaciones), para poder utilizar funciones avanzadas. Estas funcionalidades se reflejan como opciones. Por lo tanto, el protocolo Telnet ofrece un sistema de negociaciones de opciones que permite el uso de funciones avanzadas en forma de opciones, en ambos lados, al iniciar solicitudes para su autorización desde el sistema remoto.

Las opciones de Telnet afectan por separado cada dirección del canal de datos. Entonces, cada parte puede negociar las opciones, es decir, definir las opciones que:

- Desea usar (DO).
- Se niega a usar (DON'T).
- Desea que la otra parte utilice (WILL).
- Se niega a que la otra parte utilice (WON'T).

De esta manera, cada parte puede enviar una solicitud para utilizar una opción. La otra parte debe responder si acepta o no el uso de la opción. Cuando la solicitud se refiere a la desactivación de una opción, el destinatario de la solicitud no debe rechazarla para ser completamente compatible con el modelo NVT.

Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar). Esto facilita que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas, y así acceder él también a todas esas máquinas. Por esta razón dejó de usarse, casi totalmente, hace unos años, cuando apareció y se popularizó el SSH, que puede describirse como una versión cifrada de telnet, actualmente se puede cifrar toda la comunicación del protocolo durante el establecimiento de sesión (RFC correspondiente, en inglés) si el cliente y el servidor lo permiten, aunque no se tienen ciertas funcionalidad extra disponibles en SSH.

Hoy en día este protocolo también se usa para acceder a los BBS, que inicialmente eran accesibles únicamente con un módem a través de la línea telefónica. Para acceder a un BBS mediante telnet es necesario un cliente que dé soporte a gráficos ANSI y protocolos de transferencia de ficheros. Los gráficos ANSI son muy usados entre los BBS. Con los protocolos de transferencia de ficheros (el más común y el que mejor funciona es el ZModem) podrás enviar y recibir ficheros del BBS, ya sean programas o juegos o ya sea el correo del BBS (correo local, de FidoNet u otras redes).

Para iniciar una sesión con un intérprete de comandos de otro ordenador, puede emplear el comando telnet seguido del nombre o la dirección IP de la máquina en la que desea trabajar, por ejemplo si desea conectarse a la máquina purpura.micolegio.edu.com deberá teclear telnet purpura.micolegio.edu.com, y para conectarse con la dirección IP 1.2.3.4 deberá utilizar telnet 1.2.3.4.

Una vez conectado, podrá ingresar el nombre de usuario y contraseña remota para iniciar una sesión en modo texto a modo de consola virtual. La información que transmita (incluyendo su clave) no será protegida o cifrada y podría ser vista en otros computadores por los que se transite la información (la captura de estos datos se realiza con un packet sniffer).

Una alternativa más segura para telnet, pero que requiere más recursos del computador, es SSH. Este cifra la información antes de transmitirla, autentica la máquina a la cual se conecta y puede emplear mecanismos de autenticación de usuarios más seguros.

6.1.1. Seguridad.

Hay tres razones principales por las que el telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los demonios de uso general del telnet tienen varias vulnerabilidades descubiertas sobre los años, y varias más que podrían aún existir.

- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.

- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

¿Dónde no utilizarlo?

En ambientes donde es importante la seguridad, por ejemplo en el Internet público, telnet no debe ser utilizado. Las sesiones de telnet no son cifradas. Esto significa que cualquiera que tiene acceso a cualquier router, switch, o gateway localizado en la red entre los dos anfitriones donde se está utilizando telnet puede interceptar los paquetes de telnet que pasan cerca y obtener fácilmente la información de la conexión y de la contraseña (y cualquier otra cosa que se mecanografía) con cualesquiera de varias utilidades comunes como tcpdump y Wireshark.

Estos defectos han causado el abandono y depreciación del protocolo telnet rápidamente, a favor de un protocolo más seguro y más funcional llamado SSH, lanzado en 1995. SSH provee de toda la funcionalidad presente en telnet, la adición del cifrado fuerte para evitar que los datos sensibles tales como contraseñas sean interceptados, y de la autentificación mediante llave pública, para asegurarse de que el computador remoto es realmente quién dice ser.

Los expertos en seguridad computacional, tal como el instituto de SANS, y los miembros del Newsgroup de Compos.linux.security recomiendan que el uso del telnet para las conexiones remotas debiera ser descontinuado bajo cualquier circunstancia normal.

Cuando el telnet fue desarrollado inicialmente en 1969, la mayoría de los usuarios de computadoras en red estaban en los servicios informáticos de instituciones académicas, o en grandes instalaciones de investigación privadas y del gobierno. En este ambiente, la seguridad no era una preocupación y solo se convirtió en una preocupación después de la explosión del ancho de banda de los años 90. Con la subida exponencial del número de gente con el acceso al Internet, y por la extensión, el número de gente que procura crackear los servidores de otra gente, telnet podría no ser recomendado para ser utilizado en redes con conectividad a Internet.

6.2. ICMP

ICMP es el Internet Control Message Protocol. Al igual que IP, ICMP reside en la capa de la red Modelo OSI.

A diferencia de los protocolos de la capa de transporte TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) que operan en la parte superior de IP, ICMP existe junto a la propiedad intelectual.

La capacidad de comprender ICMP es un requisito para cualquier red IP-dispositivo compatible. Sin embargo, muchos dispositivos de seguridad tales como firewalls permiten bloquear o desactivar la totalidad o parte de la funcionalidad de ICMP con fines de seguridad.

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (*Internet Control Message Protocol,* protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no solo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema.

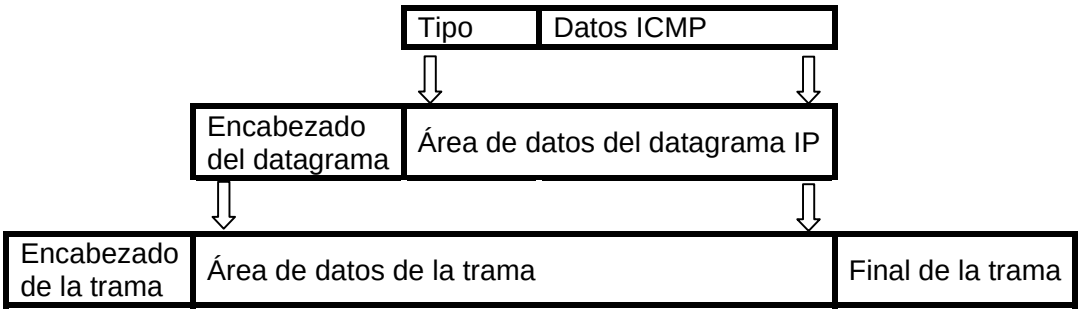


Figura 6.1 *ICMP.*

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creara un nuevo mensaje ICMP sino que el primero se descartara sin más.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje ICMP, según se muestra en la tabla siguiente:

Tabla 6.1 *Tipos de mensajes ICMP.*

0	Respuesta de eco (*Echo Reply*)
3	Destino inalcanzable (*Destination Unreachable*)
4	Disminución del trafico desde el origen (*Source Quench*)
5	Redireccionar (cambio de ruta) (*Redirect*)
8	Solicitud de eco (*Echo*)
11	Tiempo excedido para un datagrama (*Time Exceded*)
12	Problema de parámetros (*Parameter Problem*)
13	Solicitud de marca de tiempo (*Timestamp*)
14	Respuesta de marca de tiempo(*Timestamp Reply*)
15	Solicitud de información (obsoleto) (*Information Request*)
16	Respuesta de información (obsoleto) (*Information Reply*)
17	Solicitud de máscara (*Addressmask*)
18	Respuesta de máscara (*Addressmask Reply*)

El Protocolo de Mensajes de Control y Error de Internet, ICMP, es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

El protocolo ICMP solamente informa de incidencias en la entrega de paquetes o de errores en la red en general, pero no toma decisión alguna al respecto. Esto es tarea de las capas superiores.

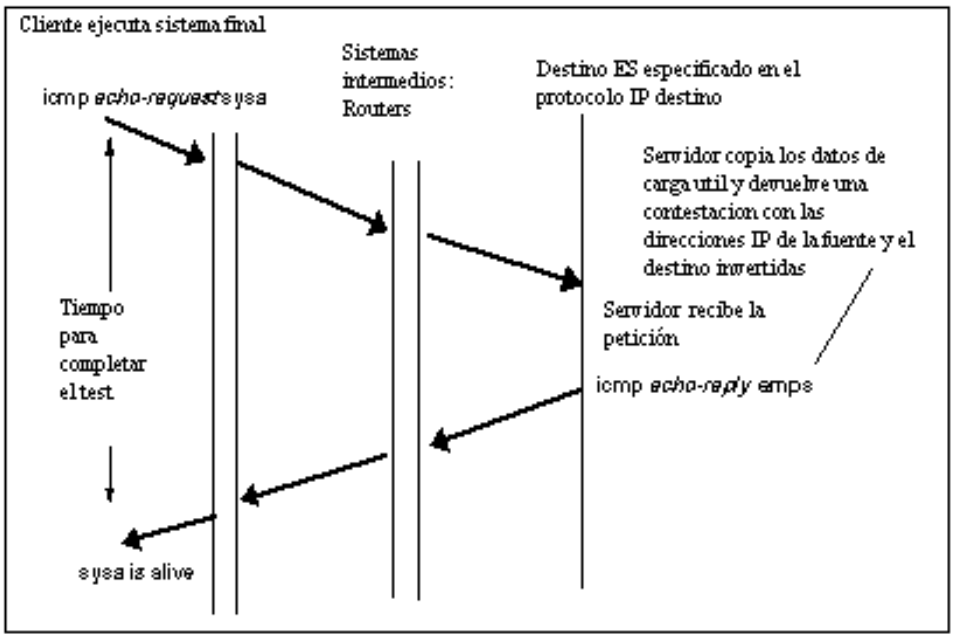


Figura 6.2 *Trayectoria del mensaje ICMP.*

6.2.1. Aspectos técnicos.

Los mensajes ICMP son comúnmente generados en respuesta a errores en los datagramas de IP o para diagnóstico y ruteo. La versión de ICMP para IPv4 también es conocida como ICMPv4. IPv6 tiene su protocolo equivalente.

Los mensajes ICMP son construidos en el nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP (para obtener los mensajes de respuesta desde el host original que envía), y transmite el datagrama resultante de manera habitual.

Por ejemplo, cada router que reenvía un datagrama IP tiene que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en una unidad; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama.

Cada mensaje ICMP es encapsulado directamente en un solo datagrama IP, y por tanto no garantiza la entrega del ICMP.

Aunque los mensajes ICMP son contenidos dentro de datagramas estándar IP, los mensajes ICMP se procesan como un caso especial del procesamiento normal de IP, algo así como el procesamiento de un sub-protocolo de IP. En muchos casos es necesario inspeccionar el contenido del mensaje ICMP y entregar el mensaje apropiado de error a la aplicación que generó el paquete IP original, aquel que solicitó el envío del mensaje ICMP.

La utilidad del protocolo ICMP es controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Muchas de las utilidades de red comunes están basadas en los mensajes ICMP. El comando traceroute está implementado transmitiendo datagramas UDP con campos especiales TTL IP en la cabecera, y buscando los mensajes de "Tiempo de Vida en tránsito" y "Destino inalcanzable" generados como respuesta. La herramienta ping está implementada utilizando los mensajes "Echo request" y "Echo reply" de ICMP.

6.2.2. Mensajes informativos.

Entre estos mensajes hay algunos de suma importancia, como los mensajes de petición de ECO (tipo 8) y los de respuesta de Eco (tipo 0). Las peticiones y respuestas de eco se usan en redes para comprobar si existe una comunicación entre dos host a nivel de capa de red, por lo que nos pueden servir para identificar fallos en este nivel, ya que verifican si las capas física (cableado), de enlace de datos (tarjeta de red) y red (configuración IP) se encuentran en buen estado y configuración.

6.2.3. Mensajes de error.

En el caso de obtener un mensaje ICMP de destino inalcanzable, con el campo "tipo" a 3.

Este tipo de mensajes se generan cuando el tiempo de vida del datagrama a llegado a cero mientras se encontraba en tránsito hacia el host destino (código=0), o porque, habiendo llegado al destino, el tiempo de reensamblado de los diferentes fragmentos expira antes de que lleguen todos los necesarios (código=1).

Los mensajes ICMP de tipo= 12 (problemas de parámetros) se originan por ejemplo cuando existe información inconsistente en alguno de los campos del datagrama, que hace que sea imposible procesar el mismo correctamente, cuando se envían datagramas de tamaño incorrecto o cuando falta algún campo obligatorio.

Por su parte, los mensajes de tipo=5 (mensajes de redirección) se suelen enviar cuando, existiendo dos o más routers diferentes en la misma red, el paquete se envía al router equivocado. En este caso, el router receptor devuelve el datagrama al host origen junto con un mensaje ICMP de redirección, lo que hará que éste actualice su tabla de enrutamiento y envíe el paquete al siguiente router.

6.2.4. Solicitud y respuesta de eco.

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre dos host a nivel de capa de red. Estos mensajes comprueban que la capas físicas (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden ping envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

- A envía un mensaje ICMP de tipo 8 (*Echo*) a B.
- B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (*Echo Reply*) a A.
- A recibe el mensaje ICMP de B y muestra el resultado en pantalla.

6.3. Ping.

En general el comando ping se utiliza para comprobar que exista comunicación de Capa 3 entre dos dispositivos. Por ejemplo de PC a PC, PC a Switch, PC a Server Web, PC a Router.

Cuando se menciona que comprueba la conexión de capa tres se esta haciendo referencia a OSI ISO, que establece las capas del Networking.

1. Capa Física
2. Acceso al medio
3. Red

Entonces que dos PC tengan ping exitoso no quiere decir que puedan acceder los servicios que nosotros deseamos. Mas bien significa que la maquina se ha podido localizar y esta respondiendo utilizando su dirección IP.

Un claro ejemplo seria que tuviéramos un WEB Server con problemas, pero el Ping funciona. De manera que eso no quiere decir que todo el sistema este en correcto funcionamiento, sino únicamente la capa 3 para abajo. De manera que el Web Server se ejecuta en una capa superior la 7 por ejemplo y allí reside el problema.

Un ping (Packet Internet Grouper) se trata de una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

Muchas veces se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos, y por ello, se utiliza entre los aficionados a los juegos en red el término PING para referirse al lag o latencia de su conexión.

Existe otro tipo, Ping ATM, que se utiliza en las redes ATM (como puede ser una simple ADSL instalada en casa) y, en este caso, las tramas que se transmiten son ATM (nivel 2 del modelo OSI).

Este tipo de paquetes se envían para probar si los enlaces ATM están correctamente definidos.

Cuando hacemos **ping** a un equipo (ejecutamos el comando **ping**) o a una dirección IP lo que hace el sistema es enviar a esa dirección una serie de paquetes (normalmente cuatro) de un tamaño total de 64 bytes (salvo que se modifique) y queda en espera del reenvío de estos (eco), por lo que se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.

Una de las ventajas de ejecutar este comando es que los paquetes se envían atacando directamente la IP a la que dirigimos el ping, lo que hace que una de sus utilidades es comprobar la conectividad de nuestra red, ya que no están influidos por ningún controlador del servidor.

6.3.1. Interpretación de resultados.

En los mensajes de ping podemos distinguir un par de leyendas las cuales es importante conocer su significado. Cuando el Ping es exitoso distinguimos que en la tercera línea se distingue Respuesta desde EL IP PINGEADO.
Eso como es lógico significa que el dispositivo en cuestión esta respondiendo satisfactoriamente la petición de capa 3.

Nota: Es importante mencionar que a veces los dispositivos se configuran para no responder al PING. Eso es debido a que es fácilmente identificable cuando el PC esta encendido y por lo tanto puede ser Objeto de ataques mal intencionados.

Se distingue además la leyenda bytes=64. Nos menciona que el paquete de prueba enviado contiene un cuerpo de 32 bytes. Ese parámetro se puede modificar pero para el uso habitual de la red, no tiene interés alguno.

Al final nos muestra un resumen de los paquetes que han sido recibidos satisfactoriamente o los que no alcanzaron el destino.
Una cantidad grandes de paquetes perdidos significa bajo rendimiento, problemas en la red, en las conexiones o incluso el cable.

```
C:\>ping 127.0.0.1

Haciendo ping a 127.0.0.1 con 32 bytes de datos:

Respuesta desde 127.0.0.1: bytes=32 tiempo=12ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 12ms, Media = 3ms
```

6.3.2. Descripción de datos mostrados

Cantidad de bytes enviados: Eso ya se ha explicado

Tiempo: Es la cantidad de milisegundos que tarda el paquete en recorrer el camino. Tiempos mayores de 5 milisegundos en redes pequeñas (ámbito local) son patológicos y a menudo señal de fallo. Lo ideal es que siempre sean menos de 1 milisegundo como en el caso representado.

TTL: Este es el tiempo de Vida del paquete. Se disminuye en una unidad en cada salto de Router. Eso es cada Router que atraviesa. Si no existiera un TTL los paquetes estarían en un LOOP indefinido lo que causaría complicaciones en la RED y colisiones, síntomas de una mala configuración.

6.3.3. Ejemplo de ping.

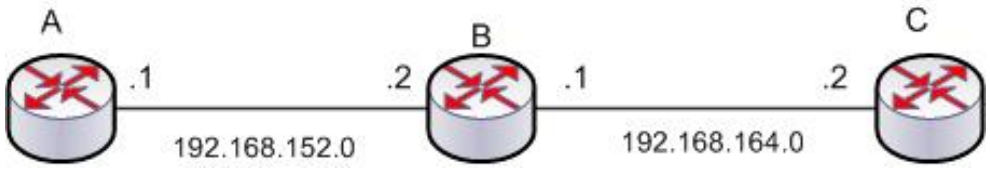


Figura 6.3 *Esquema de red donde se simula el proceso de PING.*

En general ping se utiliza para comprobar la existencia de la comunicación de capa 3 entre dos dispositivos. Esto significa que la comprobación solo implica la capa 3 e inferiores a ella como la capa física y de enlace de datos, el hecho de que el ping sea exitoso no significa que las demás capas superiores a la 3 funcionen correctamente. Para comprobar esto deberás hacer uso de otra opción.

En este ejemplo se ejecuto ping del router A al router B. Esto significa que la dirección IP origen es **192.168.152.1** y la dirección IP destino es **192.168.164.2.**

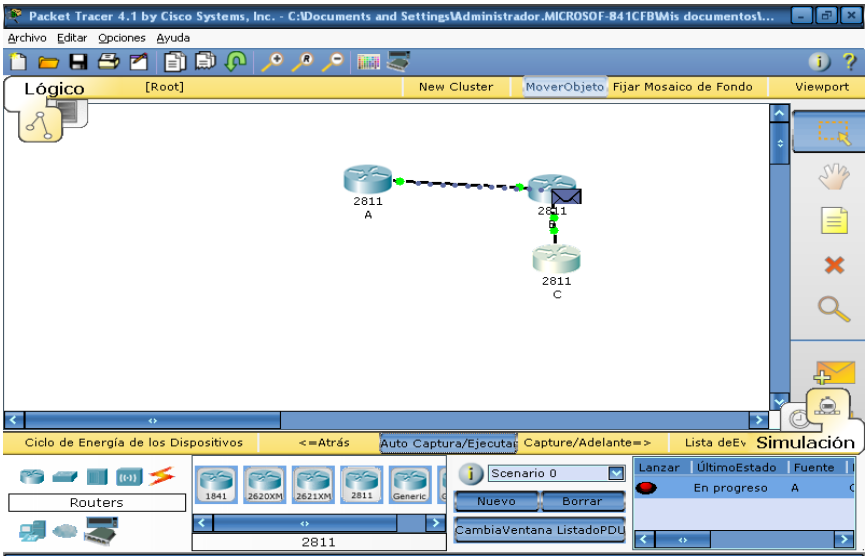


Figura 6.4 *Esquema de red.*

La orden **ping** envía mensajes de solicitud de eco a un host remoto e informa de las respuestas. Los mensajes que envían son mensajes **ICMP** que envía el router origen al destino pasando por todos los routers intermedios hasta llegar al router destino y este destino enviara de la misma manera la respuesta al mensaje recibido. Este procedimiento sigue un procedimiento como el siguiente:

- A envía un mensaje ICMP de tipo 8 (Echo) a B.
- B recibe el mensaje ICMP y se da cuenta que no es para el, si no para alguien mas, entonces verifica si el puede alcanzar la dirección IP destino que lleva ese paquete, descubre que si lo puede encaminar y lo envía a esa dirección IP destino.
- C recibe ese paquete Echo y sabe que es para el, entonces envía un mensaje de tipo 0 (Echo Reply) a la dirección IP de origen que llevaba el paquete.
- B recibe el mensaje de respuesta y lo reenvía a A.
- A recibe el mensaje ICMP y muestra el resultado de éxito en pantalla.

El envió de los mensajes ICMP se muestra a continuación.

Figura 6.5 *Envió de mensajes ICMP en una petición de PING*

La notificación de un ping exitoso o erróneo se muestra en la siguiente ventana, el ping fue exitoso con esto deducimos que la conectividad hasta la capa 3 es correcta entre los router A y C.

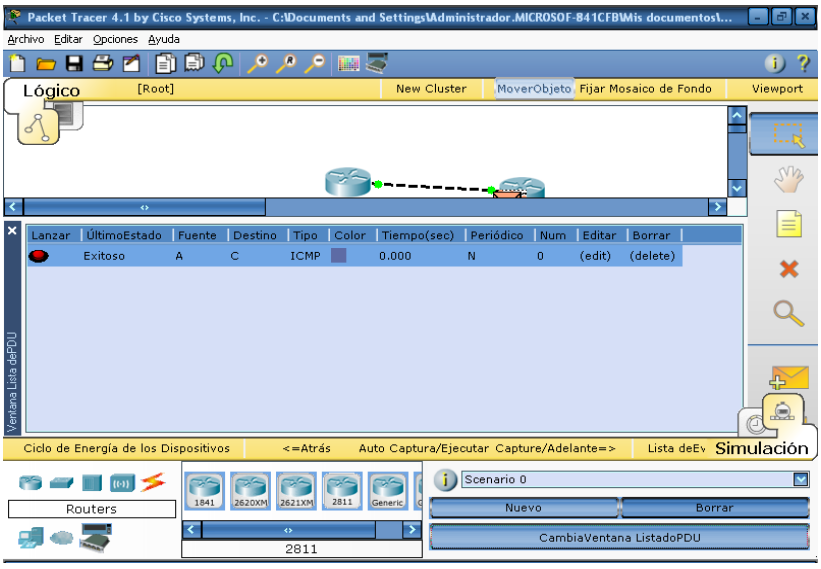


Figura 6.6 *Notificación de ping exitoso*

En la figura 6.7 se muestra un ejemplo de cómo las diferentes capas hasta la 3, realizan el reenvió hasta el destino del mensaje ICMP a través de la red. En este caso se muestra la salida del proceso en el momento que el mensaje esta en el router B.

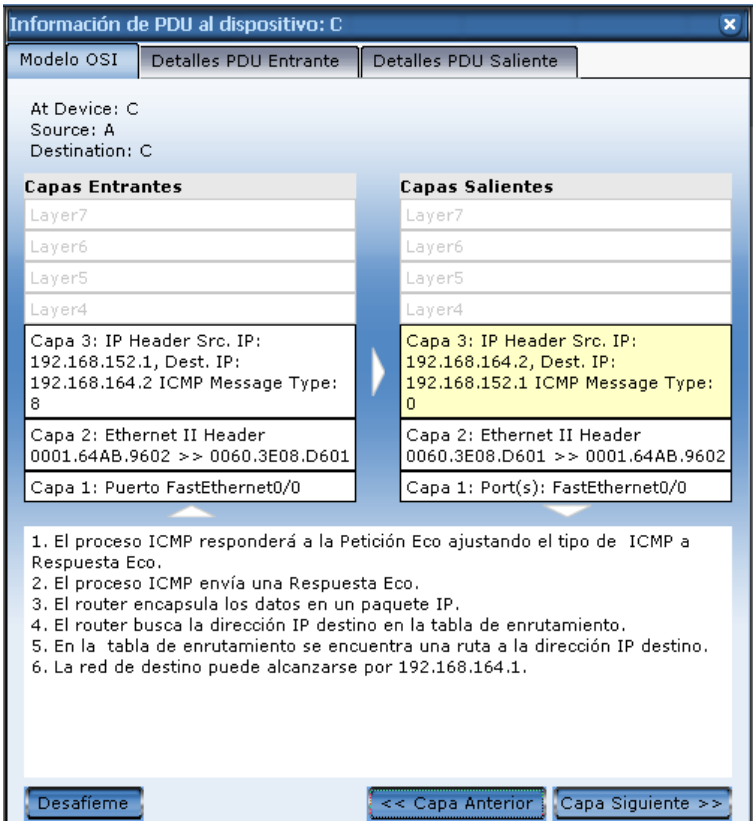


Figura 6.7 *Detalle de cada capa en el modelo OSI.*

Como puede observar en la imagen anterior se muestra la acción que realiza cada una de las capas incluidas las tres capas entrantes o del router que envía el mensaje y las tres capas salientes o del router que recibe el mensaje.

En la siguiente imagen se muestra los datos de la PDU entrante o la PDU que fue enviada por el origen que pidió el ping. El formato que se muestra con detalle son los de la capa Ethernet y la capa IP.

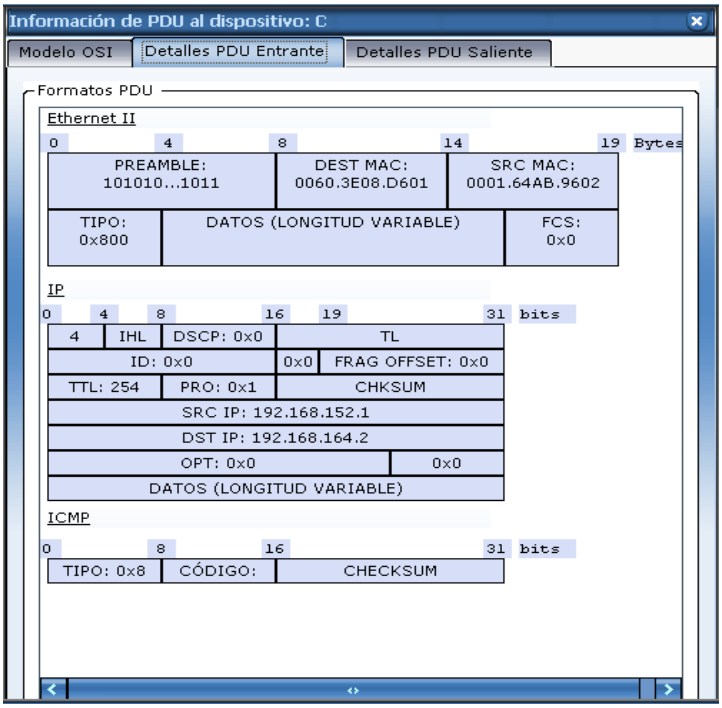


Figura 6.8 *Detalles de la PDU entrante.*

En la figura 6.9 se muestran detalles de la PDU saliente, donde se muestra el formato del mensaje en la capa Ethernet e IP, la salida mostrada corresponde al formato de la PDU cuando se encuentra en el router B.

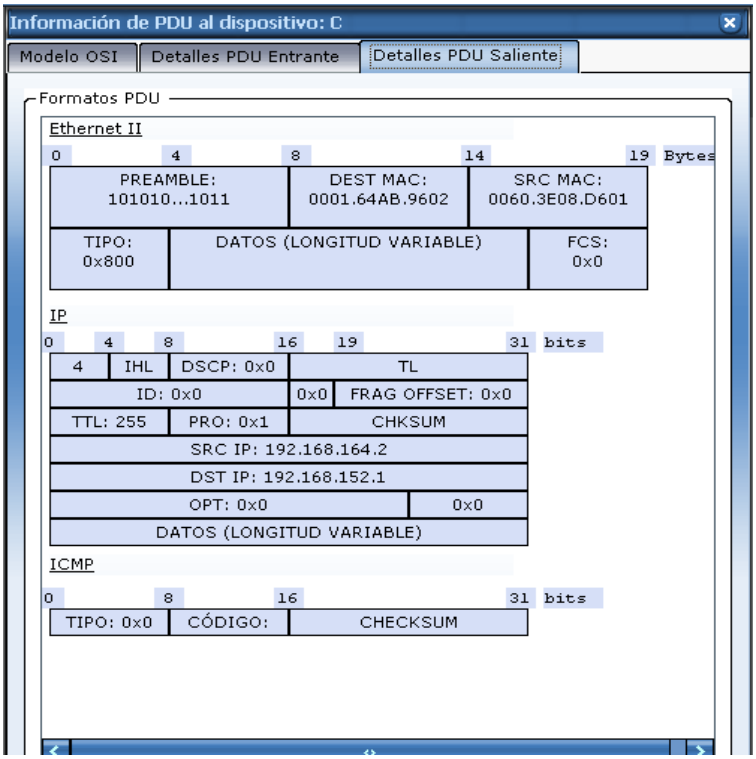


Figura 6.9 *Detalles de la PDU saliente.*

6.4. Traceroute.

6.4.1. Cómo utilizar la utilidad TRACERT

La utilidad de diagnóstico TRACERT determina la ruta a un destino mediante el envío de paquetes de eco de ICMP (Protocolo de mensajes de error de Internet) al destino. En estos paquetes, TRACERT utiliza valores de período de vida (TTL) IP variables. Dado que los enrutadores de la ruta deben disminuir el TTL del paquete como mínimo una unidad antes de reenviar el paquete, el TTL es, en realidad, un contador de saltos.

Cuando el TTL de un paquete alcanza el valor cero (0), el enrutador devuelve al equipo de origen un mensaje ICMP de "Tiempo agotado".
TRACERT envía el primer paquete de eco con un TTL de 1 y aumenta el TTL en 1 en cada transmisión posterior, hasta que el destino responde o hasta que se alcanza el TTL máximo. Los mensajes ICMP "Tiempo agotado" que devuelven los enrutadores intermedios muestran la ruta. Observe, sin embargo, que algunos enrutadores colocan paquetes que han agotado el TTL sin avisar y que estos paquetes son invisibles para TRACERT.

TRACERT imprime una lista ordenada de los enrutadores intermedios que devuelven mensajes ICMP "Tiempo agotado". La opción -d con el comando tracert le indica a TRACERT que no efectúe una búsqueda de DNS en todas las direcciones IP, de

manera que TRACERT devuelve la dirección IP de la interfaz del lado cercano de los enrutadores.

En el siguiente ejemplo del comando tracert y su resultado, el paquete viaja a través de dos enrutadores (157.54.48.1 y 11.1.0.67) para llegar al host 11.1.0.1. En este ejemplo, la puerta de enlace predeterminada es 157.54.48.1 y la dirección IP del enrutador en la red 11.1.0.0 está en 11.1.0.67.

El comando:
`C:\>tracert 11.1.0.1`

El resultado del comando:

Traza a la dirección 11.1.0.1 sobre caminos de 30 saltos como máximo –
1 2 ms 3 ms 2 ms 157.54.48.1 2 75 ms 83 ms 88 ms 11.1.0.67 3 73 ms 79 ms 93 ms 11.1.0.1
Traza completa.

6.4.2. Cómo utilizar TRACERT para solucionar problemas

Puede utilizar TRACERT para averiguar en qué lugar de la red se detuvo un paquete. En el siguiente ejemplo, la puerta de enlace predeterminada ha determinado que no existe una ruta válida para el host en 22.110.0.1. Probablemente hay un problema de configuración del enrutador o no existe la red 22.110.0.0, lo que indica que la dirección IP es incorrecta.

El comando:
`C:\>tracert 22.110.0.1`

El resultado del comando:
Traza a la dirección 22.110.0.1 sobre caminos de 30 saltos como máximo ----------1 157.54.48.1 devuelve:
Red de destino inaccesible.
Traza completa.

TRACERT es útil a la hora de solucionar problemas en las redes grandes, donde se pueden tomar varias rutas para llegar a un destino o donde existen muchos componentes intermedios (enrutadores o puentes).

6.4.3. Cómo utilizar las opciones de TRACERT

Hay varias opciones de la línea de comandos que se pueden utilizar con TRACERT, aunque generalmente estas opciones no son necesarias para solucionar los problemas normales.
El siguiente ejemplo de sintaxis de comandos muestra todas las opciones posibles:

tracert -d -h *n_max_saltos* -j *lista_host* -w *tiempo_esperahost_destino*

6.4.4. Descripción de los parámetros:

-d
Especifica que no se resuelvan las direcciones en nombres de host.

-h n_max_saltos
Especifica el número máximo de saltos para alcanzar el destino.

-j lista-host
Especifica la ruta de origen a lo largo de la lista de hosts.

-w tiempo_espera
Espera el número de milisegundos especificados en tiempo_espera para cada respuesta.

host_destino
Nombre de la dirección IP del host de destino.

CAPÍTULO 7

CDP
(CISCO DISCOVERY PROTOCOL)

7. CDP

7.1. Introducción al CDP

El uso principal de CDP es descubrir plataformas y protocolos en los dispositivos vecinos. *Cisco Discovery Protocol* (CDP) descubre y muestra información acerca de los dispositivos Cisco directamente conectados (routers y switches), tales como la versión del sistema operativo y la dirección IP. CDP es un protocolo propietario de Cisco que se ejecuta en la capa de enlace de datos (capa 2) del modelo OSI. Esto permite que los dispositivos, que puedan estar ejecutando distintos protocolos de red de capa 3 como IP o IPX, aprendan acerca de la existencia del otro. El CDP es independiente de los medios y protocolos, y es ejecutable en todos los equipos Cisco sobre el Protocolo de Acceso de Subred (SNAP). CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, *On-Demand Routing*), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

La versión 2 del CDP (CDPv2) es la versión mas reciente del protocolo. El Cisco IOS (Versión 12.0(3) o posteriores) admiten el CDPv2. En la versiones de Cisco IOS 10.3 a 12.0(3)T, la función de CDPv1 esta activada de manera predeterminada.

CDP se inicia automáticamente en el inicio del sistema de un dispositivo, sin embargo, si esta usando la Versión 10.3 o anterior de Cisco IOS deberá activarla para cada una de las interfaces del dispositivo utilizando el comando **cdp enable**. Esto permite que el dispositivo detecte los dispositivos vecinos que también están ejecutando el CDP. Este protocolo de Cisco se ejecuta en la capa de enlace de datos y permite que dos sistemas obtengan información entre si.

Solo los vecinos directamente conectados intercambian tramas CDP, conocidas como anuncios (advertisements). Un router almacena en caché cualquier información recibida (a través de mensajes SNMP) de sus vecinos CDP. Si posteriormente una trama CDP indica que parte de la información acerca de un vecino ha cambiado, el router descarta la información más antigua y la reemplaza con la información nueva.

La información contenida en los anuncios CDP varía con el tipo de dispositivo y la versión del sistema operativo que corra. Dicha información incluye la versión del sistema operativo, el nombre de equipo, todas la direcciones de todos los protocolos configurados en el puerto al que se envía la trama CDP (por ejemplo, la dirección IP), el identificador del puerto desde el que se envía el anuncio, el tipo y modelo de dispositivo, la configuración duplex/simplex, el dominio VTP, la VLAN nativa, el consumo energético (para dispositivos PoE) y demás información específica del dispositivo. La información contenida en estos anuncios puede ser extendida fácilmente gracias al uso del formato de trama TLV.

7.2. La información obtenida con CDP

El CDP se usa básicamente para detectar todos los dispositivos Cisco que se encuentran conectados directamente. Con el comando **show cdp interface** se recopila información que el CDP utiliza para su publicación y la transmisión de tramas de descubrimiento. Este comando visualiza los valores de los temporizadores de CDP, el estado de la interfaz y el encapsulamiento utilizado por CDP para su publicación y transmisión de tramas de descubrimiento. Los valores por defecto de los temporizadores establecen la frecuencia de las actualizaciones de CDP y la antigüedad de las entradas CDP. Estos temporizadores se fijan automáticamente en 60 segundos y 180 segundos, respectivamente. Si el dispositivo recibe una actualización mas reciente o si expira el valor de este tiempo de espera, el dispositivo debe descartar la entrada CDP. Los comandos **show cdp neighbors** y **show cdp neighbors detail** se utilizan para ver las actualizaciones CDP recibidas en el router local.

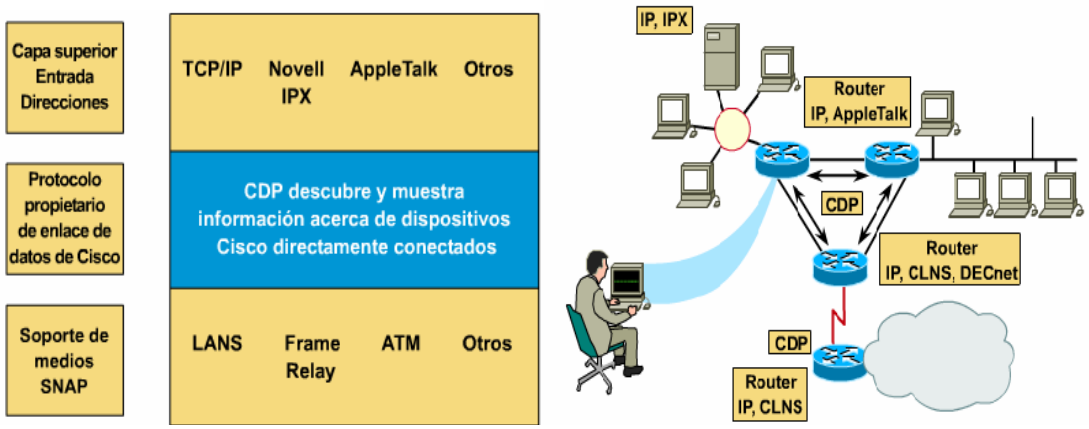


Figura 7.1 *Presentacion de CDP mostrada a un administrador*

En la figura vemos un ejemplo de cómo CDP presenta la información reunida a un administrador de red. Cada router que ejecuta CDP intercambia información sobre protocolos con sus vecinos. El administrador puede mostrar los resultados de este intercambio de información de CDP en una consola conectada a un router configurado para ejecutar CDP en sus interfaces. El administrador de red usa el comando show para mostrar información acerca de las redes que están conectadas directamente con el router. CDP suministra información acerca de cada dispositivo CDP vecino al transmitir los valores de longitud y tipo (TLVs) que constan de bloques de información incorporados en las publicaciones CDP. Los valores incluyen lo siguiente:

- ***Identificadores de dispositivos:*** Por ej., el nombre de dominio y el nombre de host configurado del router (si existe).
- ***Lista de direcciones:*** Por lo menos una dirección para SNMP, hasta una dirección por cada protocolo reconocido.
- ***Identificador de puerto:*** Por ejemplo, Ethernet 0, Ethernet 1 y Serial 0.

- ***Lista de capacidades:*** Por ejemplo, si el dispositivo actúa como un puente de ruta origen además de actuar como router.
- ***Versión:*** Información como la suministrada por el comando local show versión.
- ***Plataforma:*** La plataforma de hardware del dispositivo, por ejemplo., Cisco 7000.

Los siguientes TLVs se incluyen solo en CDPv2:

- ***Administración de nombres de dominio VTP***
- ***VLAN Nativas***
- ***Full o half-duplex***

Observe que el router que aparece más abajo en la figura no se encuentra directamente conectado al router de la consola del administrador. Para obtener información de CDP acerca de este dispositivo el administrador necesita realizar Telnet a un router directamente conectado a este objetivo.

7.3. Implementación, monitoreo y mantenimiento del CDP

Los siguientes comandos se utilizan para implementar, monitorear y mantener la información CDP:

Tabla 7.1 *Comandos para la implemenrtacion, monitoreo y mantenimiento de CDP*

Comando	Modo	Propósito
cdp run	Modo de configuración global.	Habilita CDP globalmente en el router.
cdp enable	Modo de configuración de interfaz.	Habilita CDP en una interfaz.
clear cdp counters	Modo privilegiado	Restaura los contadores de tráfico a cero.
show cdp	Modo usuario o privilegiado	Muestra el intervalo entre transmisiones de publicaciones CDP, el número de segundos durante los que la publicación CDP es valida para un puerto dado y la versión de la publicación.
show cdp entry { * | device-name [*] [protocol | version]}	Modo usuario o privilegiado	Muestra información acerca de un vecino específico. Lo que muestra, puede limitarse a información de protocolo o versión.
show cdp interface [type number]	Modo usuario o privilegiado	Muestra información acerca de las interfaces en la que CDP está habilitado.

show cdp neighbors [type number] [detail]	Modo EXEC privilegiado	Muestra el tipo de dispositivo detectado, el nombre del dispositivo, el numero y tipo de la interfaz local (puerto), el numero de segundos durante los que la publicación CDP es valida para el puerto, el tipo de dispositivo, el numero de producto del dispositivo y el ID de puerto. Al emitirse la palabra clave de detalle, se muestra información sobre el ID de la VLAN nativa, el modo dúplex y el nombre asociado con los dispositivos vecinos.

7.4. Creación de un mapa de red del entorno.

El CDP se diseño e implemento como un protocolo sencillo, de baja carga general. Aunque una trama CDP puede ser pequeña, puede recuperar una gran cantidad de información útil sobre los dispositivos Cisco vecinos conectados.

Esta información puede utilizarse para crear un mapa de red de los dispositivos conectados. Los dispositivos conectados a los dispositivos vecinos pueden detectarse al usar Telnet para conectarse con ellos, y con el comando **show cdp neighbors** para detectar cuales dispositivos se encuentran conectados a esos vecinos.

7.5. Desactivación del CDP

Para desactivar el CDP a nivel global, utilice el comando no cdp run en el modo de configuración global. Si se desactiva el CDP de forma global, no es posible activar las interfaces individuales para CDP.

En la versión 10.3 o superior del Cisco IOS, el CDP se activa automáticamente en todas las interfaces soportadas para enviar y recibir información CDP. Sin embargo, en algunas interfaces, tales como las asíncronas, el CDP se desactiva de forma automática. Si el CDP se encuentra desactivado utilice el comando **cdp enable** en el modo de configuración de interfaz. Para desactivar el CDP en una interfaz especifica después de haberlo activado, utilice el comando **no cdp enable** en el modo de configuración de interfaz.

7.6. Diagnóstico de Fallas en el CDP

Los siguientes comandos pueden utilizarse para mostrar la versión, la información de actualización, las tablas y el tráfico:

Tabla 7.2 *Comandos para el diagnóstico de fallas de CDP*

Comando	Descripción
clear cdp table	Elimina la tabla CDP de información de los vecinos.
clear cdp counters	Restaura los contadores de tráfico a cero.
show cdp traffic	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos y los errores de checksum.
show debugging	Determina cuales tipos de "debugging" están habilitados.
debug cdp adjacency	Información de vecinos CDP.
debug cdp events	Eventos CDP.
debug cdp ip	Información CDP IP.
debug cdp packets	Información relativa a los paquetes CDP.
cdp timer	Especifica la frecuencia con que el software Cisco IOS envía actualizaciones CDP.
cdp holdtime	Especifica el tiempo de espera que se enviara en el paquete de actualización CDP.
show cdp	Muestra información global de CDP, incluyendo la información de temporizador y tiempo de espera.

CAPÍTULO 8

VERIFICACIÓN, RESPALDO DEL IOS Y RECUPERACIÓN DE CONTRASEÑA

8. VERIFICACIÓN, RESPALDO DEL IOS Y RECUPERACIÓN DE CONTRASEÑA

8.1. Elementos del Routers

Router es un dispositivo basado en hardware. Esto significa que los enrutadores tienen una placa base que consta de CPU, la memoria y algunos construidos en chips junto con otros componentes internos.

Los componentes internos del Router son las siguientes:

- La memoria de sólo lectura (ROM)
- Flash
- La memoria de acceso aleatorio (RAM)
- Memoria de acceso aleatorio no volátil (NVRAM)

Usted puede verificar el estado de estos elementos con los comandos del router.

8.1.1. ROM

La memoria de sólo lectura (ROM) que contiene el micro código para funciones básicas. Básicamente es un firmware que se encuentra incorporado en algún software. ROM consta de cuatro componentes principales. El comando "show versión" muestra el estado de ROM y sus componentes, como Bootstrap.

Los cuatro componentes principales de la ROM son los siguientes:

- **El POST** (Power sobre Self Test), es el primer proceso que se ejecuta después de la ROM de arranque. Se comprueba y verifica el hardware de los dispositivos.
- **Bootstrap:** Cada Sistema Operativo tiene dos tipos de archivos, los archivos de arranque y el sistema de archivos. En primer lugar la carga los archivos de arranque y, a continuación, arranca el sistema de archivos. Bootstrap es el gestor de arranque del Cisco IOS.
- **Mini IOS:** ROM de arranque automáticamente. Proporciona el subconjunto de Cisco IOS.
- **ROM monitor:** Usted puede usar el modo de monitor ROM manualmente con el arranque boot system.

8.1.2. FLASH

Flash es un tipo de memoria usada para que residan en el archivo comprimido de la imagen Cisco IOS. Normalmente sólo hay un archivo que reside en el router flash. El tamaño del flash varía en función de la serie y el modelo del router. Puede variar de 8 a 64 MB de tamaño. Bootstrap carga de la IOS flash normal en el proceso de arranque. El comando "show flash" muestra el estado y el contenido de flash.

8.1.3. RAM

La memoria de acceso aleatorio (RAM) es la configuración actual del router que proporciona una interfaz para el usuario final. Es un tipo de memoria volátil y no guardada. RAM afecta directamente al rendimiento del router. El archivo IOS es descomprimido en RAM. También se conoce como configuración de funcionamiento.

8.1.4. NVRAM

La memoria no volátil de acceso aleatorio (NVRAM) es la configuración guardada que se carga durante el proceso de puesta en marcha de los router Cisco IOS. Es por eso que también se conoce como configuración de arranque. Se trata de un tipo no volátil de almacenamiento de memoria que funciona como el disco duro de la computadora. El comando "show startup-config" muestra el estado de la NVRAM. También tiene la configuración de registro que se pueden ver con "show versión".

Un router Cisco no puede funcionar sin el sistema operativo de internetworking de Cisco (IOS). Cada router Cisco tiene una secuencia de arranque predeterminada, para ubicar y cargar el IOS.

Los dispositivos de internetworking de Cisco requieren del uso de varios archivos para su funcionamiento. Estos incluyen las imágenes del sistema operativo de internetworking de Cisco (IOS) y los archivos de configuración. Un administrador que desee mantener una operación confiable y sin interrupciones de su red, debe poner mucha atención a estos archivos, para garantizar que se usen las versiones adecuadas y que se creen todas las copias de respaldo que sean necesarias.

El IOS se guarda en un área denominada memoria flash. La memoria flash provee almacenamiento no volátil de una imagen del IOS, la cual se puede usar como sistema operativo en el arranque. El uso de memoria flash permite la actualización del IOS, y también guardar múltiples IOS. En muchas arquitecturas de router, el IOS es copiado a la memoria RAM y se ejecuta desde allí.

Una copia del archivo de configuración se guarda en la RAM no volátil (NVRAM), para ser utilizada como configuración en el arranque. A dicha copia se le denomina "startup config" o configuración de arranque. la configuración de arranque es copiada a la RAM durante el arranque. Una vez en la RAM, es la que se pone en uso para la operación del router. Se le denomina "running config" o configuración en uso.

A partir de la versión 12, el IOS provee una interfaz única a todos los sistemas de archivos que utiliza el router. A dicha interfaz se le denomina sistema de archivos del Cisco IOS (IFS). El IFS provee un método unificado para administrar el sistema de archivos que utilizan los routers. Esto incluye los sistemas de archivos de la memoria flash, los sistemas de archivos de red (TFTP, rcp y FTP) y la lectura o escritura de datos (de o a la NVRAM, de la configuración en uso, de la ROM). El IFS usa un conjunto común de prefijos para especificar los dispositivos del sistema de archivos.

El IFS usa la convención URL para especificar archivos en los dispositivos de red y la red. La convención URL identifica la ubicación de los archivos de configuración mediante el esquema [[[//location]/directory]/filename], luego de dos puntos. El IFS también permite la transferencia de archivos mediante FTP.

8.2. Etapas de la secuencia de arranque del router

El objetivo de las rutinas de arranque del software Cisco IOS es activar el funcionamiento del router. El router debe proveer un rendimiento confiable en lo que respecta a sus funciones de interconexión de redes. Para lograrlo, las rutinas de inicio deben efectuar lo siguiente:

- Comprobar el hardware del router.
- Encontrar y cargar el software Cisco IOS.
- Encontrar y ejecutar los comandos de configuración, que abarcan las funciones de protocolo y las direcciones de las interfaces.

8.3. Mecanismo de ubicación y carga del software Cisco IOS

La fuente predefinida del Cisco IOS depende de la plataforma de hardware, pero por lo general el router busca los comandos boot system almacenados en la NVRAM. El Cisco IOS permite varias alternativas. Se puede especificar otras fuentes del software, o el router puede usar su propia secuencia de reserva o alterna para cargarlo.

Los valores particulares del registro de configuración permiten las alternativas siguientes:

- Se puede especificar comandos boot system del modo de configuración global para introducir fuentes de reserva, a fin de que el router las utilice en forma secuencial. El router utiliza estos comandos según sea necesario, en forma secuencial, cuando arranca de nuevo.
- Si el router no encuentra comandos boot system en la NVRAM, el sistema, por defecto, usa el Cisco IOS que se encuentra en la memoria flash.
- Si no hay un servidor TFTP disponible, el router cargará una versión limitada del IOS almacenada en ROM.

8.3.1. Uso de los comandos boot system

Los siguientes ejemplos muestran el uso de diversos comandos boot system, los cuales especifican la secuencia de reserva o alterna para el arranque del Cisco IOS. Los tres ejemplos muestran valores del boot system los cuales especifican que la imagen del Cisco IOS sea cargada en primer lugar desde la memoria flash, luego desde un servidor de red y, por último, desde la ROM:

- **Memoria flash:** Se puede cargar una imagen del sistema desde la memoria flash. Tiene la ventaja de que la información en la memoria flash no se ve afectada por fallas en la red, las cuales sí afectan la carga de imágenes del sistema desde servidores TFTP.

- **Servidor de red:** En caso de que el contenido de la memoria flash esté dañado, se puede cargar una imagen del sistema desde un servidor TFTP.

- **ROM:** Si la memoria flash está dañada y tampoco se puede cargar la imagen desde un servidor, la opción final programada es arrancar desde la ROM. Sin embargo, es probable que la imagen del sistema en la ROM sea sólo una porción del software Cisco IOS, y que no incluya los protocolos, las funciones y las configuraciones del Cisco IOS completo. Además, si el software se ha actualizado desde que se adquirió el router, la versión en la ROM puede ser más antigua.

El comando **copy running-config startup-config** guarda los comandos en la NVRAM. El router ejecutará los comandos boot system según lo requiera, en el orden en el que se introdujeron originalmente al hacer la configuración.

8.3.2. Registro de configuración

El valor del campo de arranque del registro de configuración determina el orden en el cual el router busca la información de arranque del sistema. Los valores por defecto del registro de configuración se pueden cambiar con el comando config-register del modo de configuración global. El argumento de este comando es un número hexadecimal.

El registro de configuración en la NVRAM es de 16 bits. Sus cuatro bits inferiores (un dígito hexadecimal) conforman el campo de arranque. Para garantizar que el valor de los 12 bits superiores se conserve, primero debe recuperarse el valor en uso del registro de configuración, mediante el comando show version. Luego ejecute el comando config-register, con las modificaciones del valor del último dígito hexadecimal.

Para cambiar el campo de arranque del registro de configuración, siga estas pautas:

- Para ingresar al modo de monitor de la ROM, fije 0xnnn0 como el valor del registro de configuración, donde nnn representa el valor anterior de los dígitos del campo diferentes al de arranque. Este valor fija los bits del campo de arranque en 0000 binario. Arranque el sistema operativo manualmente.

- Para arrancar usando la primera imagen en memoria Flash, o para arrancar usando el IOS en memoria ROM (dependiendo de la plataforma), fije el registro de configuración en 0xnnn1, donde nnn representa el valor anterior de los dígitos del campo diferentes al de arranque. Este valor fija los bits del campo de arranque en 0001 binario. Plataformas previas, como los routers Cisco 1600 y 2500, arrancan usando una versión limitada del IOS ubicada en ROM. Plataformas mas recientes, como los Cisco 1700, 2600 y enrutadores de alta capacidad arrancarán usando la primera imagen en memoria Flash.

- Para configurar el sistema de modo que arranque automáticamente desde la NVRAM, fije el registro de configuración en cualquier valor entre 0xnnn2 y 0xnnnF, donde nnn representa el valor anterior de los dígitos del campo diferentes al de arranque. Estos valores fijan los bits del campo de arranque en un valor comprendido entre 0010 y 1111 binario.

8.4. Diagnóstico de fallas en el arranque del Cisco IOS

Si el router no arranca correctamente, eso puede deberse a fallas en alguno de estos elementos:

- El archivo de configuración incluye comandos boot system incorrectos
- El valor del registro de configuración es erróneo.
- La imagen en la flash está dañada.
- Hay una falla de hardware.

En el arranque, el router busca comandos boot system en el archivo de configuración. Los comandos boot system pueden forzar el arranque del router desde una imagen del IOS diferente a la que está en la flash. Para identificar la fuente de la imagen de arranque, ejecute el comando show version y busque la línea que identifica la fuente.

Ejecute el comando show running-config y busque el comando boot system cerca de la parte superior de la configuración. Si el comando boot system señala una imagen del IOS incorrecta, elimine el comando mediante la versión "no" de dicho comando.

Un valor erróneo del registro de configuración evita que el IOS se cargue desde la flash. El valor del registro de configuración le indica al router la fuente del IOS. Esto se puede confirmar al ejecutar el comando show version. Busque en la última línea el registro de configuración. El valor correcto varía de una plataforma de hardware a otra. Una de las partes de la documentación de la red debe ser una copia impresa del resultado de show version. Si dicha documentación no está disponible, en el CD de documentación de Cisco o en el sitio Web de Cisco se proveen recursos para identificar el valor correcto del registro de configuración. Para hacer correcciones, se debe cambiar el registro de configuración en la configuración, para luego guardarla como la configuración de arranque.

8.5. TFTP

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un Terminal X Window o cualquier otro cliente ligero inicia desde un servidor de red.

8.5.1. Algunos detalles del TFTP:

- Utiliza UDP (puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).
- No puede listar el contenido de los directorios.
- No existen mecanismos de autentificación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.

- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

8.5.2. Detalles de una sesion TFTP.

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

- La máquina A, que inicia la comunicación, envía un paquete RRQ (*read request*/petición de lectura) o WRQ (*write request*/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.

- B responde con un paquete ACK (*acknowledgement*/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.

- La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.

- El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

8.5.3. Configurar TFTP para clientes

Para permitir a los clientes usar el servidor TFTP, debe asegurarse de que el perfil QTFTP posee autorización para acceder a los directorios y archivos a los que accederán los clientes por medio del servidor TFTP. También tendrá que establecer los atributos del servidor TFTP para permitir las peticiones de los clientes que desee.

Al configurar TFTP para que lo utilicen los clientes, primero debe determinar los directorios y los archivos que van a utilizar los clientes. En este ejemplo, los clientes emplean el servidor TFTP para leer archivos del directorio /netpc/bin/system.

- Utilice el mandato MKDIR con el argumento /netpc para crear el directorio /netpc, de la siguiente manera:
- MKDIR (netpc)
- Especifique el mandato WRKLNK con el argumento /netpc, de esta manera:
- WRKLNK (netpc)
- Especifique la opción 9 para visualizar las autorizaciones actuales.
- Para los usuarios *PUBLIC, especifique la opción 2, Cambiar autorización de usuario, e indique *NONE para las nuevas autorizaciones sobre datos. Así se asegura que el archivo no queda abierto para uso público.

- Para añadir un usuario en el menú Trabajar con autorización, especifique estos valores en la primera línea: 1 para Opc, QTFTP para Usuario, y *RX para Autorización sobre datos. Pulse Intro.
- Pulse la tecla F5 para renovar el menú. Verá el ID de usuario *PUBLIC con la autorización *EXCLUDE sobre datos, el ID de usuario QTFTP con la autorización *RX sobre datos, y su propio ID de usuario con la autorización *RWX sobre datos.

Utilice el mandato MKDIR para crear los siguientes directorios:
/netpc/bin
/netpc/bin/system

Cada directorio hereda la autorización de su directorio padre, y el propietario se añade implícitamente como usuario con la autorización *RWX. Los archivos que el cliente vaya a solicitar, cópielos en el subdirectorio netpc/bin/system. Los archivos se pueden copiar de varias maneras, como utilizando el mandato COPY, el protocolo de transferencia de archivos (FTP) o Client Access/400. Debe asegurarse de que el perfil QTFTP posee la autorización *R sobre cada archivo que vaya a solicitar el cliente.
Para establecer las autorizaciones sobre los archivos, emplee el mandato WRKLNK y la opción 9,

- Especifique el mandato CHGTFTPA y pulse la tecla F4.
- Cambie el directorio fuente alternativo por /netpc/bin/system y pulse Intro. Ello permitirá al servidor TFTP solicitar archivos que tengan los debidos valores de autorización, incluyendo el directorio /netpc/bin/system en su vía.
- Para que los cambios entren en vigor, detenga el servidor TFTP con el mandato ENDTCPSVR *TFTP y reinicielo con el mandato STRTCPSVR *TFTP.

8.5.4. Cambiar los atributos de TFTP

EL comando Cambiar atributos TCP/IP de TFTP (CHGTFTPA) le permite cambiar los atributos del servidor TFTP. A continuación se indican dos maneras distintas de acceder al indicador de este comando y especificar el mandato CHGTFTPA. y seleccionar la opción 3 en la pantalla Configurar aplicaciones TCP/IP (CFGTCPAPP).

Nota: Deberá poseer la autorización especial *IOSYSCFG si desea hacer cambios en los atributos de TFTP con el mandato CHGTFTPA.

Un cliente puede terminar la transferencia en cualquier momento si envía un ACK correspondiente al último bloque o si envía un paquete de error (ERR). El cliente puede terminar esta transferencia sea o no el cliente maestro.

Nota: La opción de difusión general de subred de TFTP se ha diseñado para mejorar la transferencia simultánea de archivos de gran tamaño a múltiples clientes situados en una subred común. Esta opción no sirve de ayuda cuando los archivos solo necesitan pocos bloques para transferirse o cuando se transfiere a clientes individuales.

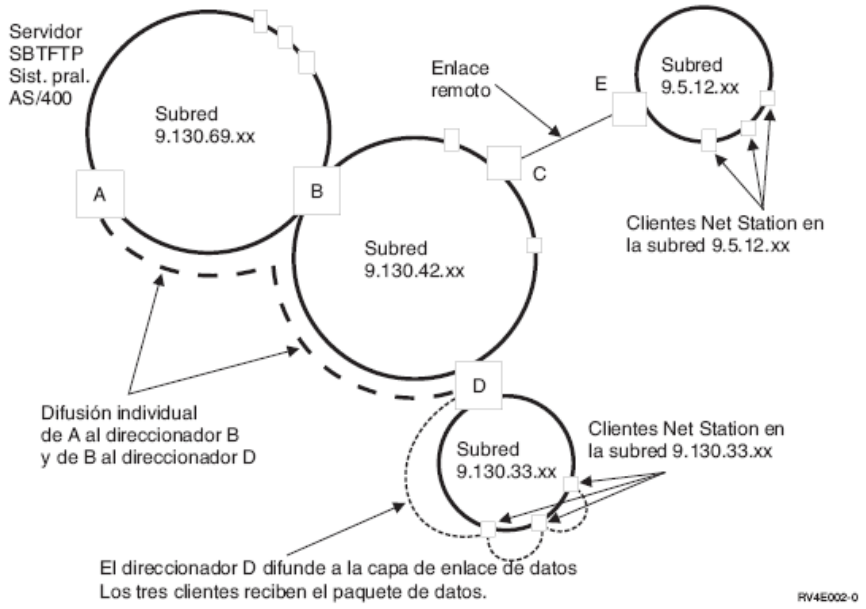


Figura 8.1 *Transferencia de archivos a través de una subred a un servidor TFTP.*

8.6. Administración de imágenes del IOS y archivos de configuración mediante TFTP.

Ocasionalmente, es necesario actualizar o restaurar el IOS del router. Al recibir un router, se debe realizar una copia de respaldo del IOS. Esta imagen del IOS se puede guardar en un servidor central junto con otras imágenes del IOS. Éstas se pueden usar para restaurar o actualizar el IOS de los routers y switches de la red.

Dicho servidor debe tener un servicio TFTP activo. El respaldo del IOS se puede iniciar desde el modo EXEC privilegiado, mediante el comando copy flash tftp.

Se puede recargar desde el servidor el IOS en su misma versión, o una superior, con el comando copy tftp flash. De nuevo, el router le solicitará al usuario que introduzca la dirección de IP del servidor TFTP. Cuando se le solicite el nombre de archivo de la imagen del IOS en el servidor, el router puede solicitar que se borre la memoria flash. Esto sucede a menudo cuando no hay suficiente memoria flash disponible para la nueva imagen. A medida que la imagen es borrada de la memoria flash, se mostrará una serie de “e’s” que indican el avance del proceso.

8.6.1. Configuración del router

Los pasos a continuación describen este proceso:

- Ejecute el comando copy tftp running-config.

- Cuando aparezca el indicador, seleccione un archivo de configuración de host o de red.
- Cuando aparezca el indicador del sistema, introduzca la dirección de IP del servidor TFTP en el que se encuentra el archivo de configuración.
- Cuando aparezca el indicador del sistema, introduzca el nombre del archivo de configuración o acepte el nombre por defecto.

Confirme el nombre del archivo de configuración y la dirección del servidor que suministra el sistema.

A medida que se descarga cada uno de los archivos de imagen del IOS, se mostrará un signo de exclamación "**!**". La imagen del IOS es de varios megabytes y su descarga puede tomar bastante tiempo.

La nueva imagen en la flash se debe verificar luego de la descarga. Ahora el router está listo para ser cargado de nuevo, y para utilizar la nueva imagen del IOS.

8.7. Administración de imágenes del IOS mediante Xmodem

Si la imagen del IOS de la flash se ha borrado o dañado, es posible que se deba restaurar el IOS desde el modo de monitor de la ROM (ROMmon). En muchas de las arquitecturas de hardware de Cisco, el modo ROMmon se indica mediante el indicador rommon 1 >.

El primer paso de este proceso es determinar por qué la imagen del IOS no se cargó desde la flash. La causa puede ser una imagen dañada o ausente. La flash se debe examinar usando el comando dir flash.
Si la imagen que se ha ubicado parece ser válida, se debe intentar arrancar desde esa imagen. Esto se hace mediante el comando boot flash: Por ejemplo, si el nombre de la imagen es "c2600-is-mz.121-5", el comando sería:

```
rommon 1>boot flash:c2600-is-mz.121-5
```

Si el router arranca correctamente, es necesario examinar varios elementos a fin de determinar por qué el router arrancó mediante ROMmon y no lo hizo automáticamente. En primer lugar, ejecute el comando show version para verificar el registro de configuración y asegurarse que esté configurado para la secuencia de arranque por defecto. Si el valor del registro de configuración es correcto, ejecute el comando show startup-config para ver si hay algún comando del sistema de arranque que le indique al router que debe usar el IOS del monitor de la ROM.
Si el router no arranca correctamente desde la imagen o si no existe ninguna imagen del IOS, es necesario descargar un nuevo IOS. El archivo del IOS se puede recuperar mediante Xmodem, para restaurar la imagen a través de la consola o mediante TFTP en el modo ROMmon.

8.7.1. Descarga mediante Xmodem en el modo ROMmon

Para restaurar el IOS a través de la consola, la PC local debe tener una copia del archivo del IOS a ser restaurado, y un programa de emulación de terminal como, por

ejemplo, HyperTerminal. El IOS se puede restaurar a la velocidad por defecto de la consola, 9600 bps. Se puede cambiar a 115200 bps para agilizar la descarga. La velocidad de la consola se puede cambiar en el modo ROMmon, mediante el comando confreg. Al ejecutar el comando confreg, el router solicitará los diversos parámetros modificables.
Cuando se le solicite "change console baud rate? y/n [n]:" si selecciona y aparecerá un indicador para seleccionar la nueva velocidad. Una vez que ha cambiado la velocidad de la consola y reiniciado el router en el modo ROMmon, se debe cerrar la vieja sesión (a 9600) e iniciar una nueva a 115200 bps, la nueva velocidad de la consola.

El comando Xmodem se puede ejecutar desde el modo ROMmon para restaurar la imagen del software IOS desde la PC. El formato del comando es xmodem -cnombre_del_archivo. Por ejemplo, para restaurar un archivo de imagen del IOS de nombre "c2600-is-mz.122-10a.bin", ejecute el comando:
xmodem -c c2600-is-mz.122-10a.bin

La -c le indica al proceso Xmodem que debe usar verificación de redundancia cíclica (CRC) para detectar errores durante la descarga.
El router no inicia la transferencia de inmediato, sino que le muestra un mensaje de advertencia. El mensaje le informa que la bootflash será borrada y le pregunta si desea continuar. Una vez que se acepta el continuar, el router le indica que puede iniciar la transferencia.

Ahora se requiere iniciar una transferencia Xmodem desde el emulador de terminal. En HyperTerminal, seleccione Transfer > Send File (Transferir > Enviar archivo). Luego, al aparecer la ventana Send File (Enviar archivo), indique el nombre y la ubicación de la imagen. Seleccione Xmodem como el protocolo e inicie la transferencia. Durante la transferencia, la ventana Sending File (Enviando archivo) mostrará el estado de la transferencia.
Al finalizar la transferencia, aparecerá un mensaje que indica que la flash ha sido borrada. Luego aparece el mensaje "Download Complete!" (¡Ha finalizado la descarga!). Antes de arrancar de nuevo el router, es necesario volver a fijar la velocidad de consola en 9600 y el config register a 0x2102. Ejecute el comando config-register 0x2102 luego del indicador EXEC privilegiado.

Mientras el router arranca de nuevo, es necesario finalizar la sesión de terminal a 115200 bps e iniciar una nueva a 9600 bps.

CAPÍTULO 9

ACL
(LISTAS DE ACCESO)

9. ACL -LISTAS DE ACCESO-

Una Lista de Control de Acceso o ACL (del inglés, *Access Control List*) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en ISDN.

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos. Aunque las herramientas de seguridad, como por ejemplo: las contraseñas, equipos de callback y dispositivos de seguridad físico, son de ayuda, a menudo carecen de la flexibilidad del filtrado básico de tráfico y de los controles específicos que la mayoría de los administradores prefieren. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero impedir a los usuarios externos el acceso telnet a la LAN.

Las ACL se definen según el protocolo, la dirección o el puerto, (Ver figura 9.1). Para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz. Las ACL controlan el tráfico en una dirección por vez, en una interfaz. Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente. Finalmente, cada interfaz puede contar con varios protocolos y direcciones definidas. Si el router tiene dos interfaces configuradas para IP, AppleTalk e IPX, se necesitan 12 ACLs separadas. Una ACL por cada protocolo, multiplicada por dos por dirección entrante y saliente, multiplicada por dos por el número de puertos.

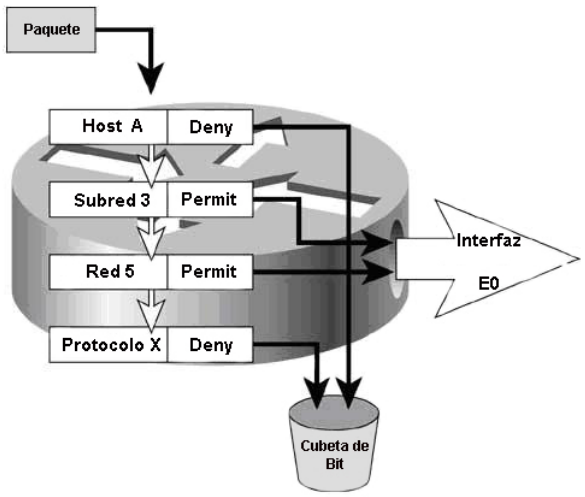


***Figura 9.1**. Una access list es una lista secuencial de filtros, cada uno define un conjunto de criterio y una acción*

9.1. Razones para crear una ACL.

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red. Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.
- Si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

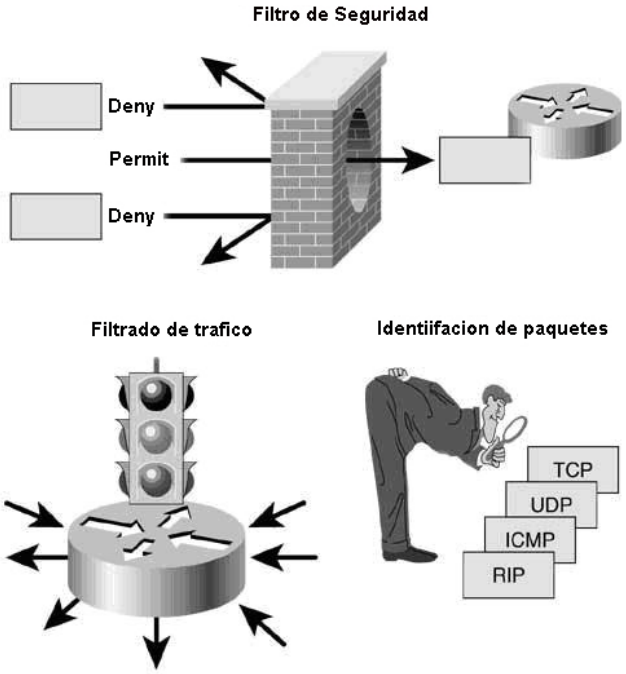


***Figura 9.2**. Las access list son usadas como filtros de seguridad, como filtros de tráfico, y para identificación de paquetes*

9.2. Funcionamiento de las ACL

El orden en el que se ubican las sentencias de la ACL es importante (Ver figura 9.3). El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

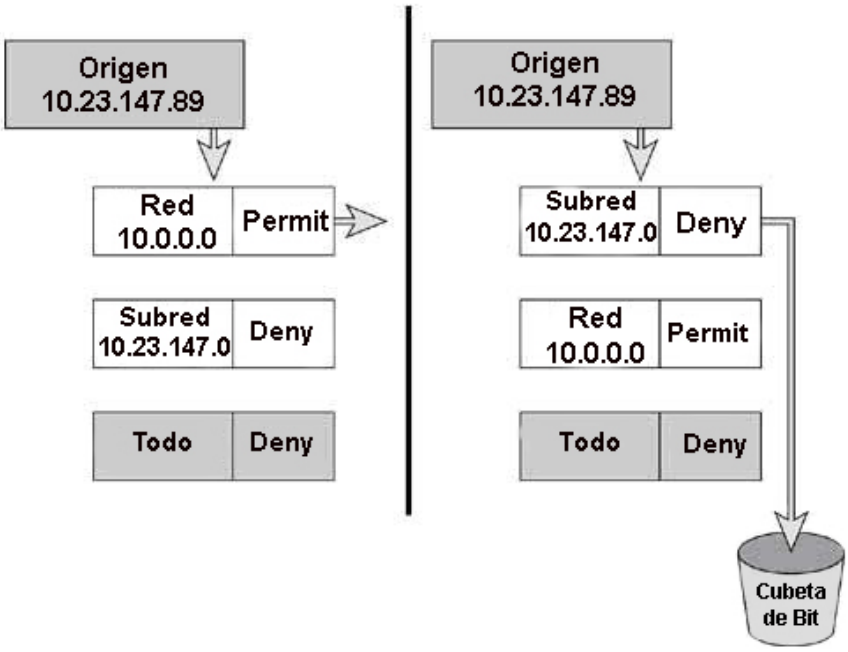


Figura 9.3 *Si la capa de un filtro individual de una access list no es configurada en la secuencia correcta, la access list no funcionará correctamente.*

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A medida que una trama ingresa a una interfaz, el router verifica si la dirección de Capa 2 concuerda o si es una trama de broadcast. Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante. Si existe una ACL, entonces se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete cumple las condiciones, se lleva a cabo la acción de aceptar o rechazar el paquete. Si se acepta el paquete en la interfaz, se lo compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. A continuación, el router verifica si la interfaz destino tiene una ACL. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se lleva a cabo la aceptación o el rechazo del paquete. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de Capa 2 y se envía por la interfaz hacia el dispositivo siguiente. (Ver figura 9.4)

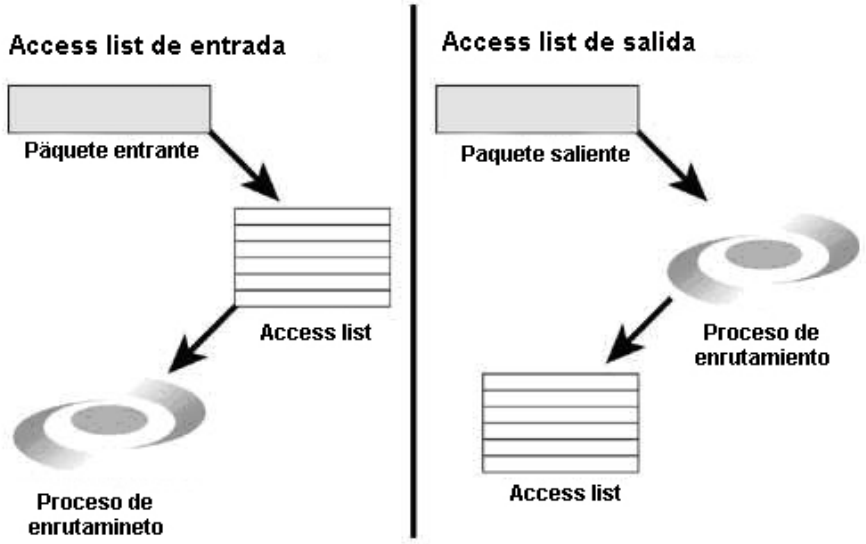


Figura 9.4 *El filtrado de paquetes entrantes es invocado antes del proceso de enrutamiento, mientras que el filtro de paquetes salientes es invocado después del proceso de enrutamiento*

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto.

9.3. Reglas para aplicar y crear una ACL.

- Una lista de acceso por protocolo y por dirección.
- Se deben aplicar las listas de acceso estándar que se encuentran lo más cerca posible del destino a restringir. (Ver figura 9.5 (a))
- Se deben aplicar las listas de acceso extendidas que se encuentran lo más cerca posible del origen a restringir. (Ver figura 9.5 (b))

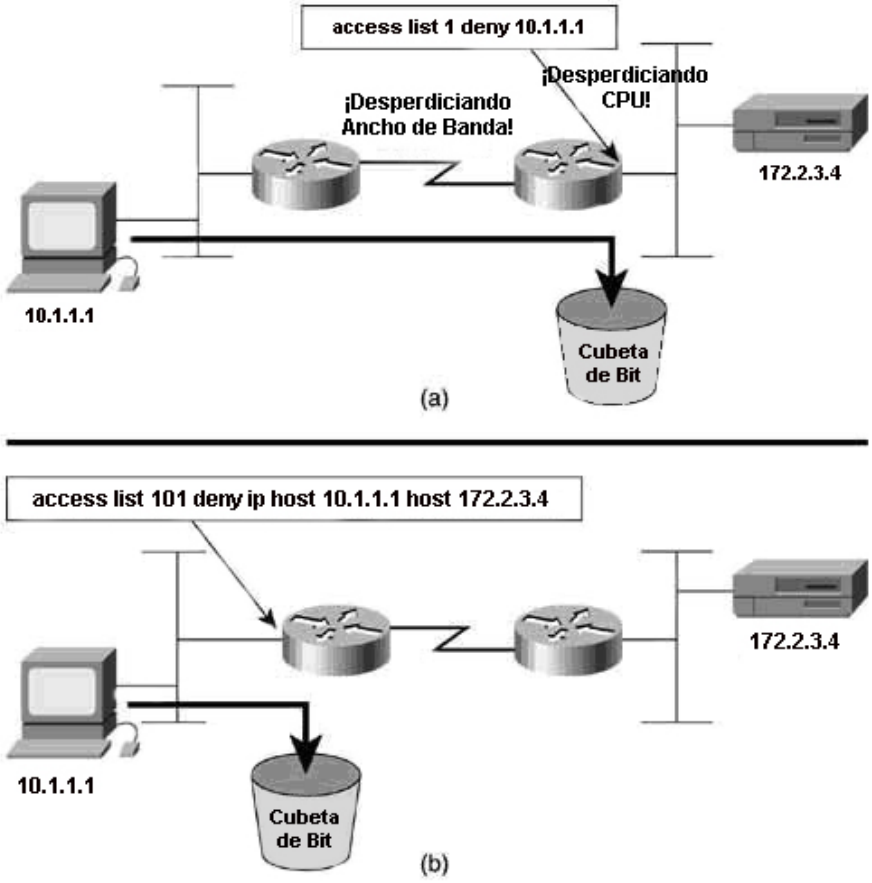


Figura 9.5 *Los filtrados que usan una access list estandar generalmente deben estar en el lugar cerca del destino (a), mientras que una access list extendida puede estar lo mas cerca del origen (b).*

- Utilice la referencia de la interfaz entrante y saliente como si estuviera mirando el puerto desde adentro del router.
- Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
- Hay un **deny any** (denegar cualquiera) implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.(Ver figura 9.6)

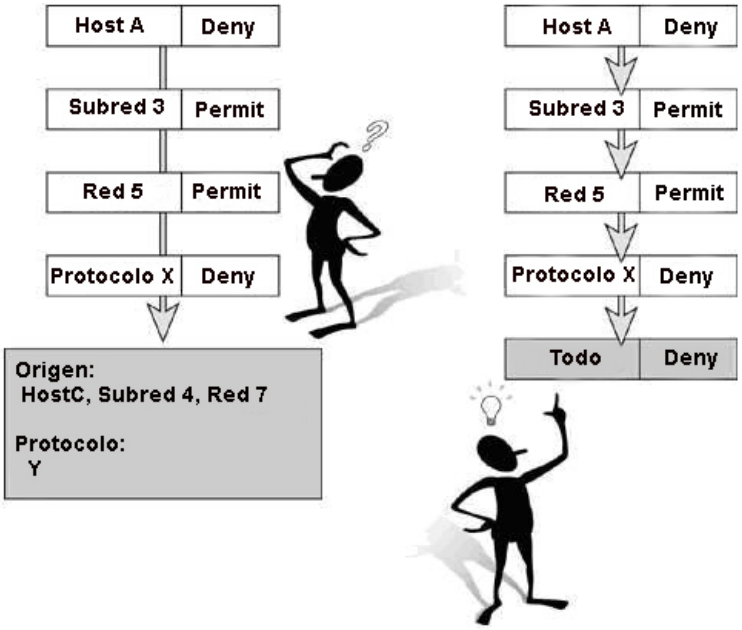


Figura 9.6 *Todas las access list finalizan con un deny any implícito, el cual descarta todos los paquetes que no corresponde con la línea de la lista.*

- Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específico y por último los grupos o filtros generales.
- Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
- Nunca trabaje con una lista de acceso que se utiliza de forma activa.
- Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
- Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando **no access-list** *x* elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.
- Una lista de acceso IP envía un mensaje ICMP llamado de host fuera de alcance al emisor del paquete rechazado y descarta el paquete en la papelera de bits.
- Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una deny any (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
- Los filtros salientes no afectan al tráfico que se origina en el router local.

9.4. Tipos de ACL.

9.4.1. ACL Estándar.

Las ACL estándar verifican la dirección origen de los paquetes IP que se deben enrutar. Con la comparación se permite o rechaza el acceso a todo un conjunto de protocolos, según las direcciones de red, subred y host. Por ejemplo, se verifican los paquetes que vienen en Fa0/0 para establecer la dirección origen y el protocolo. Si se les otorga el permiso, los paquetes se enrutan a través del router hacia una interfaz de salida. Si se les niega el permiso, se los descarta en la interfaz entrante.

9.4.2. ACL Extendidas.

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar porque ofrecen un mayor control. Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos y números de puerto. Esto ofrece mayor flexibilidad para establecer qué verifica la ACL. Se puede permitir o rechazar el acceso de los paquetes según el lugar donde se originó el paquete y su destino así como el tipo de protocolo y direcciones de puerto. Una ACL extendida puede permitir el tráfico de correo electrónico de Fa0/0 a destinos específicos S0/0, al mismo tiempo que deniega la transferencia de archivos y la navegación en la red. Una vez descartados los paquetes, algunos protocolos devuelven un paquete al emisor, indicando que el destino era inalcanzable.

Al final de la sentencia de la ACL extendida, se obtiene más precisión con un campo que especifica el Protocolo para el control de la transmisión (TCP) o el número de puerto del Protocolo de datagrama del usuario (UDP). Las operaciones lógicas pueden especificarse como igual (eq), desigual (neq), mayor a (gt) y menor a (lt) aquéllas que efectuarán las ACL extendidas en protocolos específicos. Las ACL extendidas utilizan el número de lista de acceso entre 100 y 199 (también entre 2000 y 2699 en IOS recientes).

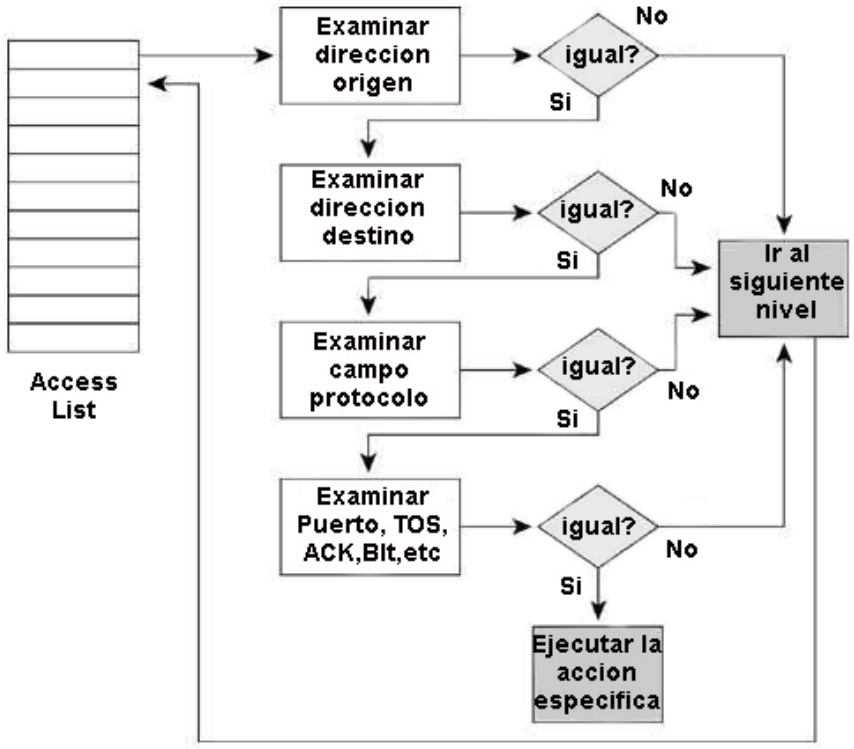


Figura 9.7 *Flujo de decisión de una access list extendida.*

9.5. Sintaxis de la listas de acceso.

9.5.1. Sintaxis de las listas de acceso estándar (Standar ACLs):

access-list número_identificador [permit|deny] condición

9.5.2. Sintaxis de las listas de acceso extendidas (extended ACLs):

- **Para el protocolo IP:**

access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

- **Para el protocolo ICMP:**

access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} icmp source source-wildcard destination destination-wildcard [icmp-type | [[icmp-type icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

- **Para el protocolo TCP:**

access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

- **Para el protocolo UDP:**

access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} udp source source-wildcard [operator [port]] destination destination wildcard [operator [port]] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

9.5.3. Aplicar una access list a una interfaz

interface tipo_de_interfaz #
ip access-group *número* [in | out]

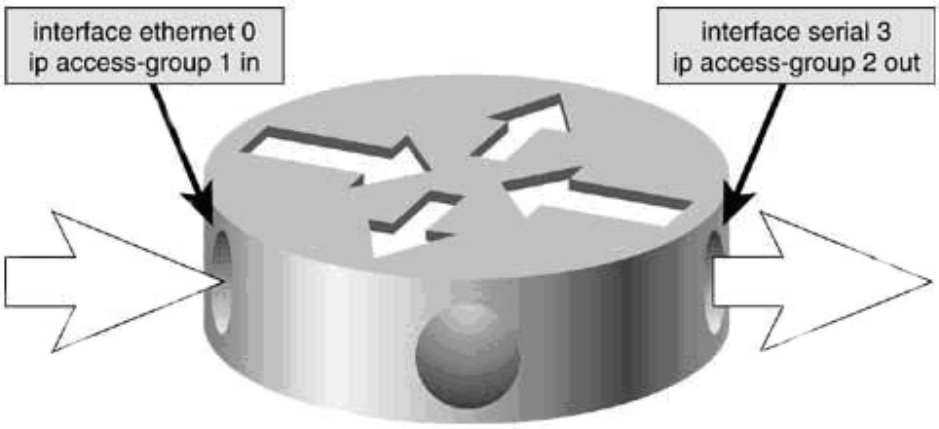


Figura 9.8 *El comando ip access-group usa una access list específica al crear un filtro sobre una interfaz para uno u otro entrada o salida de paquetes.*

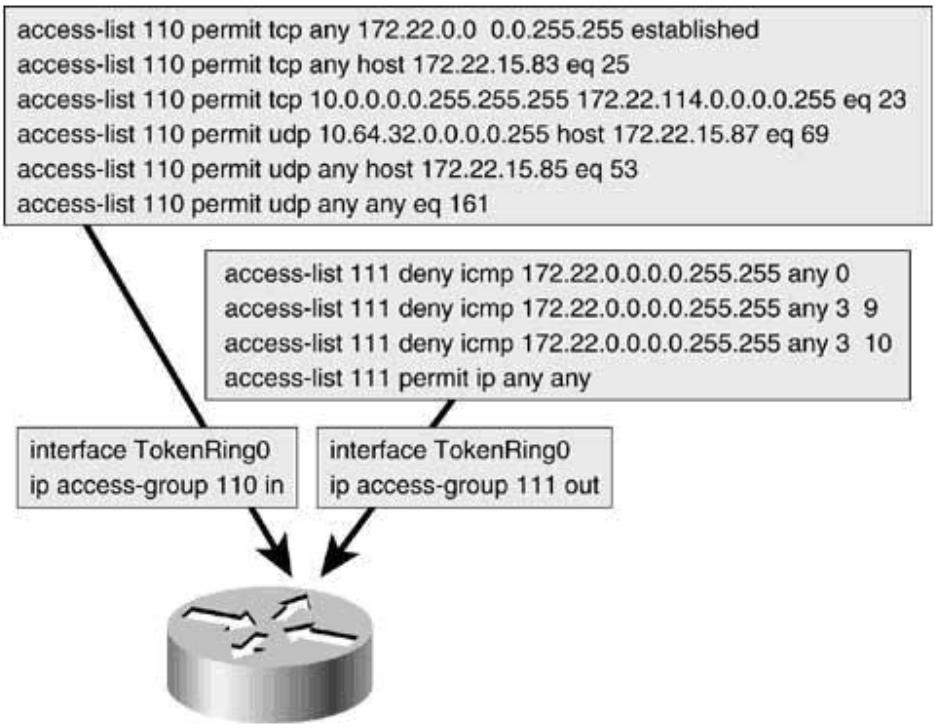


Figura 9.9 *La access list 110 es usada por el filtro de entrada de paquete sobre la interfaz token ring. La access list 111 es usada en el filtrado de paquetes de salida sobre la misma interfaz.*

9.6. Máscara Wildcard.

Una máscara wildcard es sencillamente una agrupación de 32 bits dividida en cuatro bloques de ocho bits cada uno (octetos). La apariencia de una máscara wildcard le recordara probablemente a una máscara de subred. Pero no existe relación.

Las máscaras wildcard se emplean junto con un valor IP para seleccionar direcciones IP, esto es así gracias a que la máscara wildcard indica con sus ceros y sus unos qué bits han de compararse o no. Un cero indica que el bit ha de compararse y un uno indica que se ignore.

Por lo general las máscaras wildcard se utilizan en el protocolo de enrutamiento OSPF y en el cálculo de las Listas de Acceso (ACL) para especificar que redes/subredes/host intervienen en las ACLs.

Por ejemplo, suponga que empleamos la IP 192.168.1.0 junto con la máscara wildcard 0.0.0.255 para seleccionar direcciones IP. Los ceros nos están diciendo que debemos comparar los valores de los tres primeros octetos y los unos del cuarto octeto nos dice que da igual que valor tenga dicho octeto.

Por tanto, quedarán seleccionados valores como:

192.168.1.1

192.168.1.23

192.168.1.145

Y se quedarán descartadas IP como:

192.168.2.145

100.168.1.0

192.167.1.76

Es decir, con la máscara wildcard 0.0.0.255 todas las IPs que se seleccionen deberán tener los tres primeros octetos de la forma 192.168.1, en tanto que el cuarto octeto, como queda oculto por los unos de la máscara, puede tomar cualquier valor.

Suponga que tenemos la máscara wildcard 0.0.255.255 y la IP 10.1.0.0, ¿qué valores de la siguiente lista se seleccionarán?

10.1.1.1	**10.2.1.1**	**20.1.0.1**	**10.1.255.255**	**10.10.0.1**
10.1.20.2	**11.1.3.2**	**100.1.0.0**	**10.10.1.1**	**10.3.0.1**

En efecto, las IPs seleccionadas son:

10.1.1.1 10.1.255.255 10.1.20.2

Las IPs seleccionadas deberán tener los dos primeros octetos de la forma 10.1, mientras que no importa qué valores ocupen las posiciones de los octetos tercero y cuarto.

Sin embargo, no todas las máscaras wildcard se interpretan tan rápidamente. Hasta ahora hemos visto ejemplos en los que los octetos o bien tenían todos sus bits a cero o bien a uno.

Supongamos ahora una máscara wildcard de la forma 0.0.0.15 asociada con la IP 192.168.1.48, ¿qué IPs quedarán seleccionadas?

Es fácil ver que los tres primeros octetos habrán de ser de la forma 192.168.1.
Respecto al cuarto octeto de la máscara wildcard observe que su expresión binaria es:

0000 1111

Es decir, no debemos tener en cuenta el valor de los últimos cuatros bits a la hora de compararlo con el número 48, que en binario se escribe como:

0011 0000

Analicemos, por ejemplo, si la IP 192.168.1.51 es seleccionada. Observe que 51 se escribe como:

0011 0011

Al aplicar la máscara wildcard, ignoramos el valor de los últimos cuatros bits:

0011 ~~0011~~

Fíjese que al ignorar el valor de estos bits el número resultante es 48 y por tanto la IP sí es seleccionada. Es fácil ver la lista de valores que serán seleccionados, basta con calcular el valor de las combinaciones de la

0011 0000

Hasta la

0011 1111

Es decir, desde la IP 192.168.1.48 hasta la 192.168.1.63. en resumen, la IP 192.168.1.48 con máscara wildcard 0.0.0.15 selecciona un rango de direcciones IP.

Una aplicación fundamental de la máscara wildacard es en el uso al redactar ACL. Las ACL son filtros de paquetes IP y permite aceptar o descartar paquetes en función de la IP de origen (ACL estándar) o bien en función de la IP de origen, IP destino y protocolo (tcp, udp, icmp,) (ACL extendidas). Como ha visto por los ejemplos anteriores, las máscaras wildacard nos van a permitir seleccionar rangos IPs.

9.6.1. Aplicando máscaras wildcard.

Ejemplo 1.

Dada la siguiente IP y máscara wildcard

IP	202	20	0	0
Máscara Wildcard	0	0	255	255

Decir qué IPs quedarán seleccionadas de entre las siguientes: **202.20.2.1, 102.20.0.0** y **202.20.22.0**

Solución:

En este caso, la máscara wildcard nos obliga a comparar los dos primeros octetos, que habrán de ser por tanto de la forma 202.20. Los dos últimos octetos son ignorados de modo que pueden tomar valores cualesquiera, las IPs seleccionadas serán:

202.20.2.1 202.20.22.0

Ejemplo 2

Aquí tomaremos la IP 172.16.0.0 con máscara wildcard 0.0.127.255 y la aplicaremos sobre las siguientes IPs: 172.16.130.1, 121.0.127.2 y 172.16.15.253.
Tras realizar el ejercicio, interpretaremos el siguiente significado de esta máscara-

La información más directa que podemos sacar de la IP 172.16.0.0 con máscara 0.0.127.255, es que los dos primeros octetos habrán de ser de la forma 172.16 y el último podrá tomar cualquier valor.

Es claro, por consiguiente, que la IP 121.0.127.2 queda descartada.

Estudiemos ahora qué ocurre en el tercer octeto. Para ello es útil escribirlo en forma binaria:

IP	**172**	**16**	**0**	**0**
Máscara Wildcard	**0**	**0**	**0111 1111**	**255**

El significado de esta máscara es que sólo se comparará el primer bit de tercer octeto, los demás serán ignorados. Al aplicar esta máscara sobre las dos IPs que nos quedan obtenemos:

IPs				
172.16.130.1	**172**	**16**	**1000 0010**	**1**
172.16.15.253	**172**	**16**	**0000 1111**	**253**

Tenga en cuneta que el bit no tachado es el primero y que un 1 en esa posición corresponde con el valor decimal 128. así pues, al ignorar los bits que mostramos tachados las IPs resultados son:

IPs	**IPs+Máscara wildcard**			
172.16.130.1	**172**	**16**	**128**	**0**
172.16.15.253	**172**	**16**	**0**	**0**

Observe que sólo la última IP será seleccionada.

Fíjese también que los dígitos binarios de un octeto que comienzan por 0 (cero) representan la mitad inferior de los valores de ese octeto: del 0 al 127. Los que comienzan por uno suponen la mitad superior del octeto: del 128 al 255.

Por tanto, la máscara wildcard del ejemplo anterior (0.0.127.255) estaría seleccionando la mitad inferior de las direcciones IP de la red 172.16.0.0/16.

La posibilidad de seleccionar partes de una red es muy interesante a la hora de establecer criterios de seguridad en una red. Por ejemplo, podríamos estar interesados

en dar permiso sólo a una parte de los host de una LAN para acceder a un determinado servidor.

Ejemplo 3

Cree una máscara wildcard para seleccionar los valores pares (par en el cuarto octeto) de las IPs correspondientes a la red 180.42.111.0/24.

Solución:

Lo que ya sabemos es la estructura de los tres primeros octetos:

180.42.111. -

Con máscara wildcard:

0.0.0.–

Respecto al cuarto octeto, observe en la tabla que las IPs expresadas en binario terminan siempre en cero cunado son valores pares. Una vez que nos percatamos de cuál es le patrón común el ejercicio está prácticamente resuelto.

IPs	**IPs con el cuarto octeto en binario**	
180.42.111.0	180.42.111	0000 0000
180.42.111.1	180.42.111	0000 0001
…	…	…
180.42.111.126	180.42. 111	0111 1110
180.42.111.127	180 42 111	0111 1111
180.42.111.128	180.42.111	1000 0000
…	…	…
180.42.111.254	180 42 111	1111 1110
180.42.111.255	180.42.111	1111 1111

Puesto que en este caso el valor que tomen los siete primeros bits del cuarto octeto han de ser ignorados, la máscara wildcard los tachará.

Máscara wildcard			
0	0	0	1111 1110
0	0	0	254

Al ignorar los siete primeros octetos, las IPs de la red tomarán el valor 0 si son pares y el valor 1 si son impares (vea la tabla de abajo). Por tanto debemos escoger la IP 180.42.111.0 para realizar nuestra selección.

IPs	**IPs con el cuarto octeto en binario**	
180.42.111.0	180.42.111	~~0000 000~~0
180.42.111.1	180.42.111	~~0000 000~~1
…	…	…

180.42.111.126	180.42. 111	0111 1110
180.42.111.127	180 42 111	0111 1111
180.42.111.128	180.42.111	1000 0000
…	…	…
180.42.111.254	180 42 111	1111 1110
180.42.111.255	180.42.111	1111 1111

Resumiendo la IP 180.42.111.0 con máscara 0.0.0.254 selecciona las IPs con valores pares de la red 180.42.111.0/24.

CAPÍTULO 10

VLAN
(LAN VIRTUALES)

10. VLAN

Una **VLAN** (Virtual LAN, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de emisión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador).

Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración hardware.

Los primeros diseñadores de redes solían configurar VLANs con el objeto de reducir el tamaño del dominio de colisión en un único segmento Ethernet grande, mejorando así el rendimiento. Cuando los conmutadores Ethernet hicieron desaparecer este problema (porque separan dominios de colisión), el interés se desplazó a reducir el tamaño del dominio de difusión en la subcapa MAC (Control de Acceso al medio). Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN un método común de evitar tales medidas de seguridad.

Las VLANs funcionan en el nivel 2 (nivel de enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).
En el contexto de las VLANs, el término trunk ('tronco') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports ('puertos etiquetados') de dispositivos con soporte de VLANs, por lo que a menudo son enlaces conmutador a conmutador o conmutador a enrutador más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales»); Un enrutador (conmutador de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP también permite «podar», lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino. La necesidad de confidencialidad como así el mejor aprovechamiento del ancho de banda disponible dentro de la corporación ha llevado a la creación y crecimiento de las VLANs.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.

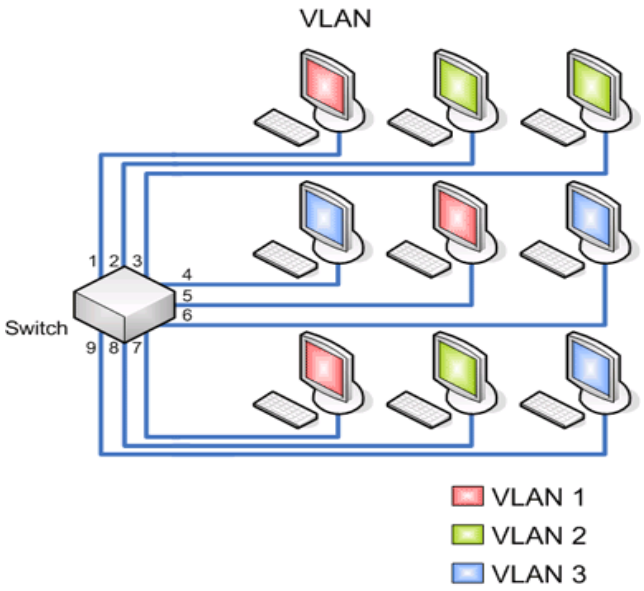


***Figura 10.1**. Representación de VLAN*

10.1. Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica micro segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

10.2. Tipos de VLANs.

10.2.1. VLAN de puerto central.

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

10.2.2. VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo. Estos pueden estar asignados por:

- Puerto
- Dirección MAC.
- Protocolo.
- Direcciones IP.
- Nombre de usuario.

10.2.3. VLANs Dinámicas.

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar a la red.

10.3. VTP (VLAN Trunk Ptotocol).

Cuando se configura VTP es importante elegir el modo adecuado, ya que VTP es una herramienta muy potente y puede crear problemas en la red. En un mismo dominio VTP la información de VLAN configurada en el servidor se transmite a todos los clientes.

- Su papel es mantener coherencia de configuración de VLAN en un dominio de administración común.
- Es un protocolo de mensajería.
- Utiliza las troncales de la capa 2 para administrar VLAN en un solo dominio:
  - Edición
  - Eliminación
  - Renombrado
- Permite cambios centralizados que se comunican a todos los switches de la red.

10.3.1. Modos de operación VTP

Modo Servidor.

El modo VTP predeterminado es el modo servidor. En modo servidor pueden crearse, modificar y suprimir VLAN y otros parámetros de configuración que afectan a todo el dominio VTP. En modo servidor, las configuraciones de VLAN se guardan en la memoria de acceso aleatoria no volátil (NVRAM). En este modo se envían y retransmiten avisos VTP y se sincroniza la información de configuración de VLAN con otros switches.

El modo servidor debe elegirse para el switch que se usará para crear, modificar o suprimir VLAN.

Modo cliente.

Un dispositivo que opera en modo VTP cliente no puede crear, cambiar ni suprimir VLAN. Un cliente VTP no guarda la configuración VLAN en memoria no volátil. Tanto en modo cliente como en modo servidor, los switches sincronizan su configuración VLAN con la del switch que tenga el número de revisión más alto en el dominio VTP. En este

modo se envían y retransmiten avisos VTP y se sincroniza la información de configuración de VLAN con otros switches.

El modo cliente debe configurarse para cualquier switch que se añada al dominio VTP para prevenir un posible reemplazo de configuraciones de VLAN.

Modo transparente.

Un switch que opera en VTP transparente no crea avisos VTP ni sincroniza su configuración de VLAN, con la información recibida desde otros switch del dominio de administración. Reenvía los avisos VTP recibidos desde otros switches que forman parte del mismo dominio de administración.

Un switch configurado en el modo transparente puede crear, suprimir y modificar VLAN, pero los cambios no se transmiten a otros switch del dominio, afectan tan solo al switch local.

El modo transparente debe usarse en un switch que necesite para avisos VTP a otros switches, pero que necesitan también capacidad para administrar sus VLAN independientemente. La pertenencia de los puertos de switch a las VLAN se asigna manualmente puerto a puerto (pertenencia VLAN estática o basada en puertos).

10.3.2. Pruning VTP.

Por defecto todas las líneas troncales transportan el tráfico de todas las Vlans configuradas. Algún tráfico innecesario podría inundar los enlaces perdiendo efectividad.

El recorte VTP permite determinar cual es el tráfico que inunda el enlace troncal evitando enviarlo a los switches que no tengan configurados puertos de la vlan destino. La Vlan1 es la vlan de administración y se utiliza para tareas de administración como las publicaciones VTP, no sera omitida por el Pruning VTP

Agrupa varios enlaces virtuales en un solo enlace físico.

Permite que el tráfico de varias VLAN viaje a través de un solo cable entre switches o entre switches y routers Un enlace troncal se puede comparar con las carreteras de distribución de una autopista.

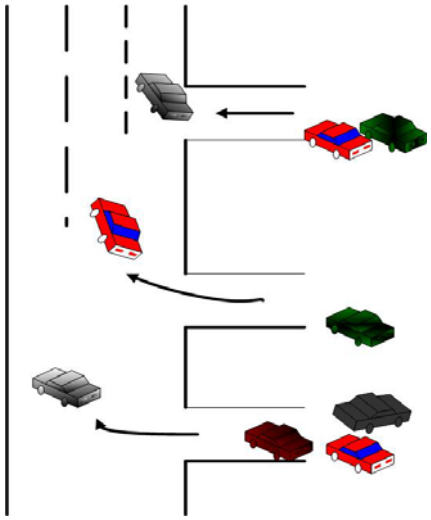


***Figura 10.2**. Pruning VLAN.*

10.3.3. Etiquetado de tramas.

- Tramas que se envían por enlaces se etiquetan para identificar VLAN a la que pertenecen.
- Existen varios esquemas de etiquetado comunes.
- Enlace inter-switch (ISL): Patentado por Cisco
- 802.1Q: Método Estándar del IEEE para insertar información de agrupación de VLAN en las tramas Ethernet.

10.3.4. Implementación de VTP

Peticiones de Publicación:

- Utilizadas por los clientes para solicitar información de la VLAN
- Servidores responden con publicaciones de resumen y de subconjunto.

Peticiones de Resumen:

- Emitidas por servidores y clientes cada cinco minutos.
- Informan a los switches vecinos lo que consideran como el número de revisión VTP actual.

Publicaciones de Subconjunto:

- Contienen información detallada sobre las VLAN: versión VTP, nombre de dominio y campos relacionados, número de revisión de configuración.
- Acciones que desencadenan estos mensajes:
  - Creación o eliminación de VLAN

- Suspensión o activación de VLAN
- Cambio de nombre de VLAN
- Cambio de unidad máxima de transferencia de VLAN.

10.4. Aspectos básicos de las VLANs.

Enlaces Troncales: Utilizados para interconectar dispositivos de VLAN que abarcan varios dispositivos.

- El enlace troncal transporta el tráfico para varias VLAN.
- Un enlace troncal puede conectar:
  - Un switch a otro switch
  - Un switch a un router
  - Un switch a un servidor instalando una NIC especial que admite enlace troncal.

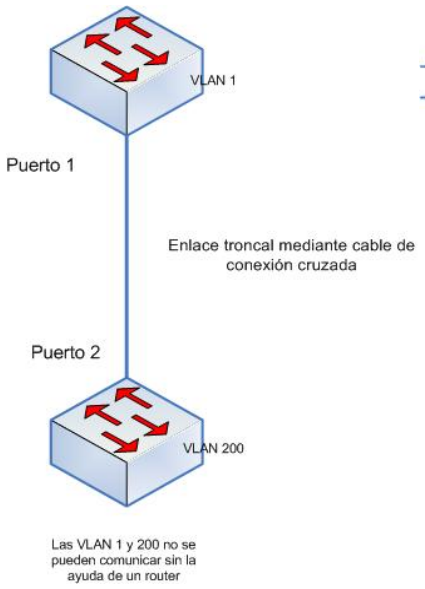


***Figura 10. 3**. Enlace troncal*

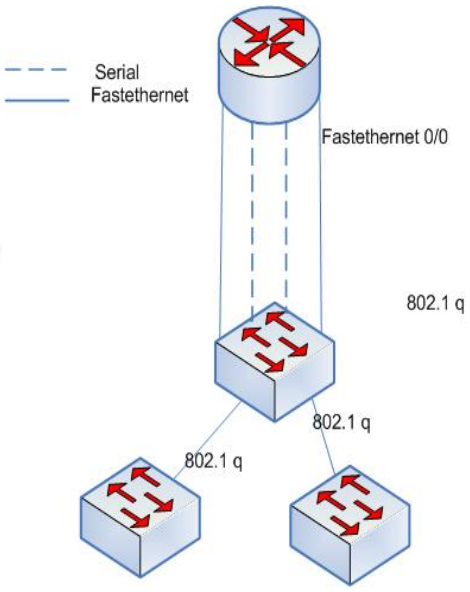


***Figura 10.4**. Enlace troncal.*

Para conseguir conectividad entre VLAN a través de un enlace troncal entre switches, las VLAN deben estar configuradas en cada switch.

El Vlan trunking protocol (VTP) proporciona un medio sencillo de mantener una configuración de VLAN coherente a través de toda la red conmutada. VTP permite soluciones de red conmutada fácilmente escalable a otras dimensiones, reduciendo la necesidad de configuración manual de la red.

VTP es un protocolo de mensajería de capa 2 que mantiene la coherencia de la configuración VLAN a través de un dominio de administración común, gestionando las

adiciones, supresiones y cambios de nombre de las VLAN a través de las redes. Un dominio VTP son varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

Problemas y soluciones entre VLANs.

Conectividad entre VLAN puede lograrse:

- ✓ Conectividad lógica:
  - Conexión única, o enlace troncal, desde el switch hasta el router.
  - Enlace troncal puede admitir varias VLAN.
  - Esta topología se denomina "router en un palo" porque existe una sola conexión al router.
- ✓ Conectividad física:
  - Implica una conexión física separada para cada VLAN.
  - Esto significa una interfaz física separada para cada VLAN.

Situación tradicional: una red con cuatro VLAN requeriría cuatro conexiones físicas entre el switch y el router externo.

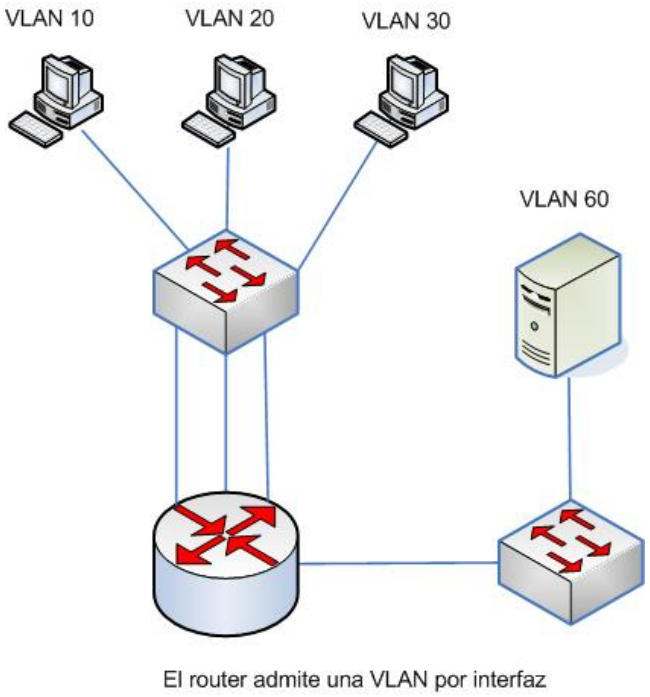


***Figura 10.5**. Conexión física de VLAN.*

10.5. Como indicar al router o switch que envié las actualizaciones VTP a los demás Switchs.

Para que un router permita traspasar tráfico de capa 2, existe el comando ip helper-address para transmitir las peticiones de broadcast en relay para los servicios UDP fundamentales como DHCP , DNS , TFTP , TACACS Por defecto el comando ip helper-address envía los siguientes 8 servicios UDP: Tiempo , TACACS , DNS, Servidor BOOTP/DHCP , Cliente BOOTP/DHCP , TFTP, Netbios Name Service, Netbios Datagram Service. Para el Protocolo de enlace troncal de VLAN (VTP) Creo que la condición necesaria es:

Si existen varias VLAN, por ejemplo desde la VLAN1 hasta la VLAN200, para enrutar tráfico entre VLAN 1 y VLAN 200 en un entorno sin troncal VLAN el router debe estar conectado a un puerto de VLAN1 y un puerto de VLAN 200. (esto se consigue por la creación de tantas subinterfaces en el interface de el router como vlan haya)

Es decir que el router debe de estar conectado a cada switch de cada distinta vlan. En una situación tradicional una red con 4 VLANs necesita 4 conexiones físicas o lógicas entre el switch y el router.

Con encapsulación ISL o 802.1Q solo se necesita una conexión física por cada switch siendo enlaces troncales.

En el router la interfaz fa 0/0 puede admitir varias interfaces virtuales fa 0/0.1, fa 0/0.2,fa0/0.3.

Show vtp status para verificar que el número de revisión de configuración VTP sea inferior al número de revisión de configuración de los demás switches en el dominio VTP antes de agregar un cliente.

10.6. Tipos de conexión y procesamiento de paquetes

10.6.1. Tipos de conexión

Los dispositivos en una VLAN pueden estar conectados de tres formas diferentes, dependiendo de que las conexiones sean con VLAN controlados o VLAN no controlados.

Los switches que transmiten los paquetes de la VLAN se dicen que son VLAN-controlados, pero las estaciones de trabajo o impresoras pueden no serlo. Solo los dispositivos VLAN-controlados saben que son miembros de una VLAN y trabajan bajo el formato de una VLAN.

Enlace troncal

Un enlace troncal conecta a dos dispositivos de LAN que sean VLAN-controlados como por ejemplo dos switches que tengan la función de ruteo (Figura 10.6). El paquete es transmitido a través del enlace es explícitamente etiquetada con el encabezado de

VLAN. El router hará llegar al destino el paquete etiquetado haciendo la consulta a la base de datos.

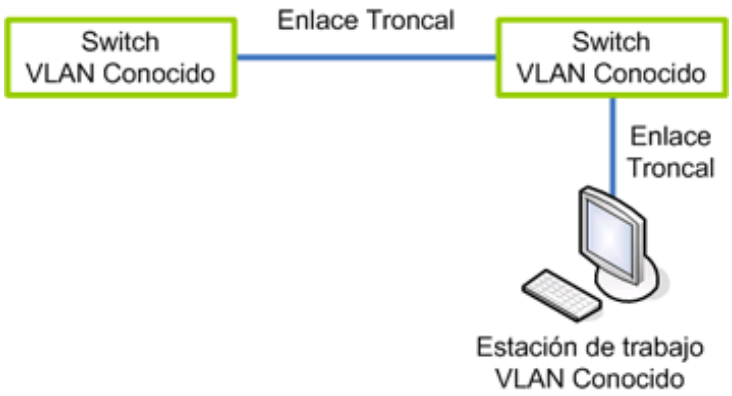


***Figura 10.6**. Enlace troncal.*

Enlace de acceso

Un enlace de acceso comunica un dispositivo VLAN-controlado con uno que no lo sea (Figura 10.7). Los paquetes son transmitidos por el enlace sin incluir el encabezado de VLAN, pero son implícitamente etiquetados por el dispositivo ruteador de la VLAN.

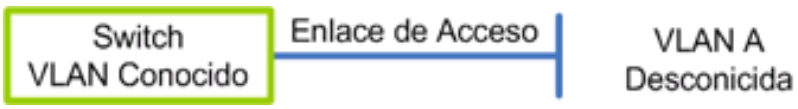


***Figura 10.7.** Enlace de acceso.*

Enlace híbrido

Conecta un dispositivo VLAN-controlado con un dispositivo que no lo sea (Figura 10.8). Para una VLAN específica los paquetes transmitidos por el enlace que pueden ser para la misma LAN todos etiquetados o para otras VLANs no etiquetados.

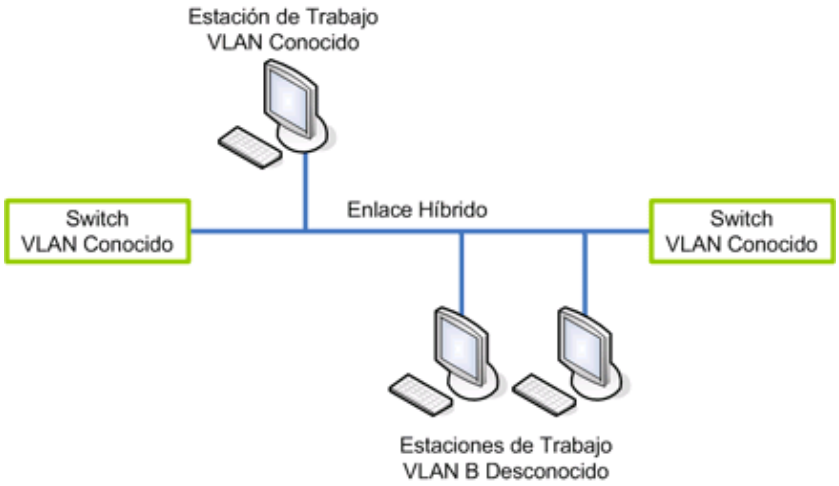


Figura 10.8. *Enlace hibrido.*

10.6.2. Procesamiento de paquetes

Un bridge recibe los paquetes y determina a que VLAN pertenecen en base a los datos que estén explícitos o implícitos en la etiqueta. En el etiquetado explícito los datos de mismo se agregan al paquete. El bridge conserva los datos de los usuarios de la VLAN para determinar que paquetes se deben enviar.

Filtrado por base de datos

La información de los miembros de la VLAN está almacenada como ya se ha mencionado en una base de datos. El filtrado por base de datos consiste en algunos de los siguientes accesos.

Acceso estático

La información es agregada, modificada o eliminada solo por el administrador. Los accesos no son automáticamente eliminados luego de un tiempo, pero si puede ser eliminado explícitamente por el administrador.

Hay dos tipos de accesos estáticos:

- **Registro de accesos:** Se especifica a que puerto los paquetes deben ser enviados, si debe ser enviado a una dirección MAC específica, la dirección de un grupo y en que VLAN específica debe ser reenviado o eliminado, o debe continuar la entrada dinámica.

- **Registro de grupo:** Especifica si los paquetes que deben ser mandados a una VLAN especifica deben ser etiquetados o no etiquetados y que puertos están registrados para cada VLAN.

Accesos dinámicos

Los accesos dinámicos son memorizados por el bridge y no creados o actualizados por el administrador. El proceso de memorización controla los puertos para cada paquete, con la dirección fuente y la identificación de la VLAN, es recibido y actualizado el filtro de la base de datos. El acceso es actualizado solo si todas las condiciones siguientes son satisfechas:

- ✓ Este puerto permite la memorización.
- ✓ La dirección origen es una estación de trabajo y no un grupo de direcciones.
- ✓ Si el espacio esta disponible en la base de datos.
- ✓ Los accesos son eliminados de la base de datos en base al tiempo que están inactivos, luego de un cierto tiempo especificado por el administrador, los accesos son automáticamente reconfigurados por el filtrado de la base de datos si la topografía de la red cambia. Hay tres tipos de accesos dinámicos.

- **Registro de acceso:** Cuando los paquetes deben ser enviados a una dirección MAC específica y hacia una cierta VLAN debe ser enviada o eliminada.

- **Registro de grupo:** Cuando se indica para cada puerto los paquetes deben ser enviados a un grupo de direcciones MAC y una cierta VLAN en la que deba ser filtrada o descargada. Estas entradas son agregadas y borradas usando Group Multicast Registration Protocol (GRMP). Estos multicast mencionados son enviados dentro de una VLAN en particular sin afectar las otras VLANs.

- **Registro de entradas dinámico:** Se especifica que puertos están registrados para una VLAN específica. Los accesos a la VLAN son agregados y borrados utilizando el protocolo de Registración de VLAN GARP (GVRP).

CAPÍTULO 11

NAT
(NETWORK ADDRESS TRANSLATION)

11. NAT (NETWORK ADDRESS TRANSLATION)

Las direcciones de Internet públicas deben de ser registradas con una autoridad de Internet como por ejemplo, el Registro americano de números de Internet (ARIN) o la Réseaux IP Européennes (RIPE), el Registro regional de Internet responsable de Europa y África del Norte. Estas direcciones de Internet públicas pueden alquilarse a una ISP también. Las direcciones IP privadas quedan reservadas y cualquiera las puede utilizar. Eso quiere decir que dos redes, o dos millones de redes, pueden utilizar la misma dirección privada. Un router nunca debe enrutar las direcciones RFC 1918 fuera de una red interna. Los ISP por lo general configuran los routers fronterizos para impedir que el tráfico direccionado de forma privada se envíe al exterior. NAT ofrece grandes beneficios a empresas individuales y a la Internet. Antes del desarrollo de NAT, un host con dirección privada no podía acceder a la Internet. Con NAT, las empresas individuales pueden direccionar algunos o todos sus hosts con direcciones privadas y utilizar NAT para brindar acceso a la Internet.

La "Traducción de Direcciones de Red", Network Address Translation (NAT), es un método mediante el que las direcciones IP son mapeadas desde un dominio de direcciones a otro, proporcionando encaminamiento transparente a las máquinas finales. Existen muchas variantes de traducción de direcciones que se prestan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT debería compartir las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones (aquí el encaminamiento se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento).
- Traducción de la carga útil de los paquetes de error ICMP.

NAT está diseñada para conservar las direcciones IP y permitir que las redes utilicen direcciones IP privadas en las redes internas.

Estas direcciones privadas e internas se convierten en direcciones públicas enrutables. Esto se logra mediante el uso de dispositivos de internetwork que ejecutan un software NAT especializado, el cual puede aumentar la privacidad de la red al esconder las direcciones IP internas. Un dispositivo que ejecuta NAT generalmente opera en la frontera de una red stub. Una red stub es una red que posee una sola conexión a su red vecina. Cuando un host dentro de una red stub desea hacer una transmisión a un host en el exterior, envía el paquete al router del gateway fronterizo. El router del gateway fronterizo realiza el proceso de NAT, traduciendo la dirección privada interna de un host a una dirección pública, enrutable y externa. En la terminología de NAT, la red interna es el conjunto de redes que están sujetos a traducción. La red externa se refiere a todas las otras direcciones.

11.1. Terminología NAT.

- **Dirección local interna:** la dirección IP asignada al host en la red interna. En general, la dirección no es una dirección IP asignada por el Centro de Información de la Red de Internet (InterNIC) o el proveedor de servicios. Es probable que esta dirección sea una dirección privada de RFC 1918.

- **Dirección global interna:** una dirección IP legítima asignada por InterNIC o un proveedor de servicios que representa una o más direcciones IP locales internas al mundo exterior.

- **Dirección local externa:** la dirección IP de un host externo, como la conocen los hosts en la red interna.

- **Dirección global externa:** la dirección IP asignada a un host en la red externa. El dueño del host asigna esta dirección.

11.2. Características principales de NAT.

- Las traducciones NAT se pueden usar para una variedad de propósitos y pueden asignarse de manera dinámica o estática.

- NAT estática está diseñada para permitir que cada dirección local se mapee a su correspondiente dirección global. Esto resulta particularmente útil para los hosts que deban tener una dirección constante que esté accesible desde la Internet. Estos hosts internos pueden ser servidores de empresas o dispositivos de networking.

- NAT dinámica está diseñada para mapear una dirección IP privada a una dirección pública. Cualquier dirección IP de un conjunto de direcciones IP públicas se asigna a un host de red. La sobrecarga, o Traducción de direcciones de puerto (PAT), mapea varias direcciones IP privadas a una sola dirección IP pública. Se pueden mapear varias direcciones a una sola dirección porque cada dirección privada se diferencia por el número de puerto.

- PAT utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones. El número de puerto se codifica en 16 bits. En teoría, el número total de direcciones internas que se pueden traducir a una dirección externa podría ser hasta 65,536 por dirección IP. En realidad, el número de puertos que se pueden asignar a una sola dirección IP es aproximadamente 4000. PAT intenta preservar el puerto origen original. Si el puerto origen está en uso, PAT asigna el primer número de puerto disponible comenzando desde el principio del grupo de puertos correspondiente 0-511, 512-1023, o 1024-65535. Cuando no hay más puertos disponibles y hay más de una dirección IP externa configurada, PAT utiliza la próxima dirección IP para tratar de asignar nuevamente el puerto origen original. Este proceso continúa hasta que no haya puertos ni direcciones IP externas disponibles.

11.3. Ventajas de NAT.

- Elimina la reasignación de una nueva dirección IP a cada host cuando se cambia a un nuevo ISP. NAT elimina la necesidad de re-direccionar todos los hosts que requieran acceso externo, ahorrando tiempo y dinero.

- Conserva las direcciones mediante la multiplexión a nivel de puerto de la aplicación. Con PAT, los hosts internos pueden compartir una sola dirección IP pública para toda comunicación externa. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir muchos hosts internos, y de este modo se conservan las direcciones IP

- Protege la seguridad de la red. Debido a que las redes privadas no publican sus direcciones o topología interna, ellas son razonablemente seguras cuando se las utiliza en conjunto con NAT para tener un acceso externo controlado.

- Conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de redes internas.

- Aumenta la flexibilidad de las conexiones con la red pública. Se pueden implementar varios conjuntos, conjuntos de respaldo y de equilibrio de la carga para garantizar que las conexiones de red pública sean confiables.

- Uniformidad en el esquema de direccionamiento de red interno. En una red sin direcciones IP privadas y NAT, cambiar de direcciones IP públicas requiere la renumeración de todos los hosts en la red existente. El costo de renumerar los host puede ser elevado. NAT permite que permanezca el esquema existente, admitiendo a la vez un nuevo sistema de direccionamiento público.

11.4. Desventaja de NAT.

- Permitir la traducción de direcciones causa una pérdida en la funcionalidad, en particular con cualquier protocolo o aplicación que implique el envío de información de dirección IP dentro de los datos del paquete (payload) IP. Esto requiere que el dispositivo NAT tenga más funcionalidad.

- NAT aumenta el retardo. Se introducen retardos en la conmutación de rutas debido a la traducción de cada dirección IP dentro de los encabezados del paquete. El primer paquete siempre se envía por la ruta lenta, lo que significa que el primer paquete es de conmutación de procesos. Los otros paquetes se envían por la ruta de conmutación rápida, si existe una entrada de caché.

- Es posible que se comprometa el desempeño, ya que, en la actualidad, NAT se logra a través de la conmutación de procesos. La CPU tiene que inspeccionar cada paquete para decidir si es necesario traducirlo. La CPU debe modificar el encabezado IP, y posiblemente el encabezado TCP.

- Una desventaja significativa que surge al implementar y utilizar NAT, es la pérdida de la posibilidad de rastreo IP de extremo a extremo. Se hace mucho más difícil rastrear paquetes que sufren varios cambios en la dirección del paquete al atravesar múltiples saltos NAT. Afortunadamente, los hackers que quieran determinar la fuente del paquete, descubrirán que es muy difícil rastrear u obtener la dirección origen o destino original.

- NAT también hace que algunas aplicaciones que utilizan el direccionamiento IP dejen de funcionar, porque esconde las direcciones IP de extremo a extremo. Las aplicaciones que utilizan las direcciones físicas en vez de un nombre de dominio calificado no llegarán a los destinos que se traducen en el router NAT. Algunas veces, este problema puede evitarse implementando mapeos NAT estáticos.

11.5. Limitaciones y problemas de NAT.

- Algunos protocolos de aplicación (ej. H.323, NetBIOS) incluyen las direcciones IP endiversos sitios de los datos del paquete. Esto requiere pasarelas del nivel de aplicación para funcionar a través de NAT.

- Generalmente las implementaciones de NAT van incorporando soporte para los nuevos protocolos estándar que aparecen y que utilizan direcciones IP en la parte de datos. Por eso cuando se usa NAT es especialmente importante utilizar las versiones de software más recientes.

- El uso de NAPT (PAT, overload) plantea problemas adicionales, por ejemplo generalmente no se pueden enviar mensajes ICMP (comandos ping o traceroute), ya que no incluye información de capa 4 o puertos.

- Con NAT no puede utilizarse la función AH de IPSec, salvo que se utilice IPSec en modo túnel y el NAT se haga antes, o en el mismo dispositivo donde se hace el túnel IPSec. Esto es por que AH, Authentication Header de IPsec corrobora la integridad de la cabecera, pero si se modifica con NAT (IPsec en modo transporte) esta función no puede implementarse.

Si se usa NAT es conveniente que la conexión al exterior se haga sólo en un router.
NAT sólo permite paquetes TCP, UDP e ICMP. No se intercambia información de routing a través de un NAT.

11.6. Funcionamiento de NAT.

Los paquetes originados en la parte interna de la red tienen una **inside local address** como origen y una **outside local address** como destino mientras el paquete viaja por la parte interna de la red. Cuando el paquete es conmutado a la red externa el origen del paquete es traducido a la **inside global address** y el destino conocido como **outside global address**.

Otra forma de verlo es cuando el paquete viene de la parte externa de la red su dirección origen será la **outside global address** y el destino será la **inside global address**. Pero cuando el paquete atraviese el router NAT y entre en la red interna el origen habrá sido traducido por la **outside local address** y su destino como **inside local address**.

El encaminamiento (*routing*) de los paquetes en un router NAT tiene lugar antes de la traducción cuando esta es de dentro a fuera (***Inside-to-outside***) y tiene lugar después cuando la traducción es de fuera a dentro (***Outside-to-inside***).

11.7. Clasificación de NAT.

Según los campos que se modifican el NAT puede ser:

- **NAT Básico:** sólo se cambia la dirección IP.
- **NAPT** (Network Address Port Translation): se modifica la dirección IP y el número de puerto (TCP o UDP). También se llama Overloading NAT o simplemente PAT.

Según la temporalidad de correspondencia entre la dirección privada y la pública el NAT puede ser:

- **Estático:** la tabla de conversión de direcciones (y puertos) se carga al arrancar el equipo que hace NAT y el tráfico no la modifica
- **Dinámico:** la tabla de conversión se construye y modifica en función del tráfico recibido. Las direcciones pueden reutilizarse. Requiere mantener en el NAT información de estado. Normalmente es unidireccional.

11.8. NAT Estático.

NAT permite la asignación de una a una entre las direcciones locales y las exteriores o globales.

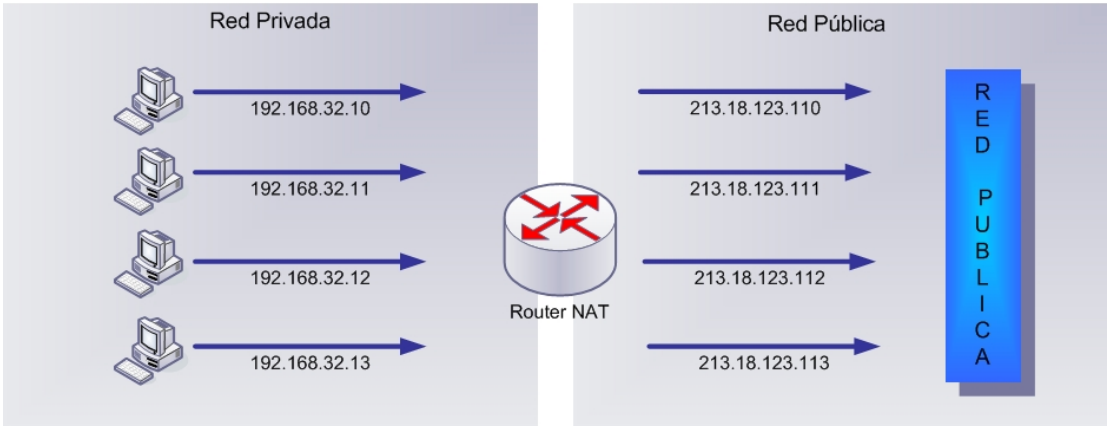


Figura 11.1*. Funcionamiento de NAT Estático.*

11.8.1.NAT INSIDE SOURCE.

En este tipo de NAT un paquete con origen **ip_local** al atravesar una interfaz definida como **inside** cambiará dicha ip origen por la **ip_global.** Igualmente, y para que todo funcione correctamente, cuando un paquete con destino **ip_global** llegue a una interfaz definida como **outside** será cambiado a destino **ip_local**.

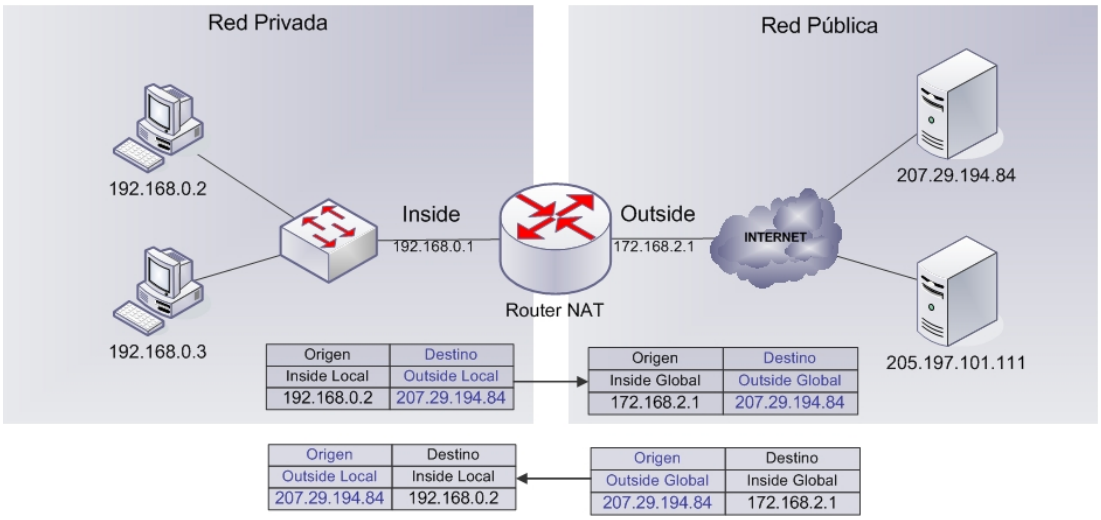


Figura 11.2. *Funcionamiento de NAT Inside Source*

La forma general de la instrucción que permite definir este mapeo es

```
ip nat inside source static ip_local ip_global
```

11.8.2.NAT OUTSIDE SOURCE

En este caso cuando el router recibe un paquete con origen **ip_global** en su interfaz **outside** dicha dirección es cambiada por la **ip_local.** De la misma forma, cuando un paquete con destino **ip_local** atraviesa una interfaz definida como **inside** será trasformado para que su destino sea la **ip_global**. Esto es importante cuando un host en la red pública tiene una dirección que se encuentra dentro del rango de direcciones privada de nuestra red.

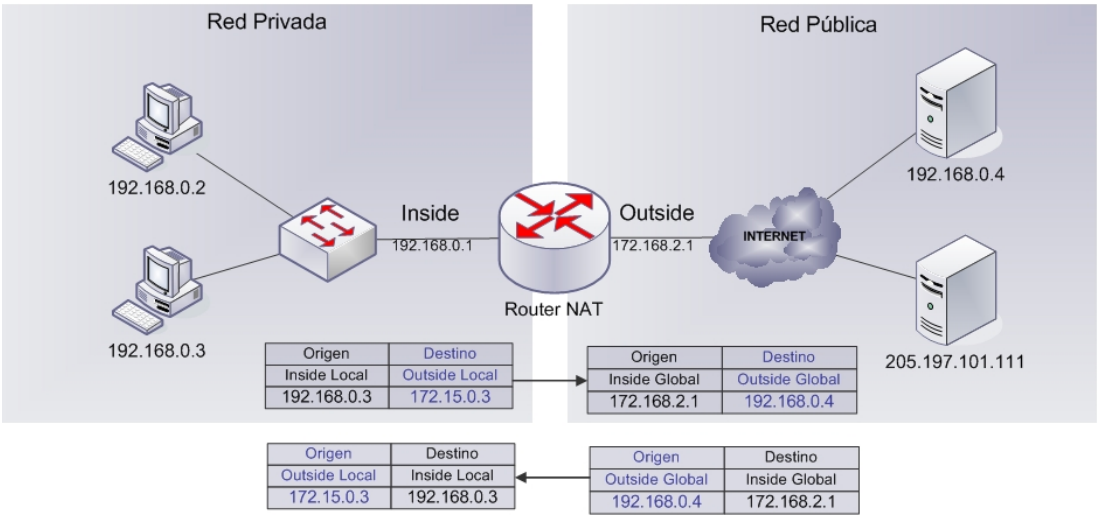


Figura 11.3. *Funcionamiento de NAT Outside Source*

La forma general de la instrucción que permite definir este mapeo es

```
ip nat outside source static ip_global ip_local
```

Una forma simplificada de considerar los puntos anteriores en la práctica consiste en estudiar las instrucciones de traducción **ip nat inside|outside source|destination static**

inside|outside hace referencia a que interfaz debe atravesar el paquete (de qué red viene).

source|destination hace referencia al campo del paquete que será traducido (nuevo origen|destino)

Así:

ip nat inside source cambia el origen de los paquetes que vienen por la interfaz inside.

ip nat inside destination cambia el destino de los paquetes que vienen por la interfaz inside.

ip nat outside source cambia el origen de los paquetes que vienen por la interfaz definida como outside.

11.8.3. Configuración de NAT Estático.

De inside local a inside global.

```
RTA(config)#ip nat inside source static local-ip global-ip
```

Especificar en las interfaces las zonas Inside u Outside

```
RTA(config)#interface type number
RTA(config-if)#ip nat inside
RTA(config)#interface type number
RTA(config-if)#ip nat outside
```

Sintaxis:

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port}
```

11.9. NAT Dinámico.

NAT permite asignar a una red IP interna a varias externas incluidas en un grupo o pool de direcciones.

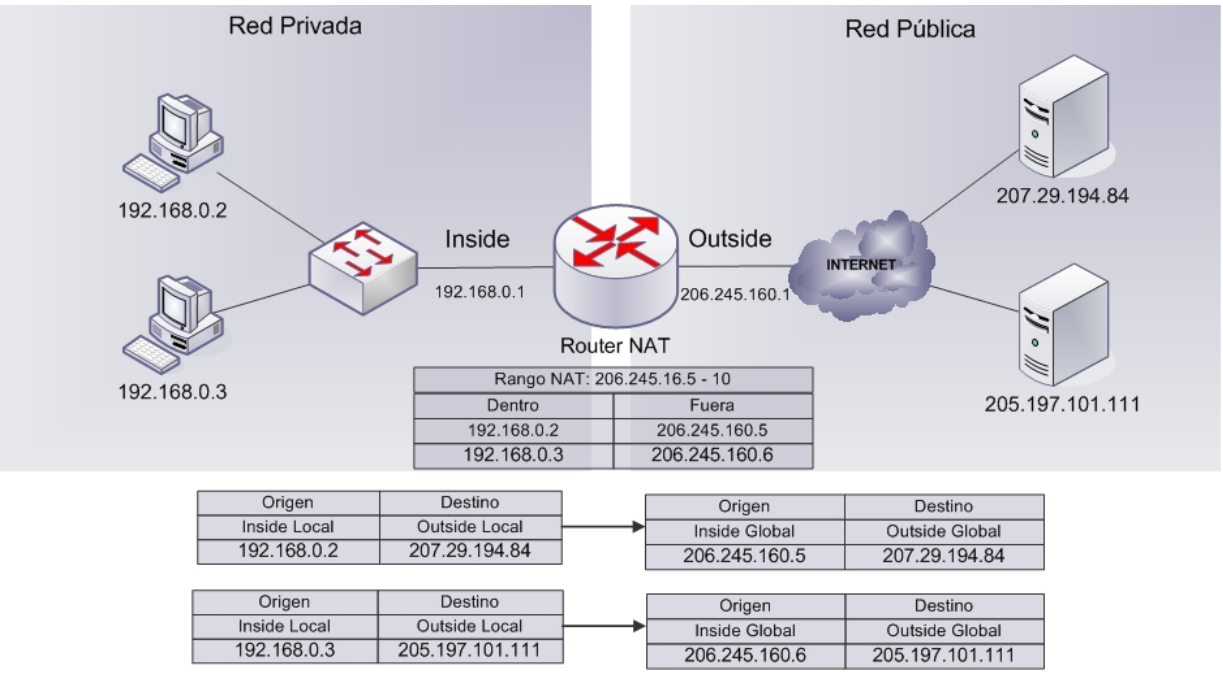


Figura 11.4. *Funcionamiento de NAT Dinámico.*

11.9.1. NAT Configuración dinámica

- **Definir el pool :**

```
Router(config)#ip nat pool name start-ip end-ip {netmask
netmask | prefix-length prefix-length} [rotary]
```

- **Definir direcciones IP permitidas para el NAT:**

```
Router(config)#access-list access-list-number
permit source [source-wildcard]

Router(config)# ip nat inside source {list
{access-list-number | name} pool name
[overload] | static local-ip global-ip}
```

- **Definir interfaces inside/outside:**

```
Router(config)#interface type number
Router(config-if)#ip nat inside
Router(config)#interface type number
Router(config-if)#ip nat outside
```

La lista de acceso debe permitir sólo aquellas direcciones que se deben traducir. Recuerde que existe un "denegar todo" implícito al final de una lista de acceso. Una lista de acceso que es demasiado permisiva puede desencadenar resultados impredecibles. Cisco no recomienda configurar listas de acceso con el comando permit any si los comandos NAT se refieren a esas listas. El uso de permit any puede hacer que NAT consuma demasiados recursos de los routers, lo que puede provocar problemas en la red.

11.10. Traducción de Dirección de Red y Puerto – NAPT o PAT.

Digamos, una organización tiene una red IP privada y una conexión WAN a un proveedor de servicio. El router de zona de la red privada es asignado a una dirección válida globalmente en la conexión WAN y los demás nodos en la organización usan direcciones IP que tienen sólo significado local. En este caso, a los nodos en la red privada se les puede permitir acceder simultáneamente a la red externa, usando la única dirección IP registrada con la ayuda de NAPT. NAPT permitiría mapeos de tuplas del tipo (direcciones IP local, número de puerto TU local) a tipos del tipo (dirección IP registrada, número de puerto TU asignado).

Este modelo es adecuado para muchos grupos de redes pequeñas para acceder a redes externas usando una sola dirección IP asignada del proveedor de servicio. Este modelo debe ser extendido para permitir acceso entrante mapeando estáticamente un nodo local por cada puerto de servicio TU de la dirección IP registrada.

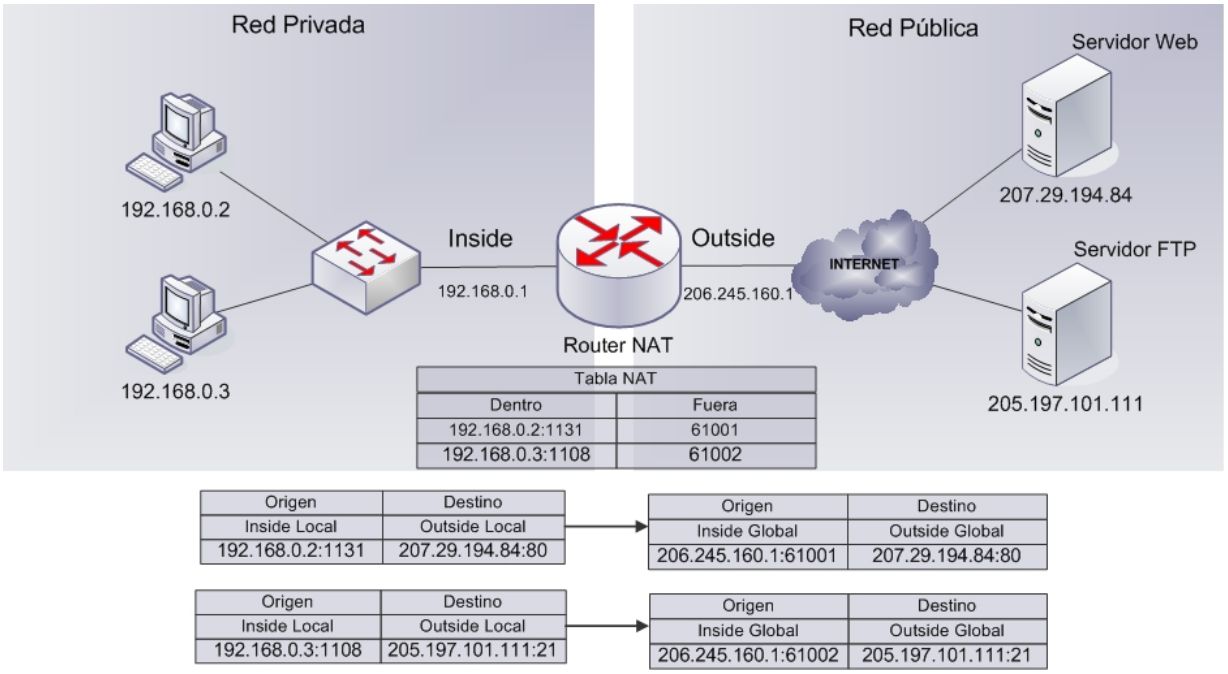


Figura 11.5. *Funcionamiento de NAT/PAT dinámico.*

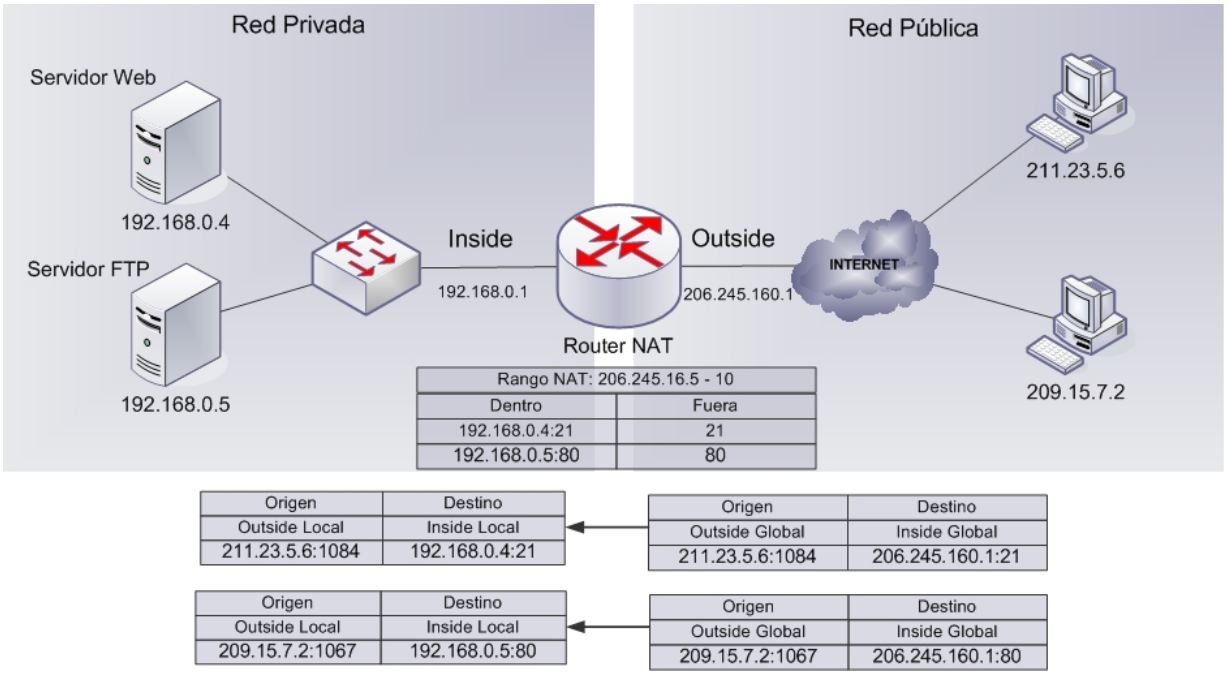


Figura 11.6. *Funcionamiento de NAT/PAT Estático.*

En la figura 11.5 cuando el host con dirección 192.168.0.2 envía un paquete http (puerto destino 80) al servidor 207.29.194.84, en la cabecera de los paquetes se envía la información mostrada en la figura 1.5 estos paquetes son enviados al router NAT ubicado al centro del gráfico, con información que se pueda enrutar.
El router tiene configurado NAPT y lo que sucede es que se traduce la tupla de dirección de origen 192.168.0.2 y puerto origen 1131 en los encabezados IP y TCP por la tupla 206.245.160.1 que es una dirección globalmente única y al puerto 61001 antes de reenviar al paquete.

Los paquetes de regreso que sean enviados por el servidor web, pasan por una traducción de dirección y puerto similar por la dirección IP de destino y puerto TCP de destino. Se observa que esto no requiere de cambios en los hosts o en los routers. La traducción es completamente transparente para los usuarios.

El NAT/PAT Estático es usado cuando tenemos servidores tras un router NAT.

11.10.1. Fases de Traducción:

- **Ligando la dirección,** con NAT Básico, una dirección privada es ligada a una dirección externa, cuando la primera sesión saliente es iniciada desde el host privado. Después de esto, todas las otras sesiones salientes originadas desde la misma dirección privada usarán la misma dirección unida por la traducción de paquete.

  En el caso de NAPT, donde muchas direcciones privadas son mapeadas a un sola dirección globalmente única, la unión sería desde la tupla de (dirección privada, puerto TU privado) a la tupla de (dirección asignada, puerto TU asignado). Como con NAT Básico, esta unión es determinada cuando la primera sesión saliente es iniciada por la tupla de (dirección privada, puerto TU privado) en el host privado.

- **Búsqueda y traducción de dirección**, Después de que una unión de dirección o unión de tupla (dirección, puerto TU) en el caso de NAPT es establecida, se puede mantener un estado para cada una de las conexiones usando la unión. Los paquetes pertenecientes a la misma sesión estarán sujetos a la búsqueda de sesión para propósitos de traducción.

- **Desligando la dirección**, Cuando la última sesión basada en una unión de dirección o de tupla (dirección, puerto TU) es terminada, su unión puede ser terminada.

11.10.2. Manipulación de cabeceras.

En el modelo NAT Básico, el encabezado IP de todos los paquetes debe ser modificado. Esta modificación incluye la dirección IP (dirección IP origen para paquetes salientes y dirección IP destino para paquetes entrantes) y la suma de control IP.

Para las sesiones TCP y UDP, las modificaciones deben incluir actualización de la suma de control en los encabezados TCP/UDP. Esto es porque la suma de control de TCP/UDP también cubre un pseudo-encabezado que contiene las direcciones IP origen

y destino. Como una excepción, los encabezados UDP con suma de control 0 no deben ser modificados. Como para los paquetes de petición ICMP, no son requeridos cambios adicionales en el encabezado ICMP como la suma de control en el encabezado ICMP que no incluye las direcciones IP.
En el modelo NAPT, las modificaciones al encabezado IP son similares a las del modelo NAT Básico. Para las sesiones TCP/UDP, las modificaciones deben ser extendidas para incluir la traducción del puerto TU (puerto TU origen para paquetes salientes y puerto TU destino para paquetes entrantes) en el encabezado TCP/UDP. El encabezado ICMP en los paquetes de petición ICMP deben también ser modificados para reemplazar el ID de petición y la suma de control del encabezado ICMP. La suma de control del encabezado ICMP debe ser corregida para contar la traducción del ID de petición.

Estas son algunas de las modificaciones efectuadas:

- **Ajuste de la suma de control**, las modificaciones de NAT son por paquete y puede ser un cómputo muy intensivo, ello involucra una o más modificaciones a la suma de control, inclusive para traducciones de un sólo campo.

- **Modificaciones al paquete de error ICMP**, los cambios al mensaje de error ICMP incluirán cambios a los encabezados IP e ICMP en la capa saliente como bien cambios a los encabezados de los paquetes embebidos en la carga útil del mensaje ICMP-error.

  El método para NAT debe ser transparente para el host-final, la dirección IP del encabezado IP embebido en la carga útil del mensaje ICMP-error debe ser modificado, el campo de suma de control del encabezado IP embebido debe ser modificado, y finalmente, la suma de control del encabezado ICMP debe también ser modificada para reflejar los cambios a la carga útil.

- **Manipulando la opción IP**, un datagrama IP con una de las opciones IP de Registrar Ruta, Encaminamiento de Origen Fijo o Encaminamiento de Origen No Estricto involucraría registro o uso de direcciones IP de routers intermedios. Un router NAT intermedio puede elegir no soportar estas opciones o dejar las direcciones sin traducir mientras que si procesa las opciones. El resultado de dejar las direcciones sin traducir sería que direcciones privadas a lo largo del encaminamiento origen son expuestas de extremo a extremo. Esto no debe poner en peligro la ruta atravesada por el paquete, de hecho, como cada router se supone que mira sólo al próximo salto.

En general, NAT no debería trabajar con ninguna aplicación que envíe direcciones IP o puertos como datos. Por ejemplo, cuando dos programas usan FTP mantienen una conexión TCP entre ellos. Como parte del protocolo, un programa obtiene un número de puerto en la máquina local, y envía los datos por la conexión TCP al otro programa. Si la conexión entre los programas pasa por medio de un router configurado con NAPT, el puerto podría ser cambiado y reemplazado por el puerto que NAPT le asigne. Así, si NAT falla al cambiar el número de puerto, el protocolo podría fallar. Las implementaciones de NAT fueron creadas para reconocer puertos conocidos como el de

FTP y hacer los cambios necesarios en el flujo de datos. Pero existen aplicaciones que no pueden ser usadas con NAT.

11.10.3. Configuración de PAT.

```
Router(config)#ip nat inside source list n° {pool
natpool|interface serial0} overload
```

Nota: el pool de NAT puede ser de sólo una IP, por ejemplo la IP pública de la interfaz de salida.

11.11. Verificando y modificando una configuración NAT

```
Router#show ip nat translations [verbose]
Router#show ip nat statistics
Router#clear ip nat *
Router#clear ip nat {inside|outside} *
Router#debug ip nat
```

Timeouts: por defecto el préstamo de IP son 24 horas (86400 sec) en TCP y 5 minutos (300 sec) en UDP. Para modificar:

```
Router#ip nat translation timeout sec
Router#ip nat translation tcp-timeout sec
Router#ip nat translation udp-timeout sec
```

11.12. Diagnóstico de fallas en la configuración de NAT y PAT

Cuando existen problemas de conectividad IP en un entorno NAT, muchas veces resulta difícil determinar la causa del problema. Con frecuencia se culpa a NAT equivocadamente, cuando en realidad hay un problema subyacente.

Al intentar determinar la causa del problema de conectividad IP, es útil excluir NAT. Siga los pasos que aparecen a continuación para determinar si NAT está funcionando correctamente:

- Basándose en la configuración, defina con claridad lo que NAT debe lograr.
- Verifique que haya traducciones correctas en la tabla de traducción.
- Verifique por medio de los comandos show y debug que la traducción se está realizando.
- Revise detalladamente lo que le está pasando al paquete y verifique que los routers tengan la información de enrutamiento correcta para enviar el paquete.

Utilice el comando debug ip nat para verificar la operación de NAT visualizando la información acerca de cada paquete que el router traduce. El comando debug ip nat detailed genera una descripción de cada paquete considerado para su traducción. Este comando

también muestra información sobre ciertos errores o condiciones de excepción, como la imposibilidad de asignar una dirección global.

11.13. NAT y la Seguridad.

Como los NAT rechazan todo el tráfico que no coincida con una entrada de la tabla de traducción, son considerados dispositivos de seguridad. Sin embargo, los NAT no pueden sustituir a los servidores de seguridad. Normalmente, hay dos conjuntos de puertos TCP y UDP abiertos en el NAT:

- El conjunto de puertos correspondiente al tráfico que se traduce, especificado en la tabla de traducción. Contiene los puertos dinámicos que abren los clientes situados tras el NAT y los puertos estáticos configurados para los servidores situados tras el NAT.

- El conjunto de puertos correspondiente a aplicaciones y servicios en ejecución en el NAT.

Los puertos estáticos para los servidores situados tras el NAT y los puertos para las aplicaciones y servicios que se ejecutan en el NAT lo hacen vulnerable a los ataques. Los puertos dinámicos no son tan vulnerables porque es difícil que un atacante adivine cuando se abrirán. Si el NAT es un equipo en lugar de un dispositivo dedicado (por ejemplo, un dispositivo de puerta de enlace de Internet), el equipo está expuesto a los ataques.
Por lo tanto, es recomendable que el NAT se use combinado con un servidor de seguridad y que los clientes de la red privada usen también servidores de seguridad basados en host para evitar la difusión de software malintencionado en la red privada.

11.13.1. Problemas del uso de un servidor tras un NAT.

Los equipos clientes que usen NAT y tengan acceso a servidores conectados a Internet no suelen tener problemas. Por el contrario, sí se pueden producir problemas si los servidores se encuentran tras un NAT en las situaciones siguientes:

- Aplicaciones para varios equipos.
- Aplicaciones del mismo nivel.
- NAT-T de IPSec.

Aplicaciones para varios equipos.

Las aplicaciones para varios equipos son aquellas en que varios equipos acuerdan comunicarse juntos a través de un servidor central para una finalidad concreta. Se pueden citar como ejemplos una aplicación de colaboración o un juego en red para varios jugadores. Si el servidor central y algunos de los clientes están tras el NAT, el uso de direcciones privadas puede crear problemas de configuración.

Por ejemplo, imaginemos que un servidor de colaboración está situado tras un NAT y hay ciertos clientes situados tras el mismo servidor y otros que están situados en

Internet. Como consecuencia del espacio de direcciones privado situado tras el NAT y el servidor situado tras el NAT, se debe configurar lo siguiente:

- Entradas estáticas en la tabla de traducción que asignen la dirección pública del NAT y los números se puerto de la aplicación del servidor a la dirección privada del servidor y los números de puerto de la aplicación del servidor.
- Para que los clientes conectados a Internet tengan acceso al servidor mediante su nombre DNS, se deben agregar entradas al DNS de Internet, de manera que el nombre del servidor (por ejemplo, collabsrv.example.com) se puedan resolver como la dirección pública del NAT.

- Para que los clientes conectados a la red privada tengan acceso al servidor mediante su nombre DNS, se deben agregar entradas al DNS de la red privada, de manera que el nombre del servidor se pueda resolver como la dirección privada del servidor.

La configuración de DNS no es necesaria si se usa la dirección privada o pública real del servidor al iniciar la conexión desde los equipos cliente. Con todo, el uso de direcciones IPv4 para establecer conexiones con servidores es complicado para los usuarios finales; hay que garantizar que se indica a los clientes de Internet que utilicen la dirección pública y a los clientes situados tras el NAT que utilicen la dirección privada.

Incluso cuando se ha definido toda esta configuración, los clientes situados tras el NAT y los clientes conectados a Internet no utilizan la misma dirección IPv4 del servidor. Si la aplicación informática de colaboración debe usar una dirección IPv4 común por razones de configuración, sincronización o seguridad, se pueden producir problemas de comunicación.

Aplicaciones del mismo nivel

Otro problema de los NAT es cómo afectan a las aplicaciones del mismo nivel. En el modelo de comunicación del mismo nivel, los equipos del mismo nivel pueden actuar como cliente o como servidor y comunicarse enviando paquetes directamente uno a otro. Si un equipo del mismo nivel está tras un NAT, tiene dos direcciones asociadas, las direcciones privada y pública. Vamos a examinar una configuración sencilla en la que los NAT pueden crear problemas en aplicaciones del mismo nivel. La siguiente figura muestra una red privada con un NAT en el extremo.

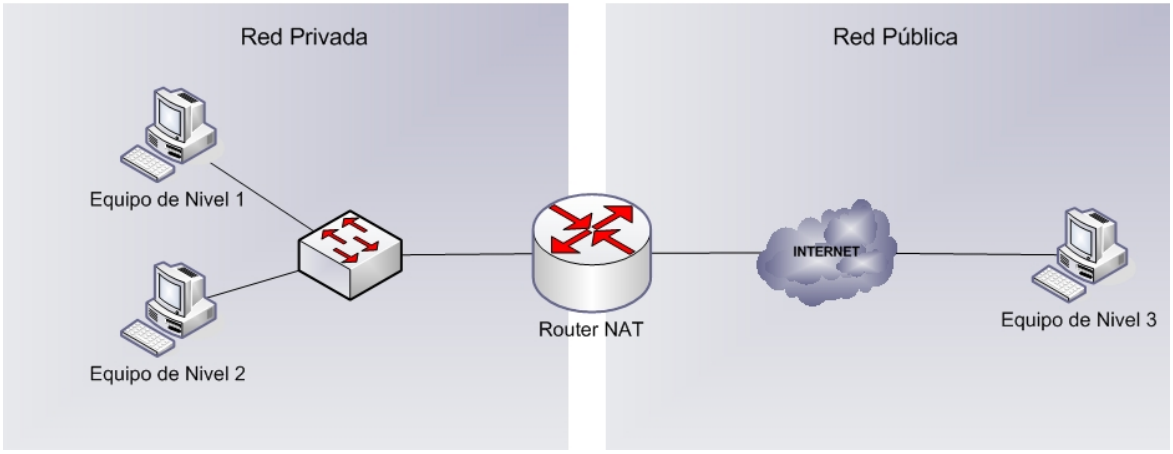


Figura 11.7. *Aplicaciones con el mismo Nivel.*

Para una aplicación del mismo nivel que se ejecuta en todos los equipos del mismo nivel, el Equipo del mismo nivel 1 puede iniciar una sesión con el Equipo del mismo nivel 2 (accesible directamente en su subred) y con el Equipo del mismo nivel 3. Sin embargo, el Equipo del mismo nivel 1 no puede comunicar al Equipo del mismo nivel 3 la dirección pública del Equipo del mismo nivel 2 porque no la sabe. Además, el Equipo del mismo nivel 3 no puede iniciar una sesión con el Equipo del mismo nivel 1 ni el Equipo del mismo nivel 2 sin configurar manualmente el NAT con una entrada estática de la tabla de traducciones que convierta los paquetes de petición de conexión entrantes en la dirección privada o el puerto del Equipo del mismo nivel 1 o el Equipo del mismo nivel 2. Incluso con dicha entrada en la tabla, el Equipo del mismo nivel 3 no puede iniciar una sesión con el Equipo del mismo nivel 1 ni el Equipo del mismo nivel 2, porque ambos host usan la misma dirección IPv4 pública y el mismo número de puerto de aplicación. Para complicar las cosas, es más frecuente que haya equipos del mismo nivel de Internet tras dos NAT distintos. Por ejemplo, en la figura anterior, el Equipo del mismo nivel 3 se encuentra tras un NAT. Para garantizar que la aplicación del mismo nivel puede funcionar en cualquier configuración con NAT, se debe modificar para que sea compatible con NAT, lo que aumenta la complejidad de la aplicación.

NAT-T de IPSec

La seguridad del Protocolo Internet (IPSec) de NAT Transversal (NAT-T) permite que los equipos del mismo nivel de IPSec situados tras un NAT detecten la presencia del NAT, negocien las asociaciones de seguridad IPSec y envíen datos protegidos mediante Carga de seguridad encapsuladora (ESP), a pesar de que las direcciones de los paquetes IPv4 protegidos mediante IPSec cambien. Para obtener información detallada sobre el funcionamiento de IPSec NAT-T consulte el artículo de The Cable Guy de agosto de 2002, que es una introducción a IPSec NAT Transversal.

IPSec NAT-T es compatible con Microsoft® Windows Server™ 2003, Windows XP Service Pack 2 (SP2), así como con Windows® XP Service Pack 1 y Windows 2000 con una descarga de Internet gratuita. Sin embargo, como consecuencia del comportamiento

de IPSec y los NAT, de manera predeterminada Windows XP SP2 ya no es compatible con el establecimiento de asociaciones de seguridad de IPSec NAT-T con servidores ubicados tras un NAT, para evitar un riesgo de seguridad advertido. La siguiente figura muestra un ejemplo de configuración.

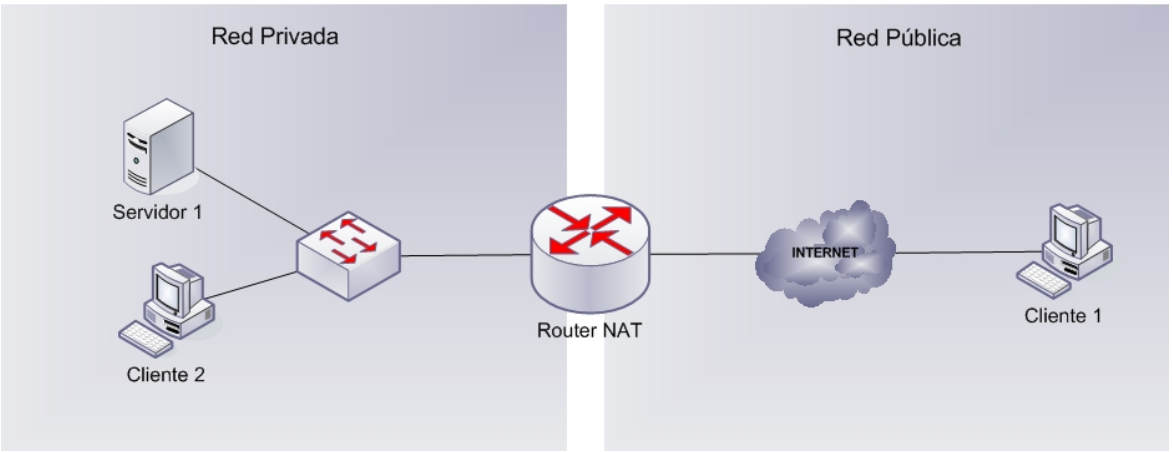


Figura 11.8. *IPSec y NAT.*

Para garantizar que el Servidor 1 está accesible tras el NAT para el tráfico de IPSec, se debe configurar el NAT con entradas estáticas de traducción que asignen el tráfico de Intercambio de claves de Internet (IKE) (mediante el puerto UDP 500) y de IPSec NAT-T (mediante el puerto UDP 4500) al Servidor 1.

En esta configuración se puede producir la situación siguiente:

- El Cliente 1, ubicado en Internet, usa IPSec NAT-T para establecer asociaciones de seguridad bidireccionales con el Servidor 1. El NAT reenvía el tráfico de IKE e IPSec NAT-T entre el Servidor 1 y el Cliente 1, como consecuencia de las entradas estáticas de la tabla de traducción.

- El Cliente 2 usa IPSec NAT-T para establecer asociaciones de seguridad bidireccionales con el Cliente 1. Cuando el Cliente 2 inicia la comunicación con el Cliente 1, el NAT crea un conjunto de entradas dinámicas en la tabla de traducción, lo que permite el intercambio de tráfico de IKE e IPSec NAT-T entre los clientes 2 y 1.
- Si el NAT elimina las entradas dinámicas de la tabla de traducción creadas por el Cliente 2 y se produce una situación que haga que el Cliente 1 vuelva a establecer asociaciones de seguridad con el Cliente 2, puede ocurrir lo siguiente:

  El Cliente 1 envía tráfico de IKE a la dirección IP pública del NAT y al puerto UDP 500. Puesto que este tráfico coincide con la entrada estática de la tabla de traducción del tráfico de IKE al Servidor 1, el NAT reenvía el tráfico de IKE al Servidor 1 en lugar de enviarlo al Cliente 2. Como el

Cliente 1 vuelve a establecer las asociaciones de seguridad, inicia la negociación de Modo principal de IPSec y podría acabar estableciendo asociaciones de seguridad con el Servidor 1 en lugar del Cliente 2. El riesgo de seguridad que se percibe es que el Cliente 1 puede establecer asociaciones de seguridad bidireccionales con un equipo del mismo nivel no deseado.

Si bien esta situación es infrecuente, el comportamiento predeterminado de los equipos en que se ejecuta Windows XP con SP2 es el de no establecer ninguna asociación de seguridad basada en IPSec NAT-T con servidores ubicados tras un NAT, para garantizar que esta situación no se produce nunca.

CAPÍTULO 12

PROTOCOLO DE ENRUTAMIENTO OSPF

12. PROTOCOLO DE ENRUTAMIENTO OSPF

12.1. OSPF

El algoritmo OSPF (Open Shortest Path First, RFC 2328) es un protocolo de enrutamiento de estado de enlace de gateway interior (intercambio de información dentro de un sistema autónomo). Fue desarrollado por el OSPF Working Groupi del IETF.

Los algoritmos de estado de enlace lo que hacen es mantener una base de datos que refleja la topología de la red en los routers; es decir, el estado de los enlaces de la red. Un router periódicamente intercambia información de estado actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento. De esta manera, cada router dispone de un mapa topológico de la red entera.

Para conocer perfectamente la topología de la red los algoritmos de estado de enlace utilizan los siguientes elementos:

- ✓ **Publicaciones estado de enlace** (LSA). Son paquetes de difusión o broadcast que contienen información acerca de los vecinos y los costos de ruta. Se utilizan para mantener actualizadas las bases de datos.

- ✓ **Base de datos topológica** Esta topología se representa mediante un grafo dirigido y se mantiene en cada dispositivo de enrutamiento.

- ✓ **El algoritmo SPF** (primero la ruta más corta) **y el árbol SPF resultante**. En caso de OSPF se utiliza el algoritmo de Dijkstra para calcular la ruta más corta y luego representa las rutas mediante árboles SPF.

- ✓ **Una tabla de enrutamiento de rutas y puertos hacia cada red.**

El grafo dirigido que se guarda en la base de datos topológica consta de:

A) Nodos, que pueden ser de dos tipos:

→ Dispositivos de encaminamiento

→ Red, que a su vez puede ser de dos tipos

i. De transito, si pueden transportar datos que no se han originado ni van dirigidos a un sistema final conectado a esa red.

ii. Terminal, si no es de transito.

B) Arcos, de dos tipos:

→ Arco de grafo que conectan vértices que son dispositivos de encaminamiento cuando los dispositivos de encaminamiento correspondientes están conectados el uno al otro por un enlace punto-a-punto directo.

→ Arcos del grafo que conectan un dispositivo de encaminamiento de vértice a una red vértice cuando el dispositivo de encaminamiento está directamente conectado a la red.

A cada lado de la salida de la interfaz de un dispositivo de encaminamiento se le asocia un coste. Este coste es configurable por el administrador. Los arcos del grafo se etiquetan con el coste de la interfaz de salida correspondiente. Los arcos que no tienen etiqueta se consideran de coste 0 (en este caso los arcos que van desde las redes a los dispositivos de encaminamiento). A partir de este grafo mediante el algoritmo de Dijkstra podemos calcular la ruta de menor coste.

El algoritmo de Estado de enlace consiste básicamente en lo siguiente:

- Cada nodo construye un paquete denominado Link State Packet (LSP) que contiene la lista de sus vecinos y el coste de alcanzarlos.
- Los LSP de cada nodo se destribuyen mediante un mecanismo de difusión, al resto de nodos de la red.
- Cada nodo recibe los LSP del resto de nodos y con ellos construye un mapa global de la red.
- Sobre el mapa global de la red se calculan las mejores rutas mediante Dijkstra o cualquier otro algoritmo.

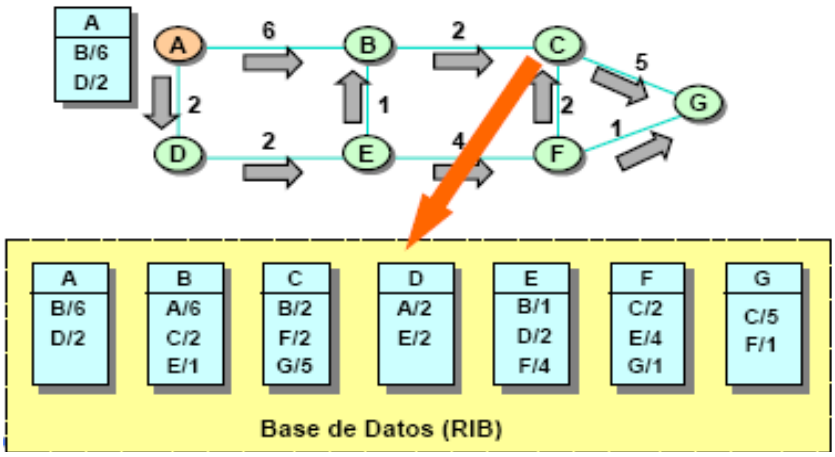


Figura 12.1. *Ejemplo de Estado de Enlaces*

El algoritmo de Distribución de LSP:

- Debe garantizar la ***total sincronización*** entre las bases de datos de cada nodo.
- Es la parte más crítica del algoritmo de Estado de Enlaces.
- Cada LSP se envía al resto mediante inundación:
  - Un nodo reenvía cada LSP recibido a través de todas sus interfaces salvo aquel por el que lo recibió.

- Procesado mínimo antes de redistribuir
  - Los LSPs llegan rápidamente a todos los nodos de la red
  - Convergancia Rápida en caso de cambios.
  - Se propagan prácticamente a la misma velocidad que los paquetes de datos.

➢ Para evitar duplicados:

- Se compara cada LSP recibido con los almacenados en la base de datos (RIB).
  - Si es idéntico al almacenado, No se reenvía.

- Cada LSP lleva un número de secuencia para distinguir entre distintas versiones en el tiempo. Si se recibe un LSP con número de secuencia:
  - Mayor que el almacenamiento: se guarda y se redistribuye.
  - Menor o igual que el almacenado: se descarta.

- Cada LSP lleva, además, un campo de "tiempo de vida", para limitar su periodo de validez.

➢ El algoritmo de distribución debe ser Fiable:

- Hay que garantizar que los LSPs llegan a todos los nodos para guardar la coherencia entre las bases de datos (necesidad de ACKs).

En el algoritmo de Estado de Enlace cada LSP lleva un número de secuencia cuyo valor puede ser entre 0 y N=2^n -1, siendo n el número de bits. El número de secuencia se inicia a 0 y se incrementa en una unidad cada vez que se genera una actualización.

El tiempo de vida de los números de secuencia:

- Se inicia a cero y se incrementa cada vez que el LSP se retransmite o mientras está almacenado en memoria.

- Cuando alcanza el valor máximo NO se descarta, pero se acepta cualquier LSP recibido, independientemente de su número de secuencia.
  - Mecanismo para invalidar LSPs: se envía un LSP con el tiempo de vida al máximo valor.

Las ventajas del Algoritmo de Estado de Enlace son:

➢ Convergencia rápida.
- Detección más LSA/SPF
- Encontrando una nueva ruta.
  - Inundación LSA a través del área.
  - Basado en reconocimiento (Ack).
  - Base de datos topológica esta sincronizada.
  - Cada router deriva la tabla de ruteo para las redes de destino.

- Crecimiento rápido.
- Detección y corrección de problemas más sencilla.

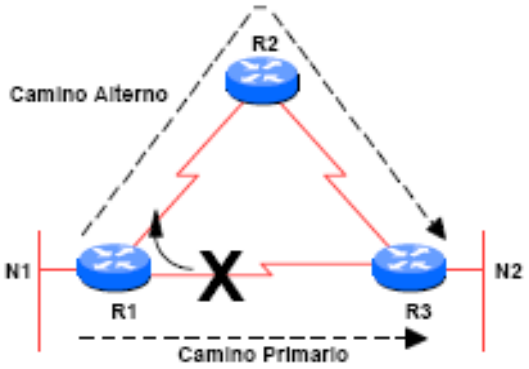


Figura 12.2. *Encontrando una nueva ruta en OSPF.*

En la Figura 12.2 se pude observar cómo en OSPF, por medio de la inundación de paquetes LSA a través del area, se pretende encontrar una nueva ruta y así lograr una convergencia rápida

Algunas de ls desventajas del algoritmo de Estado de Enlace son:

- Consumo de recursos alto:
  - CPU para ejecutar Dijkstra
  - Memoria para almacenar LSPs (cada nodo debe conocer la topología completa de la red)

- Complejo (algoritmo de difusión de LSPs complicado)

12.2. Áreas

Un sistema autónomo que use OSPF estará dividido en una o más áreas. Un **área** es un conjunto de redes y hosts contiguos junto con todos los encaminadores con interfaces conectados a las redes. Cada área tiene asignado un número. Esto le permite a OSPF dar soporte a áreas grandes. El área conectada al backbone de la red se le llama área 0.

Cada área tiene al menos un encaminador de borde de área, que es el que pertenece a varias áreas y anuncia hacia fuera del área las redes disponibles dentro del área (y en sentido contrario).

El encaminamiento dentro de un área se basa en un mapa completo de estado de enlace sólo del área. Luego si la red es muy extensa se reducirá la cantidad de información almacenada en los routers que solo necesitaran conocer la topología de su área.

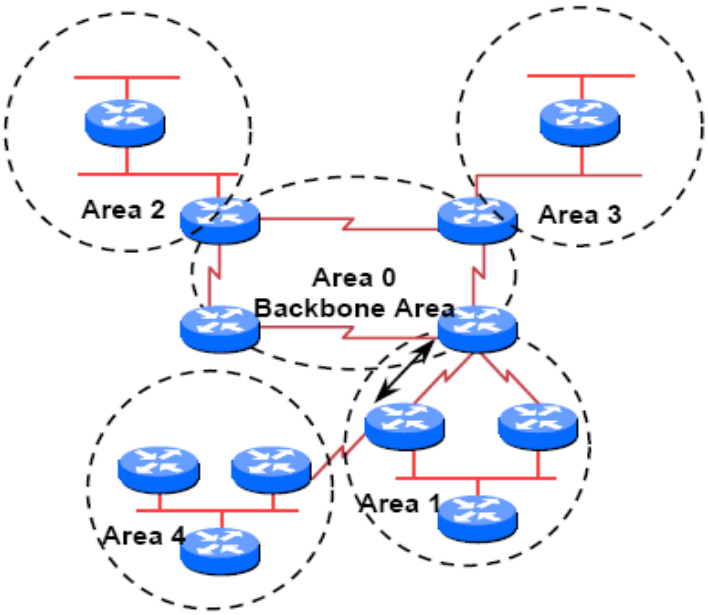


Figura 12.3. *El área 0, área troncal distribuye la información de encaminamiento entre áreas*

12.3. Clasificación de los routers y redes

Según el tipo de red OSPF trabajara de un modo u otro. Para ello OSPF define los siguientes tipos de redes:

- **Punto-a-Punto:** (point-to-point) una red en la que todas las parejas de routers están unidas. Todos los routers de una red punto a punto son vecinos.

- **Redes Broadcast:** redes que soportan más de dos routers conectados juntos con la capacidad de direccionar un solo mensaje físico hacia todos los routers conectados (broadcast). Los routers se descubren dinámicamente en estas redes mediante el protocolo Hello. Todos los routers de una red de difusión son vecinos.

- **Redes No-Broadcast:** (no-broadcast): redes que soportan más de dos routers pero sin capacidad de broadcast. OSPF se ejecuta de dos formas sobre estas redes. El primer modo es no-broadcast multiacceso o NBMA, que simula una operación de broadcast para OSPF en la red. El segundo modo se llama punto-a-multipunto y trata la red como una colección de enlaces punto-a-punto. Todos los routers de una red de no difusión son vecinos.

Para OSPF tenemos los siguientes tipos de routers:

- **Router Designado (DR):** para todas las redes de multiacceso se debe elegir un DR. Este DR tiene dos funciones principales:

    - Mantener la adyacencia con todos los demás routers de la red.

- Actuar de portavoz de todos los demás routers de la red y anunciar los cambios a otras redes, por supuesto es el encargado de mantener la información centralizada del estado de su red.

Este router es elegido por el protocolo Hello. El concepto del Router designado representa una reducción en el número de adyacencias en redes de broadcast. Esto se traduce en una reducción entre todo el tráfico del protocolo y el tamaño de la base de datos.

- **Router Designado de BackUp (BDR):** en ocasiones el router DR puede fallar y por ello se elige otro DR para poder ofrecer tolerancia a fallos.

- **Routers Internos (IR):** son aquellos que tienen todas sus interfaces dentro de la misma área.

- **BackBone Routers (BR):** los routers de backbone están situados en los límites del área de backbone y tiene al menos una interfaz conectada al área 0.

- **Routers de borde de área (ABR):** son los routers que enlazan distintas áreas. Estos routers ejecutan una o varias copias del algoritmo básico, una por cada área a la que se enlaza.

- **Router de Frontera de Sistemas Autónomos (ASBR):** un router que intercambia información con router que pertenecen a otros sistemas autónomos. Un router puede ser un router interno o un router del borde de área y al mismo tiempo ser un ASBR router.

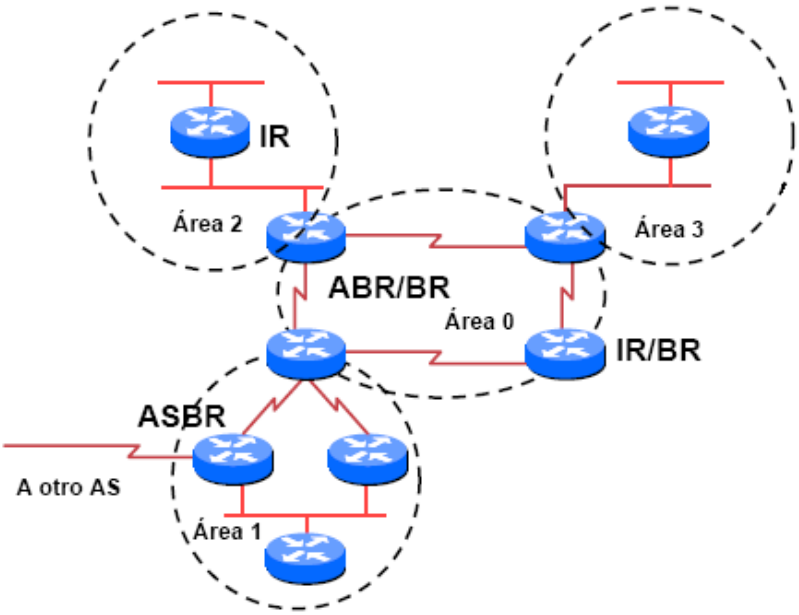


Figura 12.4. *Clasificación de los rotuers*

12.4. Funcionamiento de OSPF

Cuando un router arranca, primero inicializa las estructuras de datos necesarias para el protocolo. Entonces espera indicaciones de los protocolos de bajo nivel de que sus interfaces son operativas.

Entonces usa el **protocolo Hello** para descubrir sus vecinos. El router envía paquetes de saludo (paquetes Hello) y espera a que le sean devueltos. En redes punto-a-punto y broadcast se detectan los vecinos dinámicamente enviando paquetes de saludo multicast. En las redes en las que no es posible usar broadcast será necesaria cierta información de configuración para descubrir vecinos. El protocolo Hello en este punto también elige a un router Designado (DR) para la red si es necesario.

Todos los encaminadores están configurados con un identificador único que se usan en los mensajes. Habitualmente, la parte menor de la dirección IP de encaminador se usa como identificador único.

El router intentará formar adyacencias con algunos de sus nuevos vecinos recién descubiertos. Una **adyacencia** es una relación formada entre dos routers vecinos determinados con el fin de intercambiar información de enrutamiento. No todos los pares de vecinos son adyacencias. Las bases de datos de enlaces de estado se sincronizan entre pares de routers adyacentes. Cuando se hay un router DR es este el que decide que routers son adyacentes.

Las adyacencias controlan la distribución de la información de enrutamiento ya que las actualizaciones solo se envían entre los routers adyacentes.

Un router periódicamente advierte de su estado, que también se denomina estado de enlace. También se informa del estado de enlace de un router cuando este cambia. Las adyacencias de los routers se reflejan en los contenidos de sus LSAs. Esta relación entre las adyacencias y el estado enlace permite al protocolo detectar routers caídos de forma oportuna.

Los LSAs inundan el área. El algoritmo de inundación es fiable, asegurándose que todos los routers en un área tienen la misma base de datos de enlaces de estado. Esta base de datos consiste en una colección de LSAs originados por cada router perteneciente al área. De esta base de datos cada router calcula el árbol SPF consigo mismo como raíz. Este árbol se convierte en los campos de una tabla de enrutamiento del protocolo. Cada vez que se recibe un LSA se calcula el árbol SPF mediante el algoritmo de Dijkstra y se genera una tabla de enrutamiento. Finalmente el router construye las tablas de encaminamiento IP partiendo de los prefijos IP anunciados por cada router. En la Figura 12.5 y Figura 12.6 se muestra como cada uno de los router calcula su propia tabla de encaminamiento.

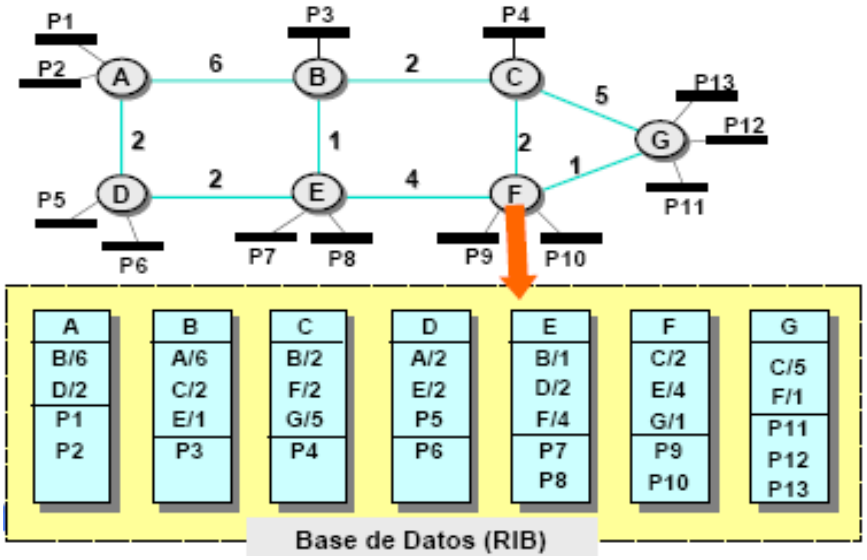
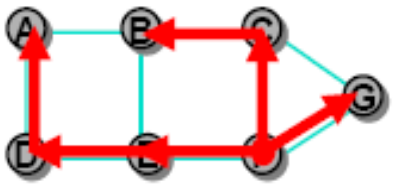


Figura 12.5. *Contrucción de la tabla de encaminamieto en los routers.*

➢**Cálculo de rutas óptimas mediante Dijkstra**



Nodo F

Destino	Siguiente	Coste
A	E	8
B	C	4
C	C	2
D	E	6
E	E	4
F	F	0
G	G	1

➢**Construcción de tablas de encaminamiento IP**

Asociación de prefijos a nodos

Destino	Siguiente	Coste
P1	E	8
P2	E	8
P3	C	4
P4	C	2
P5	E	6
P6	E	6
P7	E	4
P8	E	4
P9	F	0
P10	F	0
P11	G	1
P12	G	1
P13	G	1

Figura 12.6. *Cálculo de la ruta de menor coste mediante el algoritmo de Dijkstra.*

12.5. Tipos de paquetes en OSPF

Los paquetes del protocolo OSPF se encapsulan en paquetes IP (Protocolo 89).

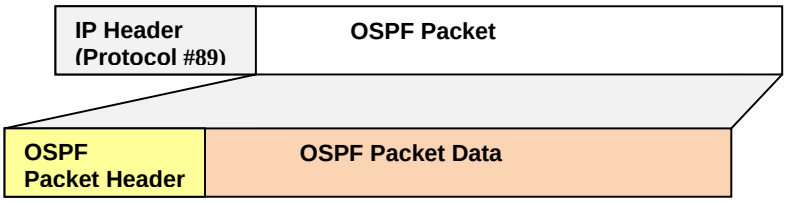


Figura 12.7. *Encapsulamiento de los paquetes OSPF.*

Tabla 12.1. *Tipos de paquetes de OSPF*

Tipo	Nombre	Función
1	**Hello**	Descubrir/Mantener los vecinos
2	**Database Description**	Resumen del contenido de la base de datos
3	**Link State Request**	Petición de una descripción la base de datos
4	**Link State Update**	Actualización de la base de datos
5	**Link State Ack**	Reconocimiento (Asentimiento).

El protocolo Hello usa paquetes Hello para descubrir y mantener las conexiones con los vecinos. Existe un intervalo **(HelloInterval)** que es el que determina la cantidad de segundos entre el envío de dos paquetes Hello por parte de un router en una interfaz. Cuando el temporizador para los paquetes Hello expira se envían los paquetes y vuelve a inicializarse para esperar otro intervalo.

También relacionado con los paquetes Hello existe un intervalo llamado DeadInterval que se define como el número de segundos antes de que los routers vecinos lo declaren caído (down), cuando dejan de recibir paquetes Hello desde él. Se advierte mediante paquetes Hello por esa interfaz.

Los paquetes de descripción de base de datos y Link State Request se utilizan para formar adyacencias. La fiabilidad del mecanismo de actualización de OSPF se implementa mediante paquetes Link State Update y Link State Ack.

Cada paquete de Link State Update contiene un conjunto de nuevos LSAs para un salto más allá del punto de origen. Un solo paquete de este tipo puede contener LSAs de varios routers. Cada LSA está identificado con el identificador de cada router y una suma de

comprobación de errores de los contenidos del estado de enlace. Cada LSA tiene un campo de tipo:

Tabla 12.2. *Campo Tipo del LSA*

Tipo	Nombre	Descripción
1	Router-LSA	Se originan en todos los routers. Describe un conjunto de estados de las interfaces de un router para un área. Solo se envían en un área.
2	Red-LSA	Se originan en los routers DR. Contiene una lista de los routers conectados a un área determinada. Se envían solo dentro de un área.
3,4	Resumen-LSA	Se originan en los routers de borde área. Cada uno describe una ruta hacia un destino fuera del área, aunque todavía dentro del sistema autónomo. El tipo 3 describe rutas hacia redes y el tipo 4 describe rutas hacia router ASBR.
5	AS-External-LSA	Originados por un router ASBR. Cada uno describe una ruta con destino a otro sistema autónomo.

Excepto los paquetes de saludo (Hello) solo se envían entre routers adyacentes. Lo que significa que los paquetes OSPF solo viajan a través de un salto, excepto aquello que son enviados a través de adyacencias virtuales.

12.6. Múltiples áreas en OSPF

Si hay más de un área, siempre debe haber un área 0 que haga de backbone. Debemos configurar el área de backbone (área 0) y a continuación el resto de áreas (diseño jerárquico). A las rutas que se generan dentro de un área se les llama **intra-area-routes** y aparecerán en la tabla de encaminamiento identificadas con la letra O. A las rutas aprendidas de otra área se les llama **inter-area-routes** o **summary-routes** y aparecerán en la tabla de encaminamiento identificadas con la letra O IA. A las rutas inyectadas desde otros protocolos de encaminamiento (usando redistribución de rutas) se les llama **external-routes** y aparecerán en la tabla de encaminamiento identificadas con la letra **O E1** (tipo 1 significa que el coste es la suma del protocolo interno más el externo) o **O E2** (tipo 2 significa que el coste es siempre el del protocolo externo). Por defecto OSPF siempre redistribuye con tipo 2.

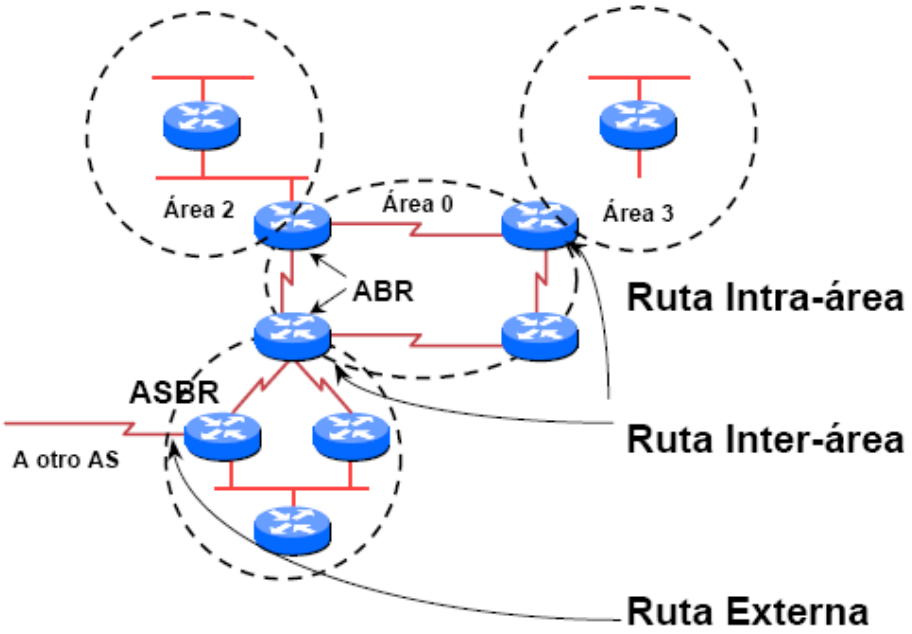


Figura 12.8. *Tipos de rutas en OSPF.*

12.7. Flujos de Información en OSPF

Entre los diferentes flujos de información se encuentran:

➢ **Hacia el exterior de un área**

- Los ABR son responsables de anunciar los prefijos disponibles dentro de cada área.
- Generan LSPs hacia el backbone incluyendo la lista de prefijos.
- Opciones:
  1. Exportar prefijos individuales
  2. Exportar un único prefijo que los englobe (Agregación)
     - Requiere asignación jerárquica de direcciones (estilo CIDR)
  3. Ambas cosas (solución mixta).

En la Figura 12.9 se puede observar como se genera el flujo de información hacia el exterior de una determinada área.

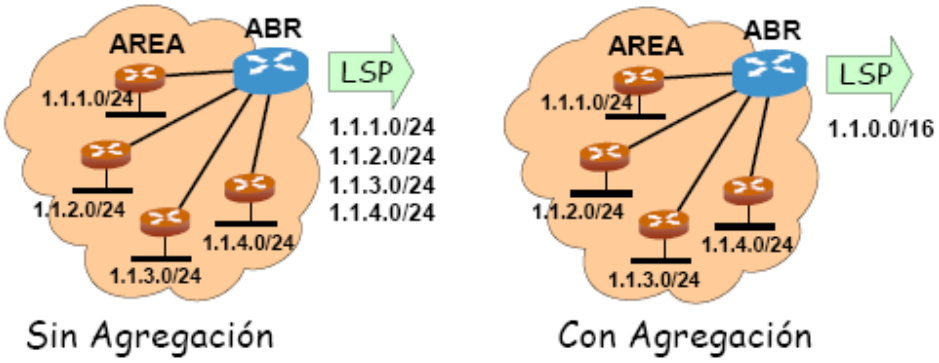


Figura 12.9. *Flujo de información hacia el exterior de un área.*

- Ventaja de la Agregación
    1. Disminución del número de prefijos exportados.
- Desventaja
    1. Posible encaminamiento subóptimo (sólo en caso de que existan varios ABRs en el área)

➢ **Hacia el interior de un área**

- Los ABR regulan si la información de encaminamiento (prefijos) que circula por el backbone debe ser redistribuida hacia el interior de las áreas.

- Opciones:

    1. No redistribuir: Inyectar únicamente una ruta por defecto.
        - El ABR distribuye una ruta hacia 0.0.0.0/0
        - Útil si el área solo tiene un ABR (STUB AREA).

    2. Redistribuir: Inyectar los prefijos del backbone.
        - Los routers internos mantienen en sus tablas destinos exteriores, lo que les permite elegir para cada destino el ABR óptimo.
        - Útil cuando el área tiene varios ABR.

En la Figura 12.10 se muestra un ejemplo de agregación e inyección de rutas del backbone en un área con dos ABR

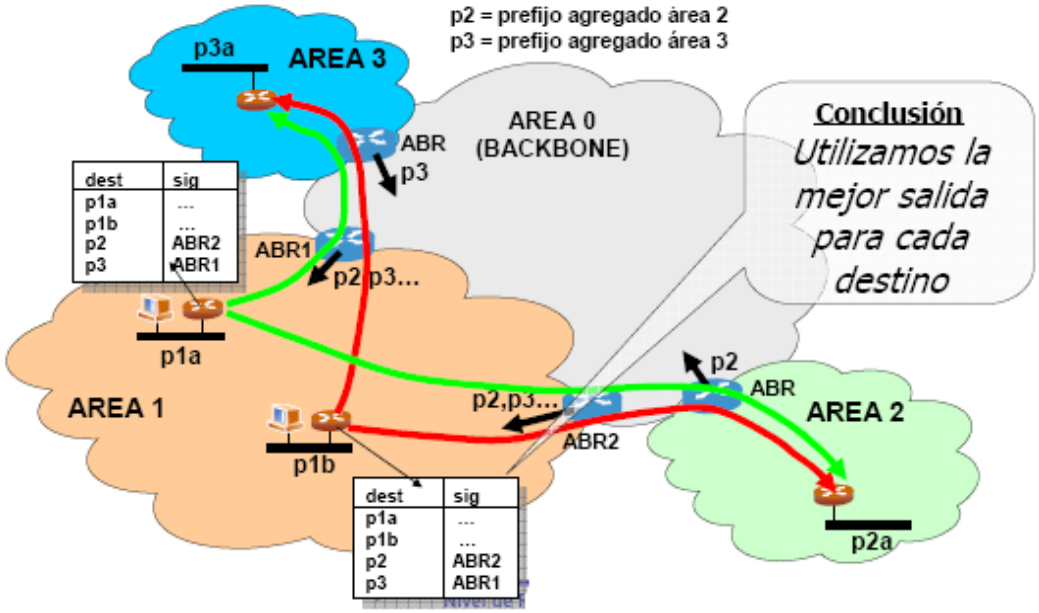


Figura 12.10. *Flujo de información generado por agregación e inyección de rutas en el backbone.*

En la Figura 12.11 se muestra un ejemplo de agregación e inyección de rutas por defecto del backbone en un área con dos ABR.

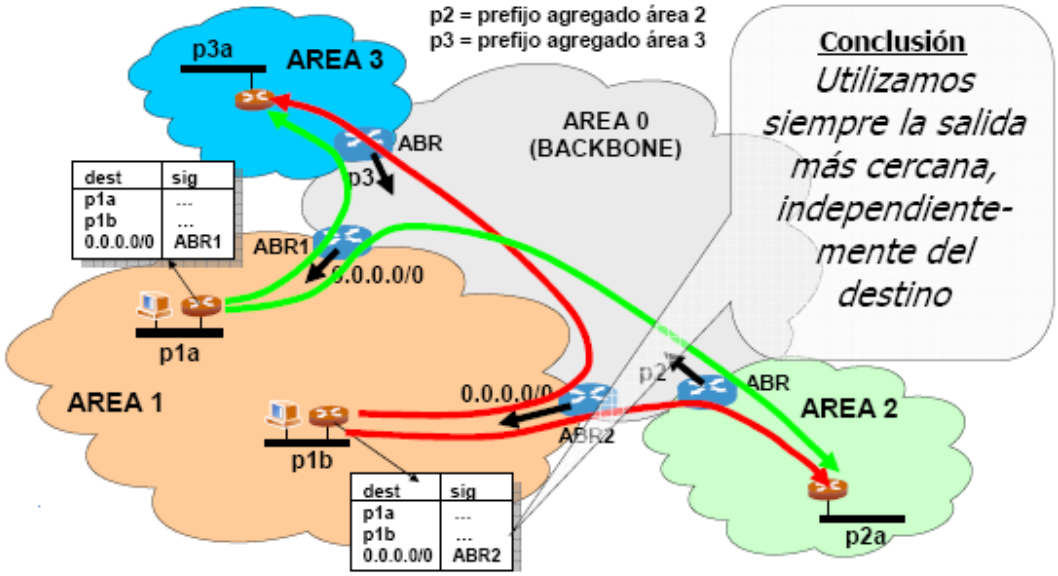


Figura 12.11. *Flujo de información generado por agregación e inyección de rutas por defecto en el backbone.*

En la Figura 12.12 se muestra un ejemplo en el que las opciones de agregación e inyección de rutas que se muestran en los ejemplos anteriores pueden coincidir, esto depende de la topología y costes de los enlaces del área y del backbone.

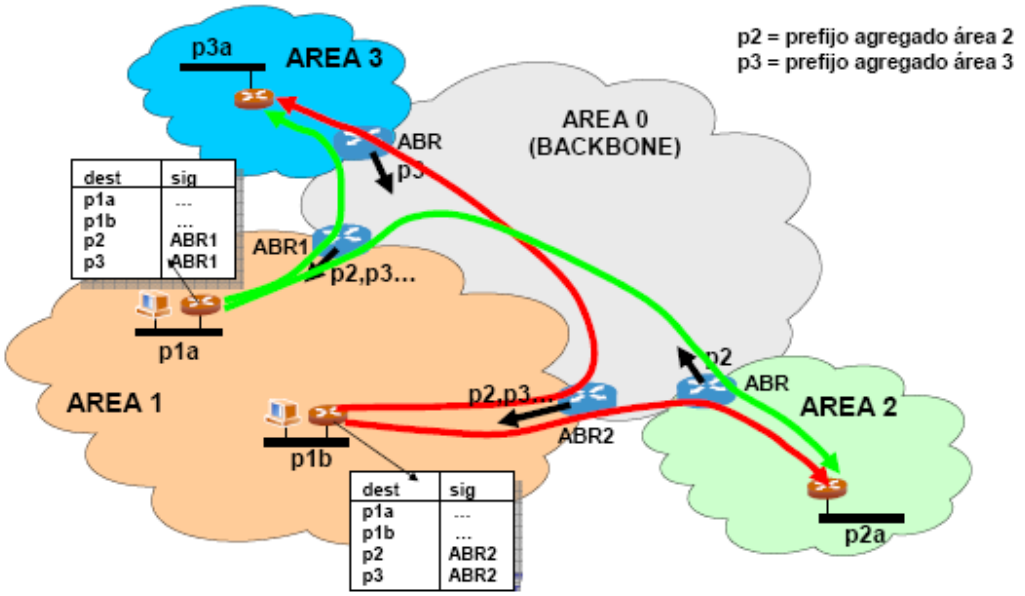


Figura 12.12. *Flujo de información generado por agregación e inyección de rutas en el backbone.*

12.8. Modificación del comportamiento de OSPF

Cada router escoge como OSPF Router ID la dirección IP mayor. Si la interfaz que tiene esa dirección IP cae, debe cambiar el OSPF router ID, cosa que puede afectar a la elección del DR y BDR. Para evitar este efecto, se suele configurar siempre una interfaz loopback con una dirección IP que no tiene por qué estar en el rango 127.0.0.0/8.

Podemos modificar también la prioridad de un router con el comando **"ip ospf priority *number*"**, donde "number" es un número entre 1 y 255. Prioridad 0 implica que el router no puede ser elegido DR o BDR, el valor por defecto es 1 y a mayor valor el router es elegido como DR o BDR.

La métrica por defecto usada en OSPF es el ancho de banda. En un router CISCO el coste de un enlace se calcula como 10^8/bandwidth (bps). Por ejemplo si tenemos un enlace Ethernet a 10 Mbps el coste sería 10^8/10^7=10, mientras que un modem a 56 Kbps tendria un coste de 10^8/56*10^3=1785. El SPF es un algoritmo de mínimo coste. Podemos modificar el coste de un enlace de dos maneras: (1) modificando el valor del coste en la interfaz de ese enlace con el comando **"ip ospf *cost*"** donde cost tiene un valor entre 1 y 65535 o (2) modificando el valor del bandwidth en la interfaz que permite calcular el coste con el comando **"bandwidth *value*"**. Note que NO se está cambiando la velocidad real del enlace, solo el coste de cara a calcular el camino más corto.

Se pueden cambiar los valores de periodicidad de los temporizadores de paquetes Hello: hello-interval (tiempo entre paquetes hello, por defecto es 10 s) y dead-interval (tiempo que considera que el enlace ha caído, por defecto es 40 s). Los temporizadores se modifican por interfaz con los comandos **"ip ospf hello-interval *value*"** y **"ip ospf dead-interval *value*"**

12.9. Estados de interfaces

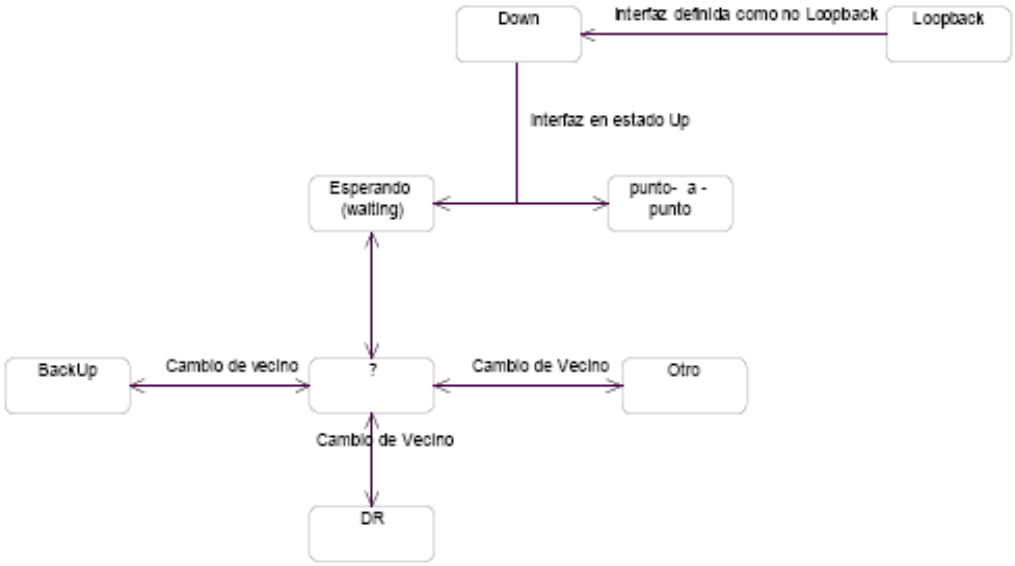


Figura 12.13. *Estado dela interfaces*

El esquema anterior representa los estados por los que puede pasar una interfaz para OSPF.

- **Down:** Es el estado inicial de las interfaces e indica que la interfaz no está en uso con lo cual no se podrá ni enviar ni recibir paquetes por esa interfaz.

- **Loopback:** En este estado la interfaz no estará disponible para el tráfico regular de datos. Sin embargo, sería deseable obtener información sobre la capacidad de la interfaz, bien mediante el comando Ping o a través de algún bit de test de error. Por esta razón, los paquetes IP podría ser direccionados a una interfaz en este estado.

- **Esperando:** En este estado el router está intentando determinar la identidad de los routers DR y BDR. Para hacer esto el router monitoriza los paquetes Hello que recibe. No se le permite elegir un router DR o un router BDR hasta que sale de esta fase. Esto evita cambios innecesarios. La duración de esta fase viene determinada por un temporizador (**wait timer**) cuya duración es el DeadInterval.

- **Otro:** La interfaz esta en una red en la cual otro router ha sido seleccionado como DR o BDR. En este estado, el router realiza las adyacencias tanto con el router DR como con el router BDR (si existe).

- **BackUp:** En este estado el router ha sido designado como BDR en la red. Será promocionado a router DR si el actual DR presenta fallos. El router establece las adyacencias con los demás routers de la red.

- **DR:** En este estado el router es el router designado en la red. Se producen adyacencias con todos los routers conectados a la red. Debe también originar un paquete red-LSA para el nodo red. Este contendrá enlaces a todos los routers (incluido el mismo) conectados a la red.

Los cambios entre vecinos que llevan a recalcular los estados otros, BackUp y DR son los siguientes:

- Se ha establecido comunicación bidireccional con un vecino.
- No hay más comunicación bidireccional con un vecino.
- Uno de los vecinos bidireccionales se ha declarado así mismo o como router DR o como router BDR. Esto se puede detectar en los paquetes Hello.
- Uno de los vecinos no se declara así mismo más como router DR o BDR aunque antes estuviera en este estado. Esto se detecta mediante los paquetes Hello.
- La prioridad de un router para un vecino ha cambiado. Esto se detecta mediante los paquetes Hello.

Se puede pasar de los estados otro, DR y BackUp al estado esperando bien porque un router detecta la existencia o la no-existencia de un router BDR para la red. Esto se detecta cuando se recibe un paquete Hello de un vecino declarándose como router BDR y a la vez otro paquete Hello de otro vecino diferente que se declara como router DR e indica que no hay un router BDR establecido.

12.10. Comandos OSPF

- Para configurar el proceso OSPF en un router se usa el comando *router OSPF*:

```
Router(config)# router OSPF numero.
```

El número será un identificador interno para el proceso de enrutamiento de OSPF. Se asigna localmente y es un número positivo entero. Se asigna un valor único para cada proceso OSPF de enrutamiento.

- Para desactivar OSPF basta con la forma no del comando:

```
Router(config)# no router OSPF numero.
```

- Para configurar manualmente el coste de una interfaz en un router se usa el siguiente comando:

```
Router (config-if)# ip ospf cost coste.
```

Donde coste es el valor que queremos darle a la métrica de la interfaz. Para restaurar el valor por defecto del coste de la interfaz basta con usar la versión no del comando**, no ip ospf cost.**

- Para establecer que una red pertenece a un área usamos el comando *area*:

```
Router(config-router)# area area-id
```

Donde tenemos que area-id será el identificador de la red.

- Para deshabilitar un área usaremos el siguiente comando:

```
Router(config-router)# no area area-id
```

- Para definir las interfaces en las que se ejecuta OSPF y definir al mismo tiempo un área para esas interfaces se usa el comando de configuración network área, cuya sintaxis es la siguiente:

```
Router(config-router)# network direccion wildcard-máscara area
area-id
```

Donde dirección será la dirección de la interfaz a añadir y area-id será el identificador del área.

- Para indicarle al router el tipo de red se utiliza el comando ip ospf network:

```
Router(config-if)# ip ospf network {broadcast | non-broadcast |
{point-tomultipoint [non-broadcast ]}}
```

- La versión no del comando desactiva el tipo de red seleccionado y vuelve al tipo de red por defecto.

```
Router(config-if)# no ip ospf network
```

- Para establecer el intervalo del protocolo Hello usamos el comando ip ospf hellointerval:

```
Router(config-if)# ip ospf hello-interval segundos
```

- El parámetro *segundos* indica en número de segundos del intervalo. Para deshacer la asignación y volver al valor por defecto usamos la versión no del comando:

```
Router(config-if)#no ip ospf hello-interval
```

- Para establecer el DeadInterval a un valor distinto al de por defecto se usa el comando ip ospf dead-interval:

```
Router(config-if)# ip ospf dead-interval segundos
```

El parámetro *segundos* indica en número de segundos del intervalo.

- Para deshacer la asignación y volver al valor por defecto usamos la versión no del comando:

```
Router(config-if)#no ip ospf dead-interval
```

- Para poder observar el tráfico de paquetes en la red originados por OSPF los router cisco tienen el siguiente comando:

```
Router# debug ip ospf packet
```

Muestra información sobre todos los paquetes recibidos.

- Para deshabilitar esta opción se puede usar la versión no del comando o bien undebug all.

- Para variar la prioridad manualmente de un router y que tenga mayores (o menores) posibilidades de ser elegido como DR (o BDR) usamos el siguiente comando:

```
Router(config –if)# ip ospf priority #numero.
```

Donde #número será un número de 8 bits (de 0 a 255) que especifica la prioridad.

- Para restaurar la prioridad previa se usa el comando no ip ospf priority.
- Para poder observar los eventos relacionados con el protocolo OSPF como adyacencias, información de inundación, o la designación del router como DR se usa el siguiente comando:

```
Router# debug ip ospf events
```

- Para deshabilitar esta opción se puede usar la versión no del comando o bien undebug all.

- Para introducir autentificación en OSPF

Para establecer la autentificación en un área usamos el comando area area-id authentication. Pero para habilitar la autentificación MD5 (Message Digest 5) en ospf se usa el comando **ip ospf message-digest-key.**

Su sintaxis es la siguiente:

```
Router(config-if)#ip ospf message-digest-key key-id md5 key
```

Y para deshabilitarlo usamos la version no del comando:

```
no ip ospf message-digest-key key-id
```

Donde key-id es un identificador en el rango desde el 1 a 255. Y key es una clave alfanumérica de 16 bytes.
Normalmente se usa una clave por interfaz para generar información autentificada cuando se envían paquetes y para autentificar los paquetes entrantes. Los routers vecinos deben tener el mismo valor de clave (key).

- Para la verificación del funcionamiento de OSPF. Usar los siguientes comandos:

  ***show ip protocols*:** permite ver que protocolos de encaminamiento hay activos listando parámetros tales como temporizadores, métricas, filtros, etc.

  ***show ip route*:** permite ver la tabla de encaminamiento.

  ***show ip route ospf*:** permite ver la tabla de encaminamiento sólo para entradas OSPF.

  ***show ip ospf interface*:** lista información relacionada con una interfaz que usa OSPF. Permite comprobar si las interfaz pertenecen al área a la que se suponen deberían pertenecer. También permite averiguar si una interfaz es DR, BDR o DROTHER (no es ni DR ni BDR), su prioridad y si la red es de tipo BMA o NBMA.

  ***show ip ospf*:** lista el número de veces que el algoritmo SPF (Short-First Path) se ha ejecutado.

  ***show ip ospf neighbor*:** lista información acerca de los vecinos OSPF por cada interfaz.

  ***show ip ospf neighbor*:** lista información detallada acerca de los vecinos OSPF por cada interfaz.

  ***show ip ospf database*:** lista los contenidos de la DB topológica.

  ***debug ip ospf "op"*:** donde "op" son distintas opciones que permiten debuguear las distintas operaciones que ejecuta OSPF (adjacency, events, etc).

CAPÍTULO 13

IS-IS
(INTEGRATED SYSTEM- INTEGRATED SYSTEM)

13. IS-IS

13.1. ISO y OSI: ¿Cuál es la diferencia?

La Organización Internacional para la Estandarización (ISO) ha desarrollado un estándar de datos para el sistema de redes.

El protocolo de Interconexión de Sistemas Abiertos (OSI) representa un sistema de estandarización internacional que facilita la interoperabilidad de equipos.

El protocolo OSI es parte de un programa internacional para el desarrollo de protocolos de sistema de redes y otros estándares que facilita la ínterconectividad de los equipos. El programa OSI nace por la necesidad de un estándar internacional para el sistema de red y facilitar la comunicación entre el sistema hardware y software a pesar de las diferencias fundamentales de la arquitectura.

ISO ha construido un cambio en el estándar de desarrollo para la información de los sistemas de red.

El trabajo de OSI en el sistema de redes incluye varios servicios de redes con las siguientes características:

- Independencia de la infraestructura de comunicación de capas inferiores.
- Transferencia de Fin-a-Fin
- Transparencia
- Selección del servicio de calidad (QoS)
- Direccionamiento

Un protocolo es transparente cuando tiene la capacidad de construir o transferir datos que no se hicieron localmente. De esta manera el encabezado fluye como datos de fin a fin sin ser modificado.

13.2. Terminología del protocolo OSI

En la red OSI, hay cuatro entidades arquitectónicas importantes: host, áreas, backbone y dominio.

- Un ***dominio*** es una porción de la red OSI que es administrada por una autoridad en común.

- Dentro de un dominio OSI puede haber una o más áreas definidas. Un ***área*** es una entidad local, y esta formada por un conjunto de routers y enlaces de datos que los conecta. Todos los routers de una misma área intercambian información de todos los host que estos alcanzan.

- Las áreas están conectadas a un ***backbone*.** Todos los router de un backbone conocen a todas las áreas que alcanzan.

- Un ***Sistema Final*** (ES) es cualquier host o nodo que no enruta. Un ***Sistema Intermedio*** (IS) es un router.

Estos términos son básicos para el OSI- ES-IS y el protocolo IS-IS.

13.3. Diferencia entre el protocolo OSI y el modelo de referencia OSI.

El desarrollo del sistema de red OSI comenzó en 1980. Ahora tiene dos grandes componentes:

- Modelo Abstracto del sistema de red, conocido como **modelo de referencia OSI**, o modelo de siete capas.

- Un conjunto de protocolos de red, conocido como Protocolo OSI, que incluye CLNP, ES-ES, etc.

El modelo de referencia OSI gusta de una gran aceptación del mismo **protocolo OSI**.

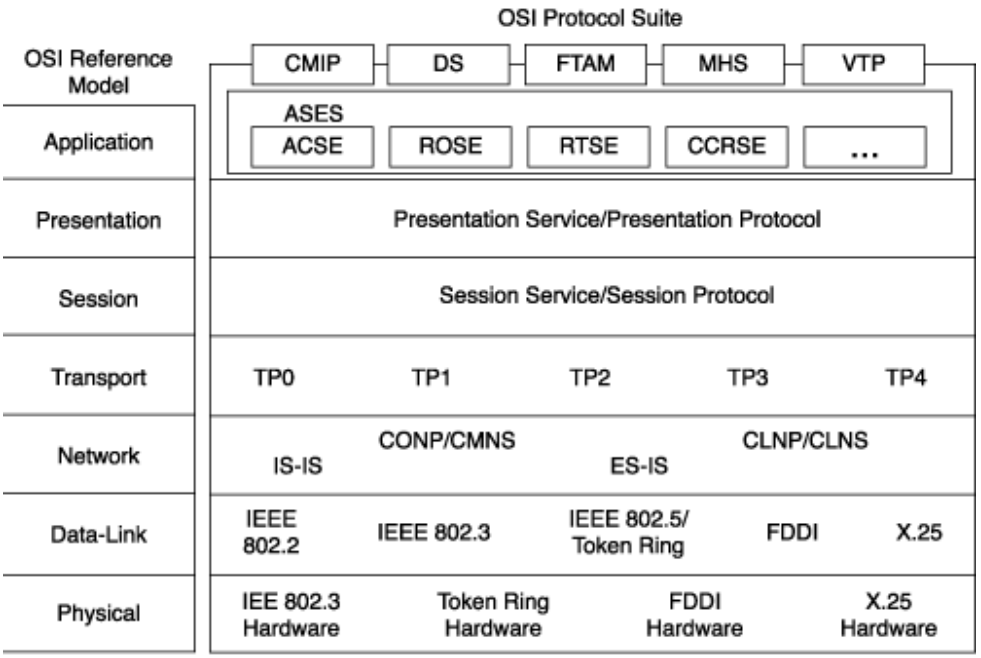


Figura.13.1. *Cómo el modelo OSI contiene al protocolo OSI.*

Diferencias entre CMNS (Servicio de red modo conexión) y CONP (Protocolo de red orientado a la conexión) son:

- CONP es un protocolo de la capa de red que transporta datos a la capa superior e indica errores sobre el enlace orientado a la conexión. CONP esta basado en el protocolo capa de paquetes (PLP) del X.25. CONP provee una interconexión entre CMNS y las capas superiores.

- CMNS ejecuta funciones relacionadas al establecimiento de caminos a través de CONP. CMNS incluye funciones de para iniciar una conexión y terminarla; este provee mecanismos para especificar QoS.

Diferencias entre CLNP (Protocolo de red sin conexión) y CLNS (Servicio no orientado a la conexión de red) son:

- CLNP es un protocolo de la capa de red para transportar datos a la capa superior e indica errores sobre el enlace de las conexiones. CLNP provee interconexión entre CLNS y capas superiores.

- CLNS provee servicios a la capa de transporte para el intercambio de información de ruteo. Cuando el soporte es proveído por CLNS , el enrutamiento usa protocolos de enrutamiento para el intercambio de información. CLNS no inicia ni termina una conexión, por que el camino o ruta son determinados de manera independiente por cada paquete que es transmitido a través de la red. CLNS provee el mejor esfuerzo de entrega, esto quiere decir que pueden perderse datos en el camino, dañarse, o duplicarse. CLNS confía en el protocolo de la capa de transporte para ejecutar la detección y corrección de errores.

13.4. Protocolos de enrutamiento OSI.

- ***Protocolo de descubrimiento ES-IS:*** ejecuta un "ruteo" entre un Sistema Final y un Sistema Intermedio referente a un ruteo a nivel 0. ES-IS es análogo a ARP en IP. Aunque este no es explícitamente un protocolo de enrutamiento, ES-IS es considerado como tal por que comúnmente es usado como un protocolo de enrutamiento para proveer el transporte de datos de fin-a-fin a través del sistema de red.

- ***Protocolo de ruteo IS-IS:*** ejecuta una jerarquía de enrutamiento (Nivel 1, Nivel 2 y Nivel 3) entre sistemas intermedios. El ruteo Nivel 3 es hecho entre dominios separados. Sin embargo, el protocolo de enrutamiento IS-IS a si mismo no es capaz de enrutar a Nivel 3.

Ruteo en un entorno OSI CLNS/CLNP

Cisco soporta los siguientes protocolos:

- ***IS-IS:*** es un protocolo dinámico del estado del enlace usado en ISO CLNS para un enrutamiento CLNP. Los routers usualmente operan como ISs y pueden cambiar

información con otros ISs usando el protocolo IS-IS. Un IS, en un router Cisco puede trabajar a Nivel 1, Nivel 2 o a Nivel 1-2.

- ***ISO-IGRP.***
- ***Static CLNS routers.***

13.5. IS-IS Integrado

¿Qué es IS-IS Integrado?

IS-IS es protocolo de enrutamiento del estado del enlace para la pila de protocolo OSI. Como tal, distribuye información de enrutamiento para la ruta de datos CLNP para el entorno del ISO CLNS.

IS-IS Integrado es una implementación del protocolo IS-IS para el ruteo de múltiples protocolos de red; éste es una versión extendida del IS-IS para el entorno mixto ISO CLNP e IP. IS-IS Integrado etiqueta los router CLNP con información relativa a redes y subredes IP. Puede ser usado por enrutamiento IP, ISO, o una combinación de ambos.

El IS-IS Integrado provee una alternativa a OSPF en un entorno IP, mezclando ISO CLNP e IP en solo un protocolo.

IS-IS Integrado tiene los siguientes rasgos:

- Longitud variable de mascara de red (VLSMs). La máscara y el prefijo son enviados en una actualización.
- Predistribución de rutas IP dentro y fuera de IS-IS.
- Sumarización de rutas IP.

13.5.1. ¿Quién usa IS-IS?

IS-IS es popular entre las compañías telefónicas y los grandes ISP. Esta popularidad fue gracias a que los ISP en torno al inicio de Internet y la elección de IS-IS sobre OSPF como IGP. En esa época se considero que IS-IS tenía pocas limitaciones técnicas que OSPF como un IGP.

El protocolo OSI soporta numerosos protocolos estándares en las capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

El direccionamiento de la capa de red OSI esta implementado paras ser usado por dos tipos de direccionamiento jerárquico: ***las direcciones NSAP*** **y** ***el subconjunto NSAP*** (NET). Un NSAP es un punto abstracto que sirve de frontera entre la capa de red y de transporte. Cada entidad de la capa de transporte tiene asignado un NSAP, en el sistema de redes OSI cada dirección usa una dirección NSAP diferente.

13.5.2. IS-IS Integrado versus OSPF.

Son dos protocolos del estado del enlace con los siguientes rasgos similares:

- Representación del estado del enlace, envejecimiento y métricas.
- Una base de datos del estado del enlace y algoritmos SPF.
- Actualizaciones, decisiones y procesos de inundación.

OSPF se basa en backbone central o área 0, con todas las áreas físicamente conectadas al área 0. En OSPF, el borde entre áreas esta dentro de la ruta, los ABRs, y cada enlace pertenece a una sola área. Con este tipo de jerarquía, es necesario sumarizar la estructura del direccionamiento IP dentro del backbone y reducir la cantidad de información que corre en el área y anunciarlo por la red.

En comparación, IS-IS Integrado también tiene una jerarquía con Niveles: Nivel 1 y Nivel 2, pero en IS-IS, los bordes de área o enlaces, mas bien esta en los routers. Cada ruta IS-IS pertenece al nivel 2 del área. Significativamente, son pocos los paquetes del estado del enlace (LSPs), conocidos como unidades de datos del protocolo del estado del enlace (PDUs), así, muchos mas routers pueden pertenecer a una misma área. Esta capacidad hace más escalable a IS-IS que OSPF. IS-IS permite mas flexibilidad al extender el backbone para engrosarlo, adicionando routers de Nivel 2., este proceso es menos complicado que OSPF.

El protocolo tiene un gran parecido con OSPF ya que en ambos se utiliza el estado de enlace para la búsqueda de caminos (utilizan puentes designados para eliminar bucles) y la asignación de redes en grupos para mejorar la eficiencia de la red. Pero IS-IS tiene ciertas ventajas respecto a OSPF tales como compatibilidad con IPv6 o que permite conectar redes con protocolos de encaminamiento distintos.

Según las pilas que posea el router este podrá ser:

- OSI-only, no admite protocolos TCP/IP.
- TCP/IP-only, no admite protocolos OSI.
- DUAL, admite ambos protocolos.

Esto hace posibles distintas topologías según se quiera que ciertas áreas con distintos protocolos puedan intercambiar tráfico o no

13.5.3. Nivel 1, Nivel 2 y Nivel 1-2 del Routers.

Una red IS-IS es llamado ***dominio*****;** este es equivalente al Sistema Autónomo en OSPF.

Dentro del dominio, en una jerarquía de Nivel 2 existe:

- ***Nivel 1 ISs*** son responsabilidad del enrutamiento a ESs dentro del área. Este es similar al OSPF interno en un área stub.

- ***Nivel 2 ISs*** ruta entre solo áreas. Este es similar al router interno en el backbone en OSPF.
- ***Nivel 1-2 ISs*** ruta entre áreas y backbone. Particularmente en el nivel 1 ruteo intra-área y el Nivel 2 ruteo inter-área. Este es equivalente a los ABR en OSPF.

Los router de Nivel 1 solo hacen referencia a estaciones (ES) de routers por que ellos habilitan la comunicación entre los otros y el resto de la red.

Nota: una estación final no puede comunicarse por la ruta CLNP.

Un grupo contiguo de rutas de Nivel 1 se definen en un área. Los routers de Nivel 1 mantienen la base de datos que definen una imagen de su misma área y sus puntos de salida a áreas vecinas.

Rutas de Nivel 2 se refieren a como las áreas están interconectadas a áreas de Nivel 1. Los routers de Nivel 2 almacenan una base de datos separada que cuenta sólo con la topología de la información de inter-área.

Rutas de Nivel 1-2 mantiene dos bases de datos separadas del estado del enlace; esto permite que actué como si ellos fueran dos routers, como sigue:

- Los que soportan el Nivel 1 funcionan comunicándose con otros routers de Nivel 1 en otras áreas y mantiene información LSP de Nivel 1 en una base de datos topológica de Nivel 1. Ellos informan a los otros routers de Nivel 1 que ellos están fuera del área.

- Los que soportan el Nivel 2 funcionan comunicándose con los restantes del backbone y mantiene una base de datos topológica de Nivel 2 separada de la base de datos de Nivel 1.

IS-IS no toma el concepto de área 0 como en OSPF. En lugar de eso, un backbone IS-IS puede aparecer como un conjunto áreas distantes interconectadas por una cadena de router de Nivel 2, tejiendo un camino a través y entre las áreas de Nivel 1. El backbone IS-IS consiste en un conjunto de routers de Nivel 1-2, y deben estar continuos.
Los LSP es un punto del estado del enlace son enviados con una dirección unicast. Los LSPs en un medio broadcast (LAN) son enviados con una dirección multicast.

Como con OSPF, un router en una LAN envía información LSP en beneficio a esa LAN. En IS-IS, este router es llamando *Sistema Intermedio Designado* (DIS). Este pseudonodos, representa la LAN, y envía los paquetes LSPs de Nivel 1 y Nivel 2 por separado en representación de la red.

Nota: El respaldo de DIS (BDIS) no es soportado en IS-IS, como en OSPF (BDR). Si el DIS falla, se hace una nueva elección.

13.5.4. Estructura de las direcciones NSAP.

Una dirección NSAP esta conformada de 20 octetos y contiene las siguientes partes:

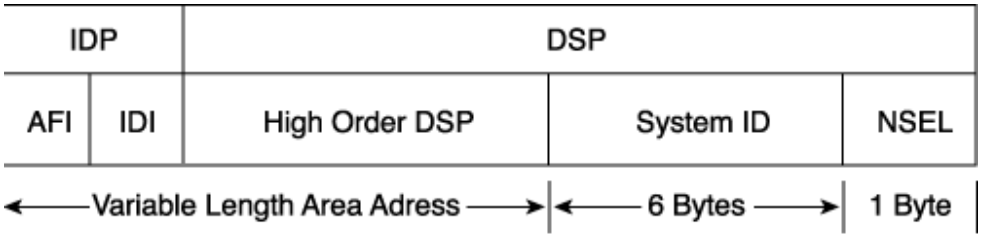


Figura 13.2. *Estructura de una dirección NSAP.*

- ***AFI (The Authority and Format ID):*** Especifica el formato de las direcciones y la jerarquía que asignan a las direcciones. El AFI es de 1 byte.

- ***El Identificador de Interdominio (IDI-Interdomain ID):*** Identifica el dominio. El IDI puede tener más de 10 bytes.

- El AFI e IDI conjuntamente forman una parte de un interdominio superior ***(IDP)*** en las direcciones NSAP. Esto puede igualar al classfull en grandes redes IP.

- ***DSP o HODSP*** *(Parte Específica del Dominio de Alto Orden):* Es usado para subdividir el dominio dentro de áreas. Esto puede considerarse como el equivalente OSI de una subred en IP.

- ***El ID de Sistemas:*** Identifica un dispositivo OSI individual. En OSI, un dispositivo tiene una dirección, como en el protocolo DECnet. Este es diferente a IP, en el cual cada interfaz tiene una dirección. OSI no especifica una longitud fija para el ID del Sistema, pero este especifica que debe ser consistente en cada dispositivo. El software Cisco fija el ID del Sistema en 6 bytes precediendo un byte NSEL (NSAP Selector).

Nota: Una dirección MAC es también usada como el ID del Sistema.

El NSEL (es también conocido como el N-Selector, el servicio identifica el proceso ID) identifica un proceso en un dispositivo. Esto es equivalente a un puerto o socket en IP. El NSEL tiene un byte de longitud. No es utilizado para decisiones de enrutamiento. Cuando el NSEL tiene un valor de 00, la dirección identifica el dispositivo y su dirección de nivel de red. En este caso el NSAP es conocido como una etiqueta de entidad de red (NET).

El HODSP, ID de Sistema y NSEL forman una parte de un dominio especifico de la dirección NSAP.

13.5.5. NSAPs de IS-IS versus ISO-IGRP

IS-IS y ISO-IGRP interpreta el NSAT de diferente forma.

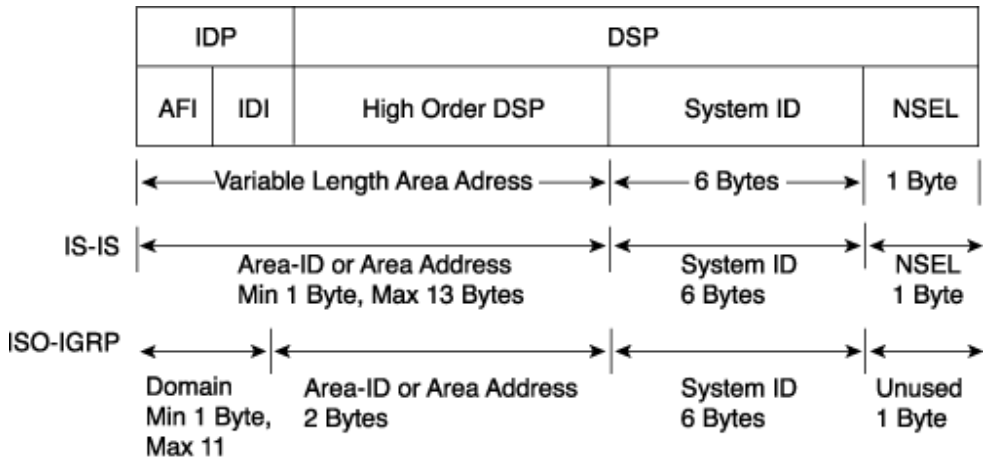


Figura 13.3. *Como IS-IS e ISO-IGRP interpreta una dirección NSAP.*

IS-IS usa una arquitectura de dos capas, uniendo el IDP y el campo HODSP para identificar una dirección de área (nivel 2), recordar que el ID de Sistema es usado para el enrutamiento de nivel 1. Cuando es usado en IS-IS, el NSAP es dividido en tres partes, 1 octeto para el NSEL, 6 octetos para el ID del Sistema, y de 1 a 13 octetos para la dirección del área o el campo Identificador de área. Un NSAP tiene una longitud variable de 8 a 20 octetos. Usualmente usa más de 8 bytes para permitir la asignación de dispositivos en las áreas.

Las rutas ISO-IGRP están basadas en una arquitectura de tres niveles:

- ***Dominio*** (utilizando los campos AFI y el IDI para el Nivel 3).
- ***Área*** (utilizando el campo HODSP para el nivel 2).
- ***El ID del Sistema*** (para el Nivel 1). El IS-IS lo trata como un simple ID de Área, ISO-IGRP lo divide en un dominio y un área. El ISO-IGRP utiliza los 2 bytes de la izquierda para el ID del Sistema como el ID del Área o el campo de dirección de área, permitiendo teóricamente 65,535 áreas en una red ISO-IGRP. Todo los demás (un máximo de 11 bytes) es tratado como un ID de Dominio. Por consiguiente, la longitud mínima para NSAP ISO-IGRP es 10 bytes (1 byte para NSEL, 6 bytes para el ID del Sistema, 2 bytes para el Área, y un mínimo de 1 byte para el dominio).

El ISO-IGRP envía información de enrutamiento basada en el Dominio (longitud de la variable), área (longitud fija de 2 bytes para el protocolo), y finalmente el ID de Sistema (fijado en 6 bytes). El NSEL no es utilizado por el ISO-IGRP.

13.5.6. Etiqueta de la Entidad de Red (NET).

Como se discutió anteriormente, si el campo NSEL tiene el valor 00, el NSAP se refiere al propio dispositivo esto es el equivalente al direccionamiento OSI de la capa 3 de ese dispositivo.

Esta dirección con el NSEL igual a 00, es conocido como NET. El NET es usado por los router para identificarse ellos mismos en los LSPs. Por consiguiente, esto forma las bases para calcular el enrutamiento OSI.

NET es un NSAP con el valor NSEL=00.

Un punto clave es que una dirección NSAP con el valor de NSEL a 00 es llamada NET.

NET y NSAP son especificados en dígitos hexadecimales y debe comenzar y terminar con un límite de un byte.

El prefijo oficial del NSAP son requisitos en el enrutamiento CLNS. Las direcciones comienzan con un determinado valor AFI = 39 para un país completo a 47 para comunicaciones internacionales, 43 ó 57 para comunicaciones de teléfono, 57 para ISDN, y 49, este ultimo valor son considerados como direcciones.privadas (análogos al RFC 1918 para las direcciones IP) estas direcciones son rotadas por IS-IS; sin embargo este grupo de direcciones no deben ser publicadas por otras redes CLNS.

El software de Cisco para el proceso de enrutamiento IS-IS interpreta las direcciones NSAP como sigue (desde la derecha o dígitos de menor peso, hasta los de mayor peso):

El último byte es el NSEL y debe ser especificado como un único byte, con dos dígitos hexadecimal, precedido por un periodo. En un NET, el campo N-Selector se le asigna el valor 00.

Los 6 bytes precedentes (esta longitud es fijado por Cisco) son el ID del Sistema. Usualmente no se utiliza para direcciones MAC en los routers (para IS-IS Integrado) o una dirección IP (por ejemplo, la dirección IP de la interfaz loopback) como parte del ID del Sistema.

El proceso de enrutamiento de IS-IS del software Cisco trata el resto de direcciones como el ID del Área, o direcciones de área como sigue:

De 1 a 13 bytes de longitud. Usando un campo de 1 byte para los limites de área para alcanzar las áreas definidas. Usualmente se usan 3 bytes para el ID de Área, con un AFI de 1 bytes y 2 bytes adicionales para el ID de Área. Por ejemplo, en la dirección 49. 0001.0000.0c12.3456. 00, el AFI es 49 y los 2 bytes adicionales son 0001 para un ID de área efectiva de 49.0001.

El Software de Cisco intenta sumarizar el ID de Área mas posible. Por ejemplo, si una red IS-IS esta organizada como un gran área subdividida en áreas menores y estas son reflejadas en el ID de área asignada, entonces:

Entre las áreas menores el software de Cisco enrutará en base a todo el ID del Área. Entre el área mayor sumarizará la porción del ID del área con el limite del área mayor.

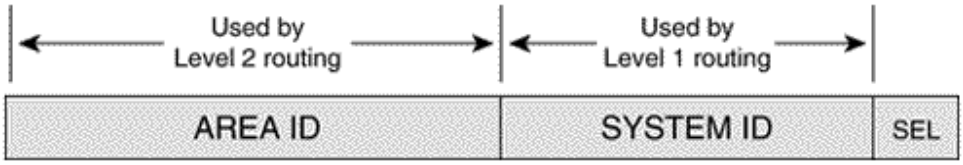


Figura 13.4. *Estructura de un NET.*

Ejemplos de NSAP

Los siguientes ejemplos ilustran como una dirección NSAP es interpretada por IS-IS e ISO-IGRP:

El NSAP 49.0001.aaaa.bbbb.cccc.00 consiste en lo siguiente:

Para IS-IS:
Área = 49.0001
ID del Sistema = aaaa.bbbb.cccc
N-selector = 00

Para el ISO-IGRP:
Dominio = 49
Área = 0001
ID del Sistema= aaaa.bbbb.cccc
N-selector = ignorado por ISO-IGRP

El NSAP 39.0f01.0002.0000.0c00.1111.00 consiste en lo siguiente:

Para IS-IS:
Área = 39.0f01.0002
ID del Sistema= 0000.0c00.1111
N-selector = 00

Para ISO-IGRP:
Dominio = 39.0f01
Área = 0002
ID del sistema = 0000.0c00.1111
N-selector = ignorado por ISO-IGRP

Identificador de Sistema en IS-IS

En IS-IS el ID del Área es asociado con el proceso de enrutamiento de IS-IS; un router puede ser miembro de una única área del Nivel 2. El enrutamiento puede pertenecer a

una única área. El ID del Área o direcciones de área únicamente identifica el router de área, y el ID del Sistema identifica cada nodo.

Restricciones de Áreas e ID del Sistema.

Son las siguientes:

- Todos los routers de un área deben utilizar la misma dirección de área. Las direcciones de áreas son compartidas por todas las áreas definidas.

- Un ES establece adyacencias con router de nivel 1 solo si ambos comparten una dirección de área común. En otras palabras los ESs reconocen solo los ISs (y ESs en la misma subred) que comparte la misma dirección de área.

- El enrutamiento de área (Nivel 1) es basado en el ID del Sistema. Si embargo cada dispositivo (ES e IS) debe tener un único ID del Sistema dentro del área, y todos los ID del Sistema deben tener la misma longitud. Cisco establece un ID de Sistema de 6 bytes.

- Todos los ISs del Nivel 2 tienen que conocer todos los otros ISs en el nivel 2 del Backbone. Por consiguiente ellos deben de tener un único ID de Sistema dentro del área.

Los ID del Sistema.

El ID de Sistema debe identificar una solo área. Como fue notificado recientemente, usualmente no se utiliza para direcciones MAC en los routers (particularmente para el IS-IS Integrado) o una dirección IP (por ejemplo, la dilección IP de la interfaz loopback) como parte del ID del Sistema.

Es generalmente recomendado que el ID del Sistema mantengan a través del dominio; de esta forma ellos nunca van a tener conflictos con el Nivel 1 y el Nivel 2, si los dispositivos son movidos a un área diferente, por ejemplo:

Todos los ID del Sistema en un Dominio deben de tener la misma longitud. Esto es una regla de OSI; Cisco enfoca esto fijando la longitud del ID del Sistema en 6 bytes en todos los casos.

13.5.7. Puntos de Adherencia de la subred y circuitos.

Los dos términos utilizados en IS-IS son: puntos de adherencia de la subred (SNPA) y circuitos.

Un ***SNPA*** es el punto con el cual los servicios de la subred son proveídos. Esto es similar a la dirección de la capa 2 correspondiente a la dirección de la capa 3 (NET o NSAP). El NSPA es usualmente tomado de lo siguiente:

- La dirección MAC en una Interfaz LAN.
- El ID del Circuito virtual para X.25 o ATM.
- El identificador del estado del enlace (DLCI) para Frame Relay.
- Para las interfaces HDLC, el SNPA es simplemente HDLC.

Un ***enlace*** es la parte entre dos vecinos ISs y es definida en lo alto cuando la comunicación es posible entre los dos vecino SNPAs.

Un ***circuito*** es una interfaz; las interfaces están únicamente identificada por el ID del Circuito.

Los router asignan un octeto al ID de Circuito para cada interfaz en el router, como sigue:

En el caso de una interfaz punto a punto, este es el único identificador para el circuito-por ejemplo, 03.

En el caso de las interfaces LAN (y otras interfaces BMA), el ID del circuito tiene el objetivo de terminar el ID del Sistema de la forma DIS a la forma de 7 bytes (ID LAN). Un ejemplo es 1921.6811.1001.03, donde 03 es el ID del Circuito.

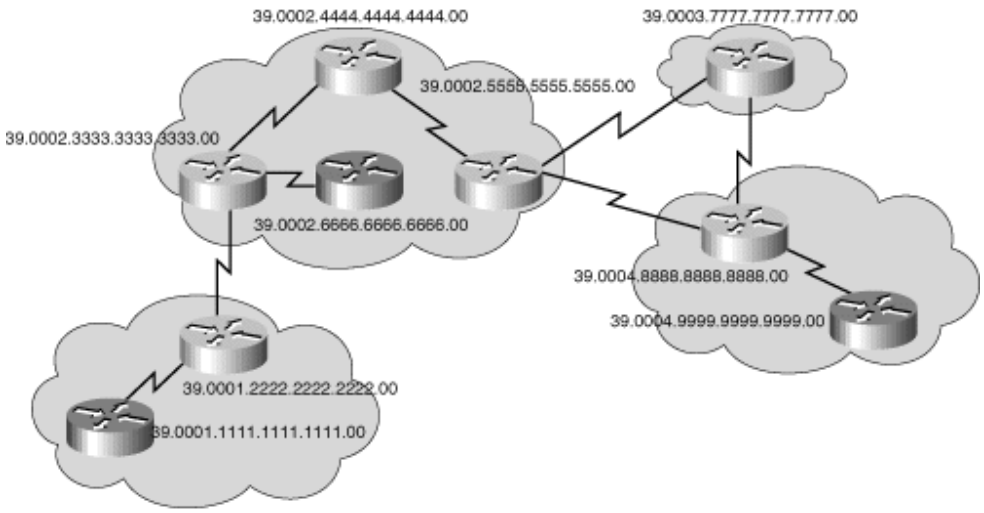


Figura 13.5. *Ejemplo de una dirección NSAP en una red IS-IS.*

13.5.8. PDUs IS-IS

La pila OSI define una unidad de datos como unidad del protocolo de datos (PDU). Un marco es definido por OSI como una PDU del estado del enlace, y paquete (o datagrama, en el mundo IP) como una PDU de red.

Las PDUs IS-IS y ES-IS contienen múltiples campos de longitud variable, dependiendo de la función de la PDU. Cada campo contiene un código de tipo, una longitud, y valores asignados.

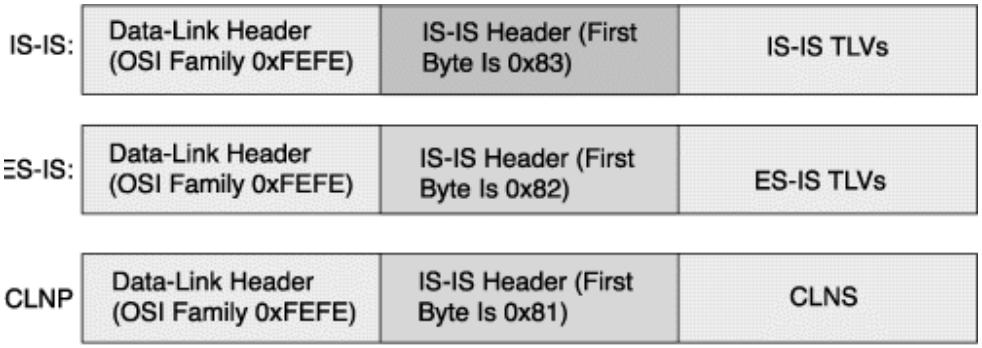


Figura 13.6. *PDU*

Formato de una PDU IS-IS

IS-IS utiliza 9 tipos de PDU en estos procesos, y cada PDU es identificada por un tipo de número de cinco bit. El PDU cae dentro de tres categorías como mostramos en la tabla 13.1.

Tabla 13.1. *Tipos de IS-IS PDU.*

Tipos de IS-IS PDU.	
IS-IS PDU	**Tipo de Numero**
Hello PDUs	
Level 1 LAN IS-IS Hello PDU	15
Level 2 LAN IS-IS Hello PDU	16
Point-to-point IS-IS Hello PDU	17
PDUs del Estado del Enlace	
Level 1 LSP	18
Level 2 LSP	20
PDUs Números de Secuencia	
Level 1 CSNP	24
Level 2 CSNP	25
Level 1 PSNP	26
Level 2 PSNP	27

Existen cuatro tipos de paquetes generalmente, cada tipo puede ser del Nivel 1 o Nivel 2:

- *LSP:* usada para distribuir la información del estado del enlace.

- *PDU Hello:* usado para establecer y mantener adyacencias.
- *PSNP:* usado para aceptar y responder información del estado del enlace.
- *CSNP:* usado para distribuir a los router la base de datos del estado del enlace.

13.5.9. Paquetes del estado.

En esta sección se describen los LSPs IS-IS.

Representación de la red.

En OSI, hay dos tipos de enlaces físicos:

- ***Broadcast:*** Medio Multiacceso, este tipo soporta direcciones que se refieren a grupos dentro del sistema y son típicamente LANs.

- ***Nobroadcast*****:** este tipo de medio debe usar direcciones ESs individuales y son típicamente usadas en enlaces WAN. Esto incluye los enlaces punto a punto, enlace multipunto y enlaces establecidos dinámicamente.

Consecuentemente IS-IS soporta solo dos tipos de medios para el estado del enlace:

- ***Broadcast para LAN.***
- ***Punto a punto para otros medios.***

IS-IS no atiende el concepto de red NBMA. IS-IS recomienda los enlaces punto a punto (por ejemplo, subinterfaces) en lugar de las redes NBMA tales como ATM nativo, Frame Relay o X.25.

13.6. Contenido LSP.

En IS-IS un router se describe a si mismo con un LSP. Los routers LSP contienen lo siguiente:

- Una cabecera LSP:
- Tipo y Longitud de la PDU.
- El ID de la PDU y el Número de Secuencia
- Tiempo de vida para este LSP (usado para la edad del LSPs).

Valor del tipo de longitud (TLV) campo de longitud variable:

- Los router vecinos ISs (usado al construir el mapa de la red)
- Los router vecinos ESs
- Información de autenticación (usado al obtener las actualizaciones)
- Conexiones de subredes IP (opcional para el IS-IS Integrado)

Los números de secuencia LSP permite que los routers confirmen la recepción solo de la ultima LSP en el calculo de rutas, de esta manera elimina los LSP duplicados al introducir las entradas en la tabla topológica.

El campo de tiempo de vida en el LSP es usado para el proceso de edad del LSP al asegurar la antigüedad y validez del LSP cuando son removidos de la tabla topológica después de un tiempo adecuado. Los LSP renuevan el tiempo de vida contando desde de 1200 segundos a 0.

13.7. Representación de Redes en IS-IS.

13.7.1. Representación de una LAN.

El algoritmo de Dijkstra usado por IS-IS requiere de un router virtual (seudo nodo) para un medio broadcast al construir el gráfico de la ruta mas corta a partir de un único vértice origen a todos los otros vértices.

Por esta razón, el DIS es seleccionado al generar un LSP representando a un router virtual, conectándolo a los otros routers al iniciarse a modelar la topología. La elección del proceso para la elección del DIS esta basada en elegir el primer router con la prioridad más alta y el segundo router con dirección MAC más alta.

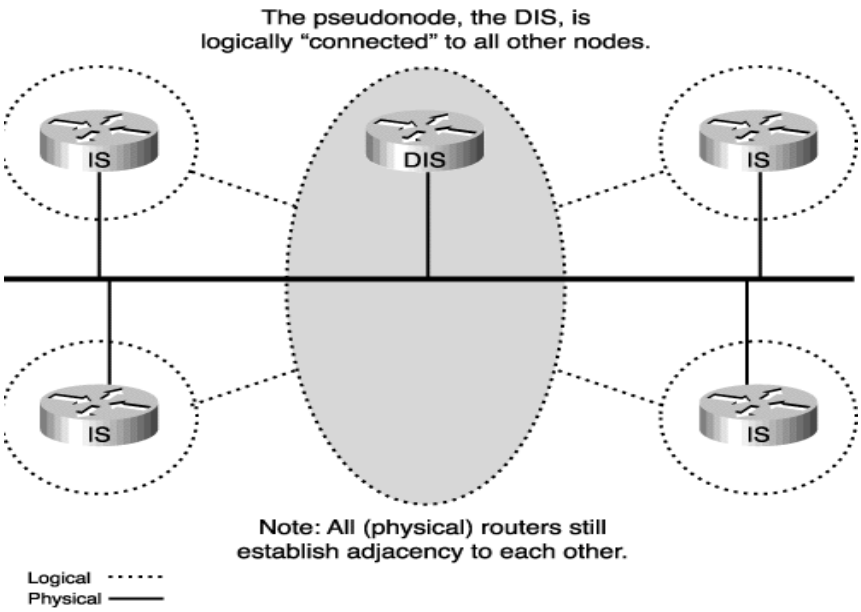


Figura 13.7. *Selección de un DR IS-IS en una LAN.*

En IS-IS, todos los routers en una LAN establecen adyacencias con todos los router y con el DIS. Esto, es si el DIS falla, así otro router puede tomar inmediatamente el cargo o fallara la topología de la red.

Esto es diferente en OSPF. Se elige un router DR y BDR, los otros routers establecen adyacencias solo con el DR y con el BDR.

13.7.2. Variables LSP.

Los LSP IS-IS incluyen específicamente información acerca de la adherencia de los routers. Esta información esta incluida en los campos TLV en el cuerpo del LSP:

- El enlace de los router vecino (ISs), incluyendo las métricas de las interfaces.
- El enlace de los vecinos ESs.

Nota: Si el IS-IS Integrado es operacional, la adherencia de las subredes IP es descrita como ESs, usando un TLV especial específico para información IP.

Las métricas de los enlaces IS-IS son asociadas con la interfaz de salida hacia el vecino IS (router). Cuatro métricas se pueden especificar, como sigue:

- ***Métrica por defecto (requerido): costo,*** el calculo no es automático comparado con algunos protocolos de enrutamiento que calculan la métrica del enlace automáticamente basándose el valor de banda ancha (OSPF) o en la banda ancha/retardo (EIGRP). Usando métricas cortas, el costo de una interfaz esta entre 1 y 63 (6 bits para el valor de la métrica). Todos los enlaces usan por defecto un valor de 10. El total del costo a un destino esta dado por la suma de todas las interfaces de salida a lo largo del camino del origen al destino, el camino mas corto es el elegido.

- ***Retardo, Costo y Error (Opcional):*** estas métricas son usadas para dar un tipo de servicio de enrutamiento (ToS). Este puede usarse como una alternativa para el cálculo de rutas referente al bit DRT (Retardo, Rendimiento y Fiabilidad) en el campo IP ToS.

13.7.3. Métrica Extendida

En IS-IS, el total de la métrica de los caminos esta limitada a 1023.
Las direcciones del software de Cisco publican el campo de la métrica con 24 bits. Usando un nuevo estilo de métrica, el enlace métrico ahora tiene un valor máximo de 16, 777,215 (2^{24} -1) con un total de métrica de 4,294,967,295 (2^{32}-1).

Corriendo diferentes estilos de métricas en una sola red presenta un serio problema: los protocolos del estado del enlace calculan rutas loop-free por que todos los routers (dentro de una área) calculan la tabla de enrutamiento basadas en la base de datos del estado del enlace.

Mensajes Hellos

IS-IS usa PDUs Hellos al establecer adyacencias con los otros routers (ISs) y ESs. Una PDU Hellos lleva información sobre el sistema, sus parámetros y capacidad.

IS-IS tiene tres tipos de PDU Hellos, como sigue:

- *ESH*, enviado por un ES a un IS.
- *ISH*, enviado por un IS a un ES.
- *IIH*, usado entre dos ISs.

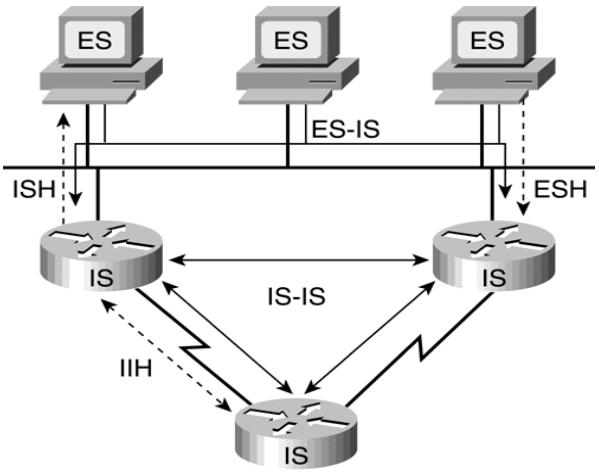


Figura 13.8. *Los tres tipos de PDUs hellos se muestren en la figura.*

Comunicación IS-IS

ISs usa IIHs al establecer y mantener las relaciones con sus vecinos. Cuando una adyacencia es establecida, el ISs intercambia información usando LSPs.

ISs también envía ISHs. ESs listan para estos ISHs y aleatoriamente eligen un IS (el que envía el primer ISH al escuchar) al enviar todos sus paquetes. OSI ESs no requiere configuración al enviar paquetes al resto de la red.

Para un destino en particular, ISs fuerza el reenvió (RD) de mensajes a los ESs que provienen de una ruta optima desconectada del segmento. Este proceso es similar al redireccionamiento IP.

13.7.4. Representación de WANs.

Categorias de WANs para IS-IS Integrado.

Típicamente las WANs son implementadas como punto-a-punto o punto-a-multipunto, y además soportan conexiones múltiples. Estas WANs, típicamente no soportan la difusión, y de este modo son clasificadas como NBMA.

IS-IS Integrado considera 3 Categorías de WANs, como las siguientes:

- Point-to-point leased circuits (Circuitos alquilados punto-a-punto). Allí son unos pocos los emitidos durante la configuración de IS-IS.

- Dialup connections (conexión de marcación): Configurar IS-IS sobre dialup podría ser evitado, excepto al usarlo como un soporte.
- Switched WANs (WANs conmutadas): Varios diseños alternativos existen para las Redes de Trabajo NBMA.

Estas 3 categorías son abordadas con detalle mas adelante en las siguientes secciones.

Point-to-point leased circuits (Circuitos alquilados punto-a-punto)

Las WANs punto-a-punto son típicamente circuitos alquilados entre 2 routers. Una WAN tiene 2 dispositivos adheridos, uno a cada fin del circuito. Usualmente tales enlaces corren con HDLC Cisco o con el Protocolo Punto-a-Punto (PPP). Este corresponde exactamente a la clasificación IS-IS Integrado de una red de trabajo punto-a-punto.

Nota: Un circuito punto-a-punto aun es considerado como una red NBMA, justamente como una conexión Ethernet back-to-back es aun considerada una LAN. Ambos son ejemplos de redes de múltiples-accesos que tienen 2 dispositivos ligados o enlazados.
Sobre un enlace Punto-a-punto un único IIH PDU es enviado. Esto especifica tanto si la adyacencia esta a Nivel-1, Nivel-2 o ambos niveles.

Cuando la adyacencia es establecida, cada vecino envía un CSNP, describiendo el contenido de la Base de Datos de Estado de Enlace. Cada router entonces instancia cualquier perdida de LSPs de los vecinos usando PSNPs y admite la recepción de los LSPs con PSNPs.

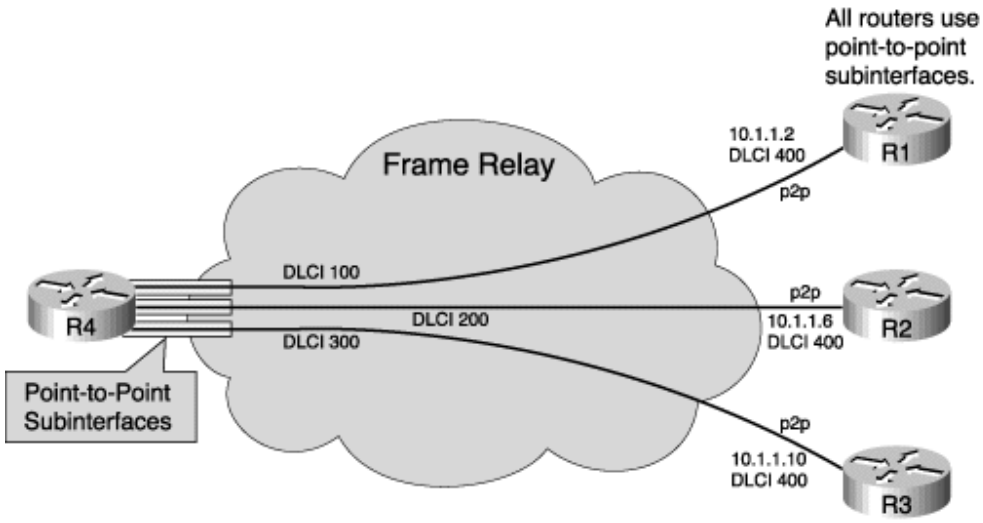


Figura 13.9. *Red Frame Relay usando subinterfaces punto-a-punto*

Dialup

La red de Dialup (marcado), usando marcar-sobre-demanda de enrutamiento (DDR) puede ser configurada como cualquier implementación de WAN (punto-a-punto o punto-a-multipunto), como sigue:

- Legacy DDR dialup connections (Esta es, usando el comando **dialer map**) son NBMA (aún si bien ellos podrían usar PPP como su línea de protocolo) porque una única interfaz puede soportar múltiples destinos.

- Dialer profiles and dialer virtual profiles are point-to-point connections (el perfil dialer y el perfil de dialer vitual son conexiones punto-a-punto)(porque un perfil dialer representa un perfil remoto), pero estos pueden sufrir de daños-de-vecinos, retardación similar a estos para las redes NBMA.

- Los perfiles virtuales Dialer son conexiones punto-a-punto en la cual la interfaz cae inmediatamente si el remoto finaliza desconectando. Este adelanta la rápida detección de los vecinos-perdidos y la rápida convergencia.

Nota: Las interfaces Dialup son no tratadas con auspicio en este libro. Como una regla general usted evitara el uso de IS-IS sobre dialup, excepto para suministrar dial-backup opcionalmente.

Switched WANs (WANs conmutadas)

IS-IS puede trabajar sobre una Red Multipunto NBMA solo si la red es configurada con una malla completa (full). Cualquier cosa menor que una malla full pude causar serias conectividades y publica el enrutamiento. Sin embargo, aun si una malla full es configurada, esta no garantiza que una malla full exista por todo el tiempo. Una falla en la subyacente Red switcheada WAN o en una configuración en uno o mas routers podría detener la malla full temporalmente o permanentemente. Por consiguiente usted abordaría la configuración multipunto NBMA para una Red IS-IS. Use más bien subinterfaces punto-a-punto.

Las subinterfaces punto-a-punto usualmente serian configuradas con su propia subred IP (típicamente con unos 30 bits, o /30 mascara de subred). En las redes IP modernas usan direccionamiento privado o sub-redes de variables-largas usualmente con suficientes direcciones IP de reservas que pueden ser aplicadas a sub-interfaces punto-a-punto.

Alternativamente, porque IS-IS Integrado usa paquetes CLNS para la propagación de rutas, el comando de configuración de interfaz **ip unnumbered** puede ser usado sobre las interfaces punto-a-punto. Sin embargo, estos trabajos solo se puede hacer sobre el mas reciente software Cisco IOS, la primera liberación falla al establecer una adyacencia IS-IS porque la subred IP no corresponde a cualquier fin de el enlace.

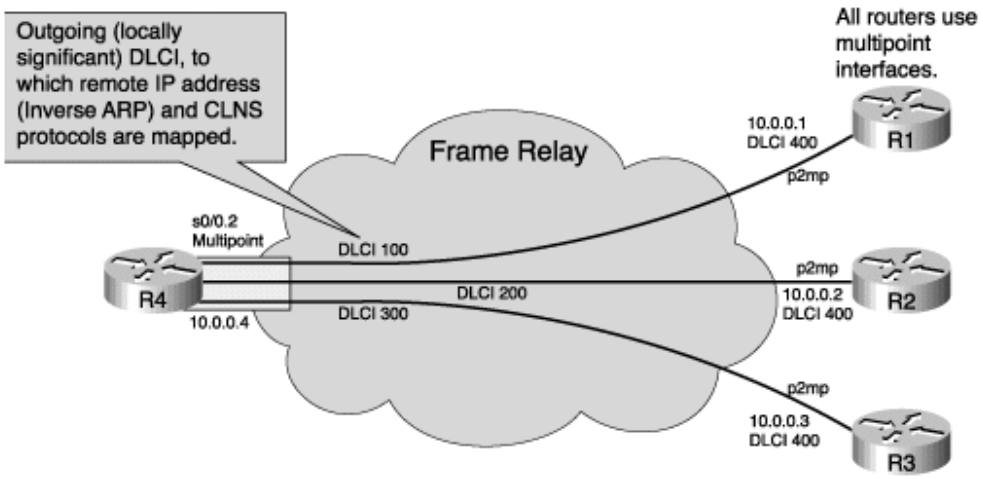


Figura 13.10. *Red Frame Relay usando Interfaces Multipunto.*

13.8. Adyacencias

El nivel 1 y Nivel 2 establecen adyacencias por separado. Si dos routers son vecinos en un área que corre en ambos niveles, ellos establecen dos adyacencias, uno para cada nivel. Las adyacencias del Nivel 1 y el Nivel 2 son almacenadas por separado en tablas de adyacencias de Nivel 1 y para Nivel 2.

En las LANs, dos adyacencias son establecidas con PDUs IIH específico de capa 1 y capa 2. Los routers de una LAN establecen adyacencias con otros routers de la LAN y envían LSPs a todos los routers de la LAN (diferente a OSPF, en el cual los routers establecen adyacencias solo con el router designado).

En un enlace punto a punto, tienen un formato común IIH, parte del cual especifica si los Hellos relaciona al Nivel 1, nivel 2, o ambos.

Por defecto, los PDUs Hellos son enviados cada 10 segundos, el intervalo al declarar un vecino como caído (esto es, tres paquetes Hellos perdidos) es 30 segundos. Estos tiempos son ajustables.

13.8.1. Adyacencias LAN

Los PDUs IIH anuncia el ID del Área. Los paquetes IIH anuncian por separado a los vecinos de Nivel 1 y Nivel 2. Las adyacencias son establecidas en base a la dirección de un área anunciada en la IIH entrante, y el tipo de router.

- Los routers de un área aceptan PDUs IIH solo de Nivel 1 de su propia área, por consiguiente, establece adyacencias solo con los router de su área.

- Los routers de una segunda área del mismo modo acepta PDUs IIH de nivel 1 solo de su propia área.

- Los routers de Nivel 2 (o procesos de Nivel 2 dentro de algún router de Nivel 1-2) acepta solo PDUs IIH de Nivel 2 y establece adyacencias solo de Nivel 2.

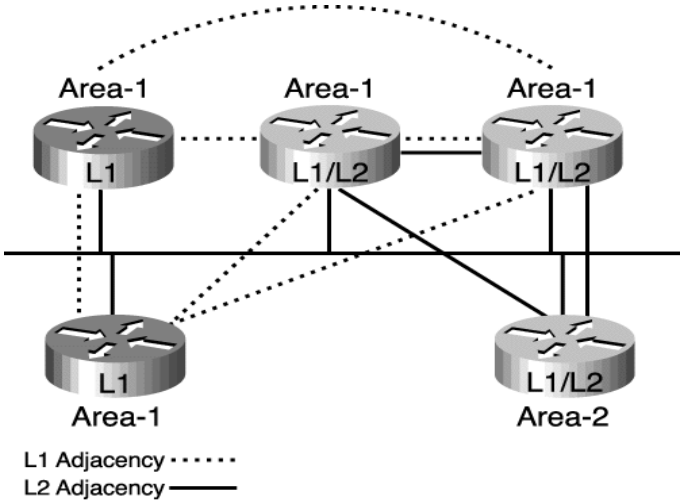


Figura. 13.11. *Adyacencias IS-IS basadas en la dirección de área y el tipo de router.*

13.8.2. Adyacencias WAN

En un enlace punto a punto (una WAN), los PDUs IIH son comunes para ambos niveles pero anuncian el tipo de nivel y el ID de Área en los Hellos.

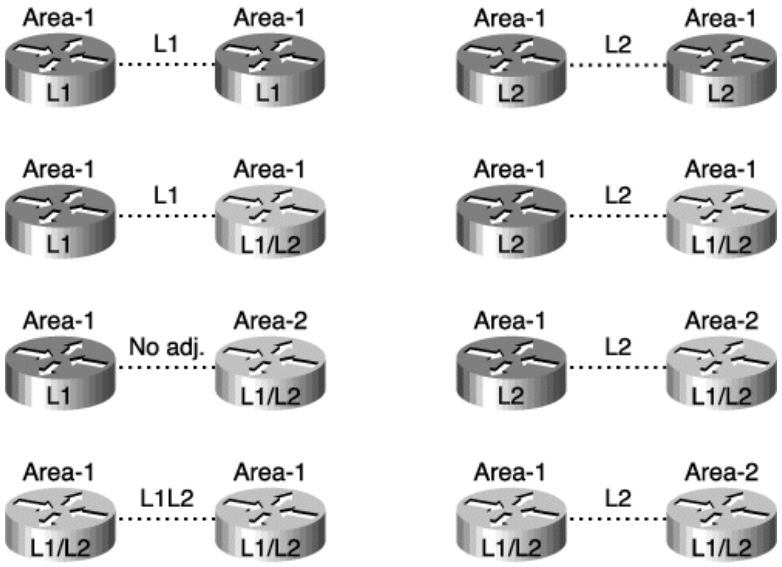


Figura.13.12. *En una WAN, las direcciones y el tipo de router son anunciados en un IIH común.*

Lo siguiente es verdad:

- Routers de Nivel 1 en una misma área (este incluye enlaces de routers entre solo nivel 1 y nivel 1-2) intercambian PDUs IIH especificando el nivel 1 y estableciendo adyacencias de nivel 1

- Routers de nivel 2 (en la misma área o entre áreas, incluyendo enlaces entre routers de solo nivel 2 y nivel 1-2) intercambian PDUs IIH especificando el nivel 2 y las adyacencias de nivel 2.

- Dos routers de nivel 1-2 en la misma área establecen ambas adyacencias de nivel 1 y nivel 2, y mantienen estas con PDUs IIH comunes de ambos niveles de información nivel 1 y nivel 2.

- Dos routers de nivel 1-2 en diferente área establecen adyacencia solo de nivel 2.

- Dos routers de nivel 1 que están conectados físicamente pero en áreas diferentes (incluyendo uno solo un router de nivel 1 a un router de nivel 1-2 en un área diferente de nivel 1) intercambia información PDUs IIH de nivel 1 pero ignora estas por que el ID de área no es igual. Por consiguiente, estos no establecen adyacencias.

13.8.3. Adyacencias de nivel 2

- Nivel 1, solo estos routers establecen adyacencias de nivel 1.

- Routers de nivel 2 establecen adyacencia solo con adyacencias de nivel 2 (entre áreas).

- Routers de nivel 1-2 establecen ambos adyacencias de nivel 1 y nivel 2 con los otros routers vecinos de nivel 1-2 en la misma área.

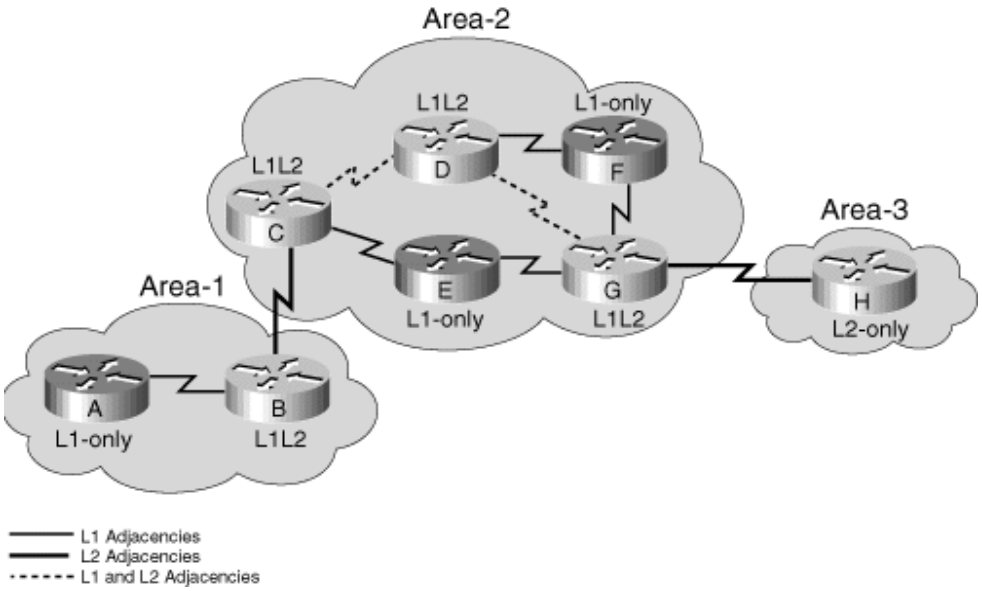


Figura. 13.13. *Adyacencias de nivel 2 deben de estar contiguos.*

Nota: en OSPF, este es un área backbone; aquí es un camino backbone. El camino de conexión de routers de nivel 2 es llamado el backbone. Todas las áreas y los backbone deben de ser contiguos. La adyacencia de nivel 2 existe independientemente si el área esta continúo.

13.9. Sincronización de la Base de Datos.

La sincronización de la base de datos del estado del enlace IS-IS es realizado usando PDUs especiales: PSNPs, y CSNPs. Estas PDUs especiales soportan un nombre genérico de número de secuencia PDUs (SNPs).

SNPs (PSNPs y CSNPs) asegura que los LSPs son enviadas de fuentes fidedignas.
SNPs contiene la descripción de la LSP, no la actual, información detallada de la LSP, pero describe el encabezado de las LSPs.

PSNPs usualmente contiene la descripción de solo una LSP. Estas son usadas como sigue:

- Al admitir la recepción de una LSP.
- Al pedir una LSP completa por una pérdida de información en el router que publicó la base de datos topológica.

CSNPs son enviados periódicamente a una LAN. La recepción de routers puede comparar el listado de LSP en el CSNP con otras bases de datos del estado del enlace y respondiendo algunos LSPs.

CSNPs son enviados a enlaces punto a punto cuando el enlace esta activo. En el software de Cisco, periódicos CSNPs pueden configurarse en los enlaces punto a punto.

- Una falla del enlace.
- El router R2 notifica la falla y publica un nuevo LSP notificando el cambio.
- El router R1 recibe el LSP, lo almacena en la tabla topológica, y envía un PSNP de vuelta al R2 al admitir la recepción del LSP.

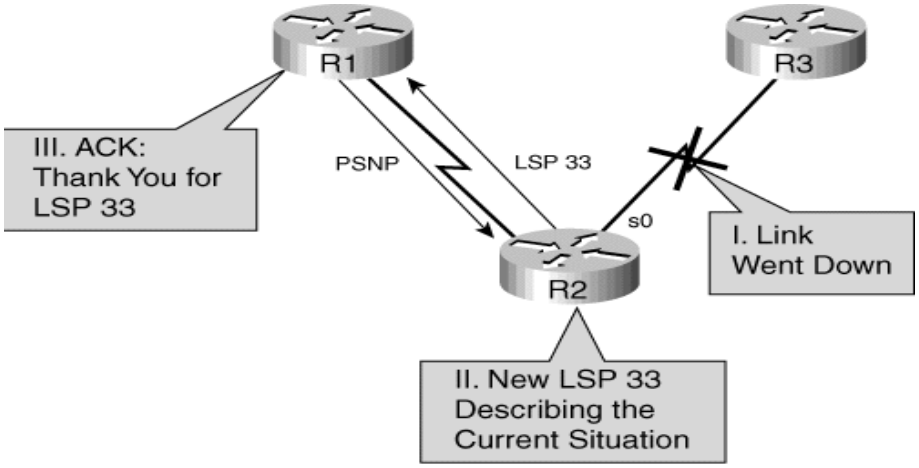


Figura 13.14. *Sincronización de la base de datos del estado del enlace en una red punto a punto.*

En una LAN, el DIS periódicamente envía CSNPs listando los LSPs que están soportando la base de datos del estado del enlace. Esta es multidifundida a todos los routers en la LAN.

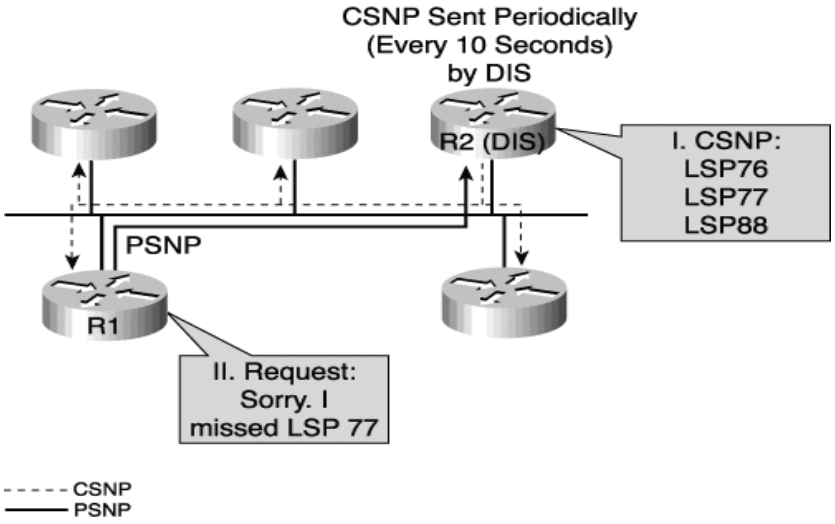


Figura. 13.15. *Sincronización de la base de datos del estado del enlace en una LAN.*

13.10. Configuración Básica de un router IS-IS.

En esta sección se muestran los comandos para la configuración y para arreglar desperfectos en un router Cisco con IS-IS Integrado.

13.10.1. Configuración del IS-IS Integrado.

En esta sección se identifican los pasos usados para la configuración básica del IS-IS Integrado en un router Cisco.

13.10.2. Pasos para configurar IS-IS Integrado.

Los pasos que se han de seguir para configurar IS-IS Integrado:

Tabla 13.2. *Pasos para configurar IS-IS Integrado.*

Paso 1	Definir el área, preparar un plan de direcciones ha ser usadas en los router (incluyendo la definición de NETs) y determinar las interfaces que deberán correr con IS-IS Integrado.
Paso 2	Habilitar IS-IS como un protocolo de enrutamiento IP en el router, etiquetar los procesos (si es requerido).
Paso 3	Configurar el NET en un router. Este identifica al router para IS-IS
Paso 4	Habilitar IS-IS Integrado en la interfaz correcta en el router. Tales como la interfaz loopback (aunque estas no deberán estar como ningún vecino CLNS en estas interfaces).

13.10.3. Comandos básicos para la configuración de un IS-IS Integrado.

Al habilitar el IS-IS Integrado en un router para enrutamiento IP, deberá necesitar tres comandos, como se describe en esta sección. Note que muchos de los comandos son usados en el procesamiento de reajuste de IS-IS, pero solo tres de ellos son para iniciar IS-IS Integrado.

El comando ***router is-is [etiqueta]*** en la configuración global habilita el IS-IS Integrado en el router. La opción ***etiqueta*** es usada para identificar múltiples procesos IS-IS para dar a conocer con un nombre el proceso de enrutamiento. Si este no se especifica, una etiqueta null (0) es asumida y el proceso hace referencia a esta etiqueta null. Este nombre debe ser único entre todos los procesos de enrutamiento IP.

Nota: la configuración de IS-IS Integrado que corre en una interfaz es ligeramente diferente que la configuración de las interfaces para otros protocolos de enrutamiento IP. En la mayoría de los otros protocolos, las interfaces son identificadas por el comando ***network*** en el modo de configuración del protocolo de enrutamiento. El comando *network* no es usado, para ello se usa el comando ***router isis***.

Para el enrutamiento de paquetes CLNS use el comando ***clns router isis [etiqueta]*** en la configuración de las interfaces.

13.10.4. Otros comandos para la configuración de IS-IS Integrado.

Por defecto, el software Cisco habilita ambos niveles (Nivel 1y Nivel 2) de operación en los routers IS-IS. Si el router esta operando solo como un área o solo como un router backbone, este puede especificar el comando ***is-type {level-1 | level-1-2 | leve-2-only}*** en la configuración del protocolo de enrutamiento. Este comando es descrito en la tabla 13.3 al especificar que acción tendrá el router, solo como un router de área (o Nivel 1), use ***leve-1****,* para que el router funcione como un router backbone (o Nivel 2), use ***level-2-only*****.**

Tabla 13.3. *Descripción del comando is-type.*

Comando is-type	Descripción
leve-1	El router funciona como una estación (final) de router. Este router deberá aprender a cerca de los destinos solo dentro de esta área. Para el enrutamiento inter-área, este depende sobre que tan cerca estén los router level-1-2.
level-1-2	El router funciona tanto como un router de estación y router de área. Este router deberá correr las dos instancias del algoritmo de enrutamiento (para cada tipo de nivel). Esto es por defecto.
level-2-only	El router funciona como router de una solo área. Este router es parte del backbone y no puede comunicarse al Leve-1 -solo los routers de su propia area.

Análogamente, aunque pueda estar en el Nivel 1-2, este puede requerir establecer adyacencias del Nivel 1 solo sobre interfaces identificadas y adyacencias de Nivel 2 sobre otras interfaces. El comando *isis* ***circuit-type {level-1 | level-1-2 | level -2-only}*** en la configuración de interfaces puede ser usado al especificar cualquier interfaz ***level 1*** o **level-2-only**. Este comando es descrito en la tabla 13.4 Puesto que por defecto el nivel es 1-2, el software Cisco intenta establecer ambos tipos de adyacencias en las interfaces si este comando no es especificado.

Tabla 13.4. *Descripción del comando isis circuit-type.*

Comando isis circui-type	**Descripción**
level-1	Una adyacencia de Nivel 1 puede establecerse si hay al menos una dirección de área en común entre la red y los vecinos. El Nivel 2 nunca deberá establecer adyacencia con estas interfaces.
level-1-2	Una adyacencia de Nivel 1 y Nivel 2 se establece si el vecino esta también configurado como level-1-2 y este esta al menos en un área en común. Si no esta en un área en común, la adyacencia de nivel 2 es establecida. Esto se hace por defecto.
level-2-only	Las adyacencias de Nivel 2 son establecidas si los otros routers son de Nivel 2 o Nivel-1-2 y sus interfaces son configuradas como Nivel-1-2 o Nivel-2. Las adyacencias de Nivel-1 nunca beben establecerse sobre estas interfaces.

Es distinto en los otros protocolos IP, IS-IS no cuenta con una línea rápida o banda ancha cuando fija métricas a los enlaces. A todas las interfaces se le asignan una métrica de 10 por defecto. Para cambiar este valor, puede usar el comando ***isis metric default-metric {level-1 | level-2}*** en la configuración de las interfaces. La métrica que tiene por defecto es diferente para el nivel 1 y para el nivel 2 en algunas interfaces. Este comando se describe en la tabla 13.5.

Tabla 13.5. *Descripción del comando isis metric.*

Comando isis metric	**Descripción**
default-metric	Especifica la métrica asignada al enlace y usada para calcular el costo de cada router a través de los enlaces en la red a otros destinos. Puede configurar esta métrica para Nivel 1 o Nivel 2 de enrutamiento. El rango es desde 0 a 63. el valor por defecto es 10
level-1	Específica que esta métrica solo deberá ser usada en el cálculo de SPF para el enrutamiento de Nivel 1 (intra-área).

level-2	Específica que esta métrica solo deberá ser usada en el cálculo de SPF para el enrutamiento de Nivel 2 (inter-área).

Al definir el nombre del mapeo NSAP puede usar los comandos NSAP. Use el comando ***clns host name nsap*** en la configuración global. La asignación del nombre NSAP será mostrado, cuando aplique el comando ***show*** y ***debug*** en EXEC. Este comando se describe en la tabla 13.6.

Tabla 13.6. *Descripción del comando clns host.*

Comando clns host	**Descripción**
Name	Describe el nombre para el NSAP. El primer carácter puede ser cualquier letra o número, pero si usa un número, las operaciones que ejecute son limitadas.
Nsap	El NSAP para los nombres de los mapas

Use el comando ***summary-address address mask {level-1 | level-1-2 |level-2-only} prefix mask*** en la configuración del router para crear agregaciones de direcciones para IS-IS o OSPF. Este comando se describe en la tabla 13.7.

Tabla 13.7. *Descripción del comando summary-address.*

Comando summary-address	**Descripción**
Address	Dirección de Sumarización designada para representar el rango de direcciones.
Mask	Mascara de la subred IP usada para la Sumarización del router.
Level-1	Solo los routers que redistribuyen dentro del nivel 1 son sumarizados con el valor de la configuración dirección/mascara.
Level-1-2	La Sumarización es aplicada a ambos cuando redistribuyen rutas dentro del Nivel 1 y el Nivel 2, las rutas de Nivel 1 son anunciadas en las áreas accesibles.

level-2	Las rutas aprendidas en el enrutamiento de Nivel 1 son sumarizadas dentro del backbone de Nivel 2 con el valor de configuración dirección/mascara, y la redistribución de routers de IS-IS de Nivel 2 también son sumarizados.
Prefix	El prefijo del router IP para el destino
Mask	La máscara de subred IP usada para la Sumarización del router.

Al configurar la prioridad del router designado, use el comando ***isis priority value {level-1 | level-2}*** en la configuración de las interfaces. Al iniciar la configuración por defecto, use la forma no del comando. Este comando se describe en la tabla 13.8.

Tabla 13.8. *Descripción del comando isis priority.*

Comando isis priority	**Descripción**
value	Establece la prioridad del router. Este es un numero entre 0 a 127. El valor por defecto es 63.
level-1	Establece la prioridad para el Nivel 1 (independientemente)
level-2	Establece la prioridad para el Nivel 2 (independientemente)

13.10.5. Comandos CLNS para localizar fallas.

Las fallas en IS-IS Integrado, son iguales que en una red IP, se requiere una investigación de datos CLNS.

Por ejemplo, la relación de vecinos IS-IS son establecidas sobre OSI, y no sobre IP, para mostrar los vecinos IS-IS se usa el comando ***show clns neighbosr*****.** Por supuesto, dos adyacencias finales CLNS pueden tener direcciones IP sobre diferentes subredes, por medio de las operaciones IS-IS.

Algunos de los comandos para detectar fallas CLNS son mostrados en el contenido de esta sección. En esta sección se describen los comandos **show** CLNS.

El comando ***show clns*** en modo EXEC despliega información general de la red CLNS.

El comando ***show clns protocol [dominio] [etiquete de área]*** en el modo EXEC despliega información de un proceso IS-IS especifico en el router. Estos comandos se describen el la tabla 13.9.

Tabla 13.9. *Descripción del comando show clns protocol.*

Comando show clns protocol	Descripción
Dominio	(Opcional) Dominio de enrutamiento ISO IGRP particular
etiqueta de área	(Opcional) área IS-IS particular

El comando ***show clns interface [type number]*** en EXEC despliega información especifica de las interfaces que corren bajo IS-IS.

Tabla 13.10. *Descripción del comando show clns interface.*

Comando show clns interface	Descripción
Type	(opcional) tipo de interfaz
Number	(opcional) número de interfaz

El comando ***show clns neighbiors [type number] [detail]*** en EXEC es muy útil para desplegar la información sobre los vecinos ISs – esto es, los routers que tienen adyacencias IS-IS. (Los vecinos ESs, si algunos de estos, también son desplegados).

Tabla 13.11. *Descripción del comando show clns neighbors.*

Comando show clns neighbors	Descripción
Type	(Opcional) tipo de interfaz
Number	(Opcional) número de la interfaz
Detail	(Opcional) cuando se especifica, las direcciones de las áreas anunciadas por los vecinos en los mensajes hello son desplegadas. Por otra parte, se despliega la Sumarización.

Al desplegar IS-IS relacionando información para router IS-IS adyacentes, use el comando ***show clns is-nieghbors [type number][detail]*** en EXEC. La entrada de vecinos son clasificadas de acuerdo al área en la que esta localizada.

Tabla 13.12. *Descripción del comando clns is-neighbors.*

Comando clns is-nieghbors	**Descripción**
Type	(Opcional) tipo de interfaz
Comando clns is-nieghbors	Descripción
Number	(Opcional) número de interfaz
Detail	(Opcional) cuando se especifica, las áreas asociadas con la red intermedia son desplegadas. Por otra parte, se despliega la Sumarización.

13.10.6. Comandos IS-IS y CLSN para detectar fallas.

El comando ***show isis route*** en modo EXEC despliega información de la tabla de enrutamiento IS-IS de Nivel 1, (esto es, todas las rutas de los ID de Sistema en un área). El comando ***show clns route [nsap]*** en modo EXEC despliega la tabla de enrutamiento IS-IS de Nivel 2 (como estático y prefijos de ruta aprendidos –ISO-IGRP).

El comando ***show isis database [level-1][level-2][\1][\2][detail][spid]*** en modo EXEC despliega información de la base de datos del estado del enlace.

Tabla 13.13. *Descripción del comando show isis database.*

Comando show isis database	**Descripción**
level-1	(Opcional) despliega la base de datos IS-IS del estado del enlace de Nivel 1
level-2	(Opcional) despliega la base de datos IS-IS del estado del enlace de Nivel 2
|1	(Opcional) abreviación de la opcion level-1
|2	(Opcional) abreviación de la opcion level-2
Comando show isis database	Descripción
Detail	(Opcional) cuando se especifica, el contenido de cada LSP es desplegado. Por lo tanto, se despliega la Sumarización.
Áspid	(Opcional) el identificador PDU del estado del enlace. Cuando se especifica, el contenido de un único LSP es desplegado por su numero ID

IS-IS para refrescar su base de datos del estado del enlace y recalcular todas las rutas, usa el comando ***clear isis [etiqueta | *],*** se especifica la etiqueta de un proceso IS-IS o ***** (asterisco) para borrar todas las entradas IS-IS.

Nota: El comando *clear isis* no esta documentado en el software de Cisco, pero se trabaja sobre los routers.

Use el comando ***show isis spf-log*** en modo EXEC, para desplegar y ver las rutas completas del calculo de SPF.

El comando ***show ip protocols*** en modo EXEC despliega información sobre la actividad de los protocolos de enrutamiento, que interfaces están activas, que redes son enrutadas, y los parámetros para asociar los protocolos de enrutamiento.

13.10.7. Generando un ruter por defecto.

Puedes forzar el ruter por defecto dentro del dominio de enrutamiento. Siempre que especifiques la predistribución de la configuración del ruter dentro de un dominio de ruter IS-IS, no es el software de Cisco IOS, por defecto, redistribuido al ***default route*** dentro del dominio del ruter IS-IS. El siguiente comando genera un ruter por defecto dentro de IS-IS, que puede ser controlado a un mapa de ruter. Puedes usar el mapa de ruter para identificar el nivel que dentro del ruter por defecto es para ser declarado, y puede especificar filtrando otras opciones configurables dentro del mapa de ruter. Puedes usar un mapa de ruter para advertir condicionalmente al ruter por defecto, dependiendo de la existencia de otros ruter en la tabla de enrutamiento del ruter.

Tabla 13.14. *Descripción del comando default-infornmation originate*

Comando	Descripción
default-information originate [route-map map-name]	Forzar un router por defecto dentro de el dominio de enrutamiento IS-IS

13.10.8. Configurando la contraseña de autentificación IS-IS.

Puedes asignar contraseñas para areas y dominios.
La contraseña de autentificación de area es insertada en el LSPs en el nivel 1(estacion de nivel de ruter), y la contraseña de autentificación de el dominio del ruter es insertado en el LSPs de nivel 2(área del nivel del ruter).

Para configurar cualquier contraseña de autentificación de área o dominio, use el siguiente comando en modo de configuración del ruter:

Tabla 13.15. *Descripción del comando area-password*

Comando	Proposito
area-password password	Configurar la contraseña de autentificación de area
domain-password password	Configurar la contraseña de autentificación del dominio de enrutamiento.

13.10.9. Estableciendo el bit de sobrecarga.

Puedes configurar el ruter para establecer el bit de sobrecarga en este seudonodo LSPs. Normalmente el establecimiento de el bit de sobrecarga permitido solo cuando un ruter esta corriendo en problemas. Por ejemplo cunado un ruter esta experimentando una escasez de memoria, la base de datos de estado de enlace puede no ser completado, resultando en una incompleta tabla de enrutamiento.

Estos comandos pueden ser usados cuando quieres una conexión a un ruter en una red IS-IS, pero no quiere hacer tráfico real en cualquier circunstancia.

Para establecer el bit de sobrecarga, use el siguiente comando en modo de configuración del ruter:

Tabla 13.16. *Descripción del comando set-overload-bit.*

Comando	Descripción.
set-overload-bit [on-startup {seconds | wait-for-bgp}] [suppress {[interlevel] [external]}]	Establecer el bit de sobrecarga.

CAPÍTULO 14

BGP
(BORDER GATEWAY PROTOCOL)

14. BGP

Dentro de un mismo sistema autónomo el protocolo de enrutamiento utilizado es OSPF (aunque no es el único). Entre los sistemas autónomos se utiliza un protocolo diferente, el protocolo de puerta de frontera (BGP.).

Se necesita un protocolo diferente entre sistemas autónomos porque los objetivos de un protocolo de puerta de enlace interior y un protocolo de puerta de enlace exterior no son los mismos. Todo lo que tiene que hacer un protocolo de puerta de enlace interior es mover lo mas eficazmente posible los paquetes del origen al destino. No tiene que preocuparse por las políticas.

Los enrutadores de puerta de enlace exterior tienen que preocuparse en gran manera por las políticas.

En general los protocolos de puerta de enlace exterior, y BGP en particular, se han diseñado para permitir que se implementen muchos tipos de políticas de enrutamiento en el tráfico entre sistemas autónomos.

Las políticas típicas implican consideraciones políticas, de seguridad, o económicas. Las políticas en un enrutador de BGP se configuran manualmente. No son parte del protocolo.

Desde el punto de vista de un enrutador de BGP, el mundo consiste en sistemas autónomos y las líneas que lo conectan. Dos sistemas autónomos se consideran conectados si hay una línea entre un enrutador fronterizo en cada uno. Dado el especial interés de BGP en el transporte de tráfico, las redes se agrupan en tres categorías. La primera son las **redes stub**, que tienen solo una conexión con el grafo de BGP. Estas no se pueden usar para transportar tráfico porque no hay nadie del otro lado. Luego vienen las **redes multiconectadas**, estas podrían usarse para el transporte de tráfico excepto que lo rechacen. Finalmente están las **redes de transito**, como dorsales, que están dispuestas a ocuparse de paquetes de terceros, posiblemente con algunas restricciones, y normalmente por pago.

Básicamente, BGP es muy parecido a un protocolo de vector de distancia, pero muy diferente de la mayoría de otros como RIP. En lugar de mantener el costo para cada destino cada enrutador de BGP guarda el registro de la ruta utilizada, por lo que se le conoce como un protocolo de vector ruta.

Los protocolos de routing externo son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de routing externo la prioridad era buscar rutas óptimas atendiendo únicamente al criterio de minimizar la distancia medida en términos de la métrica elegida para la red.

La selección de rutas entre sistemas autónomos plantea un problema diferente, ya que la cuestión no se reduce a la selección de la ruta optima sino que se debe atender a criterios externos de tipo político, económico, administrativo, etc.

Hasta 1990 se utilizaba como protocolo de routing externo en la Internet el denominado EGP (Exterior Gateway Protocol). Este protocolo no fue capaz de soportar el crecimiento de la Red y

entonces se desarrollo un nuevo protocolo de routing externo denominado BGP. Desde entonces se ha producido 4 versiones de BGP.

BGP es un protocolo de transporte fiable. Esto elimina la necesidad de llevar a cabo la fragmentación de actualización explícita, la retransmisión, el reconocimiento, y secuenciación.

¿Qué es el número de sistema autónomo?

En BGP cada número de sistema autónomo identifica un dominio de enrutamiento diferente, lo que es equivalente a un dominio que controla un conjunto de routers y redes.

Para en este caso de ejemplo tenemos 3 Sistemas Autónomos. El de la empresa: 12345; y los de los 2 ISPs: 5678 y 6789. El número de sistema autónomo identifica unívocamente a una red en la nube de Internet.

En BGP los sistemas autónomos son además los que definen la ruta que ha de seguir un paquete, ya que BGP es un protocolo de "ruta-vector" o "vector ruta". BGP selecciona como mejor ruta la ruta que atraviesa menor cantidad de sistemas autónomos.

¿Qué es lo mínimo necesario para que comience a operar BGP?

Lo mínimo que se requiere para que comience a operar BGP en un router, es la declaración del vecino o neighbor con el que este router debe establecer una relación de adyacencia para comenzar el intercambio de información. Junto con la declaración del vecino, debe indicarse la ruta (sistema autónomo) en el que ese vecino se encuentra.

14.1. Funciones de BGP.

BGP se diseño para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarelas, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando TCP.

El repertorio de mensajes BGP es el siguiente:

- OPEN
- UPDATE
- KEEPALIVE
- NOTIFICACION

BGP tiene tres procedimientos funcionales:

- Adquisición de vecino.
- Detección de vecino alcanzable.
- Detección de red alcanzable.

Dos dispositivos de encaminamiento se considera que son vecinos si están en la misma subred. Si los dos dispositivos de encaminamiento están en sistemas autónomos diferentes, podrían desear intercambiar información de encaminamiento. Para este cometido es necesario realizar primero el proceso de adquisición de vecino. Se requiere un mecanismo formal de encaminamiento ya que alguno de los dos vecinos podría no querer participar. Existirán situaciones en las que un vecino no desee intercambiar información esto se puede deber a múltiples factores como por ejemplo que este sobresaturado y entonces no quiere ser responsable del trafico que llega desde fuera del sistema.

En el protocolo de adquisición de vecino, un dispositivo envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no indica como puede saber un dispositivo la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones se tratan en el momento de establecer la configuración del sistema o por una intervención activa del gestor de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo envía al otro un mensaje OPEN. Si el otro dispositivo acepta la relación, envía un mensaje de KEEPALIVE.

Una vez establecida la relación de vecino, se utiliza el procedimiento de detección de vecino alcanzable para mantener la relación. Este procedimiento consiste en enviarse entre los dos vecinos periódicamente mensajes de KEEPALIVE para asegurarse de que la relación sigue establecida.

El último procedimiento especificado por BGP es la detección de red alcanzable. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para llegar hasta esa red. Siempre que se realiza un cambio en esa base de datos, el dispositivo de almacenamiento envía un mensaje de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.

14.2. Mensajes BGP.

Los mensajes BGP tienen una cabecera común de 19 octetos que contiene los siguientes tres campos:

- ***Marcador*:** reservado para autentificación. El emisor puede insertar un valor en este campo para permitir al receptor comprobar la veracidad del emisor.
- ***Longitud*:** longitud del mensaje en octetos.
- ***Tipo*:** tipo de mensaje: OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

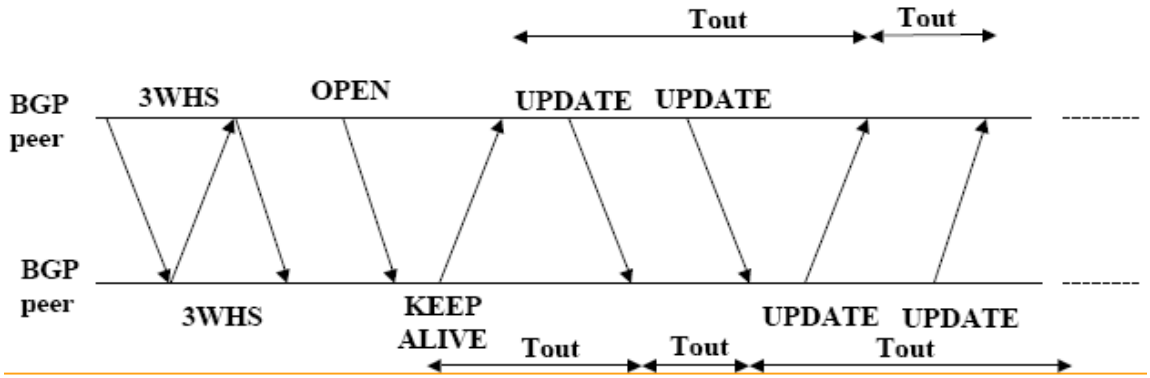


Figura 14.1. *Mensajes BGP.*

14.2.1. Mensaje OPEN.

Para adquirir un vecino, un dispositivo de encaminamiento abre primero una conexión TCP con el dispositivo vecino y después envía un mensaje OPEN. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento.

En la siguiente figura se muestra el formato del mensaje OPEN:

Tabla 14.1. *Mensaje OPEN.*

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Versión	1
AS	2
Tiempo permanen.	2
Identificador BGP	4
Long. Opciones	1
Opciones	Variable

- ***Versión*****:** Indica la versión del protocolo del mensaje. La versión actual es 4.
- ***AS:*** Identifica al sistema autónomo del emisor del mensaje.
- ***Tiempo de permanencia*****:** Indica el tiempo de que propone el emisor como Hold Time.
- ***Identificador de BGP*****:** Identifica al BGP emisor.

14.2.2.Mensaje KEEPALIVE.

El mensaje KEEPALIVE consta solo de la cabecera. Cada dispositivo de mantenimiento envía regularmente estos mensajes para evitar que expire el temporizador mantenimiento.

En la siguiente figura se muestra el formato del mensaje KEEPALIVE:

Tabla 14.2. *Mensaje KEEPALIVE.*

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1

14.2.3.Mensaje UPDATE.

El mensaje UPDATE facilita dos tipos de información.

Información sobre una ruta particular a través del conjunto de redes. Esa información se puede incorporar a la base de datos de cada dispositivo de encaminamiento que la recibe.
Una lista de rutas previamente anunciadas por este dispositivo de encaminamiento que van a ser eliminadas.

En la siguiente figura se muestra el formato del mensaje UPDATE:

Tabla 14.3. *Mensaje UPDATE.*

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Long. Rutas no factibles	2
Rutas retiradas	Variable
Long.Total atributos de camino	2
Atributos de camino	Variable
Inf. De accesibilidad de la capa de red	Variable

Un mensaje UPDATE puede contener uno o ambos tipos de información. Consideremos primero el tipo de información 1. La información sobre una ruta particular a través de la red implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI), campo de longitud de los atributos del camino total, y el campo de los atributos de camino. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de la dirección IP completa.

El campo atributos de camino contiene una lista de atributos que se aplican a esta ruta particular. Los atributos definidos son los siguientes:

- ***Origen*:** indica si la información fue generada por un protocolo de dispositivo de encaminamiento interior o exterior.

- ***Camino _ as*:** una lista de los AS que son atravesados por la ruta.

- ***Siguiente _ salto*:** dirección IP del dispositivo de encaminamiento frontera que se debe usar como siguiente salto para alcanzar los destinos indicados en el NLRI.

- ***Multi_exit_disc:*** se usa para comunicar alguna información sobre rutas internas a un AS.

- ***Local_pref**:* usado por un dispositivo de encaminamiento para informar a otros dispositivos de encaminamiento dentro del mismo AS de su grado de preferencia por una ruta particular. No tiene significado alguno para dispositivos de encaminamiento en otros AS.

- ***Agregado _ atómico**, **Agente _ unión:*** estos dos campos implementan el concepto de unión de rutas. En esencia, un conjunto de redes y su espacio de direcciones correspondiente se pueden organizar jerárquicamente, o como un árbol. En este caso las direcciones de las redes se estructuran en dos o más partes. Todas las redes de un subárbol comparten una dirección Internet parcial común. Usando esta dirección parcial común, la cantidad de información que se debe comunicar en NLRI se pude reducir significativamente.

- El atributo ***Camino _ as*** sirve realmente para dos objetivos. Ya que indica los AS que debe atravesar un datagrama si sigue esta ruta, la información de camino _ as habilita a un dispositivo de encaminamiento a que implemente un criterio de encaminamiento. Esto es un dispositivo de encaminamiento puede construir un camino para pasar por un determinado AS.

14.2.4. Mensaje NOTIFICATION.

Se envían cuando se detecta algún tipo de error. Se puede informar de los siguientes tipos de errores:

- **Error en la cabecera del mensaje**: incluye errores de sintáxis y autentificación.

- **Error en mensaje OPEN:** incluye errores de sintaxis y opciones no reconocidas en un mensaje OPEN. Este mensaje también se puede utilizar para indicar que el tiempo de mantenimiento en el mensaje OPEN es inaceptable.

- **Error en el mensaje UPDATE:** incluye errores de sintaxis y validación en un mensaje UPDATE.

- **Tiempo de mantenimiento expirado:** si el dispositivo de encaminamiento que envía no recibe mensajes sucesivos de KEEPALIVE y/o UPDATE y/o NOTIFICATION durante el tiempo de mantenimiento, entonces se comunica este error y se cierra la conexión.

- **Error en la maquina de estados finitos:** incluye cualquier error de procedimiento.

En la siguiente tabla se muestra el formato del mensaje NOTIFICATION:

Tabla 14.4. *Mensaje NOTIFICATION.*

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Código error	1
Subcodigo error	1
Datos	Variable

14.3. Existen dos formas de usar BGP.

Existen situaciones donde es necesario emplear iBGP y eBGP en una misma situación, ese es el caso que se muestra en el grafico a continuación:

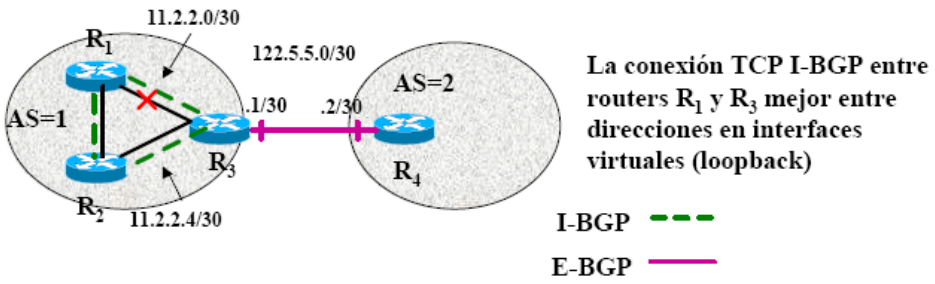


Figura 14.2. *iBGP y eBGP.*

Puede suceder que los enlaces físicos se caigan lo que provocaría que se perdiera la conexión, en tal situación seria mejor desacoplar la conexión IGP de las interfaces físicas, esto se hace utilizando interfaces virtuales (loopback) con direcciones IP distintas de las físicas como se muestra en el grafico a continuación.

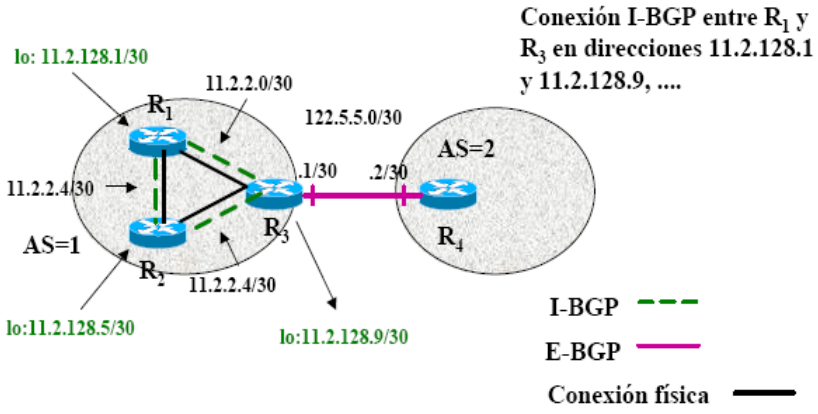


Figura 14.3. *iBGP y eBGP con loopback.*

14.3.1.iBGP.

iBGP define el peering entre dos vecinos BGP dentro del mismo AS. Se puede utilizar iBGP en los AS de tránsito. Los AS de tránsito reenvían el tráfico desde un AS hacia otro. Si no se utilizara iBGP, las rutas aprendidas por eBGP serían redistribuidas dentro del IGP y redistribuidas de nuevo en el proceso de BGP de otro router eBGP.

iBGP proporciona la mejor forma de controlar las rutas para el AS de transito. Con iBGP la información de las rutas externas (atributos) son reenviados. iBGP es preferido sobre otras redistribuciones ya que los IGPs no entienden de AS paths y otros atributos de BGP.

Es importante configurar una red totalmente mallada de vecinos iBGP dentro del AS para evitar bucles de routing. El router iBGP no redistribuye la información en otros peers iBGP.

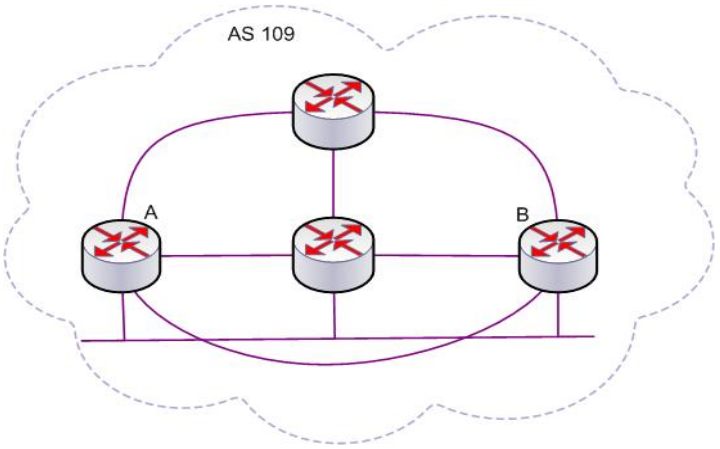


Figura 14.4. *iBGP.*

Router B:
```
router bgp 109
neighbor 131.108.30.2 remote-as 109
```

Router A:
```
router bgp 109
neighbor 131.108.20.1 remote-as 109
```

14.3.2.eBGP.

El enrutamiento eBGP se utiliza normalmente cuando tenemos el siguiente escenario.

- Entre router en AS diferentes.
- Usualmente con conexión directa.
- Con next-hop apuntando a si mismo.

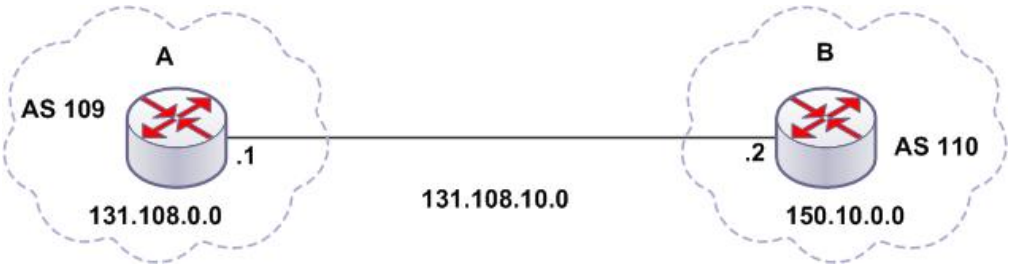


Figura 14.5. eBGP.

Router B:
```
router bgp 110
neighbor 131.108.10.1 remote-as 109
```

Router A:

```
router bgp 109
neighbor 131.108.10.2 remote-as 110.
```

eBGP Multihop

Los peers eBGP pueden ser configurados sin estar directamente conectados, saltando varias redes, mediante eBGP Multihop. eBGP Multihop también se utiliza para establecer el peering con las direcciones de loopback. Esta es una característica propietaria de Cisco IOS. El routing interno del AS (IGP) deberá de estar perfectamente configurado para que el eBGP Multihop pueda funcionar. Multihop no es posible configurarlo en iBGP.

Ejemplo de configuración de eBGP Multihop:

Figura 14.6. *eBGP Multihop.*

14.4. BGP-4 Versión 4 ("Border Gateway Protocol Version 4 ")

Los principales cambios se aplican al soporte de *"supernetting"* o *CIDR ("Classless Inter-Domain Routing")* que se describe en CIDR ("Classless Inter-Domain Routing"). En particular, BGP-4 soporta prefijos IP y agregación de rutas. Debido a que CIDR es radicalmente distinto de la arquitectura de encaminamiento normal de Internet, BGP-4 es incompatible con BGP-3. Sin embargo, BGP define un mecanismo para que dos BGPSs negocien una versión que ambos entiendan, utilizando el mensaje OPEN. Por lo tanto, es posible implementar BGPSs "bilingües" que permiten la interoperatividad entre BGP-3 y BGP-4.

Los principales cambios de BGP-4 son:

- El número de versión en la cabecera es 4.
- CIDR elimina el concepto de clase de red del encaminamiento inter-dominio, sustituyéndolo por el de prefijo IP.

- La lista de redes en un mensaje UPDATE se sustituye por el *NLRI ("Network Layer Reachability Information")*.

- BGP-4 introduce la agregación de múltiples rutas de ASs en entradas únicas o *agregados.* El uso de agregados puede reducir dramáticamente la cantidad de información de encaminamiento requerida.
- Se puede usar un nuevo atributo para una ruta AS (ATOMIC_AGGREGATE) para asegurar que determinados agregados no son desagregados. Otro nuevo atributo (AGGREGATOR) se puede añadir direcciones para agregar rutas con el fin de anunciar qué AS y qué BGPS dentro del AS causaron la agregación.

- BGP-4 modela conceptualmente los datos de un BGPS en tres series de *RIBs ("Routing Information Bases")*: uno (Adj-RIBs-In) para los datos obtenidos de vecinos BGP, otro para (Loc-RIB) datos locales obtenidos de las operaciones de las políticas de encaminamiento locales sobre la Adj-RIBs-In, y uno (Adj-RIBs-Out) para datos que han de ser anunciados en mensajes UPDDATE.

- BGP-4 permite la negociación del valor "Hold Time" por cada conexión de modo que los extremos de la misma usen el mismo valor.

- BGP-4 cambia el formato del mensaje UPDATE al formato mostrado en la figura 14.4.

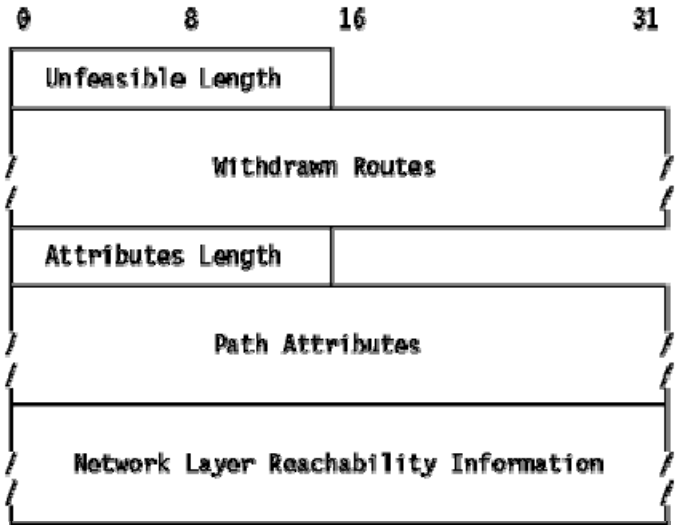


Figura 14.4. *Mensaje UPDATE de BGP*

- ***UnfeasibleLength*** *:* Es una contracción de *"Unfeasible Routes Length"* y es un campo de 2 bytes que da la longitud del campo "Withdrawn Routes". Puede ser cero.

- ***Withdrawn Routes*** *:* Una lista de prefijos IP que se están retirando del servicio. Cada entrada tiene la forma *"<length, prefix>"·* donde *length* es un sólo byte que indica la longitud del prefijo en bits, y el prefix es el prefijo IP rellenado hasta el límite

con el siguiente byte. Una longitud de cero causa coincidencia con todas las direcciones IP.

- ***Attributes Length:*** Un campo de 2 bytes que da la longitud del campo "path attributes" en bytes.

- ***Path Attributes****:* Los mismos valores que en BGP-3 excepto en ***attribute type****.*

14.5. Comandos de BGP.

14.5.1. Vecinos de BGP.

Antes de poderse intercambiar rutas BGP entre dos routers, estos deben de establecer la vecindad, se tienen que hacer vecinos.
El intercambio de información antes de establecerse como vecinos incluye lo siguiente:

- Número de Versión de BGP.
- Número de AS.
- Router ID (RID) de BGP

Para verificar los vecinos BGP utilizaremos el comando show ip bgp neighbors.

14.5.2. Anunciar Rutas

Para anunciar rutas en BGP tenemos tres formas de hacerlo.

- Comando network
- Comando aggregate-address
- Redistribución de IGPs

14.5.3. El Comando network

El comando network específica qué rutas de la tabla de routing IP local son añadidas a la tabla de BGP. Por defecto en los routers Cisco la auto sumarización está habilitada. Si la auto sumarización está desactivada, no se creará una ruta no classful sumarizada.

14.5.4. El Comando *aggregate-address*

El comando aggregate-address anuncia una ruta sumarizada si hay rutas más específicas en la tabla de BGP. Si además utilizamos la palabra clave summary-only suprimiremos el anuncio de prefijos más específicos.

14.5.5. Redistribución de BGP

Otra forma de anunciar redes en BGP es importando las rutas de los protocolos IGP en BGP mediante una redistribución. Este método se utilizará normalmente en grandes empresas con *Core iBGP*.

14.5.6. Communities de BGP

El atributo communities es un atributo global opcional y transitivo y es un número en el rango 1-4.294.967.200.

Las communities más comunes son:

- **Internet:** Anuncia esta ruta a Internet, todos los routers pertenecen a esta community.
- **No-export:** No anuncia esta ruta a otros peers eBGP
- **No-advertise:** No anuncia esta ruta a ningún peer
- **Local-as:** Envía esta ruta a otros peers en otros subsistemas autónomos dentro de la misma confederación local

14.5.7. BGP Prefix Lists

Los prefix lists filtran los envíos y recepción de las rutas que se envían o reciben desde peers.

14.5.8. BGP Distribute Lists

Los distribute lists filtran las rutas que se envían o reciben.
Al igual que podemos filtrar por redes, también podemos filtrar los ASs mediante expresiones regulares.

14.5.9. Sincronización de BGP

Por defecto la sincronización de BGP está habilitada en los routers Cisco.
El propósito de la sincronización es que el AS proporcione transito a otro AS: BGP no debe de anunciar una ruta hasta que todas las rutas del AS no se hayan aprendido por IGP.

Es posible desactivar la sincronización de BGP para acelerar el proceso de convergencia (BGP no tiene que esperar al IGP). Esto sólo se puede hacer si el AS no es de transito o si todos los routers corren BGP.

La sincronización podemos deshabilitarla con el comando no bgp synchronization.

Un ejemplo de cómo aplicar sincronización se muestra a continuación:

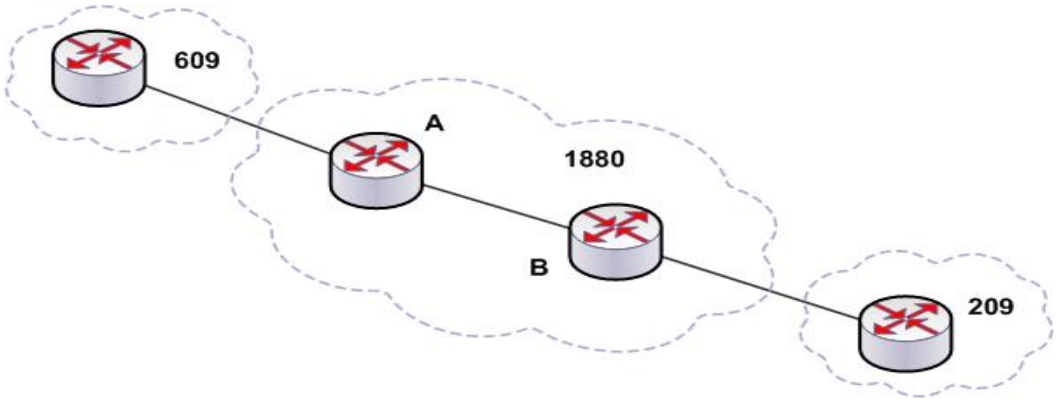


Figura 14.5. *Sincronización BGP.*

En el gráfico anterior:

- Router A no anunciará los prefijos de AS209 hasta que haya convergencia en el IGP.

- Asegurarse de que los next-hops del iBGP pueden ser vistos via IGP, entonces:
```
router bgp 1880
no synchronization
```

Este es uno de los comandos BGP que genera más confusión.
Por defecto, BGP publica solamente redes que se corresponden con una ruta interna presente en la tabla de enrutamiento del router

Aún cuando declare una red con el comando network, si en la tabla de enrutamiento no hay una ruta hacia esa red, la misma no se publicará.

A eso apunta el comando synchronization. A publicar exclusivamente redes con las cuales está en condiciones de comunicarse uitlizando una ruta aprendida por un protocolo de enrutamiento interior. Es por esto que en muchos casos se deshabilita, pues es posible que no se esté utilizando un protocolo de enrutamiento interior.

14.5.10. Atributos de BGP, Weight y el proceso de decisión de BGP

La decisión de mejor ruta BGP la realiza teniendo en cuenta los atributos y el weight.
Los atributos de BGP vienen muy bien definidos en Atributos de BGP Path.
Weight es específico de Cisco y no se propaga a otros routers. Los valores del weight están en el rango 0 - 65535, y las rutas a un destino con un weight mayor son preferidas sobre las otras.

El weight puede ser utilizado en vez de la local preference para influenciar en la selección del path a los peers externos de BGP.
La diferencia principal es que el weight no se envía entre peers y la local preference se envía entre peers iBGP.

Los atributos de BGP se dividen siguiendo el siguiente esquema:

- **Well-Known:** Se reconocen en todas las implementaciones de BGP.
- **Mandatory:** Tienen que ser incluidos en todas la actualizaciones.
- **Next-Hop:** Dirección IP que alcanza el destino.
- **Origin:** i(IGP), e(EGP), ?(incompleto).
- **AS-Path:** Número de ASs para alcanzar el destino y lista de los mismos.
- **Discretionary:** No tienen que ser incluidos en todas las actualizaciones.
- **Local-Preference:** Indica el path para salir del AS.
- **Atomic Aggregator:** Informa a los peers BGP que existe una ruta menos específica a un destino.
- **Optional:** No necesitan ser soportados por el proceso BGP.
- **Transitive:** Los routers los anunciarán, aunque ellos no los soporten.
- **MED:** Le dice al peer eBGP el path preferido para entrar en el AS.
- **Community:** Agrupa redes para asignación de políticas.
- **Agregator:** Incluye la IP y el AS del router que origina la ruta agregada.
- **Non Transitive:** Los routers no los anunciarán.

14.5.11. Atributo Next hop

Este atributo nos indica la dirección IP del siguiente salto eBGP que vamos a utilizar para alcanzar el destino. Para definir el siguiente salto como el vecino en si utilizaremos el comando next-hop-self.

14.5.12. Atributo Local Preference

El atributo local preference indica cual es el camino para salir del AS local, este atributo no se pasará a vecinos eBGP. Por defecto en routers Cisco es 100 y se prefiere la local preference más grande.

14.5.13. Atributo Origin

El atributo Origin define el origen de la información del path:

- **IGP:** Indicado con una i, presente si la ruta se ha aprendido con el comando network.
- **EGP:** Indicado con una e, presente si la ruta ha sido aprendida desde otro AS.
- **Incomplete:** Indicado con un ?, aprendido de una redistribución de la ruta

14.5.14. Atributo AS Path Length

El AS Path Length lista los ASs que se atraviesan para llegar los destinos

14.5.15. Atributo MED

El atributo MED, también conocido como métrica, indica a los peers de eBGP el path preferido para entrar en el AS desde fuera.
Por defecto el valor del MED es 0 y cuanto más bajo sea el valor es más preferible.

14.5.16. Atributo Community

Este atributo no participa en el proceso de selección de path, pero sirve para agrupar políticas o decisiones que aplican a estas rutas.

14.5.17. Atributos Atomic Aggregate y Aggregator

El atributo Atomic Aggregate informa a los peers BGP que existe una ruta menos específica a un destino y atributo Aggregator incluye la IP y el AS del router que ha generado la ruta agregada.

14.5.18. BGP Route Dampening

El Route Dampening es un método que permite detener la propagación de rutas inestables a través de la red. En BGP para conseguir eso se le asigna a cada path un valor de penalización que va aumentando cada vez que se produce una caída rápida (flappping). En el momento que el valor de la penalización llega al máximo el path es descartado.

El funcionamiento es el siguiente. Al principio se le asigna un valor de penalización, cuando la ruta lleva caída el tiempo descrito en *half-life-time* el valor de penalización (por defecto 1000) baja a la mitad, por defecto este tiempo es de 15 minutos. El *reuse-value* indica el valor al cual la ruta tiene que llegar para poder volver a ser anunciada, por defecto es 750. El valor de *supress-limit* indica el valor al que tiene que llegar para ser eliminada del todo y el *maximum-supress-time* indica la máxima duración para suprimir la ruta estable, por defecto 4 veces el *half-life-time*, típicamente 60 minutos.

14.5.19. BGP Peer Groups

Los Peer Groups son una agrupación de vecinos BGP a los cuales se les aplica las mismas políticas, de esta forma podemos configurar un montón de vecinos BGP de forma más rápida.

14.5.20. Route Reflectors

Muchas veces no es posible disponer de una red totalmente mallada y hay que utilizar Route Reflectors.

Un Route Reflector proporciona la capacidad de hacer funcionar en cluster a el mismo y a sus clientes. Utilizando router reflector con que el router reflector esté conectado mediante una red totalmente mallada con sus peers (no con sus clientes).

14.6. Comandos para configurar BGP.

Comando: *router bgp NÚMERO-SA.*
Habilita el proceso de protocolo BGP con el número de SA especificado. Después de este comando, puedes introducir cualquier comando BGP.

Comando: *no router bgp NÚMERO-SA*
Destruye un proceso BGP con el *NÚMERO-SA* especificado.

Comando BGP: *bgp router-id ROUTER-ID*
Este comando especifica el router-ID (Indetificador de router). Si bgpd conecta con zebra, obtiene la información de los interfaces y de dirección. En ese caso el router-id por defecto se obtiene tomando la dirección de mayor numeración de todos los interfaces. Cuando router zebra no está habilitado, bgpd no puede obtener la información de los interfaces y router-id se fija en 0.0.0.0. En ese caso se debe especificar a mano.

Comando BGP: neighbor VECINO remote-as NÚMERO-SA
Crea un nuevo vecino cuyo SA es NÚMERO-SA. VECINO puede ser una dirección IPv4 ó IPv6.

Comando BGP: no neighbor VECINO remote-as NÚMERO-SA
Elimina un vecino y toda la configuración asociada a él.

Comando BGP: *network PREFIJO [mask] [MASCARA].*
Este comando activa el anuncio de esa red, en las versiones antiguas de zebra, el prefijo se introducía en notación CIDR, en las versiones más modernas se debe especificar una máscara decimal con la opción mask, si la red introducida no es “classfull”. El propósito es emular el comportamiento de Cisco IOS.

Comando BGP: *no network PREFIJO*
Desactiva el anuncio de prefijo previamente anunciado.

Comando BGP: *aggregate-address PREFIJO*
Este comando específica que se agreguen un conjunto de rutas recibidas en un PREFIJO menos específico.

Comando BGP: *no aggregate-address PREFIJO*
Desactiva la agregación de prefijos.

Comando BGP: *redistribute kernel*
Inyecta las rutas del kernel que no pertenecen a zebra en el proceso de BGP.

Comando BGP: *redistribute static*
Inyecta las rutas estáticas de zebra en el proceso de BGP.

Comando BGP: *redistribute connected*
*I*nyecta las rutas conectadas de zebra en el proceso de BGP.

Comando BGP: *redistribute rip*
Inyecta las rutas de ripd en el proceso BGP.

BGP Command: *redistribute ospf*
Inyecta las rutas de ospfd en el proceso de BGP.

Comando BGP: *neighbor VECINO shutdown*
Comando BGP: *no neighbor VECINO shutdown*
Desactiva el vecino manteniendo la configuración asociada a este. Podemos desactivar un vecino con "no neighbor VECINO remote-as NÚMERO-SA pero a la vez borraremos la configuración asociada. Usa esta sintaxis cuando quieras tirar la sesión con un vecino pero preservando toda su configuración. Con la operación "no neighbor VECINO shutdown" activaremos la negociación de nuevo.

Comando BGP: *neighbor VECINO ebgp-multihop [TTL]*
Comando BGP: *no neighbor VECINO ebgp-multihop*
Activa el modo ebgp-multihop, usado para establecer sesiones BGP entre sistemas de distintos SA, con no se encuentran directamente conectados al mismo segmento de red y en ciertas configuraciones de tunnel, gre e ipip. TTL establece el número de saltos al los que se encuentra el vecino, si no se especifica, el valor por defecto es el máximo, 255. Con "no" se desactiva la configuración ebgp-multihop.

Comando BGP: *neighbor VECINO description*
Comando BGP: *no neighbor VECINO description*
Establece/Elimina una descripción del vecino en texto libre.

Comando BGP: *neighbor VECINO version VERSION*
Comando BGP: *no neighbor VECINO version VERSION*
Fija la versión BGP del vecino.

Comando BGP: *neighbor VECINO interface NOMBRE_IF*
Comando BGP: *no neighbor VECINO interface NOMBRE_IF*
Cuando conectas con un vecino BGP sobre una dirección IPv6 de enlace-local, debes especificar el nombre del interfaz usado para esa conexión.

Comando BGP: *neighbor VECINO next-hop-self*
Comando BGP: *no neighbor VECINO next-hop-self*
Este comando fuerza al encaminador a anunciarse como el próximo salto, para las rutas que distribuya a sus vecinos.

Comando BGP: *neighbor VECINO update-source NOMBRE_IF*
Comando BGP: *no neighbor VECINO update-source NOMBRE_IF*
Con este comando, BGP usará la dirección del interfaz designado para establecer la sesión BGP, es casi imprescindible cuando se usa eBGP-multihop.

Comando BGP: *neighbor VECINO default-originate*
Comando BGP: *no neighbor VECINO default-originate*
El comportamiento por defecto de bgpd es no anunciar la ruta por defecto (0.0.0.0/0), incluso si esta se encuentra en la tabla de rutas. Este comando anunciará la ruta (0.0.0.0/0) a ese vecino concreto, si existe, o le generará una.

Comando BGP: *neighbor VECINO port PUERTO*
Comando BGP: *no neighbor VECINO port PUERTO*
Especifica que puerto tcp se usará para establecer la sesión BGP con ese vecino si es distinto del puerto estándar (179).

Comando BGP: *neighbor VECINO send-community*
Comando BGP: *no neighbor VECINO send-community*
Instruye al demonio BGP a enviar las comunidades, asociadas a los distintos prefijos, este el comportamiento por defecto de bgpd, por lo que, debemos instruirle "no neighbor VECINO send-community" para deshabilitar el envío de comunidades.

Comando BGP: *neighbor VECINO weight PESO*
Comando BGP: *no neighbor VECINO weight PESO*
Este comando especifica un peso por defecto a las rutas aprendidas de ese vecino. (Es específico de Cisco).

Comando BGP: *neighbor VECINO maximum-prefix NÚMERO*
Comando BGP: *no neighbor VECINO maximum-prefix NÚMERO*
Este comando fija un tope máximo de prefijos que un vecino nos puede enviar, y se usa para evitar una inundación de prefijos que ponga en peligro la estabilidad de la red. Al llegar al número máximo de prefijos la sesión se cerrará hasta que el administrador, ejecute el comando "no neighbor VECINO shutdown"

Comando BGP: *neighbor VECINO distribute-list NOMBRE [IN | OUT]*
Comando BGP: *no neighbor VECINO distribute-list NOMBRE [IN | OUT]*
Este comando especifica una lista para el filtrado de actualizaciones enviadas a un vecino desde <IN> o hacia este <OUT>

Comando BGP: *neighbor VECINO prefix-list NOMBRE [IN | OUT]*
Comando BGP: *no neighbor VECINO prefix-list NOMBRE [IN | OUT]*
Este comando especifica una lista de prefijos, que se aceptan desde un vecino.

Comando BGP: *neighbor VECINO filter-list NOMBRE [IN | OUT]*
Comando BGP: *no neighbor VECINO filter-list NOMBRE [IN | OUT]*
Este comando especifica un filtrado de las rutas del vecino en base a su AS_PATH.

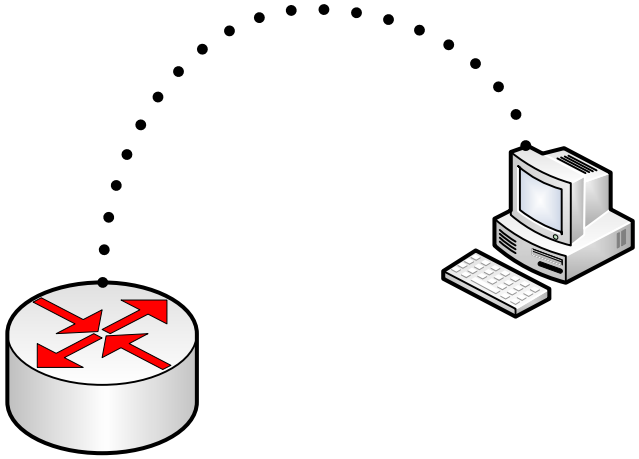
Comando BGP: neighbor VECINO route-map NOMBRE [IN | OUT]
Comando BGP: no neighbor VECINO route-map NOMBRE [IN | OUT]
Aplica un route-map a un vecino para un control avanzado de las rutas desde <IN> o hacia este <OUT>.

ENUNCIADOS DE PRÁCTICAS

Práctica Nº 1

Aspectos fundamentales de la línea de comandos.

1. Práctica Nº 1: Aspectos fundamentales de la línea de comandos.



Objetivos

- Ingresar a los modos de usuario y privilegiado del router.
- Utilizar varios comandos básicos del router para determinar la configuración del router.
- Usar la función de AYUDA del router.
- Usar las funciones de historial de comandos y de edición.
- Asignar un nombre al router

Introducción

Con la implementación de esta práctica se pretende que el estudiante se familiarice con los comandos básicos de configuración, así como aprender a utilizar el comando de AYUDA del router y otras funciones necesarias para poder realizar correctamente la configuración en los routers. Para esto el estudiante trabajará con un diagrama igual al anterior e ingresará a los modos de usuario y privilegiado del router

Requerimientos

Un router Cisco de la serie 2620.
Una computadora.
Simulador.Boson NetSim v.6

1.1. Utilizar la función de ayuda

1.1.1. Si la petición de entrada muestra “Router”, esta es la opción por defecto. Puede aparecer otra cosa si el router tiene un nombre. ¿Qué petición de entrada mostró en router?

1.1.2. ¿Qué significa el símbolo de petición después de un nombre de router?

1.1.3. Introduzca el comando **`help`** escribiendo ? en la petición de entrada del router EXEC usuario.
`Router>`**`?`**

1.1.4. Enumere ocho comandos disponibles que aparecen en la respuesta del router.

1.2. Entrar al modo EXEC privilegiado

1.2.1. Entre al modo enable con el comando **`enable.`** Si se le pide una contraseña, introduzca la contraseña **`class.`**
`Router>`**`enable`** `[intro]`

1.2.2. ¿El modo **`enable`** apareció entre los comandos disponibles del paso anterior?

1.2.3. ¿De qué forma cambio la apariencia de la petición de entrada del router y que significa este cambio?

1.3. Usar la función de ayuda

1.3.1. Entre al modo de ayuda escribiendo un signo de interrogación (**?**) en la petición de entrada EXEC privilegiado del router.
`Router#`**`?`**

1.3.2. Enumere los diez (10) comandos disponibles que aparecen en la respuesta del router.

1.4. Usando el comando SHOW.

1.4.1. Enumere todos los comandos show introduciendo **`show ?`** en la petición de entrada EXEC privilegiado del router.
`Router#show ?`

1.4.2. ¿El comando **`running-config`** aparece entre los comandos disponibles para este modo?

1.5. Examinar la configuración activa

1.5.1. Visualice la configuración activa del router introduciendo el comando **`show running-config`** en la petición de entrada EXEC privilegiado del router.
`Router#show running-config`

1.5.2. Enumere seis datos clave que aparecen con este comando:

1.6. Examinar la configuración con mas detalle

1.6.1. Siga visualizando la configuración.

1.6.2. Cuando aparezca la palabra “more” (más), presione la barra espaciadora. Al presionar la barra espaciadora, el router muestra la siguiente página de información.

1.6.3. ¿Qué ocurrió cuando presiono la barra espaciadora?

1.7. Usar el historial de comandos

1.7.1. Use el comando **`history`** para ver y reutilizar los comandos ingresados anteriormente. Presione la fecha arriba o **`Ctrl-p`** para ver el último comando ingresado. Presiónela nuevamente para ir al comando anterior a ese. Presione la flecha abajo o **`Ctrl-n`** para recorrer la lista alrevés. Esta función permite visualizar el historial de comandos.

1.7.2. ¿Qué apareció en la petición de entrada del router al presionar la flecha arriba?

1.8. Entre al modo de configuración global

1.8.1. Introduzca **`configure Terminal`** en la petición de entrada del modo EXEC privilegiado.
`Router# **Configure terminal**`

1.8.2. ¿Qué petición de entrada mostró el router?

1.8.3. ¿Qué significa esta petición de entrada?

1.9. Introducir el nombre del host GAD para este router

1.9.1. Introduzca **`hostname GAD`** en la petición de entrada.
`Router(config)# **hostname GAD**`

1.9.2. ¿Qué petición de entrada mostró el router?

1.9.3. ¿Qué significa esta petición de entrada?

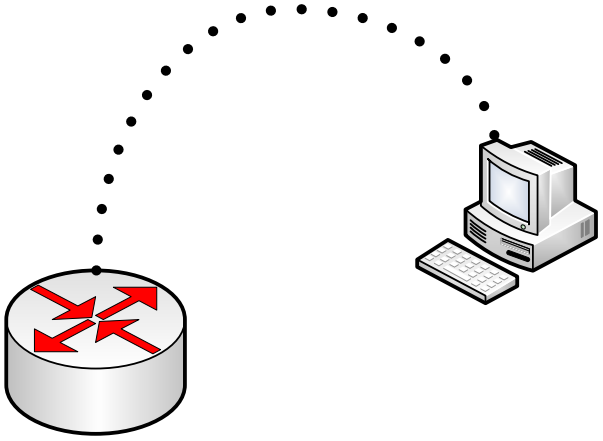
1.10. Salir del router

1.10.1. Introduzcir **`exit`** en la petición de entrada para salir del router
`GAD(config)# **exit**`

Prática Nº 2

Modos de comando y configuración de contraseñas del router

2. Práctica Nº 2: Modos de comando y configuración de contraseñas del router.



Objetivos

- Identificar los modos básicos del rotuer, EXEC usuario y privilegiado.
- Usar los comandos para entrar a modos específicos.
- Familiarizarse con la petición de entrada del router para cada modo.
- Configurar una contraseña para iniciar una sesión de consola en el modo EXEC usuario.
- Configurar una contraseña para las sesiones de Terminal virtual (Telnet).
- Configurar una contraseña secret para el modo EXEC privilegiado.

Introducción

Con la realización de esta práctica se pretende que el estudiante sea capaz de identificar los modos básicos de configuración del router, así como de configurar las contraseñas de consola, de sesiones de terminales virtuales (Telnet) y por último las contraseñas enable secret y enable password, a través de las cuales se generara mayor seguridad al momento de querer acceder a la configuración interna del router. Para esto el estudiante trabajara con un diagrama similar al anterior.

Requerimientos

Un router ¨Cisco de la serie 2620
Una computadora.
Simulador.Boson NetSim v.6

2.1. Conectarse al router en el modo EXEC usuario

2.1.1. ¿Qué petición de entrada mostró en router?

2.1.2. ¿Qué significa esta petición de entrada?

2.2. Conectarse al router en el modo EXEC privilegiado

2.2.1. Introduzca **enable** en la petición de entrada del modo EXEC usuario.
```
Router>enable
```

2.2.2. ¿Qué petición de entrada mostró en router?

2.2.3. ¿Qué significa esta petición de entrada?

2.3. Entrar al modo de configuración global

2.3.1. Introduzca **configure Terminal** en la petición de entrada del modo EXEC privilegiado.
```
Router# Configure terminal
```

2.3.2. ¿Qué petición de entrada mostró el router?

2.3.3. ¿Qué significa esta petición de entrada?

2.4. Entrar al modo de configuración del router

2.4.1. Introduzca **router rip** en la petición de entrada del modo EXEC privilegiado.
```
Router(config)# router rip
```

2.4.2. ¿Qué petición de entrada mostró el router?

2.4.3. ¿Qué significa esta petición de entrada?

2.5. Salir del modo router y entrar al modo de configuración de interfaz

2.5.1. Introduzca **exit** en la petición de entrada para volver al modo de configuración global.
```
Router(config-router)# exit
```

2.5.2. Introduzca **interface serial 0** en la petición de entrada del modo de configuración global.

2.5.3. ¿Qué petición de entrada mostró el router?

2.5.4. ¿Qué significa esta petición de entrada?

2.5.5. Introduzca **exit** en la petición de entrada para volver al modo de configuración global.

2.6. Asignar un nombre al router

2.6.1. `Router(config)# hostname GAD`

2.6.2. ¿Qué petición de entrada mostró el router?

2.6.3. ¿Qué significa esta petición de entrada?

2.6.4. ¿Qué cambio se produjo en la petición de entrada?

2.7. Configurar la contraseña de consola y salir

2.7.1. Configurar la contraseña de consola en el router y salga de la consola de línea. Introduzca las siguientes líneas de código:

```
GAD(config)# line console 0
GAD(config-line)# password cisco
GAD(config-line)# login
GAD(config-line)# exit
GAD(config)#
```

2.8. Configurar y salir

2.8.1. Configure la contraseña para las líneas de Terminal virtual y salga del modo de línea. Introduzca las siguientes líneas de código:

```
GAD(config)# line vty 0 4
GAD(config-line)# password cisco
GAD(config-line)# login
GAD(config-line)# exit
GAD(config)#
```

2.9. Configurar la contraseña enable y regresar al modo EXEC usuario

2.9.1. Configure el password de enable y salga del modo de Configuración.

2.9.2. Regrese al modo EXEC usuario mediante el comando **disable**

```
GAD# disable
```

2.10. Entrar al modo EXEC privilegiado nuevamente

2.10.1. Esta vez aparecerá una petición de contraseña. Introduzca **cisco** pero los caracteres no aparecerán en la línea.

```
GAD>enable
Password:cisco
```

2.11. Configurar la contraseña enable secret y volver al modo EXEC usuario

2.11.1. Regrese al modo de configuración mediante el comando **configure terminal:**

2.11.2. Configure la contraseña enable secret y salga del modo de configuración global:

Nota: Recuerde que la contraseña enable secret esta cifrada desde la vista de configuración. Además, no escriba **enable secret password clase,** o la contraseña secret será password, no clase. La contraseña enable no esta cifrada y se puede ver desde la configuración.

2.11.3. Volver al modo EXEC usuario introduciendo el comando disable:

2.12. Entrar al modo EXEC privilegiado nuevamente

Aparecerá una petición de contraseña. Introduzca **cisco.** Los carácteres no aparecerán en la línea. Si no funciona, continúe hasta que aparezca el mensaje “bad secrets”:

```
GAD>enable
Password: cisco
Password: cisco
Password: cisco
% Bad secrets
```

2.13. Entrar al modo EXEC privilegiado nuevamente

Aparecerá una petición de contraseña. Introduzca **clase.** Los caracteres no aparecerán en la línea:

Nota: La contraseña enable secret tiene prioridad sobre la contraseña enable. Por lo tanto, una vez que se introduce una contraseña enable secret la contraseña enable ya no se acepta.

2.14. Mostrar la configuración activa del router

2.14.1. ¿Existe una contraseña cifrada?

2.14.2. ¿Existen otras contraseñas?

2.14.3. ¿Alguna de las otras contraseñas esta cifrada?

Nota: En la información que muestra el comando **show running-config** notifica que no hay servicio de encriptación para contraseñas.

2.15. Una vez completados los pasos anteriores salga del router

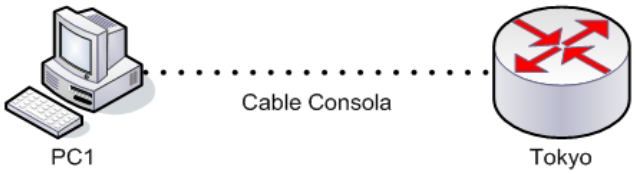
2.15.1. Introduzcir **exit** en la petición de entrada para salir del router

```
GAD(config)# exit
```

Práctica Nº 3

Comando Show

3. Práctica Nº 3: Comando Show



Objetivos

- Familiarizarse con los comandos show del router
- Conocer la importancia de los comandos show

Introducción

Con la realización de esta práctica se pretende que es estudiante se familiarice con los comandos show del router y por último que reconozca la importancia de contar con una utilidad como el comando **show** ya que através de ellos puede conocer mucha información del router porque son los comandos de captura de información mas importantes del router.

Requerimientos

Un router Cisco de la serie 1841.
Un computador.
Simulador Packet Tracer 4.0

Para la realización de la práctica deberás crear una red con una topología similar a la del diagrama anterior para lo que necesitarás los requerimientos planteados anteriormente y con las caracteristicas presentadas en la tabla anterior.

3.1. Conéctese al router. Puede iniciar una sesión desde la PC1 o desde el propio router en el simulador. Configure el nombre del router con el comando `hostname` en le modo de configuración global.

3.2. Introduzca el comando help escribiendo "?" en la petición de entrada del router. El router mostrará todos los comandos en el modo usuario. ¿El comando show aparece en la lista?

3.2.1. Muestre la ayuda del comando show, esto es escriba el signo "?" después de la palabra show.

3.2.2. Liste los comandos que aparecen.

3.3. Entre al modo EXEC privilegiado. Introduzca el comando help escribiendo "?" en la petición de entrada del router. El router mostrará todos los comandos en el modo usuario. ¿El comando show aparece en la lista?

3.3.1. Muestre la ayuda del comando show, esto es escriba el signo "?" después de la palabra show.

3.3.2. Liste los comandos que aparecen. ¿Son los mismos?

3.4. Con el comando show se puede ver la información que se encuentra en el router. Este nos ayudará a la hora de ver y analizar información que nosotros hallamos configurado si están ocurriendo fallas.

3.4.1. Con el comando **`show running-config`** puede determinar el estado actual de un router, ya que muestra el archivo de configuración activo que se ejecuta en la RAM. Introduzca este comando en el modo EXEC privilegiado.

3.4.2. El comando **`show startup-config`** muestra la copia de respaldo del archivo de configuración que se guarda en la memoria no volátil o NVRAM. Este archivo es el que se carga cuando el router arranca. Introduzca el comando en la línea de órdenes.

3.4.3. El comando **`show flash`** se utiliza para visualizar la memoria flash disponible y la cantidad utilizada. La memoria flash es el lugar donde se guarda la imagen del IOS o archivo del Sistema Operativo de Intenetworking de Cisco. Introduzca el comando.

3.4.3.1. ¿Cuánta memoria flash está disponible y cuanta se ha utilizado?

3.4.3.2. ¿Cuánto es el tamaño en bytes de la memoria flash?

3.4.3.3. ¿Qué archivo que se guarda en la memoria flash?

3.4.4. El comando **`show interface`** muestra la estadísticas para todas las interfaces configuradas en router. Introduzca el comando en la línea de órdenes.

3.4.4.1. ¿Qué significa que las interfaces presenten la siguiente información "administratively down, line protocol is down"?

3.4.4.2. ¿Qué es MTU?, ¿Qué valor tiene?

3.4.4.3. ¿Qué significa BW?, ¿Qué valor tiene?

3.4.5. Introduzca el comando **`show version.`** El router devuelve información acerca del IOS que se esta ejecutando en la RAM. Introduzca el comando en la línea de órdenes.

3.4.5.1. ¿Cuál es la versión del IOS?

3.4.5.2. ¿Cuál es el nombre del archivo de imagen del sistema (IOS)?

3.4.5.3. ¿Qué tipo de procesador (CPU) y qué cantidad de RAM tiene este router?

3.4.5.4. ¿Qué cantidad de memoria NVRAM tiene?

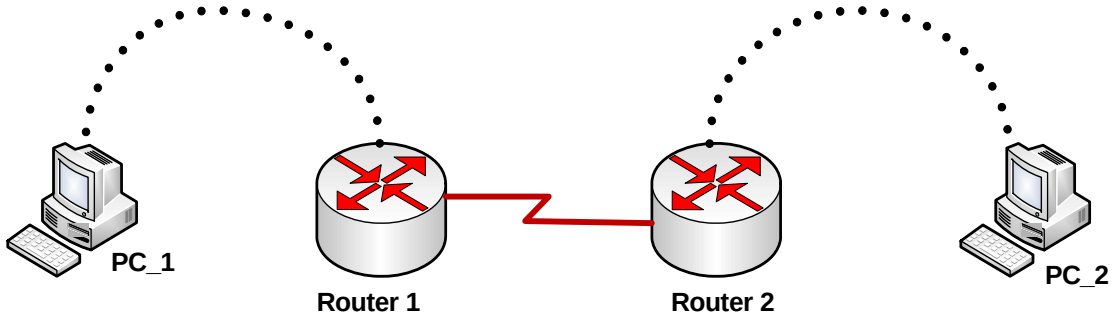
3.4.5.5. ¿Qué significa Configuration register is 0x2102?

3.4.6. Muestre el buffer de comandos con el comando **`show history`**.

Práctica Nº 4

Configuración de las Interfaces Serial y Ethernet

4. Práctica Nº 4: Configuración de las Interfaces Serial y Ethernet.



Router	Nombre del router	Dirección FA0/0	Dirección S0	Tipo de interfaz S0 DTE/DCE	Contraseña enable secret	Contraseña console 0 / vty 0 4
Router 1	GAD	192.168.14.1/ 24	192.168.15.1 /24	DCE	clase	cisco
Router 2	BHM	192.168.16.1/ 24	192.168.15.2 /24	DTE	clase	cisco

Objetivos

- Configurar una interfaz Serial en cada uno de los dos routers para que se puedan comunicar entre sí.
- Configurar una interfaz Ethernet en cada router con una dirección IP y una máscara de subred.

Introducción

En este laboratorio, el estudiante configurará las Interfaces Serial y Ethernet en cada router. Estas interfaces activas de los routers forman parte de las redes que están directamente conectadas al dispositivo, las cuales deben llevar una dirección IP y su correspondiente máscara, como un host perteneciente a esa red. Por tanto el administrador debe habilitar la interfaz para que la conexión se pueda mantener activa.

Requerimientos

2 router de la serie 2620
2 PCs
Simulador Boson Netsim v.6

4.1. Configurar el nombre y las contraseñas en los Routers

En los routers, entre al modo de configuración global y configure el nombre del dispositivo como se muestra en la gráfica. Luego configure las contraseñas de consola, de la terminal virtual y enable.

4.2. Configurar la Interfaz Serial, Serial 0

En el modo de configuración global, configure la interfaz serial 0 en el router GAD. Consulte el esquema de interfaz.

Nota: Una vez que entre al modo de configuración de interfaz, anote la dirección IP de la interfaz. Introduzca la máscara de subred. Introduzca la velocidad del reloj solamente en el lado DCE del dispositivo. El comando **no shutdown** activa la interfaz. La interfaz se desactiva con **shutdown.**

4.3. Guardar la configuración activa

Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

Nota: Guarde la configuración activa para la próxima vez que se reinicie el router. El router puede reiniciarse ya sea a través de un comando **reload** del software o debido a un corte de energía. La configuración activa se perderá si no se guarda. El router utiliza la configuración inicial al arrancarse.

4.4. Mostrar información sobre la interfaz serial 0 en GAD

4.4.1. Introduzca el comando **show interface serial0** en GAD. Consulte el esquema de interfaz.

Aparecerán los detalles de la interfaz serial 0

4.4.2. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

4.4.3. La interfaz Serial 0 está:___. El protocolo de línea es:___.

4.4.4. ¿Cuál es su dirección de internet?

4.4.5. ¿Qué tipo de encapsulamiento utiliza?

4.4.6. ¿A qué capa del modelo OSI se refiere el término “encapsulamiento”?

4.4.7. Si la interfaz serial se ha configurado, ¿por qué **show interface serial 0** dice que la interfaz está desactivada?

4.5. Configurar la interfaz Serial 0 en el Router 2(BHM)

En el modo de configuración global, configure la interfaz serial 0 en el router BHM. Consulte el esquema de interfaz.

4.6. Guardar la configuración activa

Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

4.7. Mostrar información sobre la interfaz serial 0 en BHM

4.7.1. Introduzca el comando **show interface serial 0** en BHM. Consulte el esquema de interfaz.

Aparecerán los detalles de la interfaz serial 0

4.7.2. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

4.7.3. La interfaz Serial 0 está:___. El protocolo de línea es:___.

4.7.4. ¿Cuál es su dirección de internet?

4.7.5. ¿Qué tipo de encapsulamiento utiliza?

4.7.6. ¿Cuál es la diferencia en el estado de línea y de protocolo registrado anteriormente en GAD? ¿Por qué?

4.8. Verificar que la conexión serial esté funcionando

4.8.1. Haga **`ping`** a la interfaz serial del otro router.

4.8.2. Desde GAD, haga ping a la interfaz del router BHM. ¿El ping funciona?

4.8.3. Desde BHM, haga ping a la interfaz del router GAD. ¿El ping funciona?

4.8.4. Si la respuesta a cualquiera de las dos preguntas es no, realice un diagnóstico de fallas de las configuraciones del router para detectar el error. Luego, realice los pings nuevamente hasta que la respuesta a ambas preguntas sea sí.

4.9. Configurar la interfaz FastEthernet 0 en GAD

Nota: La designación de la primera interfaz Ethernet en el router puede variar. Puede ser ethernet 0, fastethernet 0 o fastethernet 0/0 según el tipo de router.

Nota: El comando **no shutdown** activa la interfaz. La interfaz se desactiva con **shutdown.**

4.10. Guardar la configuración

4.10.1. Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

```
GAD#copy running-config startup-config
```

4.11. Despliegue la información de la interfaz FastEthernet 0

4.11.1. Introduzca el comando **show interface fastethernet 0** en GAD. Consulte el esquema de interfaz.

Aparecerán los detalles de la interfaz Ethernet

4.11.2. Haga una lista de por lo menos tres detalles descubiertos al introducir este comando.

4.11.3. La interfaz Serial 0 está:___. El protocolo de línea es:___.

4.11.4. ¿Cuál es su dirección de internet?

4.11.5. ¿Qué tipo de encapsulamiento utiliza?

4.12. Configurar la interfaz FastEthernet 0 en BHM

Nota: La designación de la primera interfaz Ethernet en el router puede variar. Puede ser ethernet 0, fastethernet 0 o fastethernet 0/0 según el tipo de router.

4.13. Guardar la configuración

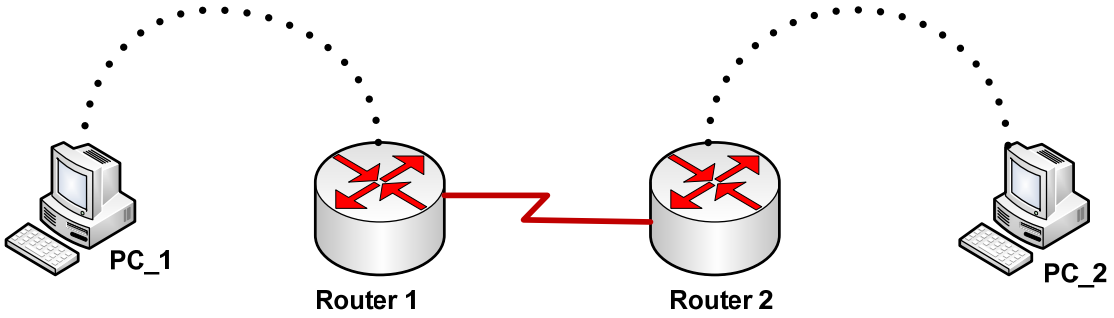
4.13.1. Guarde la configuración activa como la configuración inicial en el modo EXEC privilegiado:

```
BHM#copy running-config startup-config
```

Práctica Nº 5

Configuración de las descripciones de interfaz y del mensaje del día (MOTD)

5. Práctica Nº 5: Configuración de las descripciones de interfaz y del mensaje del día (MOTD)



Designación del router	Nombre del router	Dirección FA0/0	Dirección S0	Tipo de interfaz S0 DTE/DCE	Contraseña enable secret	Contraseña console 0 / vty 0 4
Router 1	GAD	192.168.15.1/24	192.168.16.1/24	DCE	clase	cisco
Router 2	BHM	192.168.17.1/24	192.168.16.2/24	DTE	clase	cisco

Objetivos

- Elegir una descripción para la interfaz serial en cada uno de los dos routers y utilizar el modo de configuración de la interfaz para introducir esta descripción.
- Utilizar los comandos necesarios para introducir un mensaje del día (MTOD) en el router. Este procedimiento permite a todos los usuarios visualizar el mensaje al entrar en el router.

Introducción

En este laboratorio, el estudiante establecerá una descripción para la interfaz serial en cada router. Esta descripción es un comentario asociado a la interfaz con el que se describe la utilización de la misma.

También se introducirá el mensaje del día (MOTD) en cada uno de los routers. Este mensaje de inicio de sesión se muestra al usuario al momento de hacer login en el router, y se usa para comunicar información de interés a todos los usuarios de la red, tales como avisos de próximas interrupciones del sistema. El mensaje debe de advertir que sólo los usuarios autorizados deben de intentar el acceso.

Requerimientos

Dos router de la serie 2620.
Dos PC.
Simulador Boson Netsim v.6.

5.1. Configurar el nombre y las contraseñas en los Routers

5.1.1. En los routers, entre al modo de configuración global y configure el nombre del dispositivo tal como aparece en el cuadro. Entonces configure las contraseñas de consola, de la terminal virtual y enable. Configure las interfaces FastEthernet 0/0 y Serial 0 en el router de acuerdo al diagrama. Si existen dificultades, consulte la práctica de laboratorio anterior.

5.1.2. ¿Cuál es el comando del router que se utiliza para visualizar la configuración activa?

5.1.3. ¿Qué modo de comando se debe utilizar para introducir el comando que se menciona en la última pregunta?

5.1.4. Introduzca el comando de la pregunta anterior para verificar la configuración que se acaba de introducir. Si la configuración nos es correcta, corrija los errores. Vuelva a verificarla hasta que esté correcta.

5.1.5. Guarde la configuración en el modo de comando EXEC privilegiado.

5.2. Entre al modo de configuración global

5.2.1. Introduzca **`configure terminal`** en la petición de entrada del router. Observe el cambio en la petición de entrada del router.

¿Cómo cambio la petición de entrada del router?

5.3. Entrar al modo de configuración de interfaz

5.3.1. Introduzca **`interface serial 0`** en la petición de entrada de configuración global. Consulte el esquema de interfaz.

¿Cómo es la petición de entrada del router en el modo de configuración de interfaz?

Una vez que se le indica al IOS qué modulo de interfaz físico era el que había que configurar, la linea de comandos IOS cambia a GAD(config-if)#, donde **if** es la abreviatura de <<interfaz>>.

5.4. Mostrar la ayuda para el comando description

5.4.1. Introduzca **`description ?`** en la petición de entrada del router.

¿Cuál es el número máximo de caracteres de una descripción de interfaz?

5.5. Elegir una descripción para la interfaz

5.5.1. Una descripción de interfaz incluye el propósito y la ubicación de la interfaz, los otros dispositivos o ubicaciones conectadas a la interfaz y los identificadores de circuito. Las descripciones ayudan al personal de asistencia técnica a comprender la dimensión de los problemas relacionados con una interfaz. Las descripciones también permiten una resolución más rápida de los problemas.

5.5.2. A base del diagrama y la siguiente información del circuito, elija una descripción de las interfaces seriales 0/0 para GAD y BHM. Use el siguiente formulario para documentar su elección.

Enlace	Portadora	ID del Circuito	Velocidad
De GAD a BHM	BellSouth	10DHDG551170	1.544Mbits/seg
De BHM a GAD	BellSouth	10DHDG551171	1.544Mbits/seg

5.6. Introducir una descripción para la interfaz serial 0

5.6.1. En el modo de configuración de la interfaz para la interfaz serial 0 en GAD y BHM, introduzca el texto de descripción. El texto es la descripción del paso anterior. Luego introduzca **Ctrl-z** o escriba **end** (finalizar) para volver al modo EXEC privilegiado.

Nota: esto sería lo mismo que escribir **exit** (salir) para salir del modo de configuración de interfaz y **exit** nuevamente para abandonar el modo de Configuración global. Esto constituye un atajo de teclado.

5.7. Examinar el archivo de configuración activo en GAD

5.7.1. En el modo EXEC privilegiado, introduzca el comando que hará aparecer la configuración activa. El modo EXEC privilegiado también se denomina modo enable. El router mostrará información sobre la configuración activa.

5.7.2. ¿Qué comando se introdujo?

5.7.3. ¿Cuál es la descripción de la interfaz serial 0?

5.8. Confirmar que la descripción de la interfaz sea correcta en GAD

5.8.1. Desde el modo enable, introduzca el comando **`show interface serial0`**. El router muestra información sobre la interfaz. Examine este resultado para confirmar que la descripción introducida coincida con la descripción correcta.

5.9. Mostrar la ayuda del comando `banner motd`

5.9.1. Entre en modo de configuración global.

5.9.2. Introduzca **`banner motd ?`** en la petición de entrada del router.

5.9.3. ¿Cuál es el carácter que se utiliza para indicar el principio y el final del banner?

5.10. Escoja un mensaje para configurarlo como el “mensaje del día”

5.10.1. El banner de inicio de sesión debe ser una advertencia de no intentar conectarse a menos que tenga autorización. En el siguiente espacio, introduzca en banner de advertencia apropiado para GAD y BHM. El mensaje puede contener cualquier carácter imprimible así como espacios y retornos de carro.

Mensaje a utilizar: “Este es un sistema protegido, solo personal autorizado”

5.11. Introducir el mensaje de banner deseado

5.11.1. Desde el modo de configuración global en GAD y BHM introduzca **`banner motd c`** ***`message`*** **`c`**. El símbolo **“c”** se utiliza como delimitador y ***“message***” es el mensaje de banner elegido en el paso anterior.

5.12. Probar la visualización del MOTD en GAD y BHM

5.12.1. Salga de la sesión de consola. Vuelva a entrar en el router para visualizar el mensaje del día. Esto se hace presionando la tecla **Intro**. Esto hará aparecer el mensaje introducido en la configuración.

5.13. Verificar el MOTD analizando la configuración de los routers

5.13.1. Introduzca el comando **`show running-config`.**

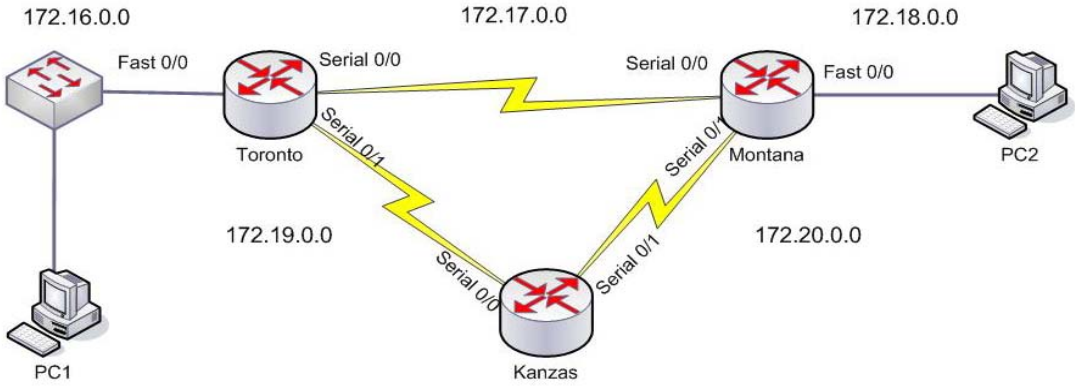
5.13.2. ¿Cómo aparece el banner MOTD en la lista de configuración?

5.13.3. Guarde la configuración desde el modo privilegiado.

Práctica Nº 6

RIP
(Routing Information Protocol)

6. Práctica Nº 6: RIP (Routing Information Protocol)



Nombre del router	Dirección FastEthernet 0/0	Tipo de Interfaz	Dirección Serial 0/0	Tipo de Interfaz	Dirección Serial 0/1	Máscara de subred
Toronto	172.16.0.1	DCE	172.17.0.1	DCE	172.19.0.1	255.255.0.0.
Montana	172.18.0.1	DTE	172.17.0.2	DCE	172.20.0.1	255.255.0.0
Kanzas		DTE	172.19.0.2	DTE	172.20.0.2	255.255.0.0

Nombre del router	Contraseña enable secret	Contraseña enable, VTY y de consola
Toronto	Clase	unan
Montana	Clase	unan
Kanzas	Clase	unan

Objetivos

- Configurar el protocolo de vector-distancia RIP
- Utilizar las rutas estáticas con el protocolo RIP
- Aprender a configurar las tablas de host

Introducción

En esta práctica se pretende que el estudiante aplique los conocimientos teóricos obtenidos, a través de la investigación y en el desarrollo del tema **protocolo RIP** usados para que el enrutamiento de la red funcione correctamente. Esta utilidad es necesaria para asegurar que la transferencia de información entre la red sea exitosa. Se pretende utilizar rutas estáticas con el protocolo RIP con el fin de ayudar a RIP en el proceso de enrutamiento.
Al final de la práctica el estudiante podrá crear tablas de host lo que le servirá para trabajar con los elementos de la red de una manera más sencilla.

Requerimientos

Tres routers de la serie.
Un switch de la serie.
Dos computadores.
Simulador Packet Tracer v4.0

6.1. Configurar los router

6.1.1. Desde el modo de configuración global, configure el nombre de host tal como aparece en el cuadro. Entonces, configure las contraseñas de consola, de la Terminal Virtual y de enable. Configure las interfaces según el cuadro.

6.2. Verificar las entradas de la tabla de enrutamiento y la tabla de enrutamiento RIP, utilice le comando `show ip route` y `show ip route rip` en cada router

6.2.1. ¿Por qué **`show ip route rip`** no muestra nada?

6.2.2. ¿Por qué **`show ip route`** muestra entradas en la tabla?

6.3. Entre al modo de configuración de router use el comando `route rip` y configure el protocolo de enrutamiento RIP en cada uno de los routers

6.3.1. ¿Para qué se usa el comando **network**?

6.4. Verifique la conectividad entre los routers haciendo ping a la interfaz FastEthernet 0/0 del otro router

6.5. Muestre la tabla de enrutamiento y la tabla de enrutamiento RIP de cada router

6.5.1. ¿Por qué ahora si muestra entradas la tabla de enrutamiento RIP?

6.5.2. ¿Cómo se interpreta la siguiente línea?
R 172.18.0.0/16 [120/1] vía 172.17.0.2, 00:00:02, Serial0/0

6.6. Asegúrese de que se estén enviando las actualizaciones de enrutamiento, use el debug `ip rip`, ejecute el comando en el router Toronto

6.6.1. ¿A dónde envía actualizaciones el router Toronto?

6.6.2. ¿De quien recibe las actualizaciones?

6.6.3. ¿Qué contiene las actualizaciones?

6.6.4. ¿Por qué en algunas redes la métrica es de 1 y en otra el valor es 2?

6.7. Inhabilite el envío de actualizaciones a través de la interfaz Serial 0/0 del router Kanzas. Use el comando `passive-interface`, verifique en el router Toronto si se envían actualizaciones por esa interfaz.

6.7.1. ¿De qué interfaces recibía información de actualizaciones el router Toronto antes de aplicar el comando?

6.7.2. Inhabilite el envió de actualizaciones

6.7.3. De que interfaces recibe actualizaciones el router Toronto después de aplicar el comando.

6.8. Redistribución estática en RIP. Configure una ruta estática por defecto en el router Kanzas de manera que los paquetes que quieran llegar a redes externas lo hagan por medio de esta ruta. Utilice la siguiente línea.

6.8.1. Muestre la tabla de enrutamiento y la tabla de enrutamiento RIP. ¿Hubo algún cambio?

6.8.2. ¿Los otros routers tienen conocimiento de esta ruta? ¿Por qué?

6.9. Configuración de la tabla de hosts. Configure la tabla de host del router Kanzas para el router Toronto y el router Montana. Use el comando ip host.

Nota: en la misma sentencia se pueden poner todas las direcciones a las que conecta el router.

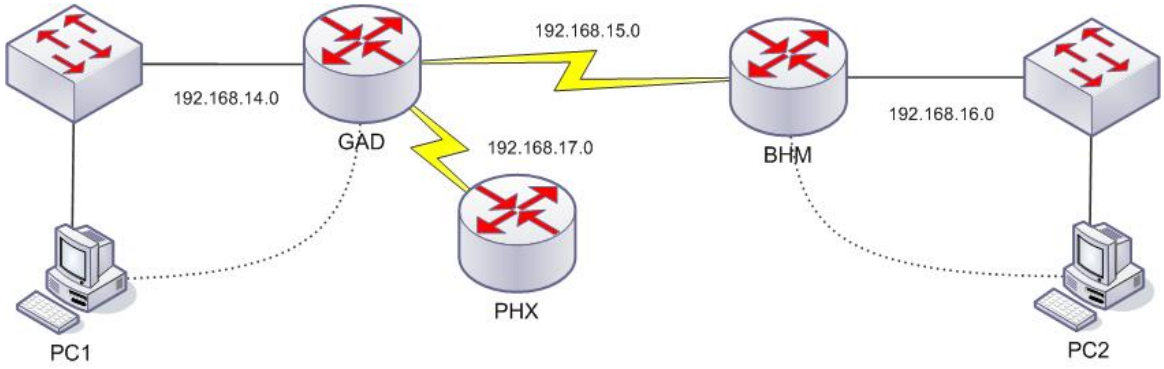
6.9.1. Muestre la tabla host con el comando show host.

6.9.2. Haga ping al router Toronto y al router Montana.

Práctica Nº 7

Telnet, Ping y Treceroute.

7. Práctica Nº 7: Telnet, Ping y Traceroute.



Nombre del Router	Contraseña enable, vty, consola	Protocolo de enrutamiento	Redes anunciadas
GAD	Cisco	rip	192.168.14.0 192.168.15.0 192.168.17.0
BHM	Cisco	rip	192.168.15.0 192.168.16.0
PHX	Cisco	rip	192.168.17.0

Nombre del rotuer	Dirección serial 1	Fast Ethernet 0	Tipo interfaz serial 0	Dirección Ip serial 0	Máscara de Subred
GAD	192.168.17.1	192.168.14.1	DCE	192.168.15.1	255.255.255.0
BHM		192.168.16.1	DTE	192.168.15.2	255.255.255.0
PHX	192.168.17.2				255.255.255.0

Objetivos

- Aplicación de las utilidades Telnet, Ping, Traceroute.
- Usar la utilidad Telnet para comprobar el correcto funcionamiento de la capa de aplicación entre el origen y el destino.
- Usar la utilidad Ping para comprobar que la conexión entre el origen y el destino funciona correctamente.
- Usar la utilidad Traceroute para evaluar la confiabilidad de la ruta extremo a extremo.

Introducción

En esta práctica se pretende que el estudiante aplique los conocimientos teóricos obtenidos, a través de la investigación y en el desarrollo del tema de las aplicaciones tales como **telnet, ping, tracert** que se usan cuando se esta trabajando en la configuración de la red. Aplicaciones necesarias para comprobar que el funcionamiento de la conexión entre el origen y el destino del tráfico sea correcto, que la capa de red entre las redes esta funcionando correctamente, comprobar que las rutas que toman los paquetes enviados a través toman la ruta correcta. Se pretende que al final de la realización de la práctica el estudiante pueda usar estas utilidades correctamente.

Requerimientos

Dos routers de la serie 1811.
Dos swiches de la serie 2900.
Dos computadores.
Simulador Packet Tracer v4.0

Cree una red con un cableado similar al del diagrama anterior, para lo que necesitará los requerimientos planteados anteriormente.
Las características de la red serán las establecidas en las tablas.

7.1. Configure la red con la información proporcionada en las tablas y verifique la configuración con el comando show `running-config`.

7.2. Inicie una sesión en el router 1 y verifique la conexión al router 2.

7.2.1. Puede verificar la conexión haciendo ping a la interfaz serial 0 del router BHM.

7.3. Hacer telnet a un router remoto.

Nota: Para poder usar la utilidad telnet se deben haber configurado las contraseñas de línea vty y línea de consola.

7.3.1. Puede usar la ayuda del comando telnet para saber las opciones disponibles con este comando.

7.3.2. Introduzca el comando **`telnet`** *dirección Ip, si aún no han sido configuradas las tablas host Ip.*

Si el comando anterior ha funcionado ahora debería estar en consola del router remoto. Por tanto ahora puede analizar las interfaces del router remoto.

7.3.3. Visualice la configuración de las interfaces en el router remoto con el comando **`show interface.`**

7.3.4. Introduzca el comando **`show ip protocols`** para mostrar los protocolos en el router remoto.

7.3.5. Visualizar la configuración activa en el router remoto con el comando **`show running-config.`**

7.3.6. Visualizar la configuración vecina con el comando `show cdp neighbors.`

7.3.7. Suspender la sesión de telnet actual. Introduzca **ctrl+shift+6** seguido de la tecla **x.**

Esto solamente deberá suspender la sesión y volver al router anterior. Asegúrese de estar en el router anterior.

7.3.8. Reanudar una sesión telnet.

Presione la tecla **Intro** en la petición de entrada del router.
Ha aparecido como respuesta lo siguiente:

```
[Resuming connection 1 to 192.168.15.2 ... ]
```

Si es así presione la tecla **Intro** y estará reanudando la sesión telnet previamente suspendida.

Asegúrese de estar ahora en el router remoto.

7.3.9. Cerrar una sesión telnet. Introduzca el comando **`exit`** durante la sesión telnet actual. Esta acción finalizará la sesión telnet.

7.4. Ahora veremos el funcionamiento de la utilidad telnet cuando se establecen varias sesiones.

7.4.1. Desde el router GAD inicie varias sesiones telnet al router BHM y el router PHX.

7.4.2. Suspenda la sesión telnet actual.

Utilice el comando **`show sesión`** para visualizar las conexiones que están en uso.

7.4.3. Reanudar la sesión telnet previamente suspendida. Para esto debe utilizar el comando **`resume`** seguido del número de sesión que desea reanudar, seguido de la tecla **Intro**. El router responderá de la siguiente manera:

```
[Resuming connection 1 to 192.168.15.2 ... ]
```

Presione la tecla **Intro** y asegúrese de estar en el router remoto de nuevo.

7.4.4. Problemas con las sesiones telnet entrelazadas en varios routers.

Nota: Cuando se trabaja con Telnet, uno de los problemas más comunes es olvidar el enfoque de la sesión. El enfoque significa el dispositivo que procesa los comandos que se están introduciendo. Muchas veces los usuarios inician una sesión Telnet a un router y luego hacen telnet desde ese router a otro, etc. Sin nombres de host o en caso de que los routers tengan nombres de host similares, se puede producir confusión.

7.4.4.1. Haga telnet al router BHM desde GAD y luego desde ese router haga telnet al router PHX.

Haga telnet al router GAD.

7.4.4.2. Utilice el comando **`show session`** para verificar el número de sesiones establecidas.

7.5. Compruebe el correcto funcionamiento de la utilidad Ping.

7.5.1. Teclee el comando **`ping`** seguido de la dirección IP de la interfaz.

7.5.1.1. ¿Funcionaron los ping?

7.5.1.2. ¿Qué prueba el comando ping y cuál es su importancia?

7.5.2. Analice y justifique con detalle la salida del comando **`ping`.**

7.5.3. Configure las estaciones de trabajo.

La configuración del host conectado al router GAD es:
Dirección IP 192.168.14.2
Máscara de subred IP 255.255.255.0
Gateway por defecto 192.168.14.1

La configuración del host conectado al router BHM es:
Dirección IP 192.168.16.2
Máscara de subred IP 255.255.255.0
Gateway por defecto 192.168.16.1

7.5.4. Hacer ping desde las estaciones de trabajo para verificar que la pila y el gateway por defecto estén configurados y funcionen correctamente.

El ping deberá responder con resultados exitosos. De lo contrario verifique las configuraciones del host y los routers conectados.

7.6. Realizar un ping extendido.

7.6.1. Entre al modo EXEC privilegiado, escriba enable y luego la contraseña.
Escriba ping y presione **Intro**. Complete el resto de las peticiones de entrada como aparece a continuación:

```
Protocol [ip]:
```

```
Target IP address: 192.168.16.1
Repeat count [5]: 50
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 192.168.16.1, timeout is 2
seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max =
32/32/40ms.
```

Durante el proceso ping, elimine el cable de conexión cruzado de la interfaz Fastethernet una vez que hayan respondido diez ping.

7.6.1.1. ¿Qué dice el resultado de este ping?

7.6.1.2. Trate de realizar esto con un ping estándar. ¿Se puede eliminar el cable antes de que el proceso ping termine?

7.7. Use el comando `traceroute`.

7.7.1. Ingrese **`traceroute ip xxxx.xxxx.xxxx.xxxx`** donde las x son la dirección ip del destino final.

7.7.2. Entre en los routers y repita el uso del comando **`traceroute`** seguido de la dirección a la que quiere llegar.

7.8. Use el comando `traceroute` desde una estación de trabajo.

Para las estaciones de trabajo el comando a usar es **`tracert`** en lugar de **`traceroute`.**

7.8.1. Introduzca **`tracert`** seguido de la dirección del destino final.

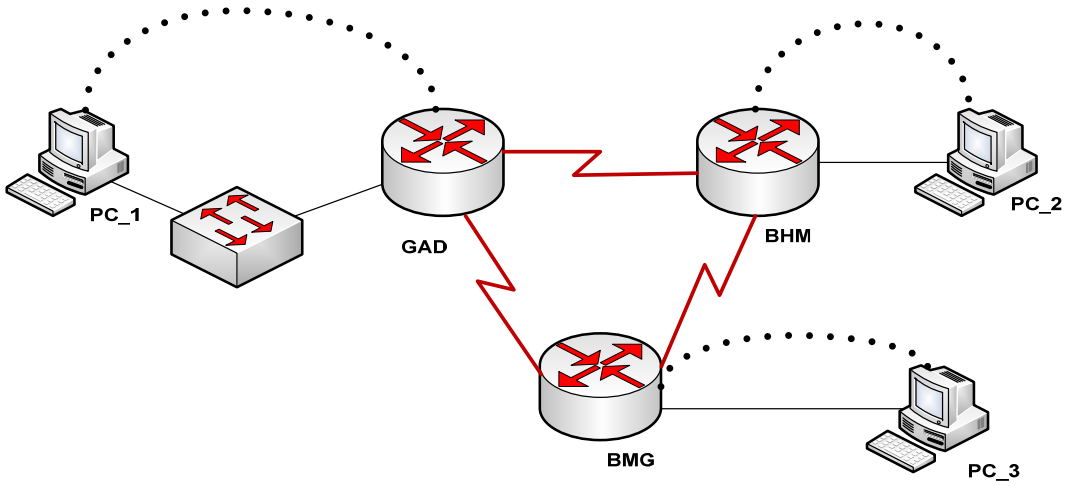
7.8.2. Haga traceroute a distintos sitios Web como Cisco.com, yahoo.com, etc.

Desde el simulador no se puede realizar la ejecución del comando porque no hay un servidor DNS.

Práctica Nº 8

Descubrimiento de vecinos: Protocolo CDP

8. Práctica Nº 8: Descubrimiento de vecinos: Protocolo CDP.



Nombre del router	Dirección FA 0/0	Dirección S0	Tipo de interfaz S0	Dirección S1	Tipo de interfaz S1
GAD	192.168.14.1/24	192.168.15.1/24	DCE	192.168.17.1/24	DCE
BHM	192.168.16.1/24	192.168.15.2/24	DTE	192.168.18.2/24	DTE
BMG	192.168.19.1/24	192.168.17.2/24	DTE	192.168.18.1/24	DCE

Nombre del router	Contraseña enable	Contraseña console 0 / vty 0 4
GAD	Clase	cisco
BHM	Clase	cisco
BMG	Clase	cisco

Nombre del Host	Dirección IP	Máscara de subred	Gateway
PC_1	192.168.14.2	255.255.255.0	192.168.14.1
PC_2	192.168.16.2	255.255.255.0	192.168.16.1
PC_3	192.168.19.2	255.255.255.0	192.168.19.1

Objetivos

- Usar el CDP para obtener información acerca de las redes y dispositivos vecinos.
- Mostrar información acerca de la forma en que esta configurado el CDP para su publicación y la transmisión de tramas de descubrimiento.
- Mostrar las actualizaciones CDP que se reciben en el router local.

Introducción

CDP detecta y muestra información acerca de dispositivos de Cisco directamente conectados, incluyendo los routers y switches. CDP es un protocolo propietario de Cisco que se ejecuta en la capa de enlace de datos del modelo OSI. La capa de enlace de datos es la Capa 2 del modelo OSI. Esto permite que los dispositivos, que pueden estar ejecutando distintos protocolos de red de capa 3 como IP o IPT, aprendan acerca de la existencia del otro. CDP se inicia automáticamente cuando arranca un dispositivo del sistema y sólo los vecinos directamente conectados intercambian información.

En esta práctica, con la utilización del CDP, se pretende que el estudiante pueda deducir cómo es la topología de la red basándose en la información reunida mientras navega por la red utilizando los comandos IOS. Mediante el uso de estos comandos, se podrán visualizar cuales son las interfaces que están activas, cuales son los dispositivos a los que el router esta conectado y de que forma el usuario puede llegar allí. Con la información obtenida a través de los comandos show, debe poder acceder de forma remota a los routers vecinos (utilizando telnet) y a través del uso de los comandos de diagnostico de fallas (ping y tracert) debe ser capaz de visualizar cuales son los dispositivos que están conectados.

Requerimientos

Tres router de la serie 2620
Tres PC
Un switch de la serie 2950
Simulador Boson Netsim v.6

8.1. Iniciar sesión en el Router GAD

8.1.1. ¿Por qué es necesario iniciar una sesión en el Router GAD para poder ver todos los dispositivos (routers y switches) en la red que aparece anteriormente?

8.2. Configuración básica de los routers

8.2.1. Configure los routers de acuerdo con la información que aparece en la tabla anterior para que el CDP pueda recopilar información acerca e ellos. Consulte prácticas de laboratorio anteriores sobre la configuración de interfaces seriales y Ethernet y los cambios de configuraciones si necesita ayuda.

8.2.2. ¿Cuál es la velocidad del reloj que se debe establecer y en que interfaz se debe establecer?

8.2.3. ¿Por qué es necesario utilizar el comando **no shutdown** en todas las interfaces?
Es necesario para poder activar las interfaces.

Nota: No use el comando **no shutdown** en ninguna de las interfaces del router en este momento.

8.3. Recopilar información sobre las interfaces del router GAD

8.3.1. Introduzca el comando **show interface** en la petición de entrada del router EXEC usuario o EXEC privilegiado.

Anote la siguiente información acerca del router:

8.3.2. Indique el estado operativo de cada interfaz:

Interfaz	**¿La interfaz esta activa o desactivada? (Señal de detección de portadora)**	**¿El protocolo de línea esta activado/desactivado? (Se reciben mensajes de actividad)**

8.4. Activar las interfaces en el Router GAD

8.5. Recopilar información sobre las interfaces del router GAD

8.5.1. Introduzca el comando **show interface** en la petición de entrada del router EXEC usuario o EXEC privilegiado.

Anote la siguiente información acerca del router.

8.5.2. ¿Cuál es el nombre del router?

8.5.3. Indique el estado operativo de cada interfaz:

Interfaz	¿La interfaz esta activa o desactivada? (Señal de detección de portadora)	¿El protocolo de línea esta activado/desactivado? (Se reciben mensajes de actividad)

8.6. Mostrar los valores de los temporizadores del CDP, el estado de la interfaz y el encapsulamiento utilizado en el router GAD

8.6.1. Introduzca el comando **`show cdp interface`** en la petición de entrada del router.

8.6.2. ¿Con qué frecuencia envía el router paquetes CDP?

8.6.3. ¿Cuál es el valor del tiempo de espera?

8.6.4. La configuración global del CDP se puede ver usando el comando **`show cdp`** por si solo.

8.6.5. ¿Qué información no aparece en el comando **`show cdp`**?

8.7. Mostrar las actualizaciones CDP que se reciben en el router local

8.7.1. Introduzca el comando **`show cdp neighbors`** en el indicador del router. El router muestra información acerca de los vecinos que tienen habilitado CDP.

8.7.2. Complete la siguiente tabla

Dispositivo e identificador de puerto	Interfaz local	Tiempo de espera	Capacidad	Plataforma

8.8. Activar las interfaces en los routers BHM y BMG

8.8.1. Introduzca el comando **no shutdown** en las interfaces de los routers. Ubíquese en GAD. Observe que ahora los routers aparecen en la pantalla del comando **show cdp neighbor.**

8.8.2. Complete la siguiente tabla:

Dispositivo e identificador de puerto	**Interfaz local**	**Tiempo de espera**	**Capacidad**	**Plataforma**

8.9. Mostrar los detalles acerca de las actualizaciones CDP que se reciben en el router GAD

8.9.1. Introduzca el comando **show cdp neighbors detail** en el indicador del router. El router muestra la(s) dirección (direcciones) de entrada, la versión de IOS y la misma información que el comando **show cdp neighbors.**

8.9.2. Complete la siguiente tabla:

Información recopilada	**Dispositivo 1**	**Dispositivo 2**	**Dispositivo 3**
Nombre del dispositivo vecino			
Tipo del dispositivo vecino			
Direccion IP de la interfaz conectada a su router			
ID de puerto de su router al cual esta conectado el vecino			
ID del puerto del dispositivo vecino al que			

esta conectado su router			
Versión de IOS del router vecino			

8.10. Observar el tráfico de paquetes de CDP en GAD

8.10.1. Introduzca el comando **show cdp traffic** del indicador del router. ¿Cuál es el resultado?

8.11. Desde GAD conéctese vía Telnet al router vecino BHM

8.11.1. Introduzca el comando **show cdp neighbor** en el indicador del router remoto. El router muestra información acerca de los vecinos que tienen habilitado CDP.

8.11.2. Complete la siguiente tabla:

Dispositivo e identificador de puerto	**Interfaz local**	**Tiempo de espera**	**Capacidad**	**Plataforma**

8.12. Desde GAD conéctese vía Telnet al router vecino BMG

8.12.1. Introduzca el comando **show cdp neighbor** en el indicador del router remoto. El router muestra información acerca de los vecinos que tienen habilitado CDP.

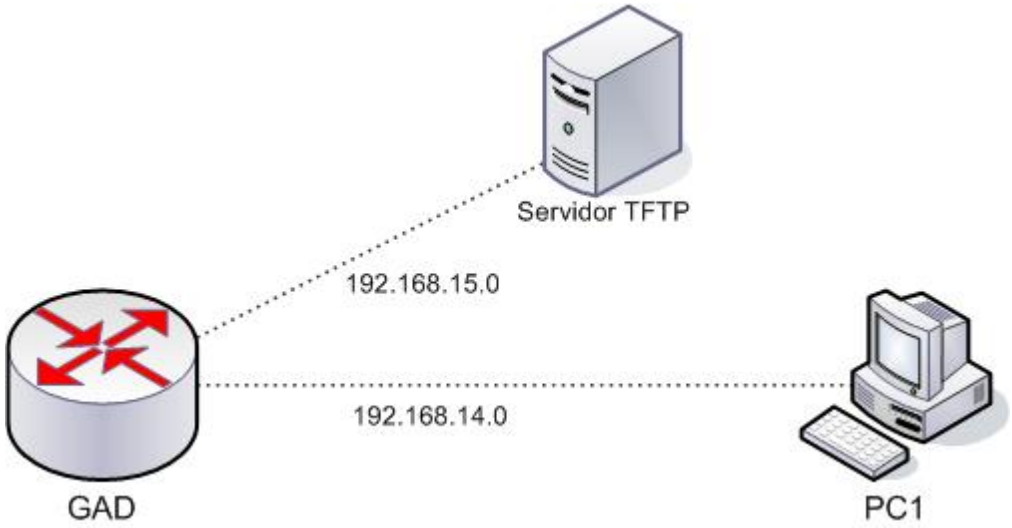
8.12.2. Complete la siguiente tabla:

Dispositivo e identificador de puerto	**Interfaz local**	**Tiempo de espera**	**Capacidad**	**Plataforma**

Práctica Nº 9

Verificación y respaldo del IOS.

9. Práctica Nº 9: Verificación y respaldo del IOS.



Nombre del router	Contraseña enable	Contraseña vty, Console 0	Interfaz Fastethernet 0/0	Interfaz Fastethernet 0/1	Máscara
GAD	gad	Gad	192.168.14.1	192.168.15.1	255.255.255.0

Objetivos

- Mostrar información acerca de la imagen activa del Software Cisco IOS.
- Verificar la cantidad de memoria RAM, Flash, NVRAM en el router.
- Verificar y documentar los ajustes del registro de configuración relacionados con el método de arranque.
- Realizar una copia del IOS de un router desde la FLASH a un servidor TFTP.

Introducción

En el momento en que se trabaja en la configuración de enrutadores pueden surgir varios problemas por lo que se recomienda que conozcas los detalles de la configuración del router y de su IOS, así como realizar un respaldo de ese Sistema Operativo en algún servidor TFTP al que el router tenga acceso. En la práctica se pretende que el estudiante aplique los conocimientos teóricos relacionados con el tema.

El estudiante podrá simular las situaciones en un simulador (Packet Tracer) como lo haría en una red física. Se deberá configurar un servidor TFTP en la red para respaldar la información. Estas acciones facilitarán al estudiante la resolución de problemas que se le puedan presentar en el área de trabajo.

Requerimientos

Un router de la serie 1811.
Una computadora conectada al router por una interfaz Fastethernet.
Un servidor configurado como TFTP.
Simulador Packet Tracer 4.0

Cree una red con el cableado similar a l del diagrama anterior para lo cual necesitará los requerimientos planteados anteriormente
Las características de la red serán las presentadas en la tabla.

9.1. Inicie una sesión en el router, entre en modo EXEC privilegiado para lo que deberá introducir la contraseña enable, y guarde la configuración activa como la configuración inicial del router.

LA configuración que estarás guardando es una configuración activa que esta en blanco.

9.2. Configure el router y visualice el archivo de la configuración activa.

9.2.1. Configure el router con la información de la tabla.

9.2.2. Introduzca el comando **`show running-config`** para mostrar la información del archivo de configuración actual.

9.3. Mostrar la información sobre la copia de respaldo del archivo de configuración.

9.3.1. Introduzca el comando **`show startup-config`** en la petición de entrada del router, la salida mostrará información sobre la copia de respaldo del archivo de configuración guardada en la NVRAM.

9.3.1.1. ¿Se muestra la información de la configuración que se acaba de introducir? ¿Si o No? ¿Por qué?

9.3.1.2. ¿Por qué es tan importante el archivo de configuración inicial?

9.4. Mostrar la información del Software Cisco IOS y otra información importante.

9.4.1. Introduzca el comando **`show versión`** en la petición de entrada de el router.

9.4.1.1. ¿Cuál es la versión del IOS y el nivel de revisión?

9.4.1.2. ¿Cuál es el nombre del archivo de la imagen del IOS?

9.4.1.3. ¿Desde dónde se arranco la imagen del router?

9.4.1.4. ¿Qué tipo de procesador y cuanta RAM tiene este router?

9.4.1.5. La copia de respaldo del archivo de configuración del router se guarda en la NVRAM. ¿Cuánta NVRAM tiene este router?

9.4.1.6. El sistema operativo se guarda en la FLASH. ¿Cuánta memoria FLASH tiene el router?

9.4.1.7. ¿Cuál es el valor del registro de configuración? ¿Cuál es el tipo de arranque que especifica este valor?

9.5. Mostrar información acerca del dispositivo de memoria FLASH.

9.5.1. Introduzca el comando **`show flash`** en la petición de entrada del router.

9.5.1.1. ¿Cuánta memoria flash esta disponible y cuanto se ha utilizado?

9.5.1.2. ¿Cuál es el archivo que se guarda en la memoria flash?
El archivo que esta guardado en la memoria FLASH es 13832032 c1841-ipbase-mz.123-14.T7.bin.

9.6. Especificar una secuencia de arranque de reserva.

9.6.1. Escriba el comando de configuración para especificar que la imagen de IOS se debe cargar desde:

- Memoria FLASH:
- Servidor TFTP:
  Memoria ROM:

9.6.2. ¿Cuál es el comando que se debe escribir a continuación para asegurarse que la próxima vez que se reinicie el router los comandos estén disponibles?

Si desea hacer un respaldo de la imagen del IOS en un servidor TFTP, deberá seguir los siguientes pasos.

Nota: Si hay un archivo en la flash, es probable que deba eliminarse antes de cargar uno nuevo. LA recuperación se lleva a cabo ejecutando el comando **`copy tftp flash`** para cargar una imagen respaldada en el servidor TFTP.

9.7. Inicie y configure el servidor TFTP. Para esto deberá investigar la configuración de servidores TFTP.

9.7.1. Haga ping al servidor desde el router GAD.

9.8. Copiar el IOS desde el servidor TFTP.

9.8.1. Antes de copiar los archivos debería de verificar los siguientes datos:

- Que el servidor TFTP este funcionando.
- Cuál es la dirección IP del servidor TFTP.
- Cuál es el nombre y la longitud de la imagen IOS almacenada en la FLASH.

9.8.2. Copiar la imagen IOS desde el servidor TFTP.

9.8.3. Desde la sesión de consola introduzca el comando **`copy tftp flash`** y complete las peticiones del proceso de acuerdo a la información recopilada. Después de iniciar el proceso deberás ver lo siguiente. No interrumpa el proceso.
!!!
!!!...........

9.8.4. Verificar la transferencia al servidor TFTP.

9.8.4.1. Verifique el archivo de registro del servidor TFTP, puede hacerlo observando las archivos en el servidor de TFTP.

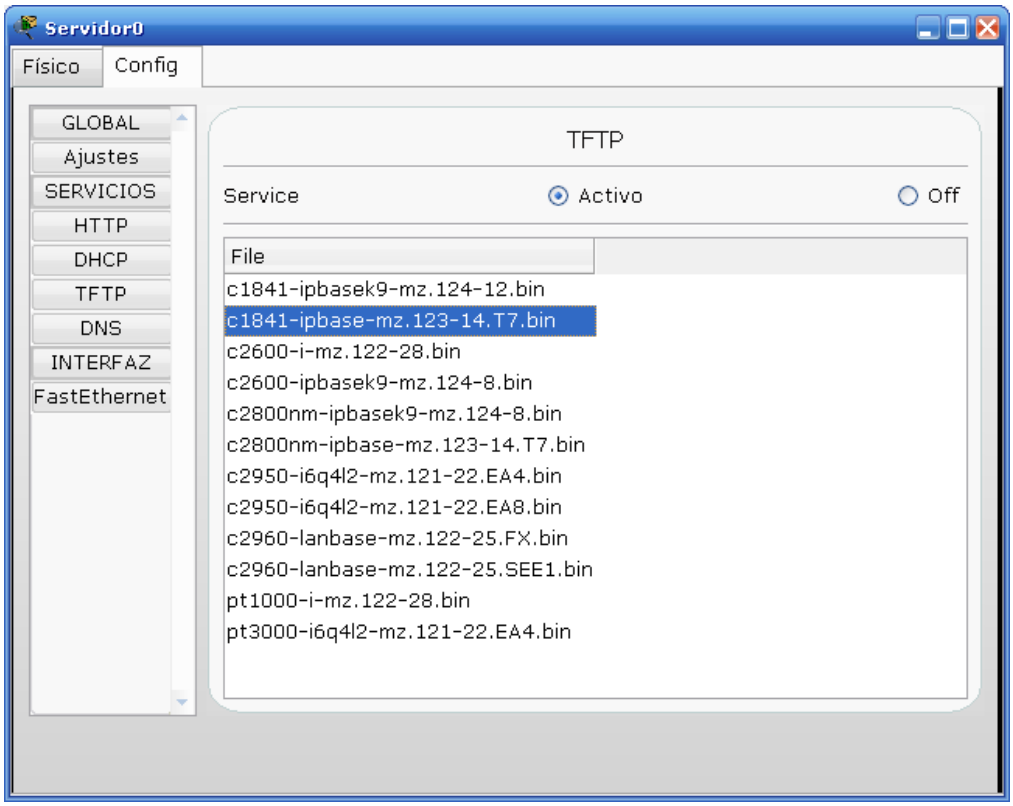


Figura 9.1. Muestra archivo de imagen del IOS en el servidor TFTP

9.8.4.2. Verifique el tamaño de la imagen FLASH en el directorio del servidor TFTP. El tamaño debe ser igual al mostrado en la información del comando **`show flash.`**

9.9. Copiar la configuración actual al servidor TFTP.

9.9.1. Realice la copia introduciendo la línea de comando **`copy running-config tftp`** y complete las peticiones del proceso.

9.9.2. Verifique que la copia de la configuración se ha realizado correctamente.

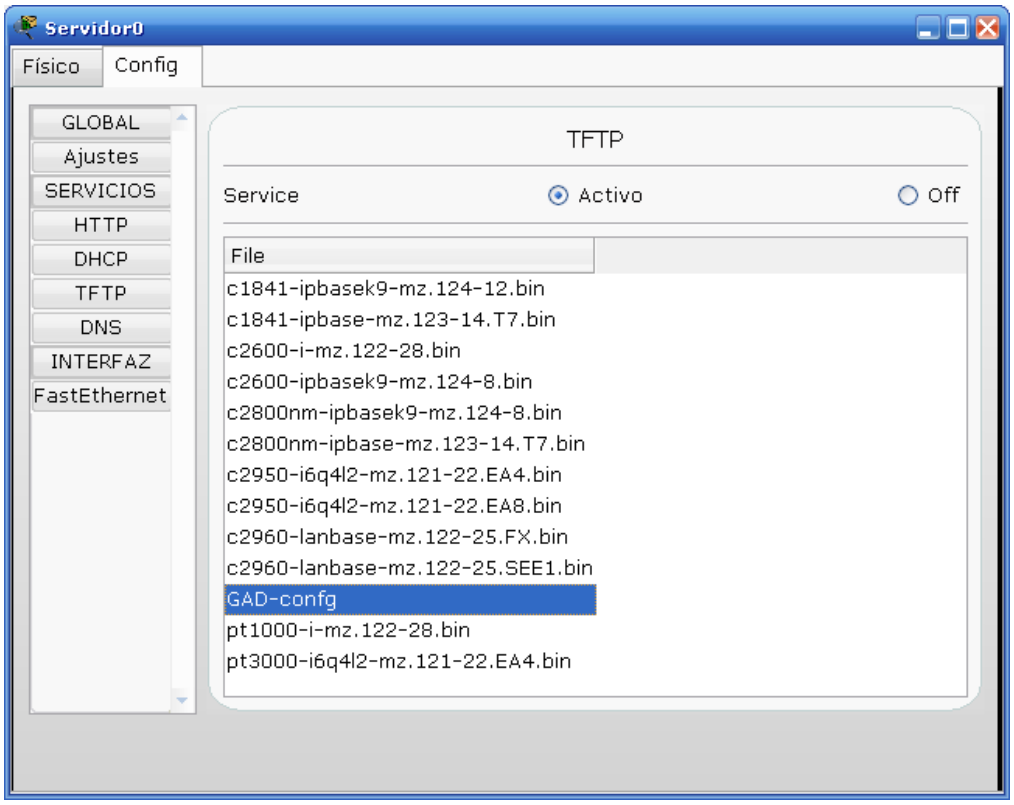
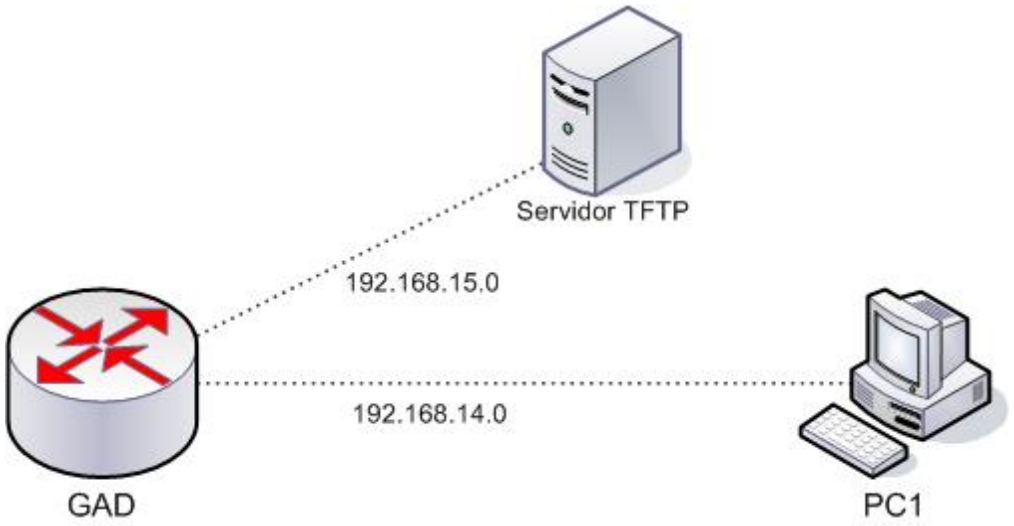


Figura 9.2. Muestra archivo de configuración actual guardado en el servidor TFTP.

Práctica Nº 10

Diagnóstico de fallas y recuperación de contraseñas.

10. Práctica Nº 10: Diagnóstico de fallas y recuperación de contraseñas



Nombre del router	Contraseña enable	Contraseña vty 0 4 , Console 0	Interfaz Fastethernet 0/0	Interfaz Fastethernet 0/1	Máscara
GAD	gad	gad	192.168.14.1	192.168.15.1	255.255.255.0

Objetivos

- Configurar el router para arrancar mediante el archivo de configuración de la NVRAM y recargar el router.
- Iniciar una sesión en el router cuya contraseña del modo privilegiado (enable) es desconocida.

Introducción

En la mayoría de los procesos de configuración de routers suelen suceder algunas fallas en la configuración que es importante detectar a tiempo para buscar una solución inmediata. También podría suceder que no recordaras la contraseña del router. En esta práctica se pretende que el estudiante tenga un claro conocimiento de como recuperarse después de una falla en el router, así como poder sobrescribir una contraseña y reiniciar el router normalmente.

Requerimientos

Un router de la serie 1811.
Una computadora conectada al router por una interfaz Fastethernet.
Un servidor configurado como TFTP.
Simulador Packet Tracer 4.0

Cree una red con el cableado similar a la de la imagen anterior para lo cual necesitará los requerimientos planteados anteriormente.
Las características de la red serán las presentadas en la tabla.

Existen formas para diagnosticar las fallas en el registro de arranque, para lo que le será útil realizar los pasos que siguen a continuación.

10.1. Debió haber configurado el nombre del router y las demás características del router, ahora introduzca los valores del registro de configuración (el valor a introducir será 0x2142).

10.2. Guarde la configuración activa como la configuración inicial. Utilizando el comando `copy running-config startup-config`.

10.3. Reinicie el router. Utilizando el comando `reload`.

Después de la recarga el router responderá de la siguiente manera:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:n
```

Escriba **n** y presione **Intro**.

10.4. Visualizar el archivo de configuración activa.

10.4.1. ¿Se muestra la configuración que se acaba de introducir? ¿Si o No? ¿Por qué?

10.5. Volver a cargar la configuración guardada. Para lo que deberá introducir en la petición de entrada del router la línea de comando copy `startup-config running-config.`

Ahora la tiene la configuración anterior, fue salvada desde la NVRAM.

10.6. Mostrar la información del Software IOS y otra información importante.

10.6.1. Introduzca el comando **`show version`** en la petición de entrada.

10.6.2. Examine con cuidado la salida del comando.

Nota: Una vez que se introduce el comando, observe que al final del resultado aparece un valor de registro de configuración de 0x2142. Este es el problema. Este valor de registro de configuración le indica al router que debe arrancar en el modo de recuperación de contraseña. Por este motivo, la configuración guardada en la NVRAM no aparece.

10.7. Cambiar el registro de configuración para arrancar desde la NVRAM, guardar y volver a cargar el router.

10.8. Verificar los valores del registro de configuración.

10.8.1. El router debió arrancar desde la NVRAM. Verifique esto introduciendo el comando **`show version.`**

En el caso que no recuerde la contraseña del router, deberá realizar los siguientes pasos para entrar y configurar una nueva contraseña.

10.9. Intente iniciar una sesión en un router en modo enable con una contraseña errónea, y anote los valores actuales de la configuración como el valor del registro de configuración.

10.10. Entrar al modo ROM Monitor.

10.10.1. Apague el router, espere unos segundos y vuelva a encenderlo cuando el router esta iniciando presione la tecla **`ctrl.`** y **`Pausa`** al mismo tiempo. Después de esto el router arrancará en modo ROM Monitor.

10.10.2. Cambiar los valores del registro para arrancar sin cargar el archivo de configuración.

10.10.2.1. Desde el modo de Monitor ROM, escriba **`confreg 0x2142`** para cambiar el registro de configuración.

10.10.3. Reiniciar el router.

10.10.3.1. Desde el modo de Monitor ROM, escriba **`reset`** o reinicie el router.

Debido a los nuevos valores de registro de configuración, el router no carga el archivo de configuración. El sistema pregunta:

Would you like to enter the initial configuration dialog [yes|no]
Introduzca **no** y presione **Intro**.

10.10.4. Entrar en modo EXEC privilegiado y cambiar la contraseña.

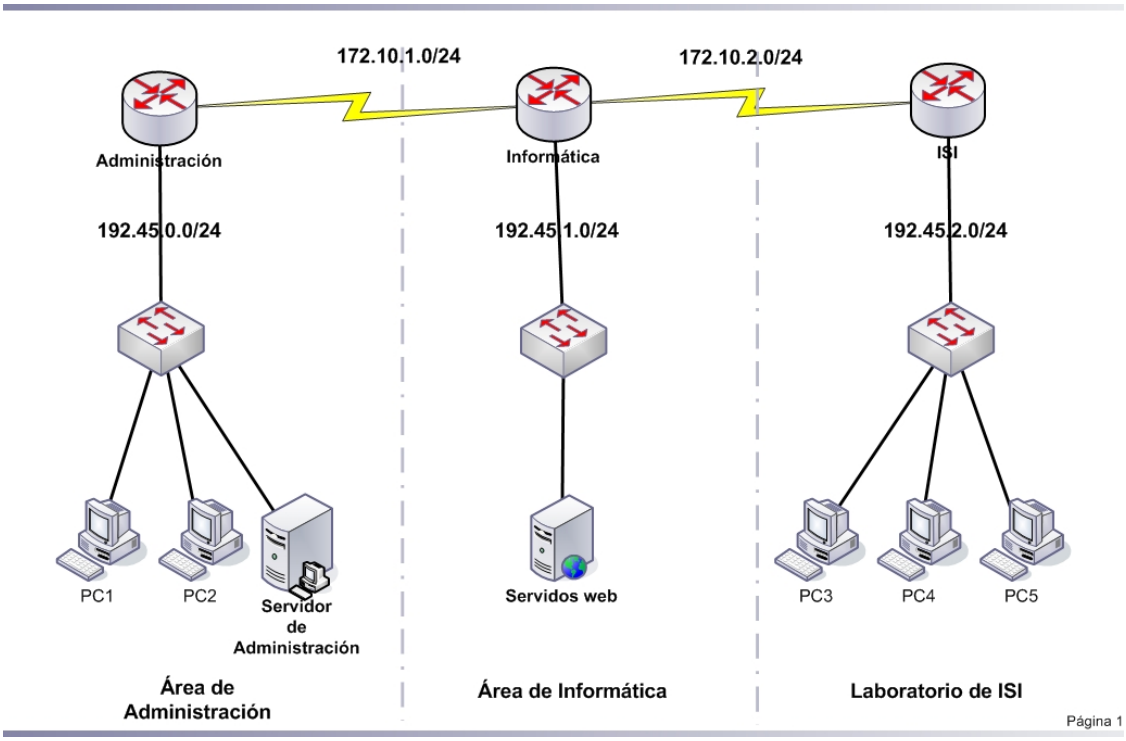
10.10.4.1. Ahora en la petición de entrada del router escriba enable y entre sin contraseña, use el comando **`copy startup-config running-config`** para restaurar la configuración existente como no esta en modo EXEC no necesita contraseña. En modo de configuración escriba **`enable secret`** **unan** para cambiar la contraseña secret.

10.10.4.2. Mientras se encuentra en modo de configuración global escriba **`confreg-register`** xxxxxxx, donde las x es el valor del registro de configuración original que tenia anteriormente, copie la configuración actual como configuración inicial para que sea la nueva configuración. Verifique que el nuevo registro de configuración sea 0x2142 con el comando **`show version`**. Teclee **`reload`** para reiniciar el router y compruebe que la contraseña debe ser **unan.**

Práctica Nº 11

ACL (Listas de Acceso)

11. Práctica Nº 11: ACL (Listas de Acceso).



Nombre del router	FastEthernet0/0	Serial 0/0/0	Serial 0/0/1
Administración	192.45.0.1/24	172.10.1.1/24	-
Informática	192.45.1.1/24	172.10.1.2/24	172.10.2.1/24
ISI	192.45.2.1/24	172.10.2.2/24	-

Servidores	FastEthernet0/0
Servidor de Administración	192.45.0.4/24
Servidor Web	192.45.1.2/24

Nombre de la PC	FastEthernet0/0
PC1	192.45.0.2/24
PC2	192.45.0.3/24
PC3	192.45.2.2/24
PC4	192.45.2.3/24
PC5	192.45.2.4/24

Objetivos

- Aprender a utilizar las ACLs nombradas estándar y extendidas.
- Comprender la importancia de la aplicación de ACL en una red.
- Entender el funcionamiento y utilización de la máscara willcard en las ACLs.

Introducción

En la esta práctica se le enseñara al alumno los diferentes tipos de ACL y la forma de aplicación según su tipo. También se verá la importancia de la máscara willcard en la aplicación de las ACLs.

Requerimientos

Tres routers Cisco de la serie 1841
Tres switches Cisco de la serie 2960
Dos servidores
Cinco computadores
Simulador Packet Tracer 4.0

11.1. Configuración de la red.

Configure cada una de las interfaces de la red de acuerdo a la información que se proporciona. Se deben configurar el servidor Web para que funcione como tal.
Primero desactive los servicios de HTTP, DNS, TFTP y DNS en el servidor de administración.

Cuando la PC hace la petición de la página index.html, envía un mensaje DNS y el Servidor Web esta funcionando como tal en la red, tiene que mandarle la dirección de la página que solicita. Para que esto ocurra introduzca el nombre de dominio “index.html” y la dirección IP donde se encuentra la página. Luego añádala.

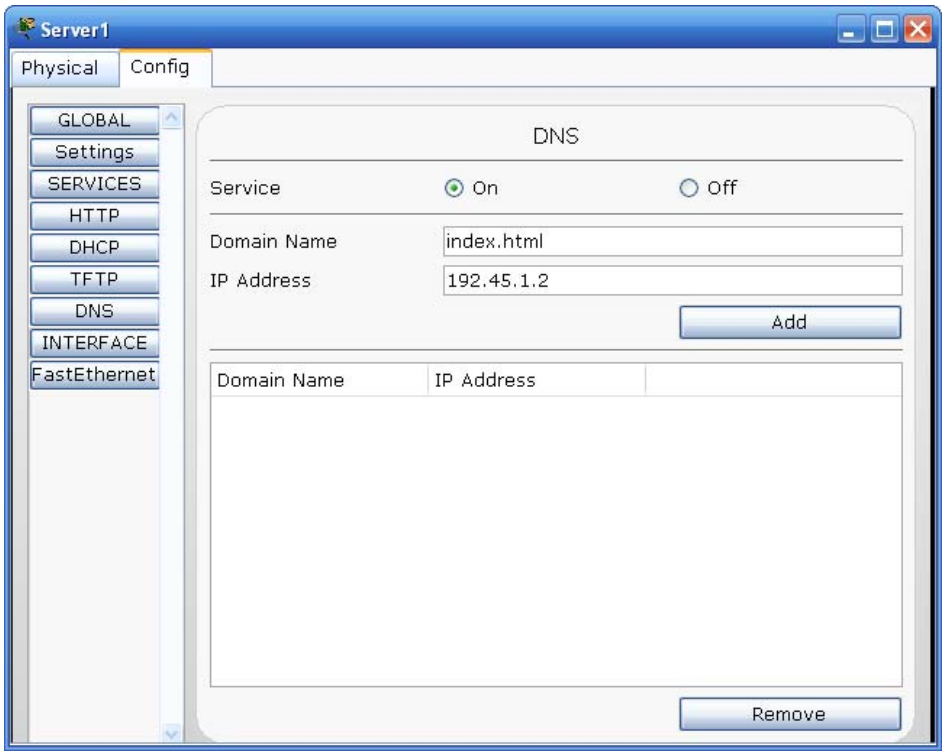


Figura 11.1. Configuración de un servidor DNS.

En cada PC indique la dirección del servidor DNS.

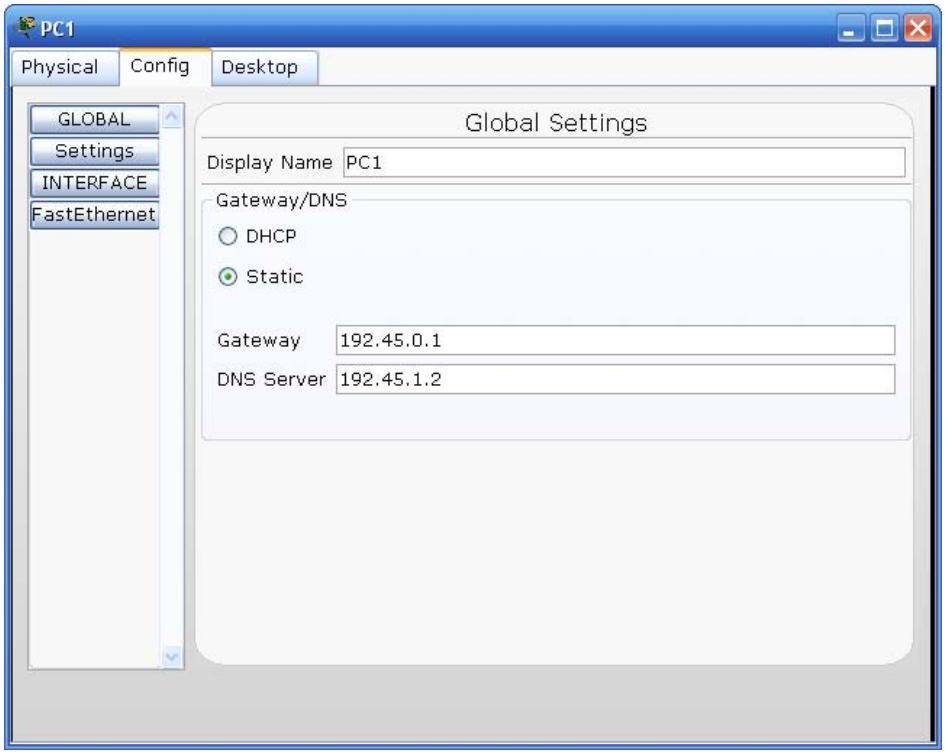


Figura 11.2. Configuración de un host para hacer solicitudes al servidor DNS.

Utilice el siguiente comando para indicar la dirección del servidor en uso **`ip name-server Dir Ip`** en cada router*.*

Pruebe desde una PC llamar a la página index.html. Para ello la PC tiene que funcionar como Web Browser, esta tiene que visualizarse en el explorador.

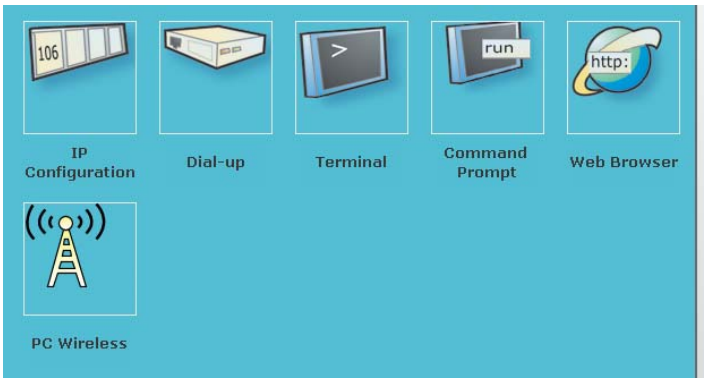


Figura 11.3. Opciones para trabajar en un host.

Esta es la página a visualizar.

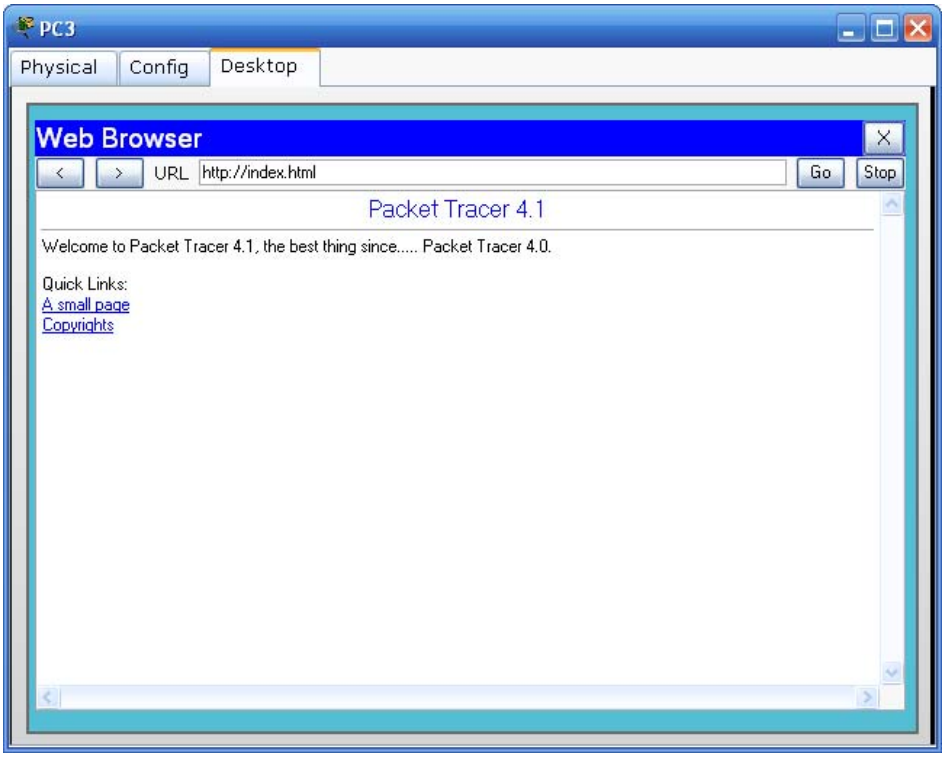


Figura 11.4. Visualización de la página index.html en un host.

11.2. Aplicación de ACL nombradas estándar.

11.2.1. Haga ping de la PC4 a la dirección 192.45.0.2 para probar la conectividad.

11.2.2. Algunos alumnos de la carrera de Ingeniería en Sistemas de Información han estado intentando acceder a la red del área de Administración, desde la red de ISI, en ella se encuentran todos los registros académicos de los alumnos. Evite que accedan a esta red. El nombre de la ACL es NO-ISI o utilice un número entre 1-99. ¿Qué ACL aplicó?

11.2.3. ¿Dónde aplicó la ACL? ¿Por qué? ¿Cómo entrada (in) o como salida (out)? ¿Por qué?

11.2.4. Vuelva hacer ping desde la PC4 a la dirección 192.45.0.2 ¿Funcionó? ¿Por qué? Verifique los resultados de la ejecución de la ACL en el panel de simulación del Packet Tracer 4.1, haga clic en una trama rechaza.

11.2.5. Haga ping de la PC1 a la dirección 192.45.2.2 ¿Funcionó? Justifique el resultado.

11.2.6. Se desea que sólo la PC3 tenga acceso a la red de Administración. Agregue la nueva ACL en NO_ISI. Anote todo el procedimiento y justifíquelo.

ACL aplicada:

Se borrara la ACL existente para volverla a editar ya que si se agrega la nueva restricción esta se agregara al final.

11.2.7. Haga ping de la PC3 y PC4 a la red 192.45.0.0. ¿Qué ocurrió? Explique.

11.3. Aplicación de ACL nombradas extendidas.

11.3.1. Haga telnet al router 172.10.2.1 desde la PC4. Realice la configuración correspondiente en los routers de Informática e ISI para que pueda realizarse el telnet.

Nota: Para que el telnet se realice correctamente se debe configurar las contraseñas de **consola**, **enable**, **enable secret** y **las líneas virtuales**.

11.3.2. Los administradores de la red se han dado cuenta que los alumnos han intentado entrar al router principal (el router de Informática). Es por ello que desean que la red 192.45.2.0 no tenga acceso a al router mediante telnet. El nombre de la ACL es NO_Telnet_ISI o el numero 101. ¿Qué ACL aplicó?

11.3.3. ¿Dónde se aplicó la ACL? ¿Por qué? ¿Cómo entrada o salida?

11.3.4. ¿Qué número de puerto uso? ¿Por qué?

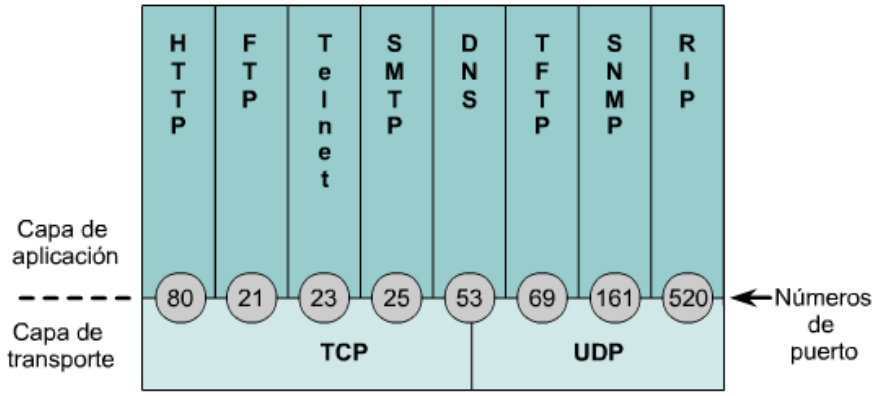


Figura 11.5. Asociación de los puertos y servicios de la capa de aplicación y de la capa de transporte.

11.3.5. Realice el telnet al router de Informática nuevamente, desde una PC de la red 192.45.2.0. Realice un ping. Explique los resultados.

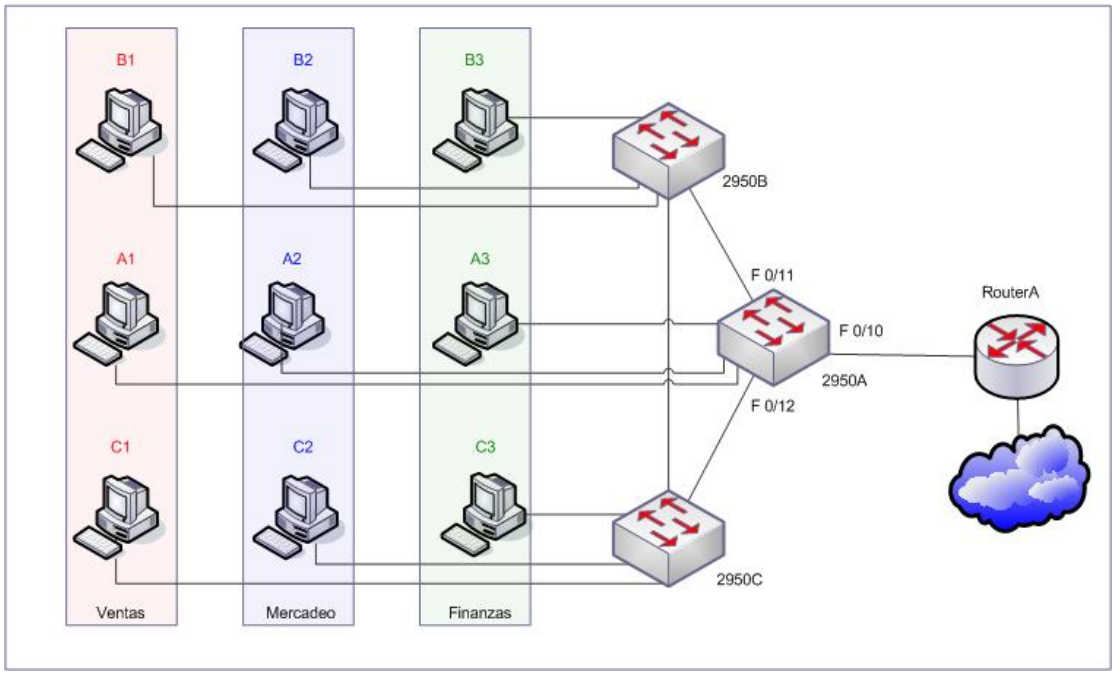
11.3.6. Se ha negado el acceso a Internet a la red de ISI, sólo la PC3 tiene acceso. Formule y aplique la ACL adecuada para lograrlo. Asegúrese que la red de Administración tenga acceso a los servicios al Servidor Web.

11.3.7. Haga la petición de la página index.html desde la PC3 y desde la PC5. ¿Qué ocurrió?

Práctica Nº 12

Configuración de VLAN

12. Práctica Nº 12: Configuración de VLAN.



Nombre el router	Dirección FA0/0	Contraseñas enable/aux	Contraseñas VTY, 4/Consola	Descripción	Banner
RouterA	192.168.100.1/24	class	cisco	Conexión LAN 100	Este es el router 2600A

Nombre Switch	Dirección VLAN 1	Contraseña Enable password	Contraseña Enable secret	Contraseña VTY 0 15 /consola 0	Gateway
Ventas	192.168.100.2/24	cisco	routersim	cisco	192.168.100.1
Mercadeo	192.168.100.3/24	cisco	routersim	cisco	192.168.100.1
Finanzas	192.168.100.4/24	cisco	routersim	cisco	192.168.100.1

Host	Dirección IP	Máscara de Subred	Gateway
A1	192.168.100.5	255.255.255.0	192.168.100.1
A2	192.168.100.6	255.255.255.0	192.168.100.1
A3	192.168.100.7	255.255.255.0	192.168.100.1
B1	192.168.100.8	255.255.255.0	192.168.100.1
B2	192.168.100.9	255.255.255.0	192.168.100.1
B3	192.168.100.10	255.255.255.0	192.168.100.1
C1	192.168.100.11	255.255.255.0	192.168.100.1
C2	192.168.100.12	255.255.255.0	192.168.100.1
C3	192.168.100.13	255.255.255.0	192.168.100.1

Objetivos

- Crear LANs virtuales diferentes en un mismo switch.
- Administrar un switch mediante consola con asignaciones IP y máscara de subred.
- Asignar puertos a las VLANs en conmutadores Cisco.

Introducción

En esta práctica se pretende que el estudiante aplique a la práctica todos los conocimientos teóricos que haya obtenido en el desarrollo del tema de las VLANs, su creación y configuración en los switches cisco.
La creación de VLANs es necesaria para dar seguridad a la red ya que brinda la facilidad para agrupar en VLANs los hosts de una red con el fin de que se creen restricciones de acceso entre hosts pertenecientes a VLANs diferentes.

Requerimientos

Para la realización de la práctica se tomarán los siguientes aspectos:

- Se trabajará con 3 Switches de la serie 2950, 1 Router de la serie 2600 y 9 Host.
- Se usarán los switches 2950s para la configuración de las VLANs y se usara el router 2600A para realizar el ruteo con ISL.
- Se crearán 3 VLANs y se aplicarán a los Switches 2950A, 2950B, y 2950C.
- La subred que se utilizará es 192.168.100.0/24.
- Simulador Packet Tracer v 4.0

12.1. Configurar el router 2600.

En el router 2600A, entre al modo de configuración global y configure el nombre de host tal como aparece en el cuadro. Entonces, configure las contraseñas de consola, de la terminal virtual y de enable. Configure la interfaz FastEthernet 0/0 cuya dirección IP será la 192.168.100.1/24 y su descripción. Luego habilite la interfaz y guarde la configuración.

12.2. En el Switch 2950A, entre al modo de configuración global y configure el nombre del host, y las contraseñas tal como aparece en el cuadro. Configure la interfaz VLAN 1 cuya dirección IP será la 192.168.100.2/24 junto con su descripción, con un Gateway por defecto de 192.168.100.1. Entonces, configure en las FastEthernet 0/10, FastEthernet 0/11, FastEthernet 0/12 su descripción que será notificar el enlace a la red a la que pertenece.

Cuando la configuración este completa, verifique la configuración haciendo ping al gateway por defecto.

12.2.1. ¿Por qué la VLAN 1 no fue creada antes de configurar su dirección IP?

12.2.2. ¿Por qué se configura para **switchport mode trunk** en cada una de las interfaces del switch?

12.2.3. ¿Por qué se configura **speed 100** en cada una de las interfaces?

12.2.4. ¿Por qué se configura **duplex full** en cada una de las interfaces?

12.2.5. Crear un dominio VTP routersim y establezca al Switch 2950 como un servidor VTP.

12.2.5.1. ¿Por qué fue configurado el switch Ventas como VTP Domain?

12.3. En el Switch 2950B, entre al modo de configuración global y configure el nombre del host, y las contraseñas tal como aparece en el cuadro. Configure la interfaz VLAN 1 cuya dirección IP será la 192.168.100.3/24 junto con su descripción, con un Gateway por defecto de 192.168.100.1. Entonces, configure en las FastEthernet 0/11, FastEthernet 0/12 su descripción.

Cuando la configuración este completa, verifique la configuración haciendo ping al gateway por defecto.

12.3.1. Configure el switch 2950B para que sea miembro de el dominio VTP routersim.

12.3.2. Configure el switch 2950B como un cliente VTP.

12.3.2.1. ¿Por qué el switch Mercadeo fue configurado como Cliente?

12.4. En el Switch 2950C, entre al modo de configuración global y configure el nombre del host, y las contraseñas tal como aparece en el cuadro. Configure la interfaz VLAN 1 cuya dirección IP será la 192.168.100.4/24, con su descripción, y con un Gateway por defecto de 192.168.100.1. Entonces, configure en las FastEthernet 0/11, FastEthernet 0/12 su descripción.

Cuando la configuración este completa, verifíquela haciendo ping al gateway por defecto.

12.4.1. Configure el switch 2950C para que sea miembro de el dominio VTP routersim.

12.4.2. Configure el switch 2950C como un cliente VTP.

12.4.3. ¿Por qué el switch Finanzas no es configurado como VTP Domain y por qué fue configurado igual que el switch Mercadeo?

12.5. Crear tres VLANs en el switch 2950A llamadas Ventas, Mercadeo y Finanzas.

Nota: La VLAN 1 es configurada por defecto en todos los switches y no podrá ser modificada o borrada. Las VLANs se crearán usando las VLAN 2, VLAN 3 y VLAN 4.

12.5.1. Ir al switch 2950B, entre al modo EXEC Privilegiado y con show VLAN verifique la información de la VLAN que ha sido propagada con VTP.

12.5.2. Ir al switch 2950C, entre al modo EXEC Privilegiado y con show VLAN verifique la información de la VLAN que ha sido propagada con VTP.

12.5.3. ¿Si las VLANs fueron creadas en el switch Ventas por qué los demás switches conocen su existencia?

12.6. Los Host A1, B1 y C1 estarán en la VLAN 2(Ventas), con la dirección de subred de 192.168.100.0/24.

El HostA1 tendrá la dirección 192.168.100.5.
El HostB1 tendrá la dirección 192.168.100.8.
El HostC1 tendrá la dirección 192.168.100.11.
El Gateway por defecto tendrá la dirección 192.168.100.1

12.6.1. Conectarse al switch 2950A y establecer al puerto f0/1 como miembro de la VLAN 2.

12.6.2. Conectarse al switch 2950B y establecer al puerto f0/1 como miembro de la VLAN 2.

12.6.3. Conectarse al switch 2950C y establecer al puerto f0/1 como miembro de la VLAN 2.

12.6.4. ¿Qué significa el comando **`switchport access vlan #`** en la configuración de la interfaces?

12.6.5. Verificar que la VLAN 2 se ha establecido correctamente, haciendo ping del HostA1 al HostB1 y viceversa.

12.7. Los Host A2, B2 y C2 estarán en la VLAN 3(Mercadeo), con la dirección de subred de 192.168.100.0/24.

El HostA2 tendrá la dirección 192.168.100.6.
El HostB2 tendrá la dirección 192.168.100.9.
El HostC2 tendrá la dirección 192.168.100.12.
El Gateway por defecto tendrá la dirección 192.168.100.1

12.7.1. Conectarse al switch 2950A y establecer al puerto f0/2 como miembro de la VLAN 3.

12.7.2. Conectarse al switch 2950B y establecer al puerto f0/2 como miembro de la VLAN 3.

12.7.3. Conectarse al switch 2950C y establecer al puerto f0/2 como miembro de la VLAN 3.

12.7.4. Verificar que la VLAN 3 se ha establecido correctamente, haciendo ping del Host A2 al HostB2 y HostC2

12.8. Los Host A3, B3 y C3 estarán en la VLAN 4(Finanzas), con la dirección de subred de 192.168.100.0/24.

El HostA3 tendrá la dirección 192.168.100.7.
El HostB3 tendrá la dirección 192.168.100.10.
El HostC3 tendrá la dirección 192.168.100.13.
El Gateway por defecto tendrá la dirección 192.168.100.1

12.8.1. Conectarse al switch 2950A y establecer al puerto f0/3 como miembro de la VLAN 4.

12.8.2. Conectarse al switch 2950B y establecer al puerto f0/3 como miembro de la VLAN 4.

12.8.3. Conectarse al switch 2950C y establecer al puerto f0/3 como miembro de la VLAN 4.

12.8.4. Verificar que la VLAN 4 se ha establecido correctamente, haciendo ping del HostA3 al HostB3 y HostC3.

12.9. Compruebe que las restricciones entre las VLANs funcionan haciendo ping desde el host A1 de la VLAN 2 al host B2 de la VLAN 3

12.9.1. ¿Funcionó el ping? ¿Si o No? ¿Por qué?

12.10. Elimine al host B1 de la VLAN 2.

Utilice el comando **`show running-config`** para verificar los cambios**.**

12.10.1. ¿Puede decir dónde se encuentra ahora el host que fue eliminado de la VLAN 2?

12.11. Asignar el host eliminado de la VLAN 2 a otra VLAN.

Se creará una nueva VLAN para asignarle el host que ha sido eliminado de la VLAN 2

12.12. Aplicar seguridad al puerto 0/1 del servidor VTP.

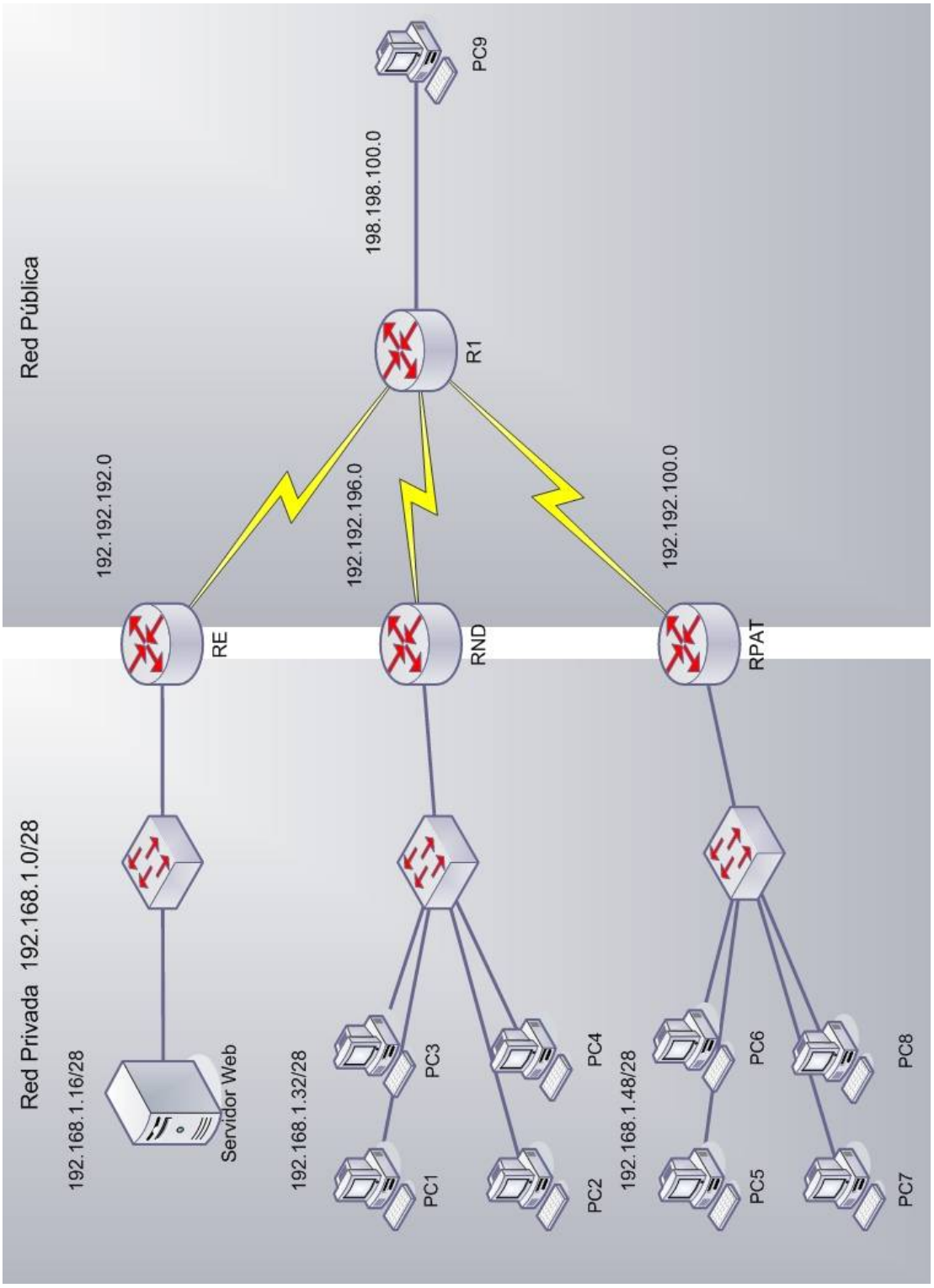
12.12.1. ¿Por qué es recomendable utilizar la seguridad en el Puerto?
El comando **`switchport port-security`** permite asociar la primera dirección MAC a dicho puerto.

12.13. Ejecute el comando show `vlan status` y analice la información que muestra.

Práctica Nº 13

NAT –Network Address Translation-

13. Práctica Nº 13: NAT –Network Address Translation.



Nombre del Router	Dirección FA0/0	Dirección S0	Tipo de interfaz S0 DTE/DCE	Contraseña enable	Contraseña console/vty 0 4
RNE	192.168.1.17/28	192.192.192.1/29	DCE	class	cisco
RND	192.168.1.33/28	192.192.196.1/29	DCE	class	cisco
RPAT	192.168.1.49/28	192.192.100.1/29	DCE	class	cisco
R1	198.198.100.1/26	192.192.192.3/29	DTE	class	cisco

Nombre del Router	Dirección S1	Tipo de interfaz S1 DTE/DCE	Dirección S2	Tipo de interfaz S2 DTE/DCE
RNE	-	-	-	-
RND	-	-	-	-
RPAT	-	-	-	-
R1	192.192.196.5/29	DTE	192.192.100.2/29	DTE

Nombre del Host	Dirección IP	Máscara de subred	Gateway
Servidor Email	192.168.1.18	255.255.255.240	192.168.1.17
Host 1	192.168.1.34	255.255.255.240	192.168.1.33
Host 2	192.168.1.35	255.255.255.240	192.168.1.33
Host 3	192.168.1.36	255.255.255.240	192.168.1.33
Host 4	192.168.1.37	255.255.255.240	192.168.1.33
Host 5	192.168.1.50	255.255.255.240	192.168.1.49
Host 6	192.168.1.51	255.255.255.240	192.168.1.49
Host 7	192.168.1.52	255.255.255.240	192.168.1.49
Host 8	192.168.1.53	255.255.255.240	192.168.1.49
Host 9	198.198.100.2	255.255.255.192	198.198.100.1

Sub-Redes	Tipos de NAT	Direcciones IPs públicas asignadas
192.168.1.16/28	NAT ESTATICO	192.192.192.2/29
192.168.1.32/28	NAT DINAMICO	192.192.196.2/29 - 192.192.196.4/29
192.168.1.48/28	NAT-PAT	192.192.100.1/29

Objetivos.

- Configurar de NAT Estático.
- Configurar de NAT Dinámico.
- Configurar de NAT/PAT.

Introducción.

En esta práctica se pretende que el estudiante aplique todos los conocimientos teóricos que haya obtenido en el desarrollo del tema, su configuración y funcionamiento.
El estudiante tendrá la posibilidad de simular el funcionamiento de una red física en la cual se podrán configurar tres tipos de NAT (Estática, Dinámica y PAT), utilizando simuladores, en este caso Bosson NetSim y Packet Tracer.

La configuración de NAT es necesaria por ser una alternativa ante la escasez de direcciones IP. NAT permite acceder a Internet traduciendo las direcciones privadas en direcciones IP registradas (públicas). Incrementa la seguridad y la privacidad de la red local al traducir el direccionamiento interno a uno externo.

Requerimientos.

Cuatro router Cisco 2811.
Tres switches Cisco 2960.
Nueve PCs.
Un servidor de Correo.
Direcciones IP públicas asignadas por el ISP.
Simulador Packet Tracert

13.1. Configurar el nombre y las contraseñas en los routers.

13.1.1. En los routers RNE, RND, RPAT y R1, entre al modo de configuración global y configure el nombre del router tal como aparece en el cuadro. Configure las contraseñas de consola, de Terminal virtual y enable y las interfaces de acuerdo al diagrama.

13.1.2. Configure el protocolo de enrutamiento RIP.

13.1.3. Compruebe la conectividad de la red privada y pública haciendo **ping.**

13.2. Configuración de NAT Estático en la subred 192.168.1.16/28.

Especifique el mapeo estático para que los clientes externos puedan acceder al servidor de Correo Electrónico interno.

13.2.1. Especifique la interfaz interna y marcarla como conectada al interior.

13.2.2. Especifique la interfaz externa y marcarla como conectada al exterior.

13.2.3. Ejecute el comando **show running-config** para verificar la configuración de NAT.

13.2.4. Utilice los comandos **show ip nat statics** para mostrar las estadísticas de NAT.

13.2.5. Muestre las traducciones de NAT activas con el comando **show ip nat traslations.**

13.3. Configuración de NAT Dinámico, en la subred 192.168.1.32/28.

13.3.1. Crear un pool con el rango de direcciones publicas que nos da el ISP y le damos un nombre (en este caso RANGO _ DINÁMICO).

13.3.2. Crear una lista de acceso estándar para hacer un filtro de las IPs privadas que podrán asignarse a las públicas.

13.3.3. Configurar la NAT Dinámica basada en la dirección de origen, asignando el rango de IPs privadas que filtramos con la access-list con el rango de IP pública del pool RANGO _ DINÁMICO.

13.3.2. Especifique la interfaz interna y marcarla como conectada al interior.

13.3.4. Especifique la interfaz externa y marcarla como conectada al exterior.

13.3.5. Ejecute el comando **show running-config** para verificar la configuración de NAT.

13.3.6 Utilice los comandos **show ip nat statics** para mostrar las estadísticas de NAT.

13.3.7. Muestre las traducciones de NAT activas con el comando **show ip nat traslations.**

13.4. Configuración de NAT/PAT, Overload.

13.4.1. Definir una lista de acceso IP estándar que permita las direcciones locales internas que se deben traducir.

13.4.2. Asocie la lista de acceso, especificando la interfaz de salida.

13.4.3. Especifique la interfaz interna y marcarla como conectada al interior.

13.4.4. Especifique la interfaz externa y marcarla como conectada al exterior.

13.4.5. Ejecute el comando **show running-config** para verificar la configuración de NAT.

13.4.6. Utilice los comandos **show ip nat statics** para mostrar las estadísticas de NAT.

13.4.7. Muestre las traducciones de NAT activas con el comando **show ip nat traslations.**

Nota: La opción Overload habilita PAT, permite que todos los hosts se asignen a una sola IP, si no ponemos esta opción seria una asociación uno a uno.

13.5. Haga ping desde el PC8 192.168.1.53 al Servidor de Correo.

Muestre y analice los cambios presentados en las direcciones Ip_destino, Ip_origen de los paquetes en su trayectoria.

13.6. Haga ping desde la PC9 192.192.192.9 al servidor de Correo Electrónico.

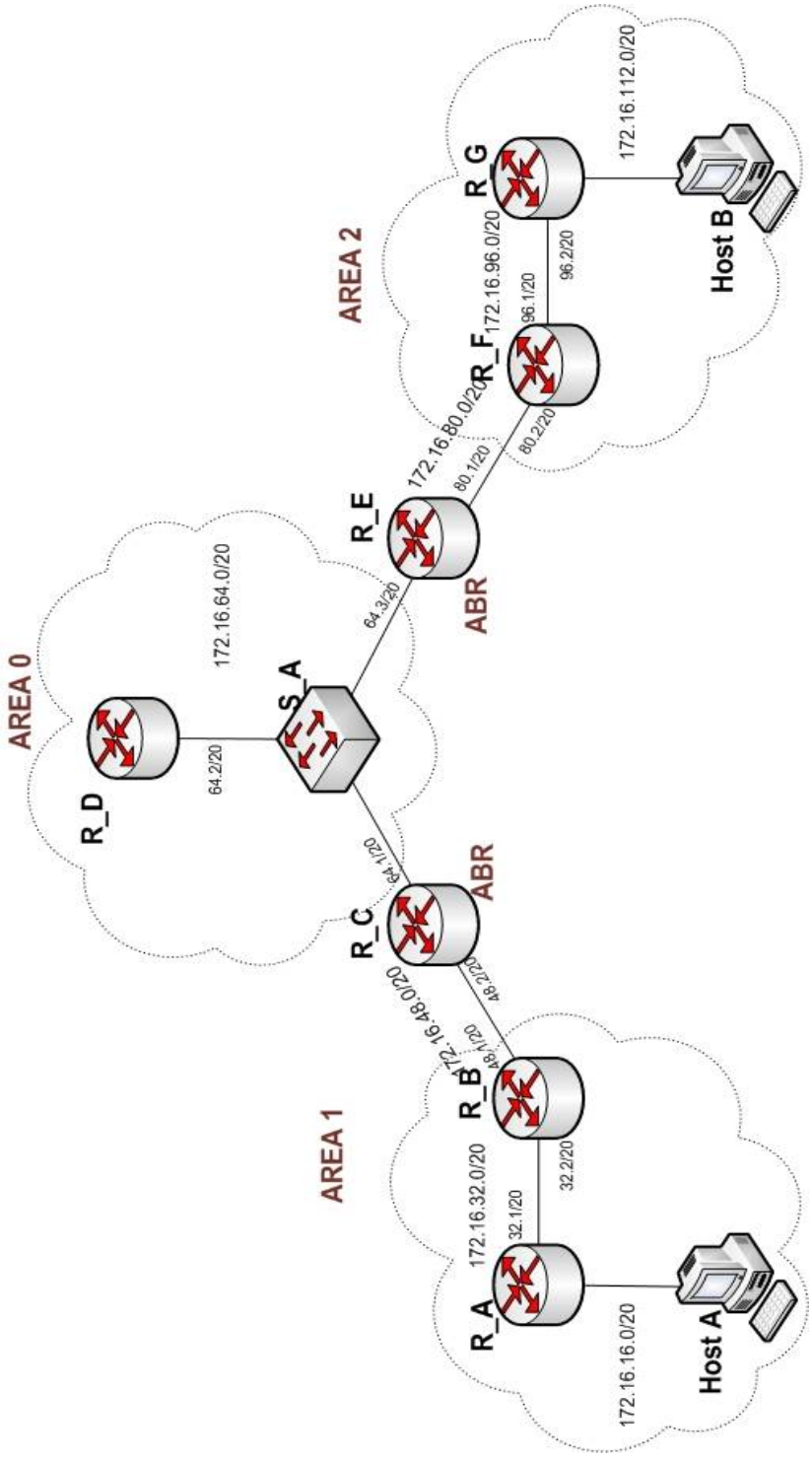
13.7. Utilice el comando show ip router en R1.

13.7.1 ¿Por qué en la tabla de enrutamiento no aparecen las redes 192.168.1.16, 192.168.1.32 y 192.168.1.48?

Práctica Nº 14

Protocolo de Enrutamiento: Configuración de OSPF

14. Práctica Nº 14: Protocolo de Enrutamiento: Configuración de OSPF.



Nombre del Router	Dirección FA0/0	Contraseña enable	Contraseña console/vty 0 4
R_A	172.16.16.1/20	class	cisco
R_B		class	cisco
R_C	172.16.64.1/20	class	cisco
R_D	172.16.64.2/20	class	cisco
R_E	172.16.64.3/20	class	cisco
R_F		class	cisco
R_G	172.16.112.1/20	class	cisco

Nombre del Router	Dirección S0	Tipo de interfaz S0 DTE/DCE	Dirección S1	Tipo de interfaz S1 DTE/DCE
R_A	172.16.32.1/20	DCE		
R_B	172.16.32.2/20	DTE	172.16.48.1/20	DCE
R_C	172.16.48.2/20	DTE		
R_D				
R_E	172.16.80.1/20	DTE		
R_F	172.16.96.1/20	DTE	172.16.80.2/20	DCE
R_G	172.16.96.2/20	DCE		

Nombre del Host	Dirección IP	Máscara de subred	Gateway
Host A	172.16.16.2	255.255.240.0	172.16.16.1
Host B	172.16.112.2	255.255.240.0	172.16.112.1

Objetivos

- Configurar OSPF como protocolo de enrutamiento.
- Determinar cuales vecinos OSPF están conectados a cuales interfaces locales.
- Verificar el funcionamiento del protocolo, probando la conectividad entre las áreas conectadas al Backbone.

Introducción

El Algoritmo OSPF (Open Shorest Path First), es un protocolo de enrutamiento de estado de enlace de gateway interior. Este algoritmo de estado de enlace lo que hace es mantener una base de datos que refleja la topológica de la red en los routers; es decir, el estado de los enlaces de la red. Un router periodicamente intercambia información de estado actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento. De esta manera, cada router dispone de un mapa topológico de la red entera.

Con la realización de esta práctica se pretende que el alumno adquiera los conocimientos prácticos sobre el protocolo de enrutamiento interno, OSPF. Con la implementación de

este protocolo se obtendrá información tanto de la Base de Datos topológica de la red como de las tablas de enrutamiento de rutas y puertos hacia cada red, por tanto el administrador del SA será capaz de monitorear la red ante cualquier fallo.
En esta práctica se utilizará la siguiente topología:

- Se creará un área 0 de backbone.
- Se crearán dos áreas (1 y 2) en la que se trabajara con una topología punto-a-punto.

Requerimientos

Siete router de la serie 2620
Dos PC
Un switch de la serie 2950
Simulador Boson Netsim v.6

14.1. Configurar el nombre y las contraseñas en los Routers

14.1.1. En los routes R_A, R_B, R_C, R_D, R_E, R_F y R_G, entre al modo de configuración global y configure el nombre de host tal como aparece en el cuadro. Entonces, configure las contraseñas de consola, de la terminal virtual y de enable. Configure las interfaces FastEthernet0/0, Serial0 y Serial1 en el router de acuerdo al diagrama. No habilitar las interfaces

14.2. Configurar el algoritmo de encaminamiento OSPF en las áreas

14.2.1. Configurar el algoritmo de encaminamiento OSPF en el área 0(router R_D)

14.2.2. Configurar el algoritmo de encaminamiento OSPF en el área 1(router R_A, R_B)

14.2.3. Configurar el algoritmo de encaminamiento OSPF en el área 2(router R_F, R_G)

14.2.4. Configurar el algoritmo de encaminamiento OSPF para los routers ABR(routers R_C y R_E)

14.2.5. Probar la conectividad entre las áreas que conectan los ABR, haciendo ping del HostA al HostB

14.3. Verificar el funcionamiento de OSPF en cada área

Para cada uno de los routers:

14.3.1. Mostrar el contenido de la Base de Datos topológica (show ip ospf database).

14.3.2. Mostrar la tabla de Enrutamiento (show ip route).

14.3.3. Listar información detallada acerca de los vecinos OSPF por cada interfaz (show ip ospf neighbor).

Responda las siguientes preguntas:

14.3.4. ¿Para qué se utiliza la Base de Datos Topológica?

14.3.5. ¿Qué significa el O y el O IA en la primera columna de las tablas de enrutamiento?

14.3.6. ¿Cuál es el valor de métrica para OSPF?

14.3.7. Analice la Base de Datos Topológica del router R_A y R_B del área 1. ¿Son iguales? ¿Si o no? ¿Por qué?

14.3.8. Analice la Base de Datos Topológica del router R_D del área 0 y del router R_F del área 2. ¿Son iguales? ¿Si o no? ¿Por qué?

14.3.9. ¿Qué información contiene **`Net Link States (Area 0)`** en el **`show ip ospf database`** de los routers que están conectados al área 0?

14.3.10. Compare las tablas de enrutamiento del router R_A y R_B del área 1¿Son diferentes? ¿Si o no? ¿Por qué?

14.4. Verificación de las métricas en OSPF

14.4.1. Calcular el coste de cada interfaz del router R_B con la formula 10^8/ancho de banda(bps)

14.4.2. Verificar los costes actuales con show ip ospf interface

14.5. Descubrimiento del DR (Router Designado) en las distintas áreas

14.5.1. Haga show ip ospf interface en cualquier router que conforme el área 0. ¿Cuál es el router que cumple la función de DR actualmente en esta área? ¿Por qué?

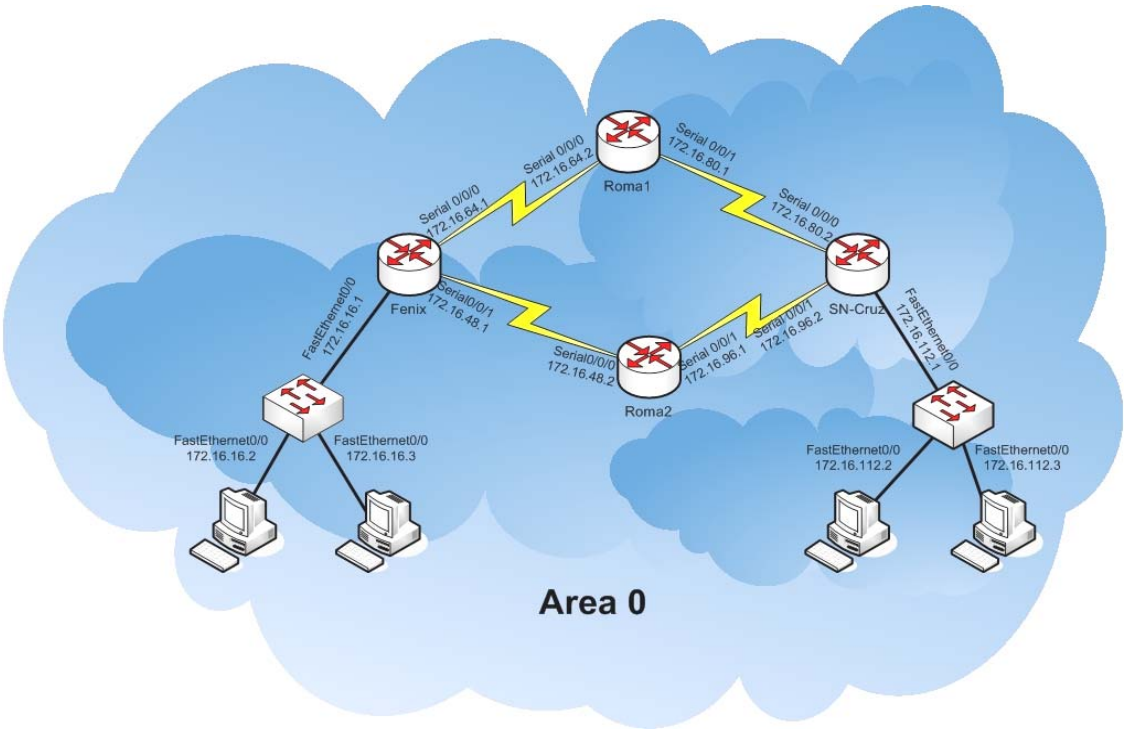
14.5.2. Haga **`show ip ospf interface`** en cualquier router que pertenezca al área 1 y área 2 para descubrir el DR.

14.5.3. ¿Existe un DR en el área 1 y área 2? ¿Si o no? ¿Por qué?

Práctica Nº 15

OSPF (Open Short-Path First)

15. Práctica Nº 15: OSPF (Open Short-Path First).



Información de Red.

Nombre del router	FastEthernet0/0	Serial 0/0/0	Serial 0/0/1
Fénix	172.16.16.1/20	172.16.64.1/20	172.16.48.1/20
Roma1	-	172.16.64.2/20	172.16.80.1/20
Roma2	-	172.16.48.2/20	172.16.96.1/20
Sn. Cruz	172.16.112.1/20	172.16.80.2/20	172.16.96.2/20
Nombre de la PC	**FastEthernet0/0**		
Pc-F1	172.16.16.2/20		
Pc-F2	172.16.16.3/20		
Pc-SC1	172.16.128.2/20		
Pc-SC2	172.16.128.3/20		

Objetivos

- Configurar un área implementando el protocolo de puerta interior OSPF en una sola área.
- Aplicar los conceptos más importantes relacionados al enrutamiento con OSPF dentro de un área.

Introducción

En esta práctica se pretende aplicar algunos conceptos del protocolo de enrutamiento de puerta interior (IGP) OSPF. En este caso no se aplicará OSPF en multiples áreas, lo haremos en una sola área. El alumno podrá ver el funcionamiento de OSPF,el concepto y elección de un router designado, la autenticación en OSPF y la temporización de OSPF dentro de una misma área esto ayudará al estudiante a tener una idea muy cercana al real funcionamiento del protocolo de enrutamiento OSPF.

Requerimientos

Cinco routers Cisco de la serie 2811
Dos switches Cisco de la serie 2960
Cuatro computadores
Simulador Packet tracer v4.0

Cree una red con la topologia similar a la del diagrama de red anterior para lo que necesitará los requerimientos especificados anteriormente y con las caracteristicas palnteadas en las tablas anteriores.

15.1. Configuración del protocolo de enrutamiento OSPF.

Antes de activar el proceso OSPF debe deshabilitar primero los protocolos EIGRP y IGRP, estos se encuentran habilitados por defecto, en cada uno de los routers. Los números de los procesos de OSPF son irrelevantes.

15.1.1. Configuración del Área 0 en cada router.

Configuración del Router Fénix.

Nota: la primera línea indica que se han de publicar todas las direcciones de la red 172.16.16.0, en la segunda y tercera línea solo se publica un bloque pequeño de la red, en el rango 0 a 3, esto es por que en ese enlace no se pueden agregar más router y solo se utilizaran estas dos direcciones.

15.1.2. ¿Hubo algún mensaje al terminar de configurar los procesos OSPF en cada router? ¿Qué significan?

15.2. Router Designado y Router Designado de Respaldo.

Active el Panel de Simulación en Packet Tracer, edite los filtros indicando que solo visualice los eventos OSPF. Haga doble clik a uno de los cuadros azules del panel de simulación, estos representan los paquetes OSPF que se están enviando por la red, conteste las siguientes preguntas.

15.2.1. ¿Por qué en la dirección destino del paquete IP tiene como dirección la 224.0.0.5?

15.2.2. Ejecute el comando **`show ip ospf interface`**. ¿Cuál es el DR en Fenix? ¿Tiene un BDR? Sino lo tiene ¿Por qué no tiene asignado uno?

15.2.3. ¿Cuál es el DR en SN-Cruz? ¿Tiene un BDR? Sino lo tiene ¿Por qué no tiene asignado uno?

15.2.4. ¿Por qué Fénix y SN-Cruz tienen DR diferente?

15.2.5. Roma 1 y Roma, ¿tienen DR? ¿Por qué no?

15.2.6. Agregue otro router (Parad). Este se conecta al router Fénix a través del switch, con una dirección 172.16.16.4. Configure el respectivo proceso OSPF en el router nuevo.

15.2.7. Utilice el comando **`show ip ospf interface`**. Indique el DR y el BDR, en el router Fénix.

15.2.8. ¿Por qué ahora si se muestra un BDR?

15.3. Modificación de las métricas de Costo OSPF.

Calcular los costos de las interfaces de SN-Cruz. Utilice la formula 10exp8 / BW. Utilice el comando **`show interfaces`** para ver el valor de banda ancha.

15.3.1. ¿Cuál es su valor por defecto de los costos? Utilice el comando **`show ip ospf interface`**

15.3.2. Hacer ping del router SN-Cruz al router Fénix a la interfaz 172.16.48.1. ¿Cuál es la ruta que sigue?

15.3.3. Agregue un enlace entre el router Roma1 y Roma2. Dirección de red: 172.16.32.0. Configure las interfaces y active los procesos de enrutamiento en las interfaces.

15.3.4. Vuelva a realizar el ping. ¿Cuál es el camino?

15.3.5. Modifique el costo de la interfaz serial 0/0/1 a 550. Vuelva hacer el ping, he indique el camino. En la tabla de enrutamiento puede verificar los caminos que tiene actualmente para el envío de la información. Utilice el comando **`show ip route`** para mostrar la tabla de enrutamiento y **`show ip ospf interface`** para comprobar el cambio del costo. Compare los resultados antes y después de haber cambiado el costo. Justifique los resultados.

15.4. Autentificación en OSPF.

15.4.1. Ejecutar los comandos **`show ip route, show ip ospf neighbor`** y probar hacer ping al router Parad.

15.4.2. Aplicar autentificación a la interfaz serial 0/0/0 del router Fénix.
ID: 123, contraseña: usuario

15.4.3. Permitir la autentificación en el área

15.4.4. ¿Qué tipo de encriptación se usa? ¿Para qué se utiliza?

15.4.5. Volver a ejecutar los comandos **`show ip route, show ip ospf neighbor`**, ¿Hubo algún cambio?

15.4.6. Haga el análisis necesario, y vuelva a ejecutar los comandos.

15.4.7. ¿Para qué se utiliza la autenticación?

15.5. Temporización OSPF.

15.5.1. ¿Cuáles son los valores de **`Hello-Interval`** y **`Dead-Interval`** en Roma2? ¿Para que son utilizados? Utilice el comando **`show ip ospf interface`** para verlos.

15.5.2. Ejecute el comando **`show ip ospf neighbor.`**

15.5.3. Ejecute el comando **`debug ip ospf events`** en el router Roma2

15.5.4. ¿Cada cuánto tiempo se ejecuta?

15.5.5. ¿De dónde provienen los mensajes?

15.5.6. Cambie el intervalo de tiempo Hello a 20 seg. Utilice los comandos **`ip ospf hello-interval`** # en la interfaz serial0/0/0.

15.5.7. Ejecute de nuevo el comando **`debug ip ospf events.`** Demuestre que el tiempo **`hello-interval`** ha cambiado. ¿Por qué en la ejecución del comando debug no se muestran los cambios en los intervalos de ejecución?

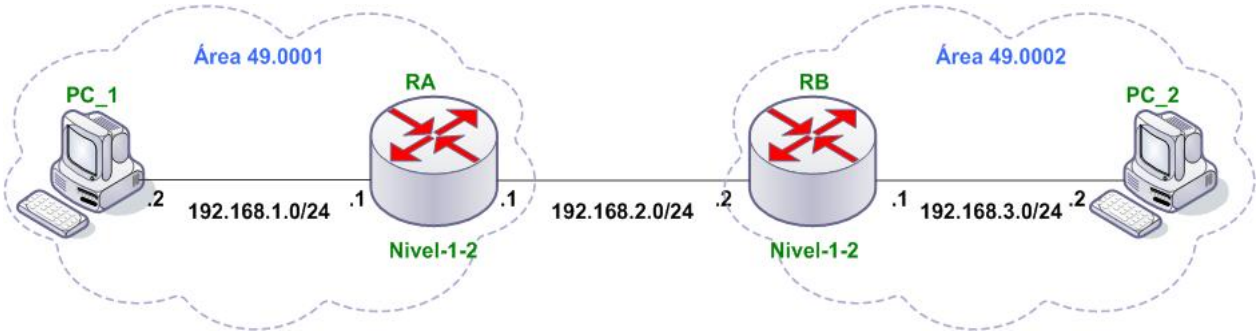
15.5.8. Vuelva a mostrar la tabla de vecinos. ¿Qué ha ocurrido?
Debido a que no se ha modificado el interval-hello en le router Fénix, esa interfaz esta caída y no tiene acceso a esa red (172.16.48.0).

15.5.9. Configure el interval-hello del router Fénix. Vuelva a mostrar la tabla de vecinos.

Práctica Nº 16

IS-IS
Integrated System- Integrated System

16. Práctica Nº 16: IS-IS (Integrated System-Integrated System).



Objetivos

- Estudiar el protocolo de enrutamiento IS-IS para los routers.
- Configurar el protocolo IS-IS Integrado en los routers.
- Analizar el funcionamiento de IS-IS Integrado.

Introducción

Se conocen hasta ahora varios protocolos de enrutamiento al que se les suma el protocolo de enrutamiento IS-IS de importancia relevante para facilitar el enrutamiento en redes agrupadas en áreas.
En esta práctica se pretende que el estudiante aplique a la práctica todos los conocimientos teóricos que haya obtenido en el desarrollo del tema de Enrutamiento IS-IS Integrado.

El estudiante tendrá la posibilidad de simular el funcionamiento del enrutamiento de una red física en la cual se podrá verificar las adyacencias y la trasferencia de mensajes entre áreas.

Requerimientos

Para la realización de la práctica se necesitaran los siguientes requerimientos:

Dos routers Cisco 1800-11(físicos).
Dos PCs conectadas a los routers.
Software HiperTerminal
Tres cables RJ45.

Construye una red con el cableado similar al del diagrama anterior, para los que será necesario que cuente con los requerimientos previamente planteados.
Las características de la red serán las mostradas en las tablas.

16.1. Definir el área y preparar un plan de direcciones ha ser usadas en los routers y determinar las interfaces que deberán correr con IS-IS.

16.2. Configurar el protocolo de enrutamiento IS-IS.

16.2.1. Habilite el ruteo IS-IS y especifique un proceso IS-IS para IP, para la cual entre en modo de configuración del router.

16.2.2. Configure NET para el proceso de ruteo.

16.3. Especificar y configurar los parámetros de las interfaces para el ruteo IS-IS de cada uno de los routers.

16.3.1. Entre en modo de configuración de la interfaz y especifique la interfaz que deberá ser activada para el ruteo IS-IS y habilite IS-IS Integrado para la interfaz especificada.

16.4. Configurar los Parámetros misceláneos en IS-IS

16.4.1. Especificar el tipo de Sistema.

16.5. Monitorear IS-IS.

Usted puede desplegar la Base de Datos del Estado de Enlace IS-IS en modo EXEC privilegiado.

16.5.1. Desplegar la Base de Datos del Estado de Enlace IS-IS.

16.5.2. Ver la tabla de vecinos.

16.5.3. Ver la tabla de enrutamiento del router.

16.6. DR o DR IS-IS (DIS).

16.6.1. ¿Cuál es el DR?

16.6.2. ¿Cuál es el BDR?

16.6.3. ¿Cómo se eligió el DR si ambos routers tiene la misma prioridad?

16.7. Cambio de las prioridades.

Cambie la prioridad de la interfaz fastethernet 1 del router RA a 32. Use el comando **`isis priority.`**

16.7.1. Verifique el cambio realizado
Con el comando **`show clns interface`** puedes verificar el cambio.

16.7.2. Se ha cambiado la prioridad de la interfaz fastethernet 1 del router RA a 32, después del cambio. ¿Quién es el DR? Para el Nivel 1 y para el Nivel 2.

16.8. Adyacencias

16.8.1. ¿Cuál es el número de adyacencias para el Nivel 1 y para el Nivel 2?

16.8.2. ¿Por qué no se han establecido adyacencias de Nivel 1?
Porque en el nivel 1 solo esta conectado a la red del host y no hay mas routers en el nivel 1.

16.9. CLNS

16.9.1. Verifique la configuración del protocolo CLNS, use el comando **`show clns.`**

16.9.2. Según la pila de protocolo ¿qué tipo de router es?

16.9.3. ¿Cuál es el valor timer? ¿Para qué se usa?

16.9.4. ¿Cuál es el valor Holding Timer? ¿Para qué se usa?

16.9.5. ¿Cuál es el valor Lifetimer? ¿Para qué se usa?

16.10. Sobrecarga del router.

16.10.1. Establecer el Bit OL a 1. Use el comando **`set-over-load-bit supress interlevel externa`**

16.10.2. Muestre la Base de Datos del Router A y justifique la salida.

16.10.4. Muestre la tabla de enrutamiento del RB antes y después de cambiar el Bit OL ¿Qué ha ocurrido?

16.10.4. Liste las razones por las que seria necesario que este bit se active.

16.11. Cambio de tipos

16.11.1. Cambie el router RA a tipo level 1.

16.11.2. Se ha establecido adyacencia con el router RB.

16.11.3. ¿Qué tipo de adyacencia estableció?. ¿Por que?

16.11.4. Muestre la base de datos del router RA. Justifique la salida.

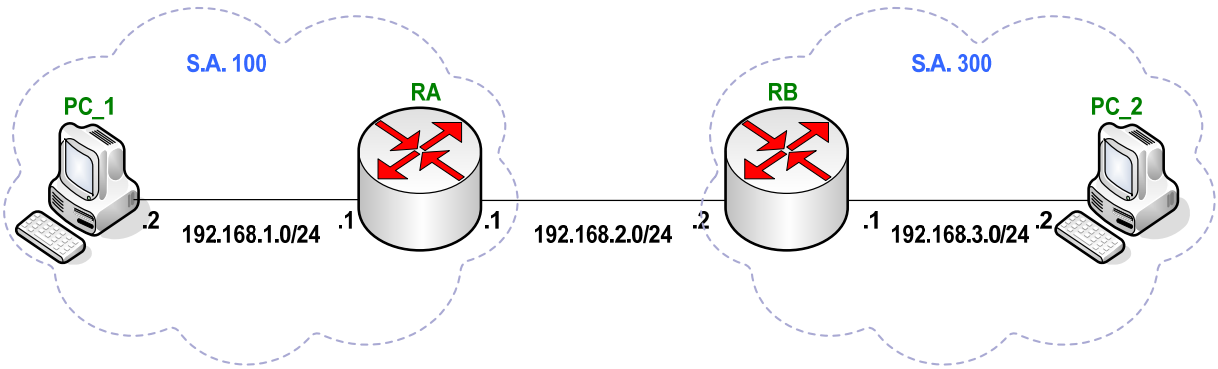
16.11.5. Muestre la tabla de enrutamiento para el router RB. Ha ocurrido algún cambio ¿Por que?

16.11.6. Haga ping de la PC al router RB.

Práctica Nº 17

PROTOCOLO DE ENRUTAMIENTO EXTERNO: BGP

17. Práctica Nº 17: Protocolo de enrutamiento externo: BGP.



Nombre del router	Dirección FA0/0	Dirección FA0/1	Enrut. Externo	Contraseña enable	Contraseña Console 0
RA	192.168.1.1/24	192.168.2.1/24	BGP	class	cisco
RB	192.168.3.1/24	192.168.2.2/24	BGP	class	cisco

Host	Dirección IP	Máscara de Subred	Gateway
PC_1	192.168.1.2	255.255.255.0	192.168.1.1
PC_2	192.168.3.2	255.255.255.0	192.168.3.1

Objetivos

- Configurar BGP como protocolo de enrutamiento externo.
- Verificar el funcionamiento del protocolo, probando la conectividad entre las áreas.

Introducción

Los protocolos de enrutamiento externo son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de enrutamiento externo la prioridad era buscar rutas óptimas atendiendo únicamente al criterio de minimizar la 'distancia' medida en términos de la métrica elegida para la red.

La selección de rutas entre sistemas autónomos plantea un problema diferente, ya que la cuestión no se reduce a la selección de la ruta óptima sino que se debe atender a criterios externos de tipo político, económico, administrativo, etc.

Hasta 1990 se utilizaba como protocolo de enrutamiento externo en Internet, el denominado EGP (Exterior Gateway Protocol). Este protocolo no fue capaz de soportar el crecimiento de la Red y entonces se desarrollo un nuevo protocolo de enrutamiento externo denominado BGP. Desde entonces se han producido 4 versiones de BGP, las especificaciones ahora vigentes de BGP-4 se encuentran en el RFC 1771.
BGP es un protocolo de transporte fiable. Esto elimina la necesidad de llevar a cabo la fragmentación de actualización explícita, la retransmisión, el reconocimiento, y secuenciación.

Requerimientos

Para la realización de la práctica se necesitaran los siguientes requerimientos:

Dos routers Cisco 1800-11(físicos).
Dos PCs conectadas a los routers.
Tres cables RJ45.
Software HiperTerminal

17.1. Configurar el encaminamiento BGP en R_A

17.1.1. Habilite el proceso de enrutamiento BGP con el número de SA especificado.

17.1.2. Establezca al router R_B como vecino BGP.

17.1.3. Anuncie la red 192.168.1.0 utilizando **network.**

Nota: Por defecto en los routers Cisco la auto sumarización está habilitada. Si la auto sumarización está desactivada, no se creará una ruta no classfull sumarizada.

17.1.4. Establezca una descripción del vecino y luego active la configuración asociada a éste.

17.1.5. Fije un límite máximo de prefijos que un vecino nos puede enviar cuyo valor será de 5, evitando así la inundación de prefijos y manteniendo la estabilidad de la Red.

Nota: Al llegar al número máximo de prefijos, la sesión se cerrara hasta que el administrador ejecute el comando "no neighbor VECINO shutdown".

17.1.6. Muestre el estado de la adyacencia BGP establecida con el router vecino con el comando **show ip bgp summary.**

17.1.7. Haga **show ip bgp** ¿Qué rutas ha recibido desde los routers BGP?

17.1.8. Haga **show ip route bgp.**

17.2. Configurar el encaminamiento BGP en R_B

17.2.1. Habilite el proceso de enrutamiento BGP con el número de SA especificado.

17.2.2. Especifique al router R_A como vecino.

17.2.3. Anuncie la red 192.168.3.0 utilizando **network.**

17.2.4. Establezca una descripción del vecino y luego active la configuración asociada a éste.

17.2.5. Fije un tope máximo de prefijos que un vecino nos puede enviar cuyo valor será de 6, evitando así la inundación de prefijos y manteniendo la estabilidad de la Red.

Nota: Al llegar al número máximo de prefijos, la sesión se cerrara hasta que el administrador ejecute el comando "no neighbor VECINO shutdown"

17.2.6. Muestre el estado de la adyacencia BGP establecida con el router vecino con el **comando show ip bgp sumary.**

17.2.7. Haga **show ip bgp** ¿Qué rutas ha recibido desde los routers BGP?

17.2.8. ¿Qué métrica utiliza BGP?

17.2.9. ¿Qué atributos son tomados en cuenta para elegir la mejor ruta BGP?

17.2.10. ¿Qué indica que la red introducida sea o no "classfull"?

17.2.11. ¿Cuál es el propósito de la sincronización en BGP?

17.2.12. Hay dos formas de desactivar un vecino, con **neighbor VECINO *sutdown*** y **no neighbor VECINO *remote-as* NUMERO-SA** ¿Cuál es la diferencia que se genera?

17.3. Verificar los vecinos BGP en R_A haciendo show ip bgp neighbors

17.3.1. ¿Cuál es el valor de **keepalive**? ¿Qué indica?

17.3.2. ¿Cuál es el valor de **hold time**? ¿Qué indica?

17.3.3. ¿Cuál es su número ID? ¿Por qué?

17.3.4. ¿Qué versión BGP utiliza?

Diseño Metodológico

Para alcanzar cada uno de los objetivos específicos, se llevaron a cabo los siguientes pasos:

1. Estudio del área de Redes de Ordenadores
2. Ámbito: Configuración de enrutadores.
3. Selección de los temas y contenido teórico a desarrollar en las prácticas.
4. Elaboración del formato de las prácticas a desarrollar.
5. Solución de las prácticas.
6. Referencias bibliográficas.

Detalles del paso 1

Como primer paso realizamos una pequeña evaluación de algunos ámbitos en el área de Redes tales como gestión de Redes, Configuración de Redes y mantenimiento de Redes, fue cuando decidimos trabajar en el ámbito de configuración de enrutadores especificamente.

Detalles del paso 2

En este punto teniendo definido el ámbito de trabajo averiguamos toda la información necesaria acerca de diferentes tecnologías y decidimos hacerlo en base a tecnologías CISCO (Enrutadores CISCO Serie 1800-11).

Detalles del paso 3

Para la selección de los temas se realizó un estudio detallado de la configuración de enrutadores. El medio utilizado para recopilar la información fue la investigación documental, específicamente la investigación bibliográfica y archivista.

Detalles del paso 4

Cada una de las prácticas estará compuesta por:

- Tema.
- Diagrama de red.
- Objetivos.
- Introducción.
- Requerimientos.
- Planteamiento de cada una de las actividades a realizar.

Detalles del paso 5

De acuerdo al tema de cada una de las prácticas se elaboró una base teórica que apoyará al alumno para llear a cabo la realización de las prácticas.
Personalmente realizamos y redactamos la solución de cada una de las prácticas con el objetivo de que exista una base de comprobación de soluciones.

Para dar solución a las prácticas, se utilizó:

Hardware utilizado:

Computadoras hp54 con las siguientes caracteristicas

- Disco duro de 20 GB.
- 512 MB de memoria RAM.
- Pentium (R)4 CPU 1.60 GHz.
- Sistema Operativo Windows XP Profesional.

Routers físico Cisco serie 1800.

Resumen del producto

Característica	Cisco 1801	Cisco 1802	Cisco 1811	Cisco 1812
Puerto DSL WAN	ADSL a través de POTS	ADSL a través de RDSI	-	-
Puertos 10/100 FE WAN	1	1	2	2
Switch Gestionado de 8-Puertos	Si	Si	Si	Si
ISDN BRI Dial Backup	Si	Si	-	Si
V.92 Analog Modem Dial Backup	-	-	Si	-
USB 2.0 Ports	0	0	2	2
802.11a/b/g Wireless Model	Si	Si	Si	Si
Puertos de Consola y Auxiliares	Si	Si	Si	Si

Requerimientos Software:

1. Simulador Cisco Boson NetSimV6.
2. Simulador Packet Tracer 4.0
3. Sistema Operativo (Windows XP).
4. Microsoft Office 2003.

Requerimientos para instalar el software CISCO.

- Procesador Pentium(r) o Talón(r) a 1000 MHz
- 256 MB de RAM.
- No es soportado por Windows 95 y Windows NT.
- Espacio libre en disco duro: 2 GB.
- TCP/IP instalado paraTelnet

Conclusiones

- Los temas elegidos y desarrollados (Conmutación y Enrutamiento) son de suma importancia para los alumnos de las carreras que imparte el Departamento de Computación, permitiendoles tener mejores oportunidades en el campo laboral.

- Los simuladores (Packet Tracer v 4.0 y Boson NetSim v 6.0) son una excelente alternativa para el desarrollo de prácticas de Redes de Computadores y brindan una gran facilidad de uso, sin embargo estos presentan algunas limitaciones con respecto a la utilizacion de algunos comandos.

- Los enrutadores físicos proporcionan el 100% de disponibilidad de comandos y una mayor fiabilidad y flexibilidad para implementar temas con funcionalidades complejas, además que le permite al alumno un contacto más real con dichos dispositivos.

- El conjunto de prácticas desarolladas son una guía detallada que servirá a alumnos y docentes en el desarrollo y comprensión de los temas teóricos.

Recomendaciones

Debido a las características, enfoque y metodología empleada en el desarrollo de nuestro trabajo planteamos las siguientes recomendaciones:

- Tomando en cuenta que últimamente se esta migrando a la utilización de direcciones IPv6, las prácticas planteadas deberían realizarse no solo con direcciones IPv4, si no también con direcciones IPv6 en enrutadores físicos.

- Las prácticas planteadas fueron creadas con una orientación específica a las tecnologías CISCO, estas mismas podrían realizarse con otras tecnologías para comprobar su funcionalidad.

- Se le recomienda al Departamento de Ingeniería en Sistemas de Información que para darle a los alumnos y personas interesadas en los temas y el conjunto de prácticas, una mayor accesibilidad, se podría crear un sitio Web donde fueran publicadas, así más y mas usuarios podrían usarlas como una opción para enriquecer sus conocimientos teóricos y prácticos en el área de Redes.

- En el mismo sitio Web crear un foro donde los visitantes den sus observaciones acerca del contenido teórico y práctico de los temas expuestos y estos puedan mejorar la información o indicar posibles deficiencias justificando su opinión.

- Se recomienda a los alumnos que deben leer acerca de Redes en general y los temas aborados en este documento.

Bibliografía Consultada

Capítulo 1: Aspectos fundamentales de la línea de Comandos

Libros:
- *Manual de Cisco, T. Shaughnessy; T. Velte , Editorial McGraw-Hill Interamericana de España, S. A. U.*

Capítulo 2: Comando SHOW

Libros:
- Manual de Cisco, T. Shaughnessy; T. Velte, *Editorial: McGraw-Hill Interamericana de España, S. A. U.*

Páginas Web:
- *http://www.aprendaredes.com*

Capítulo 3: Configuración de las interfaces

Páginas Web:
- *http://rodri.wordpress.com*
- *http://www.garciagaston.com.ar/*
- *http://www.aprenderedes.com*
- *http://www.monografias.com*

Capítulo 4: Configuración del banner y descripción de las interfaces

Libros:
- *Manual de Cisco, T. Shaughnessy; T. Velte, Editorial: McGraw-Hill Interamericana de España, S. A. U.*

Páginas Web:
- *http://www.aprenderedes.com*

Capítulo 5: RIP

Páginas Web:
- *http://es.wikipedia.org/wiki/RIP_(banda)*
- *http://www.cisco.com/en/US/docs/internetworking/technology/handbook/RIP.html*
- *http://iie.fing.edu.uy/ense/asign/redes2/material/051-RIP.pdf*
- *http://www.aprenderedes.com/*

Capítulo 6: Telnet, Ping y Tracert

Libros:
- *Tanenbaum, Andrew S., Computer Networks, Prentice-Hall, 1996.*

Páginas Web:
- *http://www2.uca.es/manual/telnet1.html*
- *http://es.wikipedia.org/wiki/Ping*
- *http://www.cisco.com/*
- *http://es.kioskea.net*
- *http://support.microsoft.com/*
- *http://gamersmafia.com/tutoriales/show/358*
- *http://www.netcom-sonora.com/~jenriquez/ICMP.html*
- *http://www.netcom-sonora.com/~jenriquez/ICMP.html*

Capítulo 7: CDP

Páginas Web:
- *http://www.aprenderedes.com/*
- *http://blog.pucp.edu.pe/*
- *http://es.wikipedia.org/wiki/CDP"*
- *http://serapa.blogspot.com*
- *http://www.tech-faq.com*
- *www.tech-faq.com/lang/es/cisco-discovery-protocol.shtml*

Capítulo 8: Verificación y Respaldo del IOS

Páginas Web:
- *http://revartm.wordpress.com/2007/05/27/copiar-cisco-ios-y-ficheros-de-configuracion-a-tftp/*
- *http://www.tech-faq.com/lang/es/cisco-router-commands.shtml*
- *http://fis.unab.edu.co/docentes/rcarvaja/cursos/penr5.pdf*
- *http://librosnetworking.blogspot.com/2006/02/sistema-de-archivos-del-cisco-ios.html*
- *http://fis.unab.edu.co/docentes/rcarvaja/cursos/penr5.pdf*
- *http://www.4shared.com/file/18509588/43b3d264/21_CCNA.html?s=1*

Capítulo 9: ACL

Páginas Web:
- *http://www.geocities.com/hilmarz/cisco/acl.htm*
- *http://en.wikipedia.org/wiki/Access_control_list*
- *http://www.aprenderedes.com/*
- *http://www.aprendaredes.com/dev/articulos/configuracion-de-los-filtros-ip-parte-ii.htm*

- *http://www.aprendaredes.com/dev/articulos/configuracion-de-los-filtros-ip-parte-ii.htm*

Capítulo 10: VLAN

Páginas Web:

- *http://en.wikipedia.org/wiki/Virtual_LAN*
- *www.textoscientificos.com/redes/redes-virtuales*
- *www.textoscientificos.com/redes/redes-virtuales/procesamiento-paquetes*
- *www.textoscientificos.com/redes/redes-virtuales/etiquetado*
- *www.smc.com/html_includes/statics/catalogs/ES_smart_switch.pdf*
- *www.eduangi.com/documentos/3_CCNA2.pdf*

Capítulo 11: NAT

Páginas Web:

- *http://www.aprendaredes.com/*
- *http://studies.ac.upc.edu/FIB/STD/lab/IOSLabv4.pdf*
- *http://es.wikipedia.org/wiki/NAT*
- *http://en.wikipedia.org/wiki/Network_address_translation*
- *http://en.wikipedia.org/wiki/NAT*
- *http://www.adslayuda.com/Generico-nat.html*
- *http://www.openbsd.org/faq/pf/es/nat.html*

Capítulo 12: OSPF

Libros:

- *Tanenbaum, Andrew S., Computer Networks, Prentice-Hall, 1996.*

Páginas Web:

- *http://sysop.com.cn*
- *http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html*
- *http://www1.cs.columbia.edu/~ji/F02/ir10/10-ospf.pdf*
- *http://www1.cs.columbia.edu/~ji/F02/ir11/11-ospf.pdf*

Capítulo 13: IS-IS

Páginas Web:

- *http://vcappuccio.wordpress.com*
- *http://en.wikipedia.org/wiki/IS-IS*
- *http://serapa.blogspot.com/search/label/Module%207%3A%20IS-IS*
- *www.ie.itcr.ac.cr/faustino/Redes/Clase10/LaCapadeRed.pdf*
- *http://elqui.dcsc.utfsm.cl/apuntes/redes/2001/pdf/3-7-Red-IP.pdf*

Capítulo 14: BGP

Libros:

- *Tanenbaum, Andrew S., Computer Networks, Prentice-Hall, 1996.*

Páginas Web:

- *http://www.wikilearning.com/monografias/wikilearning/categoria/0-1*
- *http://vcappuccio.wordpress.com/bgp/*
- *http://serapa.blogspot.com/search/label/Module%209%3A%20BGP*
- *http://web.madritel.es/personales3/edcollado/bgpd.htm*